General Data Protection Regulation ("GDPR") – Where to Start?

Does the organization collect and process personal data of European Union ("EU") data subjects when providing goods, services (paid or free) or completing behavior monitoring activities? Are international transfers of personal data undertaken as part of the business operations? Is the business processing personal data in the context of activities as a controller or processor in the EU, regardless of whether the processing takes place in the EU?

Did your business answer yes to any or all of the activities? Then GDPR pertains, no matter where your business or data storage is geographically located. In preparation for the May 2018 enforcement date, may require enhancement to your privacy program. This document outlines a two year phased approach to reduce the "overwhelming" group of activities that should be addressed.

Development of the implementation plan, should include Operations, HR, Compliance, Legal, IT and Marketing departments. Inclusion of these departments will aid in the defining the scope of funding, resources and executive management support needed to be successful.

Year 1, Phase A; document types of data collected from the consumer, customer, employee or client

- Review the consent language, validate the purposes of use are consistent with the language;
- When necessary update and sync consent language where differences are noted;
- Identify the types of data, sources, and storage locations;
- Is there data collected and transferred that may be exempt (i.e. HR data).

Year 1, Phase B; document the data flows, organizational access and security measures

- Complete a data flow map to include: source systems (on-line, retail, product/service promotions, etc.), cross border transfer means, storage locations and backup sites/systems;
- Validate user access, role and functionality (view only, extract, modify, etc.);
- Identify security measures in place (encryption, intrusion detection, audit logs, etc.).

Year 1, Phase C; develop, update and document administrative procedures

- Complete an assessment of call center operations capabilities to handle choice, access, correction and erasure requests;
- Update and document procedures to include key measurements (handling time, percentage completed, number of escalations, etc.);
- Determine frequency of reporting metrics and recipients' within executive management team;
- Define and document data breach response procedures.

Year 2, Phase A; review, update or execute cross border agreements (BCR, Model Contracts, etc.)

- Complete an assessment of all entities (internal and external) that collect, use or transfer personal data;

- Identify which category the entity falls within; controller or processor;
- Update or execute cross border agreements as necessary.

Year 2, Phase B; review, update and implement data protection training as necessary

- Complete an assessment of training materials to identify any potential gaps in content or delivery;
- Update training content, expand to address role based training for employees, vendors that handle choice, access, correction and erasure requests;
- Update training content, expand to address role based training for employees, vendors that manage data breach events.

Year 2, Phase C; review, update and implement data management practices as necessary

- Based on the data flow assessment, regulatory and legal obligations; define or update the records retention schedule;
- Identify the systems, databases or physical storage that maintain the personal data;
- Validate any technology and resources necessary to implement data destruction processes;
- Identify data managers within each of the functions to implement and complete data destruction;
- Measure and report progress or barriers to destruction to executive management on a scheduled period.

In addition, if your organization does not have a Data Protection Officer ("DPO"), recommend the search start yesterday. Experienced resources who have managed and operated a privacy program to this scale are limited, attracting them will take an extensive period of time. However hiring a DPO who grasps these concepts will engage staff who are specialized in each or a few of these areas and unite them to create a privacy program that excels.

For assistance in development and implementation of a GDPR program or defining the DPO role, advising executive management, insight on privacy requirements or recommendations on local or global requirements, feel free to contact us at privacy-internationallp.com or Jim Keese, at jmkeese@privacy-internationallp.com.