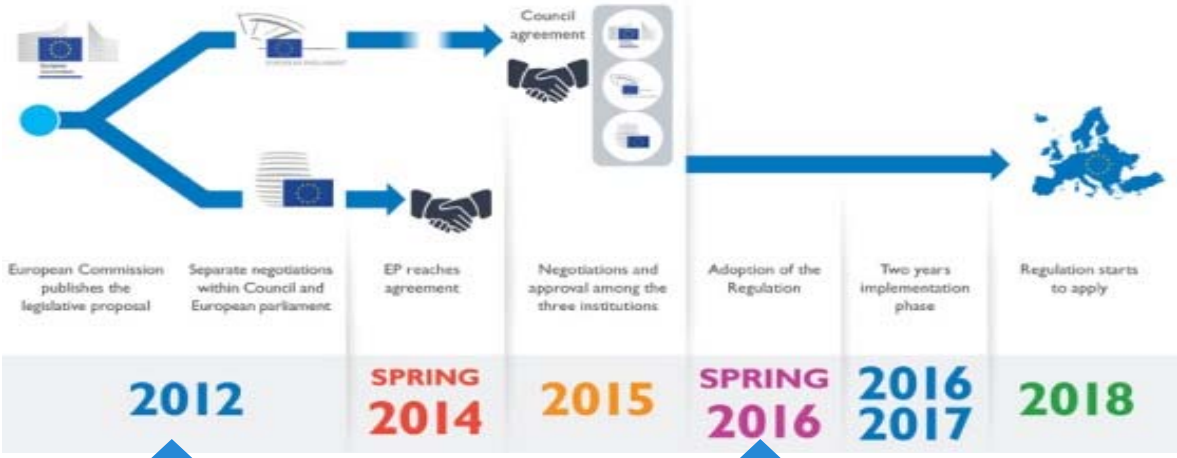
DLA PIPER

EU GENERAL DATA PROTECTION REGULATION FOR STATE AGs AND US COMPANIES

– WHAT DOES IT REALLY MEAN?

GDPR - Timeline




EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

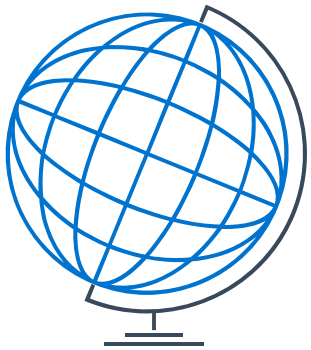
New EU Privacy Framework

- Expands on a 1995 EU Data Protection Directive – clamps down on flexiblity
- Separate e-Privacy Regulation will follow and require opt-in consent for all online tracking.
- Very demanding operational and legal requirements
  - Multi-nationals typically have tens of millions of dollars in compliance costs
  - Very difficult for smaller companies to deal with, some closing down in EU
- Significant uncertainty even now about some key areas for country interpretation – employee privacy, what is sensitive data, age limits for obtaining consent from children.
- Huge boon for consultants and lawyers (we are working on more than 300)
- GDPR does not resolve and magnifies risks regarding US law enforcement requests, cybersecurity monitoring, access to the Who Is database

One Stop Shop

- Each Member State: One (or more) supervisory authority.
- **Cross-border processing**: One-stop-shop: one lead supervisory authority.
- **Lead supervisory authority**: The authority where the main establishment or the single establishment of the controller or processor is located.
- **Exceptions** may apply – for example, issues arising in a single Member State; employee data processing; healthcare data processing.
- **Questions**: 'cross-border processing', 'main establishment'?

Extend Territorial Scope to Reach



- GDPR applies to the processing of personal data:
  - by parent company or subsidiary controller or processor established in the EU.
  - of EU residents when they are in the EU even if the data controller has no presence in the EU if the data are used for:
    a) offering goods or services, (including free services), to data subjects in the EU; or
    b) monitoring EU residents' behavior when they are in the EU (e.g., placing a cookie on an EU resident's device).

