THE GDPR & ORIGAMI RISK

Origami Risk ("Origami") is committed to compliance with the European Union (EU) General Data Protection Regulation (GDPR) and to continuing to offer our clients a secure Risk Management Information System solution. We are also dedicated to helping our clients and prospective clients comply with the GDPR with regard to our services.



What is the GDPR?

The GDPR is a comprehensive data protection law that updates existing EU laws to strengthen the protection of "personal data" (any information relating to an identified or identifiable natural person). The GDPR took effect on May 25, 2018.

Does the GDPR affect my organization?

The GDPR applies to organizations located within the EU and also applies to organizations located outside of the EU if they offer goods or services to, or process personal data of, EU data subjects. It applies to all companies, such as Origami, that "process" the personal data of data subjects residing in the EU, regardless of the company's location. "Processing" means any operation performed on personal data, such as collection or storage.

How does Origami ensure GDPR compliance?

Origami handles client data in compliance with applicable law, including GDPR.

Under the GDPR, organizations processing personal data are divided into "controllers", or the entities that control the personal data, and "processors", the entities that process personal data only on the instructions of the controllers. The GDPR applies to both controllers and processors (although there are different requirements for controllers and processors).

If you have any questions regarding Origami and GDPR compliance, you can contact Origami at legal@origamirisk.com or our Data Protection Officer at **dpo@origamirisk.com.**

ORIGAMI RISK

Origami is a "processor" for all client data stored in our system. While many requirements in the GDPR apply to the "controller" of the data, certain portions of the GDPR apply directly to Origami as the "processor" of the data.



Origami addresses certain GDPR requirements as follows:

1 Security Measures

Article 32 of the GDPR requires that each controller and processor of EU personal data implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In determining the appropriate level of security, each controller and processor must take 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.

Data security has always been paramount at Origami. Here are some measures Origami uses to protect all client data (including EU personal data):

Application Security

With a web application such as Origami Risk, there are a number of fronts that must be managed in order to help ensure that data is secure. One of the major focuses for Origami is within the application itself. Origami takes a number of steps to help ensure application security, including the following:

- **Penetration Testing:** Origami conducts regular testing to help ensure that the defenses employed in the application and environment are sufficiently keeping up with vulnerabilities that could be exploited to compromise our clients' data.
- **Vulnerability Assessment:** Origami uses state-of-the-art tools to regularly perform scans for vulnerabilities within its information system and client applications.
- **User Security:** Origami's role-based security provides clients the ability to manage their users' access and capabilities down to the field level. In addition, Origami is built to accommodate Single Sign-On authentication, allowing clients to authenticate their users to specific roles through their own network.
- **Encryption:** All data is encrypted in transit and at rest within Origami's Amazon Web Services Elastic Cloud environment and all Origami databases use file-level encryption. In addition, all web traffic is encrypted using Transport Layer Security (TLS).
- **Intrusion Detection and Prevention tools** are also utilized to establish a security perimeter that provides Origami with real-time alerts of suspicious activities and traffic that are indications of an active or attempted compromise.

ORIGAMI RISK

Data Center Security

Origami's servers are housed in the Amazon Web Services Elastic Cloud environment. Amazon Web Services Elastic Cloud maintains several data centers with the highest standards in data security.

Amazon Web Services Elastic Cloud data centers are housed in nondescript facilities that have extensive setback and military grade perimeter control berms, as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security standards utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means.

