FORTRA

General Data Protection Regulation

Any enterprise that operates or does business affecting European Citizens

Article 17

Right to be forgotten. On request, all personal data must be destroyed.

How Vera Helps

Eliminating particular files simply by making them inaccessible Documents isolated to singular individuals can be encrypted with a singular key- at which time a user requests their data to be “forgotten” revoking access or deleting the key for this user would render that data useless - even data that is out of the companies physical control

Article 25

Data protection by design, and by default, ongoing protections and tracking.

How Vera Helps

Vera leverages military-grade encryption for protecting customers’ sensitive file data. Automated protection enforced for employees, partners operate securely and our customers have control of their data. Vera’s dynamic access control ensures only the right people/parties have access to the data. Granular document policies enforce data in use protections restricting 3rd party processors from exfiltrating sensitive personal information Vera logs. every action taken by any user on a Vera file

Article 28

Data controllers can only use sub-processors with adequate security; enforcing protection while working with 3rd parties.

How Vera Helps

Vera’s dynamic access control ensures only the right people/parties have access to the data. Granular document policies enforce data in use protections restricting 3rd party processors from exfiltrating sensitive data. Vera logs every action taken by any user on a Vera-protected file

Article 30

Maintain records of processing activities, who had and has access to data.

How Vera Helps

logs every action taken by any user on a Vera-protected file. Vera logs every administrative or system action within the Vera system

Article 32

Security of processing.

How Vera Helps

Data encryption. Dynamic control of access and usage of data. Detailed audit and tracking to ensure data integrity

Article 33

Notification of a personal data breach to the supervisory authority. 72-hour breach notification. Any data encrypted is not required to be disclosed.

How Vera Helps

Vera’s detailed audit logs provide defensible proof against data breaches. Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred. Audit log reduce overall financial and brand implications associated with a breach

Article 34

Notification of a personal data breach to the supervisory authority. 72-hour breach notification. Any data encrypted is not required to be disclosed.

How Vera Helps

Vera’s detailed audit logs provide defensible proof against data breaches. Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred. Audit log reduce overall financial and brand implications associated with a breach

Article 5

Personal data must be protected and used for only specific purposes.

How Vera Helps

Vera protection leverages military grade encryption
Vera provides both manual and automated file protection based on a cloud-based rule/configuration engine. Dynamic real-time access control and granular data in use protection within native applications

Article 9

“Special categories” of personal data must carry extra protection.

How Vera Helps

Vera protection leverages military grade encryption Vera provides both manual and automated file protection based on a cloud-based rule/configuration engine. Dynamic real-time access control and granular data in use protection within native applications