Scope - Data Processors

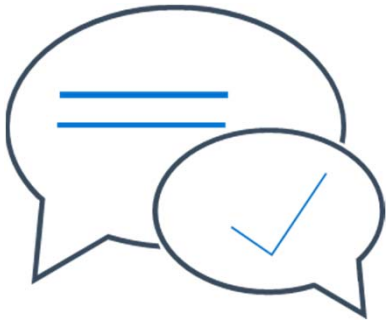
- Service providers processing data on behalf of other companies will be required to comply with a number of specific data protection related obligations
  - adoption of security measures
  - management of sub-contractors (and ecosystem)
  - register of processing activities
  - managing access rights
- They will be liable for sanctions if they fail to meet those obligations.
- Joint liability with controllers for the same processing.
- Significant impact on supply chain management / vendor contracts / ecosystems

US Processors Can No Longer Hide!

- The GDPR has broad reach:
  - use and collection of customer data
  - integrated HR databases and processes
  - cybersecurity and data security monitoring systems (inbound / outbound)
  - profiling and other data analytics

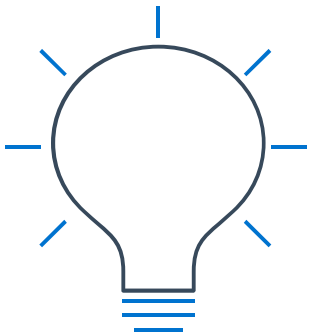
- Controllers are jointly liable with processors and threat of high fines will force them to work out compliance with processors in the US
- EU privacy requirements flow through to Ecosystem partners
  - will need to define responsibilities for EU data through the ecosystem
  - this implicates smaller service providers
  - as with data security under US law, will need to develop compliance frameworks

Fair processing



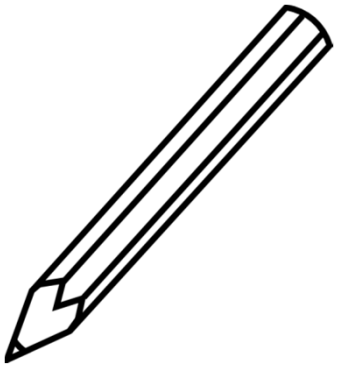
- Legal grounds for data processing remain the same (e.g. contractual agreement, legal obligation, legitimate interest, consent, etc.)
- **Consent** of limited utility:
  - freely given, specific, informed, unambiguous
  - Long list of requirements makes it often impractical
  - Opt-in to separate consent language
  - easy right to withdraw
- **Legitimate Interest of controller** surer ground:
  - data subjects can "object"
  - controller must respect unless "overriding interests"
- Use of preference centers

Transparency



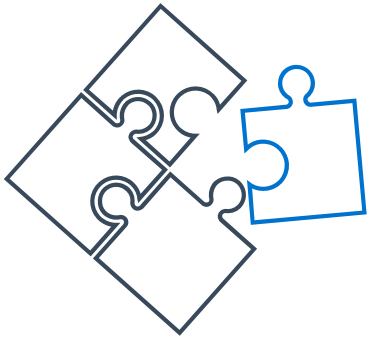
- Organizations will have increased transparency obligations; privacy notices
  - will need to include much more detailed privacy notices
  - beyond FTC best practices
  - including description of rights to withdraw consent
  - layered approach recommended

Rights of Individuals



- Information (notice) prior to actual data processing
- Right of access
- Right to rectification
- Right to object
- Right to restriction
- Right to data portability
- Right to be forgotten vs. 1st Amendment
- Right not to be subject to automated decision making

Data Portability

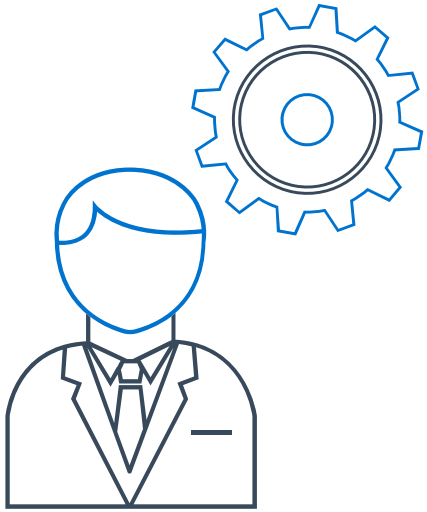


- Organizations must ensure data subjects can easily receive personal data concerning them and/or transfer such data (if feasible) from one service provider to another.
- Designed in hopes that EU residents will switch to more privacy-focused European services

