Vaultastic – GDPR Shared responsibility model

Article	Article Summary	Customer's Responsibility	Vaultastic
	General Provisions		
1	**Subject-matter and objectives—** This Regulation contains rules on processing personal data and the free movement of personal data to protect the fundamental rights and freedoms of natural persons and their right to protection of personal data	Mithi has customers all over the world, who use Vaultastic in their business to protect data and improve compliance. Our customers who may serve and handle data of users from the European Union, are subject to GDPR. Since Vaultastic transports data in an encrypted form, Vaultastic cannot distinguish the kind of data being processed through the platform. It is the customers' responsibility to notify Mithi of its intent to use Vaultastic to process personal data of European Union data subjects and use the Vaultastic capabilities to govern and manage data to stay compliant with GDPR norms.	NA
2	**Material Scope—** This Regulation applies to the processing of personal data which form part of a filing system.		
3	**Territorial Scope—** This Regulation applies to controllers and processors in the Union and controllers or processors not in the Union if they process personal data of data subjects who live in the Union.		
4	Definitions: https://gdpr-info.eu/art-4-gdpr/		
	General Principles		

5	**Principles relating to processing of personal data—** Personal data shall be processed lawfully, fairly, and in a transparent manner; collected for specified, explicit, and legitimate purposes; be adequate, relevant, and limited to what is necessary; etc.	It is the customers' responsibility to collect personal data of EU subjects in a lawful, fair, and transparent manner for specified, explicit, and legitimate purposes adhering to data minimization principles. Vaultastic's ediscovery and administration console are designed to enable customers to manage and govern the preserved email data. Since Vaultastic transports data in an encrypted form, Vaultastic cannot distinguish the kind of data being processed, which includes personal data. Vaultastic will never process customer data inconsistent with the purpose viz. data protection, data discovery and management.	
6	**Lawfulness of processing—** There are six reasons that make processing lawful if at least one is true (e.g. data subject has given consent, processing is necessary for the performance of a contract, etc).	Vaultastic ingests/archives only those email that are journaled from the primary mail platform. Vaultastic has no way to distinguish email carrying data that makes the processing unlawful. Customers must identify the kind of emails they want to preserve and deploy appropriate filters on their primary mail server to only archive those emails that make the processing lawful (falls into one of the six reasons)	If the customer would like to use Vaultastic to store email data which carry personal information, then the Customer and Mithi should enter into an agreement to clarify and state this intent.

7	**Conditions for Consent—** When processing is based on consent, whoever controls the personal data must prove consent to the processing, and the data subject can withdraw consent at any time.	It is the customers' responsibility to ensure that the data subjects have freely consented to processing as well as managing individuals' right to revoke such consent.	Since all data is encrypted in transit, Vaultastic has no way to distinguish the kind of the email data being processed. Customers must identify the kind of emails they want to preserve and deploy appropriate filters on their primary mail server to only archive those email that match the conditions of consent. If the customer chooses to archive all email, without any filtration, the customer is advised to obtain end user's consent.
8	**Conditions applicable to child's consent in relation to information societal services—** Information society services can process personal data of a child if the child is over 16. If the child is under 16, the legal guardian must consent.	Complying with this article falls under the customers' responsibility. Customers must ensure that personal data of children is processed appropriately and that end users have provided appropriate notices and obtained parental consent, as applicable.	Since all data is encrypted in transit, Vaultastic has no way to distinguish the kind of the email data being processed. Customers must identify the kind of emails they want to preserve and deploy appropriate filters on their primary mail server to only archive those email that match the conditions of this article. If the customer chooses to archive all email, without any filtration, it is expected that the end users have provided appropriate notices and obtained parental consent, as applicable.

