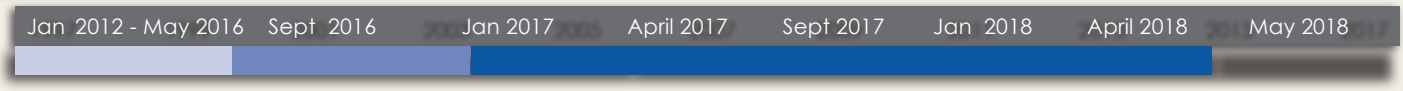
Privacy International, LLP

INTERNATIONAL DATA PROTECTION, PRIVACY, AND INFORMATION GOVERNANCE SERVICES

TIMELINE AT A GLANCE



GDPR Ratified	Guidelines, New Laws	Gap Assessment, Secure Funding, Implementation, Culture Changes
EU Parliament Completed 17 Milestones	WP29 - Data Portability, DPO Role Guidelines, France Adopts Digital Republic	Complete an Organizational Risk and Gap Assessment ("ORGA"). Utilize Results for Funding, Secure Resources, and Technology. Drive Awareness and Culture Changes Through Training Programs

Plan Globally, Execute Locally... Many organizationa are in the planning stage for their GDPR compliance program and envisioning a start date in late Q1 2017. Leaving only **14 months** to complete assessments, close gaps and implement changes. To aid in development of your program, take the time to review the sensible approach outlined. Remember, involvement of all functional areas of the company is necessary, as the privacy office can't do it alone.

Privacy International, LLP can assist in providing a practical approach for your GDPR compliance program. We can scope the funding and resource estimates, provide a high level project plan and coordinate the overwhelming activities to be completed. Our suggestion is start now, as May 2018 will be here in next to no time...

Complex and Significant Tasks

Data Retention

Organizations collect, store and backup personal data, typically the data is not classified and retained for a period of time beyond the business need. **Actions** - identify the data owner, data content in the record/file and apply retention, this typically take years to address.

Data Flows, Access Controls and Security Measures

Information governance, document the flow of personal data from the point (system) of collection thru back-up and recovery. The mapping of the data flow will identify the systems/databases. **Actions** - deduplication, validate/update access controls (role or individual based) and apply security measures required to protect against unauthorized use, extract or duplication.

Resources - DPO, Privacy Managers & Analysts

A detailed plan has been completed, who will execute, implement the plan and manage the updated program? The inability to monitor and manage the program will only increase the potential of regulatory fines. **Action** - start hiring now, staffing will be a signifcant challenge due to the pending demand for experienced resources.

Data Breach - Incident Response

A incident response plan requires an data inventory, access controls, audit trails configured and who is on the response team. **Actions** - test the plan with assigned resources, complete a mock investigation, create notifications and test the call center knowledge.

International Data Transfers

Company's under estimate the time to complete qualified transfer mechanisms and secure internal/external approvals, an additional burden on the privacy office. **Actions** - completion approved Code of Conduct, BCR's, or Model Contracts and updated processors agreements to process and transfer personal data. (note: prior approval is no longer necessary)

Target Areas of Risk

ADDITIONAL AREAS

Legitimate Interest... documented justification for all data they collect on EU residents. Legitimate interest exists when there is a relevant and appropriate connection between the individual and the company.

Individual Rights... data portability to request the company to export the individual data to themself or a new service provider, to object the processing of their data and to be forgotten.

Territorial Scope... extends coverage to companys based outside of the EU but process data related to EU residents either for purpose of providing services, goods, or monitoring behavior.

Consent and Notices... companys must obtain and preserve proof of the individual unambiguous, informed, affirmative, specific and freely-given consent. Explicit consent is required in certain activities, e.g. profiling data received by consent or sensitive data.

Privacy International, LLP **privacy-internationallp.com** **1-720-638-5064**

jmkeese@privacy-internationallp.com