Right to be Forgotten

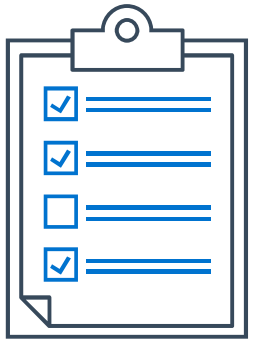
- The GDPR incorporates the “right to be forgotten”, allowing data subjects the right to require a controller to delete data about them if there are no legitimate grounds for retaining it.
- Largely limited to publicly available search engines
- Lawful in Europe because of lesser protection for free speech

Privacy by Design and by Default



- Companies must take privacy risk into account throughout the process of designing a new product or service, and adopt appropriate mechanisms to ensure that e.g., minimal personal data is collected.
  - Like the FTC approach, but more demanding outcomes
- Approved certification mechanisms can be used to demonstrate compliance with these requirements.

Privacy Impact Assessment (PIA)



- A PIA will become mandatory before processing personal data for operations that are likely to present high privacy risks to data subjects due to the nature or scope of the processing operations.
- Authorities will issue list of the type of operations subject to PIA.

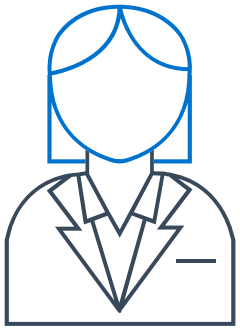
Record of processing activity

- Each controller and, where applicable, the controller's representative in Europe, shall maintain a record of processing activities for which it is responsible.
- Also applies to processors in the US who access EU personal data.
- Instead of registering data processing with privacy authority, but simple failure to keep records is a violation that can be sanctioned.

Data Breach

- Personal data breach *means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.*
- Notification to the **privacy authority**: without undue delay and where feasible **within 72 hours** of discovery unless unlikely to result in a risk to rights and freedoms.
- Notification to **data subjects: without undue delay** if the breach is likely to result in a high risk to the rights and freedoms of individuals so that they may take the necessary precautions.
- **Contractual arrangements** with data processors regarding data security and data breach notice strongly recommended.

Data Protection Officer



- Obligation applies to controllers and processors.
- Applies when core activities:
  - require regular and systematic **monitoring of data subjects on a large scale**;
  - consist of processing on a large scale **"special categories of data"** (Art. 9) or data relating to **criminal convictions**.
- Who:
  - a **staff member or a consultant** (service contract)
  - Must be independent
  - a group may appoint a **single DPO**.

Data Protection Officer (cont'd)

- Tasks include:
  - **inform and advise** the controller / processor (and employees) of their obligations;
  - **monitor** compliance with the GDPR;
  - **advise** on privacy impact assessmenst;
  - **cooperate** with the supervisory authority (including acting as point of contact).

Eye Popping Potential Sanctions

- Administrative fines up to **20,000,000 EUR**, or up to **4% of the total worldwide yearly revenues** of the preceding financial year, whichever is higher.
- Some countries will have class actions

Sanctions (cont'd)

- Factors to be considered when determining fines:
  - **nature, gravity and duration** of the infringement;
  - **intentional character** of the infringement;
  - **actions taken to mitigate** the damage;
  - **degree of responsibility** (e.g. data protection by design or by default) or any relevant **previous infringements**;
  - **cooperation with the supervisory authority** (and the manner in which supervisory authority learned of infringement);
  - **sensitivity of personal data** affected;
  - **compliance with measures** ordered;
  - **adherence to a code of conduct** (or certification mechanism);
  - **other aggravating or mitigating factors** (e.g. profiting from the violation. strong governance framework, etc.).

Consequences for State AGs – Evidence in EU

- EU law restricts data transfers to the US and other countries with different privacy regimes
  - Snowden revelations have produced somewhat hypocritical concern about personal data transfers to the US
- GDPR blocks foreign court orders to transfer personal data unless pursuant to an MLAT or international agreement
  - Allows transfers between antitrust regulators (but not direct subpoenas to EU targets)
  - No exception for consumer protection transfers
- GDPR big fines will make EU recipients reluctant to comply with US process
- Only solution is a US-EU law enforcement info sharing agreement
  - UK-US one being negotated, full reciprocity
  - EU early draft does not apply to contents

Consequences for State AGs – Who Is Gone?

