Privacy and data security forum: Countdown to GDPR – Legal and operational must dos for compliance

May 24, 2017
The General Data Protection Regulation will take effect on **May 25, 2018**. It replaces the current 1995 Data Protection Directive (95/46/EC).

Bill as the legal framework for the digital era. But **e-Privacy Regulation** mandating opt-in consent for all online tracking will follow.

GDPR means **detailed, risk-based rules** for processing personal data; **more obligations** for controllers and processors; **greater regulatory risk exposure; severe potential liability**.

GDPR invites plenty of forthcoming legislation, official guidance, as well as codes of conduct and similar soft law.

GDPR does not resolve pending issues relating to transatlantic data transfers.
In general -- a single set of rules on data protection, directly applicable in all EU Member States, thereby mitigating the current fragmentation of national data protection laws.

BUT -- some local variations may persist or expand, including on

types of sensitive data,
age limits for obtaining consent from children,
employee privacy and
medical research exception.
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'.
Sweeping Definition of Personal Data

Personal data:

any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

IP address or MAC address alone are personal data

Exceptions coming for pseudonymous data
Scope - Data Processors

Organizations 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
- Register of processing activities
- Managing access rights

They will be liable for sanctions if they fail to meet those obligations.

Unless responsibilities spelled out by contract, joint liability with controllers for the same processing.

Major Impact on supply chain management / vendor contracts.
Fair processing

Legal grounds for data processing remain the same (e.g. contractual agreement, legal obligation, legitimate interest, consent, etc.)

Consent:
freely given, specific, informed, unambiguous
by a statement or by a clear affirmative action
separate consent language
easy right to withdraw

Legitimate Interests
data subjects can "object"
controller must respect unless "overriding interests"

Use of preference centers
Organizations will have increased transparency obligations; privacy notices will need to include much more detailed information including description of rights to withdraw consent lawyered approach recommended
Expanded 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
Right not to be subject to automated decision making
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.

→ Need to apply governance in the product or service design process

• An approved certification mechanism can be used to demonstrate compliance with these requirements (if palatable)
A PIA will become a mandatory requirement 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, shall maintain a record of processing activities for which it is responsible.

Also applies to processors.

Replaces data registrations with DPAs
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 supervisory authority: without undue delay and where feasible within 72 hours unless unlikely to result in a risk to rights and freedoms. (Harmtrigger)

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 breach critical, as in the US.
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)
a corporate group may appoint a single DPO.
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.

**Designed to Get the Board’s Attention**

In practice? Many questions:

- e.g., controller/processor? controller group, processor group?
Factors to be considered when determining fines:

- nature, gravity and duration of the infringement;
- Was the violation intentional;
- actions taken to mitigate the damage;
- degree of responsibility (e.g. data protection by design or by default) or any relevant previous violations;
- cooperation with the supervisory authority (and the way supervisory authority learned of infringement);
- type of personal data affected;
- compliance with measures ordered;
- adherence to a code of conduct (or certification mechanism);
- other aggravating or mitigating factors (e.g. financial benefit from violation, etc.)
Should GDPR be your global standard?

| EU Clients Moving to GDPR compliance as global standard throughout the organization | US often have use another approach and adapt to GDPR starting point |

Identify outliers

| Jurisdictions with divergent rules | That have high enforcement risk |

Assess compliance risk based on key markets

| Combine outliers/key markets | Balance risk appetite |
Practical Steps

- **Set a time line**
  - Include milestones
  - Deadline: May 25, 2018

- **Build a team**
  - Multidisciplinary
  - Outside experts

- **Get board support**
  - High risk area
  - Culture shift

- **Allocate budget**
  - Data mapping & compliance assessment
  - Remedies & monitoring
HOW TO BUILD YOUR GLOBAL PRIVACY COMPLIANCE PROGRAM

PRIVACY PRINCIPLES
- "Umbrella" privacy principles in line with organisational values

PRIVACY FRAMEWORK
- Internal policy setting out the framework and practical do's and don'ts for data processing within the organisation

IMPLEMENTATION
- Creating sets of documents, implementing the privacy framework (privacy policy, cookie policy, consent forms, data processing agreements, security policy etc.)
- Creating sets of tools and procedures (such as access request procedures, data breach procedures, privacy impact assessments, etc.)

