BACKSTOP SOLUTIONS
+1 (312) 277-7701
info@backstopsolutions.com

FREQUENTLY ASKED QUESTIONS ABOUT GDPR

There has been a lot of talk lately about the "GDPR." Backstop has prepared this "Frequently Asked Questions" (FAQ) document to help address some of the questions we are hearing from our clients, common misconceptions, and actions Backstop has taken regarding the GDPR.

1. WHAT IS THE GDPR?

The GDPR (General Data Protection Regulation) is a new EU regulation designed to enhance the protection of personal information of EU residents, and heighten the obligations of organizations who collect or process this personal data. The GDPR becomes effective on May 25, 2018.

The GDPR arguably represents the most important change to data protection regulations in decades. The GDPR replaces the EU's 1995 Data Protection Directive, and was designed to replace a patchwork of existing regulations and frameworks. The GDPR aims to protect EU residents and empower EU residents with the right to control their personal data, while redesigning the way that organizations handle personal data.

With the precipitous growth of the Internet, including social media and "the cloud," more personal data is being created and processed than ever before. The GDPR was created to update data privacy standards with modern technologies and realities in mind.

2. WHAT'S IN THE GDPR?

The GDPR builds on the principles of the EU's 1995 Data Protection Directive, but includes stronger conditions for consent to process personal data, increased obligations for both data processors and data controllers in their handling of personal data, including increased transparency, increased control over personal data for data subjects, strong accountability requirements, and substantial fines for non-compliance.

3. TO WHOM DOES THE GDPR APPLY?

The territorial scope of GDPR is broad. Current data privacy legislation in the EU governs entities within the borders of the EU. However, the GDPR also applies to non-EU businesses who either offer goods or services to people in the EU or who monitor the behavior of people in the EU. In other words, even if a company is based outside of the EU but controls or processes the data of EU residents, the GDPR may apply to the company.

4. IS GDPR THE FIRST LAW OF ITS KIND IN THE EU?

No. The GDPR will replace the EU's 1995 Data Protection Directive. The GDPR builds on and enhances the framework and principles of the EU's 1995 Data Protection Directive, while substantially increasing penalties for non-compliance.

5. WHAT DOES THE GDPR REQUIRE COMPANIES TO DO?

Companies must limit their possession and use of individuals' personal data and must implement reasonable data protection measures to protect personal data against loss or unauthorized exposure. To retain or use an individual's personal data, companies generally must obtain the explicit consent of that individual ("opt-in" consent), which must be obtained for each separate processing activity. Additionally, the GDPR gives data subjects more control over personal data. Companies must provide individuals with access to their own personal data upon request, the right to transfer personal data between service providers (the "right to portability"), the right to have inaccuracies in personal data corrected (the "right to rectification"), the right (in certain circumstances) to have personal data erased upon request and to ensure that personal data is destroyed once the specific activity for which it was collected is completed (the "right to be forgotten"), the right to object to certain uses of personal data, and the right at any time to revoke consent to retain or use personal data.

In certain cases, the GDPR also requires companies to appoint a Data Protection Officer, whose role is to facilitate compliance with the GDPR. A company must appoint a Data Protection Officer if the company regularly and systematically monitors data subjects or processes certain sensitive personal data. The GDPR also addresses data breach notifications, and contains specific requirements for notifying supervisory authorities in the case of a breach of personal data, including requirements regarding the content and timeliness of notifications. In cases where the data breach causes a high risk to data subjects, notifying the data subjects also may be required.

6. WHAT QUALIFIES AS "PERSONAL DATA"?

Personal data is broadly defined as information that relates to a natural person (known as a "data subject") that could be used directly or indirectly to identify the individual. Specific identifiers include names, physical addresses, email addresses, birthdates, health and biometric information, demographic information, and computer IP addresses. Note that the GDPR protects the personal data of EU residents, not just EU citizens.