9	**Processing special categories of personal data—** Processing personal data revealing race, political opinions, religion, philosophy, trade union membership, genetic data, health, sex life, and sexual orientation is prohibited unless the subject gives explicit consent, it's necessary to carry out the obligations of the controller, it's necessary to protect the vital interests of the data subject, etc.	It is customer's responsibility to ensure that the data subjects have freely consented to processing sensitive data as well as managing individuals' right to revoke such consent.	Since all data is encrypted in transit, Vaultastic has no way to distinguish the kind of the email data being processed. Customers must identify the kind of emails they want to preserve and deploy appropriate filters on their primary mail server to only archive those email that match the conditions of this article. If the customer chooses to archive all email, without any filtration, the customer is advised to obtain end user's consent. In other words, it is customer's responsibility to ensure compliance for processing of sensitive data.
10	**Processing personal data related to criminal convictions and offenses—** Processing personal data related to criminal convictions can only be carried out by an official authority or when Union or Member of State law authorizes the processing.	It is customer's responsibility to ensure that they have the authority to process email data of criminal convictions or compliance with Union or Member State laws.	Since all data is encrypted in transit, Vaultastic has no way to distinguish the kind of the email data being processed. Customers must identify the kind of emails they want to preserve and deploy appropriate filters on their primary mail server to only archive those email that ensure compliance with applicable Union or Member State laws with regards to processing of criminal convictions data. To re-iterate, it is the customers' responsibility to ensure compliance with laws for processing of email data with information about criminal convictions.
11	**Processing which does not require identification—** The controller does not need to get or process additional information to identify the data subject if the purpose for which the controller processes data does not require the identification of a data subject.	It is customer's responsibility to ensure that the email data protected or processed through Vaultastic is consistent with the purpose of processing.	NA
Rights of Data Subject			

12	**Transparent information, communications, and modalities for the exercise of the rights of the data subject—** When necessary, the controller must provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and the controller needs to provide information on action taken on request by and to the data subject within one month.	It is customer's responsibility to ensure compliance with this article. It is not expected that the data subject will directly contact Mithi to comply with any such request. If they ever do, Mithi shall communicate such requests to customer as soon as possible to allow compliance with this article	If the data subject contacts the customer requesting any such information, the customer can take help of the Vaultastic ediscovery and the administration console to comply with this article
13	**Information to be provided where personal data are collected from the data subject—** When personal data is collected from the data subject, certain information needs to be provided to the data subject.	It is the customers' responsibility to provide appropriate privacy notices at the point of data collection from data subjects.	Review Mithi's privacy policy here: https://www.mithi.com/privacy-policy
14	**Information to provide to the data subject when personal data has not been obtained from data subject—** When personal data is not obtained from the data subject, the controller has to provide the data subject with certain information.		
15	**Right of access by the data subject—** The data subject has a right to know whether their personal data is being processed, what data is being processed, etc.	It is customer's responsibility to respond to data subject's request to access the data subject's personal information.	Mithi does not have access to the customers' data processed by using Vaultastic. Any individual request to access data must be processed from Vaultastic's ediscovery console.
16	**Right to rectification—** The data subject can require the controller to rectify any inaccurate information immediately.	It is customer's responsibility to respond to data subject's request to rectify any inaccurate information.	As such email stored in Vaultastic are immutable and cannot be modified. Hence there can be no rectification of email. This clause cannot apply to email data stored on Vaultastic.

17	**Right to be forgotten**—In some cases, the data subject has the right to make the controller erase all personal data, with some exceptions.	It is the customers' responsibility to ensure compliance with this article. Vaultastic can support the customers to comply with this requirement.	Mithi does not have access to the customers' data processed by using Vaultastic. Any individual request to access data must be processed from Vaultastic's administration console. Since Vaultastic, by design, does not support deletion of individual emails in the vaults, the customer has to delete the entire vault belonging to the data subject.
18	**Right to restriction of processing**—In some cases, the data subject can restrict the controller from processing.	It is customer's responsibility as a data controller to ensure compliance with these articles.	NA
19	**Notification obligation regarding rectification or erasure of personal data or restriction of processing—** The controller has to notify recipients of personal data if that data is rectified or erased.		
20	**Right to data portability—** The data subject can request to receive their personal data and give it to another controller or have the current controller give it directly to another controller.	It is the customers' responsibility to ensure compliance with this article. Vaultastic can support the customers to comply with this requirement.	Mithi does not have access to the customers' data processed by using Vaultastic. Any request to transmit data can be fulfilled using the Legacyflo tool from Mithi. This tool can extract data to local files, or copy data from Vaultastic to any other email solution target or even send the data on a physical medium to the customer.