MONITORING COMPLIANCE
- Data protection officer responsible for compliance
- Training for staff to create awareness around privacy compliance
- Audit to verify overall compliance, including regular security audits
- Monitoring legislative developments and updating relevant policies and procedures accordingly
Data processing lifecycle

Privacy law governs the processing of personal data. Processing can be defined as any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, use, recording, organization, structuring, storage, alteration, retrieval, erasure dissemination.
Shifting focus

The General Data Protection Regulation (GDPR) is different in form and function from the current regime

- More Accountability
  - Internal documentation more defined
  - Privacy by design and privacy by default must be embedded
  - Data Protection Impact Assessments (DPIAs) required
  - Higher fines
  - Extended Supervisory Authority (SA)* powers
  - Data Protection Officer required
  - Immediate notification for data breaches

- Fewer Formalities
  - SA notification not required
  - SA approval not necessary for international data transfers under EU model contracts
  - SA authorizations not required, but prior consultations required

* “Supervisory Authority” is a term that was introduced in the GDPR as a replacement for the more commonly-known “Data Protection Authority” or “DPA”. Although the term DPA is still used in common parlance, Deloitte identifies them as SAs under the GDPR.
Roles and responsibilities under the GDPR

Data Protection Officers (DPOs)

Mandatory DPO

Under certain conditions, appointing a DPO is mandatory

A Data Protection Officer is required if:
• Processing is carried out by a public authority or body
• Engages in regular and systematic monitoring on a large scale*
• Processes special categories of personal data on a large scale

Main characteristics of DPO

Designation

• Professional qualities (including expert knowledge)
• Possible to have one DPO for several entities
• Internal/external
• Full-time/part-time

Independent

• No interference or retaliation
• No conflicts of interest
• Reports directly to the highest management level
• Maintains secrecy and confidentiality with regard to his/her duties, according to applicable law

Responsibilities of DPO

Tasks and roles of the DPO

• **Inform and advise** the controller or the processor and the employees who are processing personal data of their obligations pursuant to the Regulation
• **Monitor compliance** with the Regulation, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits
• **Provide advice** where requested as regards a data protection impact assessment and monitor its performance
• **Monitor responses** to requests from the supervisory authority and, within the sphere of the data protection officer's competence, to cooperate with the supervisory authority at the latter's request or on the data protection officer's own initiative
• **Act as the contact point** for the supervisory authority on issues related to the processing of personal data, including the prior consultation, and consult, as appropriate, on any other matter

Source: http://bit.ly/1TtydR4

* "Large scale" is not defined in the GDPR but further guidance may be forthcoming
Roles and responsibilities under the GDPR
Governing supervisory authority

Determining Lead Supervisory Authority (Lead SA):

- Member State where controller or processor are established
- Member State where substantially affected (or likely to be) data subjects reside
- SA with whom a complaint was filed

Responsibilities:

- A lead SA shall cooperate and exchange relevant information with other SAs regarding issues raised.
- The lead SA may request at any time that other SAs provide mutual assistance and may conduct joint operations and enforcement measures, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
- The lead SA shall, without delay, (a) communicate relevant information on a matter and (b) submit a draft decision to the other SAs concerned for their opinion and take due account of their views.
- SAs shall provide each other with relevant information and mutual assistance (including, authorizations and consultations, inspections and investigations) in order to implement and apply this Regulation in a consistent manner.
- SAs shall put in place measures for effective cooperation with one another.
- Each SA shall take all appropriate measures required to reply to a request of another SA without undue delay.
- Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, an SA of each of those Member States shall have the right to participate in joint operations.

Source: http://bit.ly/1TtydR4

Copyright © 2017 Deloitte Development LLC. All rights reserved.
Administrative, technical and physical safeguards pursuant to the GDPR

Security for Privacy

Data security
Taking appropriate technical and organizational measures to ensure security

Both the controller and the processor must implement appropriate technical and organizational measures to provide an appropriate level of security, taking into account:

• The state of current technologies and technical capabilities
• The cost of implementation
• The nature, scope, context, and purpose of the processing
• The likelihood and potential impact on the rights and freedoms of individuals that would be impacted by a security breach
• The risks presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed

Any person acting for the controller or the processor must only act upon their instructions. Adherence to approved codes of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the requirements.