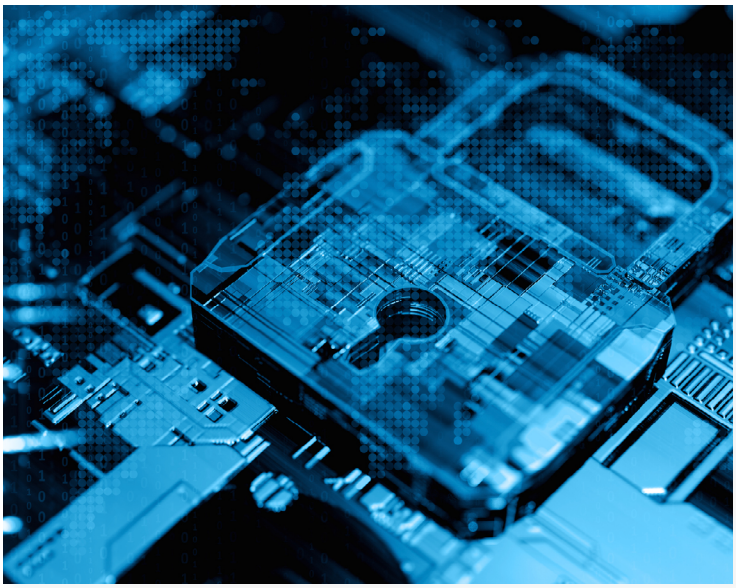
Authorized personnel must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification, are signed in, and continually are escorted by authorized staff. Amazon also provides environmental controls in its data centers to assure the proper working condition of its systems, including fire prevention/suppression, power management, and temperature controls.

Origami utilizes Amazon regions confined to the United States, Ireland, and Germany. Data maintained by Origami is kept in these regions and will not be moved to other offshore regions. More details can be found at https://aws.amazon.com/security/

Amazon Web Services has confirmed that its services comply with the GDPR. Origami has entered into a GDPR contractual addendum with Amazon Web Services to ensure that Amazon Web Services is meeting its GDPR obligations.

Audits and Compliance

Origami maintains compliance with the following standards, attesting to our commitment to provide world-class security:

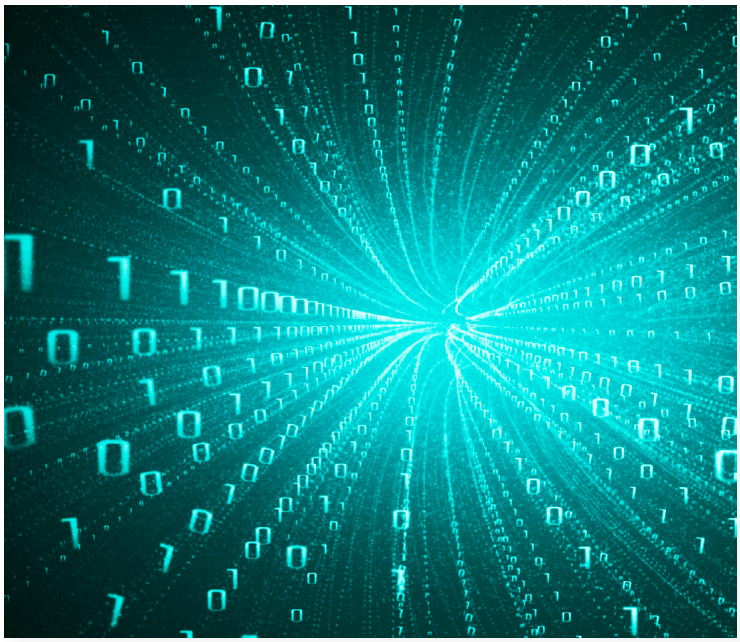


- **SOC 2** is a reporting framework created by the American Institute of Certified Public Accountants (AICPA) that assesses the controls of service companies such as Origami. Origami's SOC 2 report, prepared pursuant to an independent third-party examination, demonstrates how Origami achieves compliance with important controls related to security and confidentiality. Origami's SOC 2 report contains a description of its controls environment and an external audit of its controls that meet the AICPA Trust Services Security and Confidentiality Principles and Criteria. Origami's service is audited under this framework on an annual basis by an accredited firm. Origami also receives an annual SOC 1 audit that focuses on internal controls that are likely to be relevant to financial reporting.

- **FISMA**: Origami service has received Authorization to Operate (ATO) by a U.S. federal authorizing agency for its AWS GovCloud environment, based on NIST 800-53 Revision 5 controls.

