Tecplot is GDPR Compliant!

What is GDPR?

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue-based. The General Data Protection Regulation covers all companies that deal with data of EU citizens, so it is a critical regulation for corporate compliance officers at banks, insurers, and other financial companies. GDPR came into effect across the EU on May 25, 2018.

Why Is This Important?

At Tecplot, we strongly value the people we work with every day (customers, prospective customers, business partners, and employees). Our interactions with these parties generate data of all kinds, and we value the rights of each of these parties to keep their data confidential, secure, and available. We adhere to the high standards of GDPR.

Tecplot strives to adhere to the following principles when developing practices that govern its information systems:

- Privacy by design: Systems and processes should be secure by default.
- Defense in depth: Implement as many layers of security as is reasonable in order to decrease the chances of a successful attack or exploit.
- Confidentiality, Integrity, Availability ("CIA"): We measure our success in terms of our ability to ensure these.

Security

As Tecplot continues to make the security of data entrusted to us a priority, and in light of GDPR, we have included more detail on the specific measures we have in place. The following are some of the measures we implement as part of our information security policy:

- Role-Based Access Control
- Annual employee password changes and two-step verification
- Encryption of GDPR data in transit and at rest
- Ongoing vulnerability management and remediation
- Formal security incident response
- Security awareness training for all employees
- Workstation, server, and mobile device policies
- EU-US Privacy Shield Certified
- Periodic reviews of all of the above

An Information Security Policy containing more granular detail can be made available to our Enterprise customers. Please contact us at privacy@tecplot.com if you would like to receive a copy.

Personal Customer Data

We maintain records of all personal data elements we store, where we store it, how we capture it, and how we use it. Any new creation, usage, storage, or processing of customer information must be approved by our Data Security Team and documented in our Information Asset Register. At the request of the individual or a government authority, Tecplot will furnish all of the data it has collected on an individual to that individual or authority within thirty days, as well as any data that is maintained on our behalf by one of our approved Data Processors. Any personal data transmitted over the internet is encrypted with a modern implementation of TLS. Personal data stored offsite is encrypted at rest.

Data Minimization, Accuracy and Retention

Privacy by design and privacy by default are a fundamental part of our systems and processes. We have company-wide data retention policies. Tecplot acknowledges the right of individuals to have access to their personal information. Individuals have access to the personal information about them that Tecplot holds and are able to review, correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. Individuals can access this personal information via our My Tecplot portal or by contacting the Subscription Services Manager at subscriptions@tecplot.com.

Opt-In Policy

Our Tecplot website allows visitors and customers to give opt-in consent to receive future email communication. This communication consists of email newsletters, product updates and invitations to events and training. Every Tecplot marketing email contains a link for recipients to update the types of communications received, and an option to opt out of all email communications with Tecplot.

Security Incidents and Breaches

Our Data Security Team has detailed security incident policies and procedures in place for rapid response to any security incident or data breach. Access to systems is logged in order to facilitate detecting unauthorized access or responding to a security incident.

We are committed to keeping our customers fully informed of any matters relevant to the security of their data and to providing customers with all the information necessary for them to meet their own regulatory reporting obligations under GDPR.

Data Backup and Recovery

All relevant data sets are backed up nightly and retained on- and off-site according to Tecplot's retention policy. Backup sets are stored in an encrypted format and are tested regularly to ensure the integrity of the data and the recovery process. This is validated by the Data Security Team.

Our Employees Are Trained

Every employee at Tecplot has received GDPR training. Our program is designed to ensure all employees across all functions within the company understand our obligations under GDPR and the importance of protecting the personal data of our customers. In addition to the general training program we continually run privacy and security education programs internally for different functions across our organization.

Distributors & Third-Party Data Processors

Distributors who sell and support Tecplot products and all third-party agencies who process personal customer data on our behalf are required to be GDPR compliant. Distributors of Tecplot software are required to sign a Tecplot Distribution Agreement Amendment that outlines their responsibilities as pertains to GDPR. These executed agreements are archived and can be furnished to authorities upon request.

All third party data processors must validate that they adhere to GDPR requirements by providing an authorized Data Protection Addendum. These documents are archived and can be produced upon request.

Data Security Team

Tecplot has appointed a cross-functional Data Security Team to be responsible for all matters relating to GDPR. Their responsibilities include:

- Ensuring that company policies properly comply with all applicable laws and best practices
- Ensuring that company practices are carried out in accordance with all company policies
- Ensuring that all levels of the company understand and agree to company policies and practices
- Authorizing, reviewing, and removing third party access to data sets
- Evaluating the impact of security vulnerabilities on an ongoing basis
- Determining whether a security incident or data breach has occurred and how to respond

Monitoring Compliance

Tecplot's Data Security Team meets several times per quarter to fulfill its responsibilities, review IT deliverables, and set priorities related to GDPR.

How To Contact Us

For additional information about GDPR or Tecplot's Information Security Policy please contact us at privacy@tecplot.com