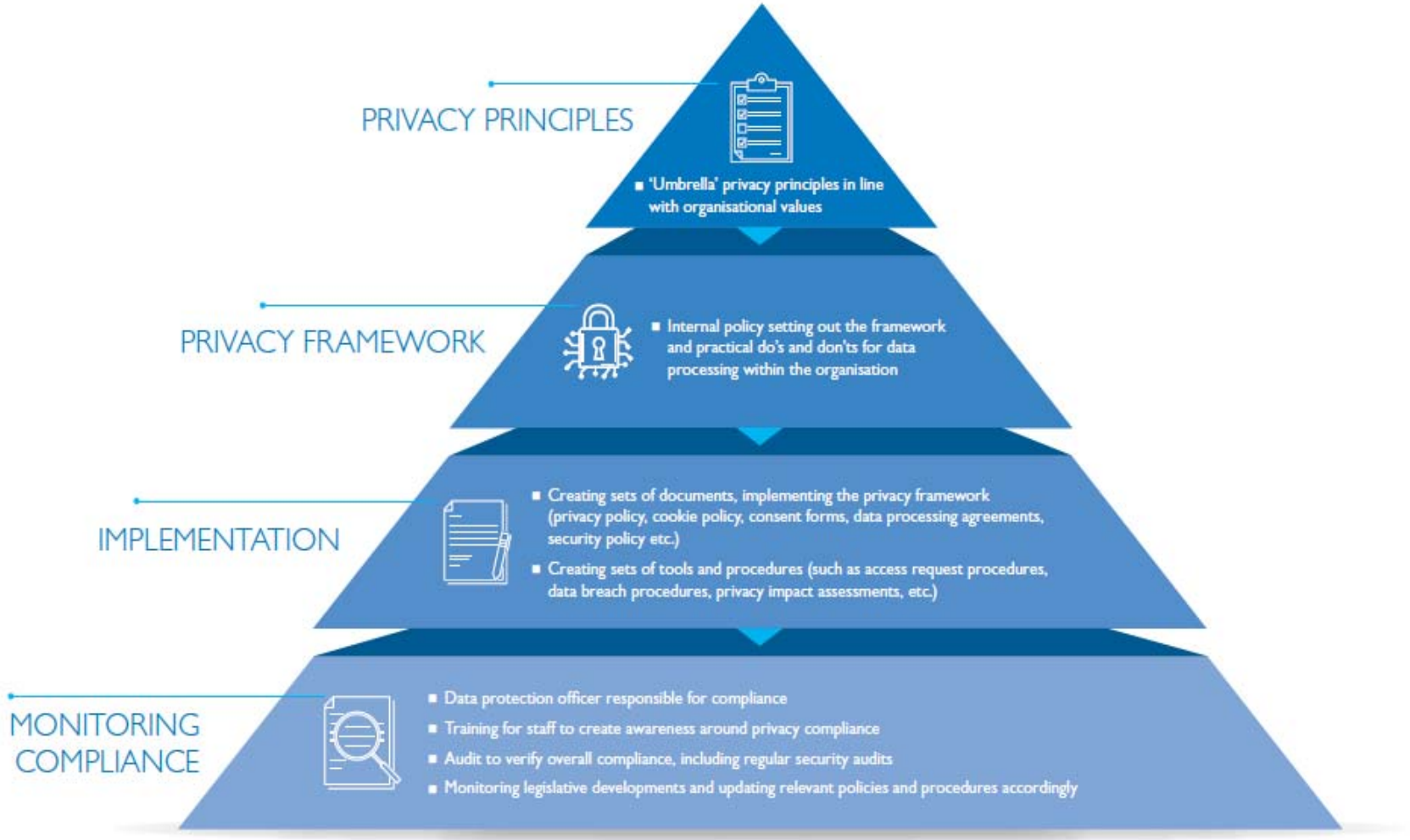
- GDPR requires affirmative consent to make personal data available
- EU Data Protection Authorities have refused an ICANN request for an extension so that access to Who Is can continue
- May 25th Who Is may go dark for EU registrants, loophole for others too
  - Eventual compromise likely to be one-time only access → harder to trace and follow serial fraudsters