Practical considerations and mechanisms for appropriate security measures:

- The ability to provide the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Pseudonymization and encryption of personal data
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- The process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for confirming the security of the processing

Source: http://bit.ly/1TtydR4
Administrative, technical and physical safeguards
Privacy by design & privacy by default

EU legal context
Concepts in the new GDPR
What does it mean:
• An initiative to embed privacy in design from the beginning

Privacy by Design:
• Implement technical and organizational measures commensurate with the risks to effectively provide data protection
• At time of determination of the means of processing and processing itself

Privacy by Default:
• Minimize scope, ensuring only necessary personal data for each specific purpose are processed
• Amount of data, the extent of their processing, storage period and accessibility based on purpose
• Settings, technologies and preferences are privacy protective by default so that personal data are protected from the outset

Mechanisms
Practical implementation
• Pseudonymization
• Data Deidentification
• Anonymization
• Data Minimization
## Establishing the privacy program foundation

<table>
<thead>
<tr>
<th>Activity</th>
<th>High-level summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational model</td>
<td>The organizational model for data privacy determines the placement of the privacy function within the organization, the constituents of the privacy office, and the roles and responsibilities associated with data privacy.</td>
</tr>
<tr>
<td>Policies and notices</td>
<td>Data privacy policies and notices are used to establish governance and communicate data privacy practices to data subjects. An internal employee privacy policy governs the collection and processing activities of Personal Data. A privacy notice provides a written description of the organization's practices with respect to its collection, use, disclosure, and protection of Personal Data.</td>
</tr>
<tr>
<td>Data privacy procedures</td>
<td>A number of privacy procedures and guidelines are required to support the implementation of privacy notices and policies.</td>
</tr>
<tr>
<td>Training and awareness</td>
<td>Privacy training and communication strategies are important components to roll out the privacy program. These are generally administered to employees who might come in contact with Personal Data and help build a consistent understanding of the organization's privacy program and requirements around handling of Personal Data.</td>
</tr>
<tr>
<td>Metrics and reporting</td>
<td>Privacy metrics and reporting help monitor the health of the privacy program and report its status to key stakeholders so that they are better informed to make the necessary adjustments to the program.</td>
</tr>
<tr>
<td>Incident response</td>
<td>A privacy incident response procedure helps organizations respond to incidents in alignment with identified regulatory, contractual, and policy requirements. It also improves business and employee awareness, understanding, and participation in the privacy incident process.</td>
</tr>
<tr>
<td>International privacy</td>
<td>International privacy considerations include cross-border data transfer strategy and country-specific privacy requirements, such as engaging with works councils, notifying the DPAs and complying with local labor laws.</td>
</tr>
<tr>
<td>Localization plan</td>
<td>A localization plan involves identifying the program components that are likely to vary across jurisdictions and developing an approach to carry out their localization.</td>
</tr>
</tbody>
</table>
Privacy Program Sample Framework

Appropriate data use

Governance

Privacy governance council

Sales & marketing working group
R&D working group
Information security working group
IT & finance working group
Human resources working group
Regulatory & compliance working group

Governance

+ Strategy and Roadmap
+ Program Framework
+ Policies & Procedures
+ Business Partnership
+ Executive Sponsorship

Operating components

Privacy risk management
+ Applicable laws & regulations
+ Privacy risk assessment
+ Data inventory & data maps
+ Third-Party assessment
+ Baseline controls

Data breach handling
+ Data impacted
+ Regulatory impacts
+ Breach management
+ Breach response

External communications
+ Privacy notices
+ Event response
+ Regulatory inquiries
+ Customer communication
+ Regulatory registrations & consultations

Privacy education & training
+ Privacy awareness
+ Program processes
+ Customer resources
+ Regulatory changes
+ Localization

Program monitoring
+ Key performance indicators & metrics
+ Data lifecycle management
+ Program audit framework
+ Privacy impact assessment
+ Reporting

Foundation components

Plan
Analyze
Design
Build
Implement
Assess
Improve
Operate

Accountability

Privacy by design & privacy by default

Industry & organizational context

Copyright © 2017 Deloitte Development LLC. All rights reserved.
Critical success factors

The following factors are important considerations for the effective establishment and implementation of an enterprise privacy program:

- **Cross-functional executive support** – An effective privacy program requires strong executive support and involvement from specific areas, such as business, IT, HR, and Legal.