If you have any questions regarding Origami and GDPR compliance, you can contact Origami at legal@origamirisk.com or our Data Protection Officer at **dpo@origamirisk.com.**

- **HIPAA Security Rule**: Alignment with NIST 800-53 allows Origami, by way of existing security controls, to meet security requirements established by the HIPAA Security Rule in accordance with NIST SP800-66, *"An Introductory Resource Guide for Implementing the HIPAA Security Rule".*



Data Backup and Disaster Recovery

All data maintained within the Origami database goes through a backup process. Backups occur on multiple levels to provide for redundancy, reliability, and multiple recovery paths. Database level backups are taken incrementally for all client data.

Origami maintains disaster recovery policies and controls that are tested at least annually. Origami's servers and data are housed within the Amazon Web Services Cloud platform, which provides a highly redundant and reliable environment

2 Legal Documentation

Article 28 of the GDPR requires that each controller put in place certain contractual commitments with processors that are processing any EU personal data. We are dedicated to helping our clients comply with the GDPR with regard to our services, which includes providing GDPR-related assurances in our contractual commitments. We will agree with our clients and prospective clients to include this language in our contract in order to address these requirements.

3 Transfers of Personal Information Outside the EU

Origami stores all client data in the United States, Ireland, and Germany. Furthermore, while there is no obligation under the GDPR for data to be stored only in the EU, the GDPR does place certain requirements on any transfers of personal data from the EU to a country outside the EU. In furtherance of satisfying those requirements, Origami has obtained certification under the EU-US Data Protection Framework ("DPF"). Origami also works with our clients to put in place any other agreements as necessary to meet these requirements, including completing any additional assessments reasonably deemed necessary by our clients to meet these requirements. Additionally, for clients based in the UK and Switzerland, Origami has also obtained certification under the Swiss-US DPF and the UK Extension to the EU-US DPF.

4 Data Protection Officer

The GDPR requires certain organizations to appoint a data protection officer, which Origami has done. To speak with our Data Protection Officer, please email dpo@origamirisk.com

ORIGAMI RISK

How does Origami assist its' clients to ensure their GDPR compliance?

Certain GDPR obligations apply directly to our clients. The following is a list of some of these obligations and the ways that Origami can assist with the compliance process.

GDPR Requirement	GDPR References	How Origami Helps Address the Requirement
Consent	Articles 6 and 7	The GDPR requires that any processing of EU personal data shall only be lawful if it meets one of six listed conditions. One of these conditions is consent of the data subject, which must be freely given, specific, informed, and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. To the extent that an Origami client needs to obtain the consent of data subjects to store their personal data in Origami, this would be an obligation of such client, but we will promptly forward any requests received directly by Origami from a data subject relating to their personal data.
Rights of the data subject	Articles 12 through 23	The GDPR provides certain rights to EU data subjects in relation to their personal data, which includes a right of access, right to rectification, right to erasure, and right to restriction of processing. These rights apply directly with the controller and not with Origami as the processor. However, we will promptly forward any requests received directly by Origami from a data subject relating to their personal data, and will work with the client to ensure that the client is meeting these GDPR obligations.
Data Protection Officer	Articles 37 through 39	The GDPR requires certain organizations to appoint a data protection officer. This applies to both data controllers and data processors. While we appointed our own data protection officer, our clients may need to appoint their own data protection officer to ensure their own compliance with the GDPR.

Additional Steps Necessary for Compliance

The fundamental requirements listed above are just a subset of the GDPR. Please ensure your internal teams review all of the GDPR requirements in order to maintain compliance. This document is not intended as legal advice, and Origami clients and prospective clients should seek appropriate legal advice to ensure their own GDPR compliance.

Where Can I Find Out More Information?

If you have any questions regarding Origami and GDPR compliance, you can contact Origami's legal department at **legal@origamirisk.com** or our Data Protection Officer at **dpo@origamirisk.com**.