Consequences for State AGs – Employee Privacy Restrictions

- GDPR and EU country employee privacy laws pose significant barriers to monitoring employee communications on corporate networks
  - GDPR makes employee consent almost always invalid
  - Personal communications of employees have criminal and civil protection
- Unions (Works Councils) must agree to monitoring program in most of Europe
- Monitoring of BYOD devices is particularly hard
- Significantly complicates evidence-gathering from EU residents, as well as network monitoring of attacks launched through EU servers

DLA PIPER

HOW TO BUILD YOUR GLOBAL PRIVACY COMPLIANCE PROGRAM



MAY16 | 3104708

GLOBAL PRIVACY COMPLIANCE PROGRAM
ROADMAP

DLA PIPER

	Scope	Assess	Build	Manage
OBJECTIVE	Confirm project scope, resources and timetable aligned to relative business risk.	Carry out data processing analysis to identify compliance gaps. Determine risk appetite.	Establish an effective governance structure to manage privacy risk across the organisation.	Routine management of privacy risk consistent with current regulatory requirements.
OUTPUTS	▪ project plan ▪ budget ▪ outline risk report	▪ data processing summary ▪ risk analysis report ▪ action plan	▪ privacy principles ▪ privacy framework ▪ documents, tools and procedures	▪ DPO (and support desk) ▪ training and audits ▪ legislative updates

TIMELINE

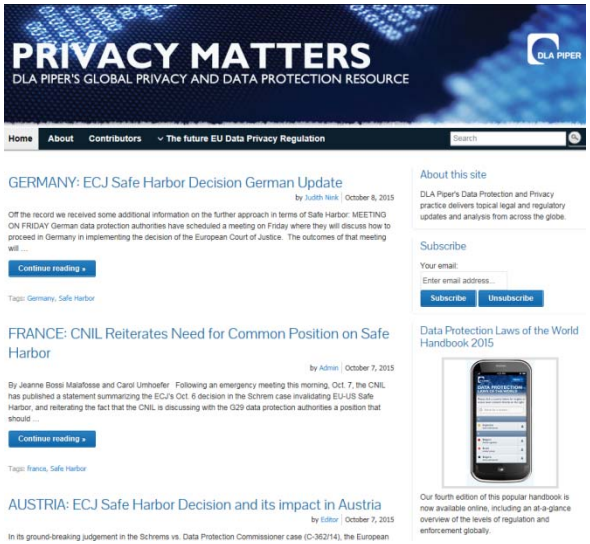
Implement/Build

- **Governance:** DPO; training; compliance reviews and audits
- **Record keeping:** registry of data processing activities
- **Policies and Procedures:** PIAs; requests to access, object, and rectify; right to be forgotten; data portability
- **Data Processing:** Privacy by Design & Default; document legal bases for processing; privacy notices; consents
- **Data Transfers:** Identify cross-border data flows; assess transfer mechanisms; intragroup agreements; monitor developments
- **Vendor Management:** Review vendor contracts; vendor due diligence; develop vendor privacy and security contract templates
- **Incident Response Program:** Implement or review and update; address EU Breach Notice Obligations
- **Security:** Pseudonymization and encryption; confidentiality, integrity and availability; business continuity; testing; ISO certification?

Manage

- DPO oversight
- Compliance reviews
- Adjust processes and procedures
- Sustainable program
- Measurement and reporting
- Change management
- Training

Stay Informed



Access our

Data Protection Laws of the World Handbook at

www.dlapiperdataprotection.com

Subscribe to our **Privacy Matters blog** for regular updates

http://blogs.dlapiper.com/privacymatters/

Stay Informed

See our **New Microsite:**

The EU General Data Protection Regulation

https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/home/

Our newest tool aims to help you assess your data protection maturity level.

Access the **Data Privacy Scorebox** at

http://dlapiperdataprotection.com/scorebox/