- **Data lifecycle** – Before you can understand how to implement reasonable controls, you first need to understand where the data is and how it is used, from collection through destruction.

- **Risk-based approach** – Focusing on business risk (as opposed to merely compliance) and identifying and prioritizing high-risk items can enhance the value the privacy program can deliver.

- **Change management** – The success of the privacy program will come down to what people do on a day-to-day basis, and preparing, educating, and holding accountable appropriate professionals is vital.

- **Implementation focus** – Because most serious problems occur due to policies not matching operational practices and capabilities, it is critical to go beyond policy development to actually operationalizing the policies in business processes and technology.
<table>
<thead>
<tr>
<th>Activity</th>
<th>High-Level Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationalized requirements and controls</td>
<td>Rationalized requirements and controls are derived from commonalities between data privacy requirement sources (e.g., privacy laws, regulations, standards, etc.) and are foundational to defining business process, system, and governance privacy controls.</td>
</tr>
<tr>
<td>Business process/data inventory &amp; risk ranking</td>
<td>A business process/data inventory provides a starting point to understand the risks to Personal Data. After the inventory is available, a risk-ranking framework can help prioritize key business processes and functions that should be evaluated for data privacy risks.</td>
</tr>
<tr>
<td>Data flow analysis/maps</td>
<td>Understanding how an organization processes data assets entails taking a risk-based view of its business processes, supporting systems and associated data repositories that contain data. A data flow map identifies the flow of Personal Data through its collection, storage, use, transfer, and destruction.</td>
</tr>
<tr>
<td>Gap analysis and maturity Ranking</td>
<td>A privacy risk assessment is conducted against identified privacy requirements to determine gaps and, optionally, maturity ranking. This summary usually provides executives within the organization a starting point to understand data privacy risks and their criticality.</td>
</tr>
<tr>
<td>Strategy and roadmap</td>
<td>Based on the gap analysis, a privacy strategy and roadmap is created to mitigate potential improvement areas associated with the data privacy program.</td>
</tr>
</tbody>
</table>
Notice and consent under the GDPR
Stronger data subject rights

Information notice
Required disclosure to the data subject

When obtaining personal data, the controller must provide the data subject the following in a concise, transparent, intelligible and easily accessible form, using clear and plain language:

• Identity & contact details
• Legal basis & purposes of processing
• If processing is necessary for controller’s legitimate interests, a description of the legitimate interest
• Recipients or categories of recipients
• Transfers to other countries
• Data retention period
• Right of access, rectification, erasure, data portability, restriction of and objection to processing
• Right to withdraw consent at any time
• Right to lodge a complaint with an SA
• Whether the provision of personal data is a statutory or contractual requirement
• Existence of automated decision-making and the significance of such processing
• Whether provision is mandatory or voluntary and consequences of failure to provide
• Whether Personal Data has been obtained by someone other than the data subject (must also inform data subject regarding the categories of data concerned)

Reinforced consent
Conditions for consent to begin collecting data

• Unambiguous, informed and explicit consent was given by the data subject prior to collection
• Request for consent must be presented in a manner that is clearly distinguishable from the other matters, for which consent is sought, using clear and plain language
• Data subjects have the right to withdraw the consent at any time
• Withdrawal of consent must not affect the lawfulness of processing based on consent before its withdrawal

The processing of the personal data of a child is lawful for children age 16 and over. Where the child is below the age of 16 years, such processing is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. The organization should make reasonable efforts to verify that consent is given or authorized by the parent, taking into consideration available technology.

Member States of the European Union may lower this threshold, setting the maximum age at 13 years old for processing without parental consent.

