The Process of GDPR Compliance

MAP DATA, DOORS O(PEN)

By:Ryan J. Perry
July 02, 2018

The new European Union General Data Protection Regulation (GDPR) took effect on Friday, May 25, 2018, but many companies are still hard at work becoming compliant with this broad and stringent regulatory scheme governing privacy and data security. This new law reaches companies located in the United States who process any information (personal data) of identified or identifiable natural persons (data subjects) located in the European Economic Area (EEA), and regulates how, when and what security measures apply to the processing of that personal data by businesses. Personal data may be anything from a business contact's email address to IP addresses of European visitors to a company's website to human resources data on European employees. The penalties for violation can be steep – €10 million to €20 million or 2% – 4% of annual global turnover – whichever is greater. For additional details on the GDPR, please see *4 SCARY Facts about the New European Union General Data Protection Regulation*.

Not only might GDPR compliance be legally necessary, it also fosters good business practices and facilitates business growth by opening doors with potential business partners. Because your business customers' own compliance with GDPR may depend on your compliance, having your privacy and data security house in order can help assure a potential customer that your business is right for the job. Although there is no silver-bullet for GDPR compliance, once you have concluded that you might have this type of data making its way through your systems, these are the types of tasks a company can expect to undertake as it seeks to become compliant. Just remember: ***MAP DATA, DOORS O(PEN)***:

1. Data **M**apping (completion of data flows questionnaire)

    a. Please see our article *The First Step in Developing a GDPR Compliance Strategy: Assess Your EU Personal Data Flows* regarding assessing the ways in which your business intersects EU personal data.

2. **A**nalysis to determine lawful basis of processing for data for which client is data controller

3. Revisions to **P**rivacy policy to include provisions necessary under the GDPR, including access rights for data subjects

    a. To include Cookie Policy, as well as banner on the website disclosing use of Cookies

4. **D**ata processing addendum

    a. All customer and vendor contracts involving EU personal data to be amended to include this document

    b. Often, companies have two forms based on their role in the business relationship – one for when they are a service provider, once for when they are a service recipient

5. Privacy impact **A**ssessment, if required

6. Data **T**ransfer mechanism

    a. Data transfer has been part of the European data protection regime for a while and continues to be under the GDPR, but it is all the more important now given the severity of the fines under the GDPR

    b. When a company transfers persona data from the EEA to a country that the European Commission has not deemed "adequate" (e.g. the United States), the business is expected to commit to processing that personal data in accordance with European data protection principles

    c. This is often the Standard Contractual Clauses, a contract the client would have to enter into with all business partners touching the client's EU data

7. Documentation of processing **A**ctivities

8. **D**isaster recovery plans (potentially in connection with the security policy)

9. Revisions to **O**nline terms of service

10. Mechanisms for **O**pt in/opt out for marketing materials and roll out/acceptance of updated privacy policy and online terms

11. Incident **R**esponse plans (potentially in connection with the security policy)

12. Internal **S**ecurity policies (including data subject access rights and retention policies)

13. Appointment of data protection **O**fficer, if required

It is crucial to note that GDPR compliance is highly fact specific. The list above is intended to provide a flavor of the types of documents and issues that tend to surface during the compliance process and should not be used as a definitive compliance strategy. There is no "off-the-shelf" GDPR compliance strategy; rather, the strategy must be tailored to the business at issue.

Morse's Privacy & Data Security team has gained significant experience in tailoring bespoke GDPR compliance strategies for our clients. For more information on how your business can become GDPR compliant, please contact **Ryan Perry**.