# Data Privacy Services:
## GDPR and Privacy Shield

## Data Privacy Regulations are About to Go Public

If your company does business with or handles the data of individuals in the European Union ("EU") then you are probably required to comply with **EU/U.S. Privacy Shield** directives, and (soon) the **EU General Data Protection Regulation ("GDPR").** The GDPR applies to all EU member states, as well as organizations that do business in the EU. The EU has been on the forefront of privacy legislation over the last 20+ years, and the GDPR is intended to strengthen and standardize previous privacy legislation into a unified standard. U.S.-based organizations have not traditionally put the same emphasis on the protection of private information as their EU-based counterparts, and privacy is suddenly an extremely important topic.

### What this Means for Your Organization

Since the EU does not deem the United States to have adequate privacy protection laws, their member states require U.S. organizations that handle Personally Identifiable Information (PII) collected in the EU to meet EU privacy standards through the Privacy Shield program, and soon through the GDPR (effective May 2018) as a condition of transferring data. U.S. companies that handle EU customer or employee data categorized as PII will need to demonstrate their compliance with EU privacy standards, and **companies that do not meet the regulations will risk large fines (up to 4% of the company's annual turnover or 20M Euros) and/or termination of contracts with EU partners.**

**Each Privacy engagement is designed to help you:**

- ✓ Understand your Privacy requirements so you can efficiently allocate the right resources, where they count
- ✓ Provide visibility into your Privacy posture to all levels of the organization
- ✓ Verify that your controls, tools, and processes are effective in addressing regulatory and legal risks
- ✓ Avoid reputational risk and fines by making sure you are meeting all facets of Privacy regulations
- ✓ Develop operational processes and technical controls related to Privacy as part of a sustainable Privacy Program
- ✓ Increase your market share by demonstrating your commitement to Privacy to customers and partners

**If this sounds complicated, that's because it is.** To meet the EU requirements, U.S.-based companies will be required to make a number of significant administrative and technical changes to their data handling processes, including:

- Implementation of a privacy program, which must include requirements for right to erasure, processing restrictions, and defined processes for how data collection and consent is handled
- Determining if a Data Protection Officer is required
- Following specific data breach notification and privacy complaint requirements
- Implementing the appropriate privacy policies, procedures, and notices
- Performing a data inventory and analysis as part of a Data Protection Impact Assessment (DPIA)

# How We Do It:

Our process begins with a lot of listening. We'll determine your key drivers, industry and regulatory requirements, company culture, organizational structure, goals, data types and locations, and concerns. From there we work with your stakeholders to define your Privacy objectives, based on the data you control and how it is shared. We then assist you in mapping out your data, figuring out how data is shared and managed, and building out the controls and processes required to meet all facets of Privacy regulations.

Our Privacy services will help you determine the real risk to your business, prioritize issues in a manner that aligns with organizational goals, and define a clear roadmap for continuous improvement so that you can make smart, informed decisions about your Privacy Program.

## Our mission is to help our customers move past fear, uncertainty, and doubt, and take full control of their Privacy Program.

### About AppSec Consulting:

We've been doing this for over 12 years, and our continuum of services is designed to fit just about everyone's security needs. Every service we provide comes with a level of experience and focused attention you won't find anywhere else. Our Security Testing team will help you identify the technical issues you should be thinking about, and our Strategic Advisory Services team will work with you to develop strategies for addressing them - that means assurance for you, your customers and your partners. And because we're independently owned, you'll find us completely agnostic regarding the solutions and vendors we recommend – this means you get the solution that fits your needs, not ours.

## This can't wait, so give us a call at 408.224.1110 today.

**You'll speak with an Information Security expert, not a sales person — we'll listen a lot, determine your needs, and provide clear, actionable recommendations. We look forward to seeing how we can help.**

***Information. Security. Handled.™***

**appsecconsulting.com | 408.224.1110**