



EagleMercury It Security Services



General Data Protection Regulation (GDPR)

What you need to know, and how EagleMercury can help you comply with the GDPR's requirements

Effective May 25, 2018, the General Data Protection Regulation (GDPR) is a European privacy law that imposes significant new requirements on any company or entity that handles, stores, collects, processes, uses or analyzes any personal data of residents of the European Union (EU). It gives EU residents greater control over the data that companies have about them, and it creates heightened security, disclosure, access and notification obligations on any business that interacts with EU residents.

EagleMercury is based on extensive expertise managing a highly secure infrastructure and complying with complex regulations. We currently self-certify compliance with the EU-US Privacy Shield framework and are committed to comply with the GDPR across our services. EagleMercury maintains a security environment that meets the requirements of the GDPR, and we offer GDPR-compliant Data Processing Addendums to our partners and customers to help assure them that our processing and handling of their data will meet the GDPR's standards. Ultimately, every business needs to carefully assess their own business activities and their compliance with the GDPR, but we can help by managing GDPR compliance on the services we provide.

What are the key elements of the GDPR?

The GDPR is complex, but the following is a high-level summary of its key elements:

- **Individuals Have Greater Control over Their Data:** Under the GDPR, EU residents have “data subject rights,” which include the right to (a) receive information about how their personal data is used; (b) access that data; (c) make corrections to, or delete, incorrect information about them; (d) “be forgotten” (which means they have the right to insist that their personal data be deleted under certain circumstances); (e) limit or object



to automated processing of their personal data; and (f) receive a copy of their personal data.

- **Companies Must Maintain a Comprehensive Security Program:** Entities that handle, store, collect, process, use or analyze any personal data of EU residents must implement and maintain a comprehensive security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes, at a minimum, specific security measures identified in the GDPR (such as pseudonymization and encryption of Personal Data and a process for regularly testing, assessing and evaluating the effectiveness of those technical and organizational security measures).
- **Companies Have Stricter Disclosure and Notification Obligations:** The GDPR imposes duties on companies to provide prompt notification of security breaches to data protection authorities and affected individuals. The GDPR also obligates entities to disclose to individuals if their data is being processed by third parties and to inform individuals how their data will be used – and obtain consent for such use.

What data is subject to the GDPR?

The GDPR applies to any “personal data” of an EU resident. “Personal data” consists of any information that can be used to identify a person. In some cases, it’s easy to identify “personal data” – for example, an email address, taxpayer or employee ID number, or a person’s name accompanied by a work or home address. However, “personal data” may also include less obvious types of information, such as a person’s biometric data, location information and/or IP address. It is very broadly defined.

What types of agreements does EagleMercury offer regarding GDPR compliance?

The GDPR states that data controllers (such as EagleMercury’s customers) may only use data processors that provide sufficient guarantees to meet key requirements of the GDPR. EagleMercury meets that requirement, and we are pleased to offer a Data Processing Addendum to any EagleMercury partner or customer. That addendum contains contractual commitments to comply with the GDPR, as well as the other commitments described below. Please contact your EagleMercury account representative for assistance putting a Data Processing Addendum in place.

What commitments are contained in EagleMercury’s Data Processing Addendum?

EagleMercury’s Data Processing Addendum includes a number of commitments on the part of EagleMercury, in its capacity as a processor of EU residents’ data, to comply with the GDPR. The GDPR requires that processors such as EagleMercury commit to:

- Obtain the controller's consent before using subprocessors and remain liable for the activities of any subprocessors;
- Only process EU residents' personal data on instructions from the controller;
- Ensure that personnel, such as employees and contractors, who process personal data are trained and committed to confidentiality;
- Implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk;
- Assist controllers in complying with their obligations to respond to data subjects' requests to exercise their GDPR rights;
- Upon becoming aware of a security breach, provide timely notice of the breach and help the controller comply with its disclosure obligations;
- Assist controllers with data protection impact assessments and consultation with supervisory authorities;
- Make reasonable information available to customers to help them assess the processor's security program;
- Delete or return personal data once the services are terminated (except as needed by the processor to continue to provide services or manage its business); and
- Support the controller with evidence of the processors' compliance with the GDPR.

Once I sign a Data Processing Addendum with EagleMercury, am I done with GDPR compliance?

No! The GDPR is a far-reaching privacy law that touches any business that handles any personal data of EU residents. EagleMercury can definitely help you comply with the GDPR, by fulfilling our obligations as a processor of any data that you, your customers and your users submit to EagleMercury in connection with the services we provide. But there are a number of other actions you should be considering, such as:

- Consider the types of data you handle, store, collect, process, use or analyze in the conduct of your business.
 - Do you have any employees in the EU?
 - Do you have any customers with offices in the EU?
 - Do you (or, if you resell EagleMercury services, do your customers) handle personal data of individuals, potentially residing in the EU, in the normal course of business (such as medical insurance billing, HR or payroll services, etc.)?

- Do you collect individualized tracking information (including the use of cookies) regarding users of your website, some of whom may be EU residents?
- Do you provide services to your customers where you do not know the content of what you are processing (such as email or archiving services)?

Any data that you have in connection with these or similar activities may be subject to the GDPR's requirements.

- Review your own security infrastructure and ensure that it is sufficient to protect any personal data that you store that may be subject to the GDPR.
- Make sure you understand and can comply with the GDPR's notification, disclosure, consent and other requirements in your handling of any possible personal data of EU residents.
- Obtain Data Processing Addendums from any vendor or service provider to which you or your customers may be sending personal data of EU residents for processing.
- Prepare and offer GDPR-compliant Data Processing Addendums to your own customers who may require such agreements for the services you provide to them.

GDPR compliance obviously requires a very detailed and business-specific analysis. EagleMercury provides GDPR-related assurances regarding the services we provide. Most companies that, directly or indirectly, have contacts or dealings with the EU are working with outside legal and compliance advisors to help them understand how the law applies to their own business and what they need to do to comply. If you have any questions, EagleMercury is happy to point you to additional resources that may help you look into these issues.