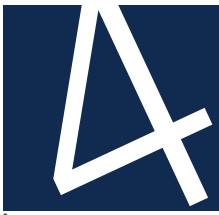
PREPARING FOR BUSINESS WITH EUROPE:
THE AGE OF PRIVACY SHIELD AND GDPR

PART ONE | By Stephanie Hadley

For most of the world, Brexit was the big news out of Europe this Summer. The EU-US Privacy Shield and the European Union's General Data Protection Regulation (GDPR) are garnering just as much attention from those of us in the information security industry. Organizations in the US and Europe are gearing up for the adoption of the two separate, but tangential, programs. Most CISOs agree that the new requirements promote good data protection strategies, and should be a part of any data security effort.

Andy Matthiesen, Vice President of Security at Gen Re, a global provider of reinsurance solutions, said "GDPR is both one of the most ground breaking regulations on data privacy and what we should already be doing from a security perspective." He believes that GDPR is a game changer for security executives and their programs because it will bring greater attention and mindshare to security efforts. The extra attention will bring extra budget in addition to increased scrutiny. He continued, "The potential fines are up to 4% of global revenue (per incident) and a company doesn't even need to have a physical presence in the EU in order to be liable. As a result, international security will get much more attention from Boards and CEOs."

Currently, businesses are assessing their own programs against the standards, identifying gaps and implementing policy and procedural changes to ensure alignment and adherence with the regulations. We break down the most important things to know about GDPR and the Privacy Shield. K logix Director of Program Management Don Cook gives his advice on how companies can prepare their security programs for the changes in Europe.



Things to know about PRIVACY SHIELD

The Privacy Shield is a proposed framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. It replaces Safe Harbor, which the European Union invalidated in October 2015 when a high court judge ruled that US businesses did not have the appropriate controls in place on US-based servers that stored personal information of members of the EU.

1 **US COMPANIES THAT RECEIVE PERSONAL INFORMATION OF EU MEMBERS MUST TAKE STEPS TO ENSURE THEY ARE IN COMPLIANCE WITH PRIVACY SHIELD**

2 **UNDER THE PRIVACY SHIELD, THE US IS REQUIRED TO BEEF UP ITS MONITORING AND ENFORCEMENT OF US COMPANIES THAT RECEIVE EU MEMBER PERSONAL INFORMATION**

3 **COMPANIES THAT DO NOT COMPLY WITH THE PRIVACY SHIELD MAY BE SANCTIONED OR EXCLUDED FROM BUSINESS WITH EU MEMBERS**

4 **INDIVIDUAL EU MEMBERS SHOULD EXPECT QUICK RESPONSE AND REDRESS FROM US COMPANIES. US COMPANIES MUST OUTLINE A MECHANISM TO QUICKLY AND EFFEECTIVELY ADDRESS PRIVACY COMPLAINTS OR RISK FACING FTC INVESTIGATION, OR INVESTIGATION BY A PRIVACY SHIELD PANEL**

What about the United Kingdom after Brexit?

Brexit brings another challenging layer to the equation, as it is unclear how GDPR and the Privacy Shield would apply to companies holding data in the UK or transferring data out of it to European or US-based businesses. In Data Privacy Monitor, Melinda L. McLellan and Jenna N. Felz, attorneys with BakerHostetler write, "the Privacy Shield agreement may not cover transfers of personal data from the UK. That said, the UK International Commisioner's Office could explicitly approve Privacy Shield certification as an adequate means of data transfer from the UK to the US, or it could establish a similar mechanism for such transfers, not unlike the US-Swiss Safe Harbor framework that served as an analog to the US-EU Safe Harbor framework. It will take at least two years for the UK to effect its withdrawal from the EU, with many estimating that the complicated negotiations will take much longer. In the interim, the existing EU-US data transfer landscape will continue to include the UK."

Understanding GDPR

The GDPR replaces an earlier directive with specific regulations to strengthen data protection for individual members of the European Union. Its regulations apply to businesses in the EU and outside of it.

- Multinational companies working across the EU will be required to appoint an independent Data Protection Officer.
- If a data breach occurs, the organization is required to notify the appropriate supervising parties within 72 hours.
- Data Protection Impact Assessments will evaluate how and why companies handle Big Data
- A new "Right to be Forgotten" allows individuals to request erasure of all persona data from a company's systems.

A Q&A with our expert, Director of Program Management Don Cook

Please explain the difference between Privacy Shield and GDPR?

Cook: The Privacy Shield is specific to EU member personal data transferred between the US and EU companies. The GDPR is a broader set of regulations governing acceptable use and protection of EU member personal data by any corporation or entity that does business, whether goods or services, with EU members. Essentially, Privacy Shield is specific to data transfer and GDPR casts a bigger and wider net. Any US company doing any business with EU customers must be concerned about both.

Should businesses tackle one requirement before, or over, another?

Cook: There is a nine month grace period for compliance with the Privacy Shield for any business that begins the process by September 30 of this year, so timeliness matters there. While GDPR is bigger and broader, an assessment for Privacy Shield readiness can be a jumping off point for GDPR compliance, which is required by mid-2018.

What are the three most important takeaways for a business that is preparing to comply with GDPR?

Cook: While the GDPR sets specific requirements for things like data breach notifications, and gives customers the ability to request removal of records, the basic steps that companies need to take are standard security best practices. So, the first thing I would say is know your data. Just like for any other data protection strategy a business needs to know what data it has and how it uses that data in order to protect it.

Second, make sure that you conduct regular risk assessments to understand your exposures. Third, prepare and practice an Incident Response Plan to respond to exposures in a timely manner and mitigate losses.