21	**Right to Object—** Data subjects have the right to object to data processing on the grounds of his or her personal situation.	It is the customers' responsibility to ensure compliance with this article	It is not expected that the data subject will directly contact Mithi to comply with any such request. If they ever do, Mithi shall communicate such requests to customer as soon as possible to allow compliance with this article.
22	**Automated individual decision-making, including profiling—** Data subjects have the right not to be subjected to automated individual decision-making, including profiling.	It is the customers' responsibility to ensure compliance with this article.	Vaultastic has no context to participate in automated individual decision-making.
23	**Restrictions—** Union or Member State law can restrict the rights in Articles 12 through 22 through a legislative measure.	It is the customers' responsibility to ensure compliance with this article. The customer could need to stay abreast of the applicable Member State laws pertaining to the content of customer data and the responsibilities of the controller	Vaultastic provides the tools to discover, extract and dispose of content as they apply in the context of the member state laws. The customers will assume responsibility of using these tools to comply with these laws.
	Rights of Data Subject		
24	**Responsibility of the Controller—** The controller has to ensure that processing is in accordance with this Regulation.	The customer is the data controller and Vaultastic is the data processor for the email data processed through Vaultastic's cloud platform.	NA

25	**Data protection by design and by default—** Controllers must implement data protection principles in an effective manner and integrate necessary safeguards to protect rights of data subjects.	It is customer's responsibility as a data controller to ensure security of personal data.	Vaultastic maintains appropriate safeguards to protect the privacy, security, and integrity of customer email data (includes personal data contained). The multi-layered security framework and the vigilance and resilience framework are designed to store customer data in an immutable state and protect the data from loss, alteration, unauthorized access, use, acquisition, disclosure, or accidental or unlawful destruction. These measures include, but are not limited to data segregation, data encryption in flight and at rest, network security, audit trails, monitoring and regular vulnerability tests. Learn more about the security framework in Mithi's cloud platform: https://mithi.com/res/Securityframework-for-cloud-M
26	**Joint Controllers—** When there are two or more controllers they have to determine their respective responsibilities for compliance.	Contextual to the Customer.	NA
27	**Representatives of controllers or processors not established in the Union—** When the controller and processor are not in the Union, in most cases they have to establish a representative in the Union.	It is customer's responsibility to ensure compliance with this article.	NA

28	**Processor—** When processing is carried out on behalf of a controller, the controller can only use a processor that provides sufficient guarantees to implement appropriate technical and organizational measures that will meet GDPR requirements.	NA	Mithi is committed to helping our customers meet the GDPR requirements. As described in our response to article 25, Mithi has put in appropriate technical and organisational measures to help customers meet GDPR requirements. Mithi is happy sign a Data Processing Agreement with the customer.
29	**Processing under the authority of the controller or processor—** Processors can only process data when instructed by the controller.	It is the customers' responsibility to instruct Mithi regarding the processing of email carrying personal information.	Vaultastic only processes emails carrying personal data in accordance with customer's instructions and to the extent necessary for providing the cloud services as described in the SLA.
30	**Records of Processing Activities—** Each controller or their representatives needs to maintain a record of processing activities and all categories of processing activities.	It is customer's responsibility to ensure compliance with this article. Customers are responsible for maintaining an inventory of the emails carrying personal data processed through Vaultastic's cloud services.	Vaultastic maintains audit logs of all processing activity done.
31	**Cooperation with the supervisory authority—** The controller and processor have to cooperate with supervisory authorities.	It is Mithi's and the customers' shared responsibility to cooperate with supervisory authorities. If the customer receives an audit, inquiry or investigation by a government body, data protection authority or law enforcement agency regarding the processing of Personal Data, the customer will seek help from Mithi to locate and provide the required information to the authorities. Customer shall reimburse Mithi reasonably for any additional costs incurred to fulfil this obligation to the law	In case Mithi is to receive an audit, inquiry or investigation by a government body, data protection authority or law enforcement agency regarding the processing of Personal Data, Mithi shall promptly notify the customer unless prohibited by applicable law. If Mithi is expected to fulfil the request for data access, the customer will cooperate and provide all required documents, information to help Mithi fulfil the legal request. Customer shall reimburse Mithi reasonably for any additional costs incurred to fulfil this obligation to the law.