Source:  http://bit.ly/1TtydR4
Copyright © 2017 Deloitte Development LLC. All rights reserved.
Access, correction, amendment and deletion under the GDPR
Stronger rights of access and control

Right of access

The right to obtain information on one's data getting processed

A data subject has the right to obtain:

- Confirmation as to whether or not the controller processes their personal data
- Sufficient information on how this personal data is processed (specific information must be provided to data subject)

Implications:

- Controllers may request additional information to confirm identity of data subject
- Communication relating to the processing of data must be in an understandable form in clear language and must be provided free of charge
- Controllers must respond within one month of receipt of request (may extend to two months if request is complex)
- When the request is manifestly unfounded or excessive, controller may refuse to act on request or impose a fee
- This is not the right to inspect, but the right to have a copy of the personal data

Right to erasure

Right to erase personal data

A data subject has the right to have the controller erase his/her personal data *without undue delay*, and the control shall comply, if:

- The data is no longer necessary for the purposes for which it was collected or otherwise processed
- The data subject withdraws consent on which the processing is based and there is no other legal ground for the processing to continue
- The data subject objects to the processing of personal data and the processing is based on the legitimate interests of the controller and there are no other legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes
- The data has been unlawfully processed
- Erasure is necessary for compliance with a legal obligation

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, *shall take reasonable steps*, including technical measures, to inform other entities and organizations that may be processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Source: http://bit.ly/1TtydR4

Copyright © 2017 Deloitte Development LLC. All rights reserved.
Access, correction, amendment and deletion under the GDPR
Increased personal control over data

Right to object
The right to object to processing

A data subject has the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her even if the processing:
- Takes place for the performance of a task carried out in the public interest or official authority
- Is based on the legitimate interest of the controller, including profiling based on these provisions

Note: when personal data is processed for direct marketing purposes, the data subject has the right to object at any time.

Upon receiving the objection, the controller can no longer process the personal data, unless that controller demonstrates compelling legitimate grounds for:
- The processing which override the interests, rights and freedoms of the data subject, or
- The establishment, exercise, or defense of legal claims

Right to data portability
Right to receive personal data

A data subject has the right to receive his or her personal data in a structured, commonly-used and machine-readable format and the right to transmit those data to another controller (directly when technically feasible) where:
- Processing is based on consent or necessary for the performance of a contract
- Processing is carried out by automated means

This right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Right of rectification
Right to rectify personal data

A data subject has the right to obtain from the controller, without unreasonable delay:
- Rectification of inaccurate data
- Completion of incomplete personal data

Source: http://bit.ly/1TtydR4
Copyright © 2017 Deloitte Development LLC. All rights reserved.
Access, Correction, Amendment and Deletion
Increased Protections for Automated Processing

Right to Restrict Processing
Right to control personal data use

A data subject has the right to restrict processing of his or her personal data (the marking of stored personal data with the aim of limiting future processing) when:

- The **accuracy of the data is contested** by the data subject, for a period enabling the controller to verify the accuracy of the data,
- The **processing is unlawful** and the data subject requests the restriction of their use rather than erasure,
- The controller **no longer needs the personal data** for the purposes of the processing, but is required by the data subject for the establishment, exercise or defense of legal claims, or
- Data subject objects to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

**Restricted data can only be stored, not processed.** Other processing can only take place after consent, in case of use in legal claims, or the protection of rights of another person, or for reasons of important public interest.

Restrictions on Automated Decision-Making
Control over adverse impacts of automated decision-making

A data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her.

Automated decision-making is only allowed:
- If necessary for entering into or for the performance of a contract between a data subject and the data controller
- If authorized by a law
- If it is based on the data subject’s explicit consent

Restrictions on Profiling
Profiling is more limited

Profiling is any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person.

The restriction on profiling protects the right of a data subject not to be subject to a form of automated processing that evaluates in particular the following aspects:
- Health
- Performance at work
- Personal preferences
- Economic Situation
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 timeline and map obligations

Security: Pseudonymization and encryption; confidentiality, integrity and availability; business continuity; testing; ISO certification?
LEGAL QUESTIONS?

DLA PIPER EXPLORE GDPR MOBILE APP

GDPR APP
ACCESS THE TEXT IN FULL ON YOUR PHONE

Download on the App Store
GET IT ON Google Play
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.