BACKSTOP SOLUTIONS
+1 (312) 277-7701
info@backstopsolutions.com

FREQUENTLY ASKED QUESTIONS ABOUT GDPR

7. WHAT ARE DATA CONTROLLERS VS. DATA PROCESSORS VS. DATA SUBJECTS?

The GDPR distinguishes between, and contains different obligations for, data controllers and data processors. A data controller is a company that collects personal data and determines the purposes and means of the processing of personal data. A data processor is a company that processes data on behalf of a data controller. A data subject, on the other hand, is an identified or identifiable natural person.

For example, a company who provides a web-based CRM platform to its client, a financial institution, would be a data processor, and the financial institution would be a data controller.

8. PENALTIES FOR NON-COMPLIANCE

The GDPR contains significant penalties for non-compliance: fines of up to 20,000,000 EUR or 4% of total worldwide annual revenue of the preceding year (whichever is greater). These financial penalties, of course, do not include loss of business, loss of goodwill, reputational damage, and legal fees in connection with responding to a GDPR inquiry.

9. WHAT ARE SOME STEPS A COMPANY CAN TAKE TO PREPARE FOR GDPR?

While the deadline for GDPR is fast approaching, there are practical steps a company can take to prepare:

- Determine whether your company is a data controller and/or a data processor
- Decide and document why your company has collected or retained personal data and who has access to the personal data
- Inventory your data for any personal data of EU residents
- Set up a method to be able to easily locate personal data on request
- Purge any personal data that has outlived its usefulness or is no longer relevant in regards to the reasons for which it was collected
- Review your company's data security posture to ensure that reasonable data protection measures and procedures are in place to protect against loss or unauthorized access or exposure of personal data
- Appoint a Data Protection Officer if, as part of your company's core activities, your company regularly and systematically monitors data subjects or processes certain sensitive personal data

10. WHAT IS BACKSTOP DOING IN RESPONSE TO THE GDPR?

Backstop continues to monitor regulatory guidance and interpretations of key GDPR requirements to guide Backstop in complying with the GDPR, as the GDPR may be applicable to Backstop, and to assist Backstop's customers with their own compliance efforts. Backstop's efforts include:

A. Product and Security Changes

Backstop will leverage it organizational focus on data security, the careful handling of customer information, and its compliance culture, as Backstop prepares for the GDPR's effective date of May 25, 2018. Like nearly all cloud service providers, Backstop is reviewing its information security policies and procedures and making necessary modifications in response to the GDPR.

B. Changes to Legal Documentation

Backstop has updated its legal documentation, and will continue to update its legal documentation, to reflect GDPR obligations as they may be applicable to Backstop. This likely will include a new Data Processing Addendum to Backstop's existing Subscription Agreement, and changes to Backstop's Privacy Policy and other information security policies and procedures.

C. Backstop is EU-US and US-Swiss Privacy Shield certified

Under the GDPR (as well as its predecessor, the EU's 1995 Data Protection Directive), personal data of EU residents may be transferred outside of the EU only if the personal data is "adequately protected." For transfers to "inadequate" jurisdictions, such as the US, data controllers and data processors must rely on an adequacy measure in order to be able to transfer personal data into the relevant jurisdiction.

Privacy Shield certification is one such adequacy measure. Backstop is certified with the U.S. Department of Commerce under the EU-US and US-Swiss Privacy Shield programs. These programs are designed to ensure that adequate safeguards are in place when Backstop transfers (or Backstop customers transfer to Backstop) personal data from the EU to the US, and from Switzerland to the US.

Disclaimer: This FAQ document offers general information regarding Backstop and the GDPR. The above is not a complete explanation of the GDPR, nor legal advice for your company in regards to complying with the GDPR or any other data privacy laws. You may not rely on the information above as legal advice nor a recommendation as to any legal understanding or course of action. Please consult an attorney if your company would like legal advice on GDPR compliance with respect to your company's particular circumstances.