32	**Security of processing—** The controller and processor must ensure a level of security appropriate to the risk.	It is the customers' responsibility to maintain appropriate internal security protocols to safeguard customer's personal data. Vaultastic, cloud data protection service, helps the customers to protect their users' email data (including personal information)	Vaultastic maintains appropriate safeguards to protect the privacy, security, and integrity of customer email data (includes personal data contained). The multi-layered security framework and the vigilance and resilience framework are designed to store customer data in an immutable state and protect the data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction. These measures include, but are not limited to data segregation, data encryption in flight and at rest, network security, audit trails, and monitoring and regular vulnerability tests. Learn more about the security framework in Mithi's cloud platform: https://mithi.com/res/Securityframework-for-cloud-M
33	**Notification of a personal data breach to the supervisory authority—** In the case of a breach, the controller has to notify the supervisory authority within 72 hours, unless the breach is unlikely to result in risk to people. And the processor needs to notify the controller immediately.	It is customer's responsibility to inform the applicable supervisory authority of the breach reported by Mithi.	Mithi shall report to customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to customer data that it becomes aware of without unnecessary delay.
34	**Communication of a personal data breach to the data subject—** When a breach is likely to cause risk to people, the controller has to notify data subjects immediately.	It is customer's responsibility to ensure compliance with this article.	Mithi will reasonably cooperate with customers' requests for information and reporting on any security incident that is likely to result in risk to people

35	**Data protection impact assessment—** When a type of processing, especially with new technologies, is likely to result in a high risk for people, an assessment of the impact of the processing needs to be done	It is the customers' responsibility to comply with this article by seeking help from Mithi to help them do an impact assessment.	Mithi's responsibility is to extend reasonable cooperation to the customer to conduct this assessment.
36	**Prior consultation—** The controller needs to consult the supervisory authority when an impact assessment suggests there will be high risk if further action is not taken. The supervisory authority must provide advice within eight weeks of receiving the request for consultation	It is customer's responsibility to ensure compliance with this article.	NA
37	**Designation of the data protection officer—** The controller and processor must designate a data protection officer (DPO) if processing is carried out by a public authority, processing operations require the systematic monitoring of data subjects, or core activities of the controller or processor consist of processing personal data relating to criminal convictions or on a large scale of special categories of data pursuant to Article 9.	Customers must appoint a data protection officer to ensure their compliance with GDPR norms.	Mithi's DPO can be reached via the helpdesk assigned to each customer.
38	**Position of the data protection officer—** The DPO must be involved in all issues which relate to the processor must provide all necessary support for the DPO to do their tasks and not provide instruction regarding those tasks.		
39	**Tasks of the data protection officer—** The DPO must inform and advise the controller and processor and their employees of their obligations, monitor compliance, provide advice, cooperate with the supervisory authority, and act as the contact point for the supervisory authority.		

40	**Codes of conduct—** Member States, the supervisory authorities, the Board, and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR.	These articles do not directly apply to customers/controllers or the processors.	NA
41	**Monitoring of approved codes of conduct—** A body with adequate expertise in the subject-matter and is accredited to do so by the supervisory authority can monitor compliance with a code of conduct.		
42	**Certification—** Member States, the supervisory authorities, the Board, and the Commission shall encourage the establishment of data protection certification mechanisms to demonstrate compliance.		
43	**Certification bodies—** Certification bodies accredited by Member States can issue and renew certifications.		
Transfers of Personal Data			
44	**General principle for transfers—** Controllers and processors can only transfer personal data if they comply with the conditions in this chapter.		
45	**Transfers on the basis of an adequacy decision—** A transfer of personal data to a third country or international organization can occur if the Commission has decided the country or organization can ensure an adequate level of protection.		

46	**Transfers subject to appropriate safeguards—** If the Commission has decided it can't ensure an adequate level of protection, a controller or processor can transfer personal data to a third country or organization if it has provided appropriate safeguards.	It is the customers' responsibility to ensure data transfer in compliance with the articles of this chapter.	Vaultastic is currently available in the AWS regions of Singapore and India. The technical and organizational safeguards deployed on all the SaaS sites of Vaultastic follow a standard common security framework. The customers processing EU citizens data can choose to use Vaultastic from any site and still benefit from the robust security and privacy systems deployed to protect customer data.
47	**Binding Corporate rules—** The supervisory authority will approve binding corporate rules in accordance with the consistency mechanism in Article 63.		
48	**Transfers or disclosures not authorized by Union law—** Any decision by a court or administrative authority in a third country to transfer or disclose personal data is only enforceable if the decision is based on an international agreement.		
49	**Derogations for specific situations—** If there is no adequacy decision (Article 45) or appropriate safeguards, a transfer of personal data to a third country or organization can only happen if one of seven certain conditions are met.		
50	**International cooperation for the protection of personal data—** The Commission and supervisory authority have to do their best to further cooperation with third countries and international organizations		
Independent Supervisory Authority			
51	**Supervisory authority—** Each Member state has to supply at least one independent public authority to enforce this regulation.		

52	**Independence—** Each supervisory authority has to act with complete independence, and its members have to remain free from external influence.	These provisions are not directly applicable to the controller or processor.	NA
53	**General conditions for the members of the supervisory authority—** Member states need to appoint members of the supervisory authority in a transparent way, and each member must be qualified.		
54	**Rules on the establishment of the supervisory authority—** Each Member State needs to provide, in law, the establishment of each supervisory authority, qualifications for members, rules for appointment, etc.		
55	**Competence—** Each supervisory authority must be competent to perform the tasks in this Regulation.		
56	**Competence of the lead supervisory authority—** The supervisory authority of a controller or processor that is doing crossborder processing will be the lead supervisory authority.		
57	**Tasks—** In its territory, each supervisory authority will monitor and enforce this Regulation, promote public awareness, advise the national government, provide information to data subjects, etc		
58	**Powers—** Each supervisory will have investigative, corrective, authorization, and advisory powers.		

59	**Activity Reports—** Each supervisory authority must write an annual report on its activities		
Cooperation and Consistency			
60	**Cooperation between the lead supervisory authority and the other supervisory authorities concerned—** The lead supervisory authority will cooperate with other supervisory authorities to attain information, mutual assistance, communicate relevant information, etc		
61	**Mutual assistance—** Supervisory authorities must provide each other with relevant information and mutual assistance in order to implement and apply this regulation.		
62	**Joint operations of supervisory authorities—** Where appropriate, supervisory authorities will conduct joint operations.		
63	**Consistency mechanism—** For consistent application of this Regulation, supervisory authorities will cooperate with each other and the Commission through the consistency mechanism in this section.		
64	**Opinion of the Board—** If a supervisory authority adopts any new measures, the Board will issue an opinion on it.		
65	**Dispute resolution by the Board—** The Board has the power to resolve disputes between supervisory authorities.		

66	**Urgency Procedure—** If there is an urgent need to act to protect data subjects, a supervisory authority may adopt provisional measures for legal effects that do not exceed three months.	These provisions do not directly apply to the controller or the processor.	NA
67	**Exchange of information—** The Commission may adopt implementing acts in order to specify the arrangements for the exchange of information between supervisory authorities.		
68	**European Data Protection Board—** The Board is composed of the head of one supervisory authority from each Member state.		
69	**Independence—** The Board must act independently when performing its tasks or exercising its powers.		
70	**Tasks of the Board—** The Board needs to monitor and ensure correct application of this Regulation, advise the Commission, issue guidelines, recommendations, and best practices, etc.		
71	**Reports—** The Board will write an annual public report on the protection of natural persons with regard to processing.		
72	**Procedure—** The Board will consider decisions by a majority vote and adopt decisions by a two-thirds majority		

73	**Chair—** The Board elects a chair and two deputy chairs by a majority vote. Terms are five years and are renewable once.		
74	**Tasks of the chair—** The Chair is responsible for setting up Board meetings, notifying supervisory authorities of Board decisions, and makes sure Board tasks are performed on time		
75	**Secretariat—** The European Data Protection Supervisor will appoint a secretariat that exclusively performs tasks under the instruction of the Chair of the Board, mainly to provide analytical, administrative, and logistical support to the Board.		
76	**Confidentiality—** Board discussions are confidential.		
Remedies Liability and Penalties			
77	**Right to lodge a complaint with a supervisory authority—** Every data subject has the right to lodge a complaint with a supervisory authority.		
78	**Right to an effective judicial remedy against a supervisory authority—** Each natural or legal person has the right to a judicial remedy against a decision of a supervisory authority		
79	**Right to an effective judicial remedy against a controller or processor—** Each data subject has the right to a judicial remedy if the person considers his or her rights have been infringed on as a result of non-compliance processing.		

80	**Representation of data subjects—** Data subjects have the right to have an organization lodge a complaint on his or her behalf.	These provisions do not directly apply to the controller or the processor.	NA
81	**Suspension of proceedings—** Any court in a Member State that realizes proceedings for the same subject that is already occurring in another Member State can suspend its proceedings.		
82	**Right to compensation and liability—** Any person who has suffered damage from infringement of this Regulation has the right to receive compensation from the controller or processor or both.		
83	**General conditions for imposing administrative fines—** Each supervisory authority shall ensure that fines are effective, proportionate and dissuasive. For infringements of Articles 8, 11, 25 to 39, 41, 42, and 43 fines can be up to €10,000,000 or two percent global annual turnover. For infringements of Articles 5, 6, 7, 9, 12, 22, 44 to 49, and 58 fines can be up to €20,000,000 or four percent of global annual turnover.		
84	**Penalties—** Member States can make additional penalties for infringements.		
	Specific Processing Situations		
85	**Processing and freedom of expression and information—** Member States have to reconcile the protection of personal data and the right to freedom of expression and information (for journalistic, artistic, academic, and literary purposes).		

86	**Processing and public access to official documents—** Personal data in official documents for tasks carried out in the public interest may be disclosed for public access in accordance with Union or Member State.	These provisions do not directly apply to the controller or the processor.	NA
87	**Processing of the national identification number—** Member States can determine the conditions for processing national identification numbers or any other identifier.		
88	**Processing in the context of employment—** Member States can provide more specific rules for processing employees' personal data.		
89	**Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes—** Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is subject to appropriate safeguards (data minimization and pseudonymization).		
90	**Obligations of secrecy—** Member States can adopt specific rules for the powers of the supervisory authorities regarding controllers' and processors' obligation to secrecy.	These provisions do not directly apply to the controller or the processor.	NA
91	**Existing data protection rules of churches and religious associations—** Churches and religious associations or communities that lay down their own rules for processing in order to protect natural persons can continue to use those rules as long as they are in line with this Regulation.		
Delegating acts and implementing acts			

92	**Exercise of the delegation—** The Commission has the power to adopt delegated acts. Delegation of power can be revoked at any time by the European Parliament or the Council.	These provisions do not directly apply to the controller or the processor.	NA
93	**Committee procedure—** The Commission will be assisted by a committee		
Final Provisions			
94	**Repeal of directive 95/46/EC—** 1995 Directive 95/46/EC is repealed	These provisions are provided for informative purposes only.	NA
95	**Relationship with Directive 2002/58/EC—** This Regulation does not add obligations for natural or legal persons that are already set out in Directive 2002/58/EC (processing of personal data and the protection of privacy in the electronic communications sector).		
96	**Relationship with previously concluded Agreements —** International agreements involving the transfer of data to third countries or organizations that were setup before 24 May 2016 will stay in effect.		
97	**Commission reports—** Every four years the Commission will submit a report on this Regulation to the European Parliament and to the Council.		
98	**Review of other Union legal acts on data protection—** The Commission can submit legislative proposals to amend other Union legal acts on the protection of personal data.		

99	**Entry into force and application—** The Regulation applies from 25 May 2018.		

Vaultastic, a data management SaaS powered by AWS, is helping organisations #GainAgility with Cloud #DataProtection.

Talk to an expert from our team to discuss your unique data management use case.

		© Mithi Software Technologies	