EVERSHEDS SUTHERLAND

The right steps

How to make sure your business is GDPR compliant

GDPR requires a new approach to privacy and the protection of personal details and their use. Organizations must plan for privacy and integrate the principle of data minimization into their business processes.

1 Develop Project Team

- assign responsibility for driving forward GDPR compliance within your organisation and create your GDPR compliance team
- determine whether the GDPR compliance strategy will be led at group level or within individual operating companies
- secure board approval for the resources necessary to deliver your GDPR compliance project
- determine which of your locations in the EU will be your main establishment

2 Data Mapping

- understand and map your personal data processing activities
- create clear documentary records of the processing activities under your responsibility
- update your implementation plan having verified it against your data mapping findings

3 Gap Analysis

- analyse all policies, procedures and data processing activities against the requirements of the GDPR
- consider your organisation's appetite for risk on data protection compliance matters
- produce a report to the highest level of management which identifies compliance gaps and recommends options for remedial action (including details of the anticipated resources required, timescales for completion and priority level)
- prioritise areas of most risk when implementing solutions
- integrate ICO and Article 29 Working Party guidance as it becomes available

4 DPO

Consider whether or not to appoint a data protection officer ("DPO"). A DPO must be appointed by:

- a public authority
- a private body if its core activities involve large scale processing of sensitive/special category personal data, or involve systematic and regular data subject monitoring

5 Third Party Engagement

- audit your suppliers and renegotiate third party contracts to ensure that all GDPR-prescribed processor terms are suitably covered
- ensure that all new suppliers are appointed on GDPR compliant contracts
- consider how you carry out supplier due diligence and prepare appropriate checklists and paperwork to evidence it
- consider the impact of GDPR exposure on other provisions of your contracts (e.g. liability)

6 Updating Policies and Privacy Documentation

- update existing policies and create new policies to address compliance gaps identified during gap analysis
- will include fair processing notices, consent wording, record retention policies, subject access request policy, data protection policies etc

7 Implementing Procedures

- introduce and embed privacy by design templates and data protection impact assessments
- update procedures for dealing with data subject rights (e.g. subject access requests, data portability requests, rectification requests and objections)
- update security breach procedures
- conduct mock security breach reporting scenarios

8 Training

- train decision-makers and project team prior to commencing GDPR project
- ensure that all personnel are suitably trained in their responsibilities

Enforcement:
Organisations failing to comply with the GDPR can face fines of up to **4% of annual global turnover or €20 million**, whichever is the greater!

For more information, contact:

Paula Barrett
Co-Lead of Global Cybersecurity and Data Privacy
paulabarrett@eversheds-sutherland.com

Liz Fitzsimons
Partner
lizfitzsimons@eversheds-sutherland.com

Gayle McFarlane
Partner
gaylemcfarlane@eversheds-sutherland.com

Key concepts

Need-to-know elements of the GDPR

Core concepts

Territorial scope: GDPR applies to organisations:

- processing personal data as a controller or processor in the EU (regardless of whether the processing takes place in the EU)
- processing personal data as an EU controller, even where actual processing takes place outside the EU
- processing personal data as a processor on behalf of a client controller subject to GDPR even if based outside the EU, or processing outside the EU
- that are not established in the EU but process personal data about data subjects who are in the EU in relation to: (a) offering goods or services to them, irrespective of payment by them, or (b) monitoring their behaviour taking place within the EU

One stop shop: Where an organisation has more than one establishment in the EU, it may be able to deal only or mainly with a single national data protection authority as its "lead supervisory authority" for regulation of cross-border processing activities carried out by that organisation

Accountability: A controller is responsible for, and must be able to demonstrate compliance with, the principles relating to the processing of personal data

Consent: Consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. Implied consent and pre-ticked boxes will no longer be valid

Data minimisation: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

Direct processor obligations: Data processors have direct obligations under the GDPR when processing on behalf of client controllers in relation to matters including data security, international data transfers, appointment of sub-processors and security breach notification

International transfers: The GDPR codifies new adequate safeguards for data transfers outside the EEA, including:

- binding corporate rules
- standard contractual clauses approved by a local supervisory authority
- approved codes of conduct
- approved certification mechanisms

Data subject rights

Subject access requests: Individuals have the right to request a broader scope of information, including details of:

- the safeguards that the data controller has in place for international data transfer
- the period for which the controller envisages retaining their personal data

In most cases, the information requested by an individual must be provided without undue delay and in any event within one month of receipt of the request. Unless manifestly unfounded or excessive, the information must be provided free of charge

Erasure: Personal data must be erased without undue delay where:

- processing the data is no longer necessary
- consent is withdrawn and there is no other legal reason for processing
- the individual objects and there is no overriding legal reason to continue processing
- data is unlawfully processed
- erasure is required for compliance with another law

Portability: If personal data has been provided by the individual and the processing is carried out by automated means based on consent or where the processing is necessary for the performance of a contract, a controller must, if required by the individual, provide the relevant personal data to the data subject or their nominated controller in a structured, commonly used and machine readable format

Profiling and automated decisions: Individuals have the right not to be subject to a decision evaluating personal aspects relating to them which is based solely on automated processing and which produces legal or other significant effects concerning them (e.g. online credit applications or e-recruiting practices)

Rectification: Individuals have the right to require a controller to rectify inaccurate personal data concerning him or her without undue delay

Restriction of processing: Individuals have the right ro restrict processing where:

- the accuracy of the personal data is contested by the individual (where the restriction will apply during the period enabling the controller to verify the accuracy of the personal data)
- the processing is unlawful and individual requests the restriction of the use of their personal data instead of erasure
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the individual in connection with any legal claims
- the data subject has objected to processing pursuant to the right to object (in which case the restriction will apply for the period necessary to determine whether the legitimate grounds of the controller override those of the individual)

Right to object: Individuals have a right to object, on grounds relating to his or her particular situation, at any time to processing of personal data which is based on public interest or legitimate interest grounds

Procedural requirements

Privacy by design: A data controller must, at the time that the means of processing is determined and at the time of processing itself, implement appropriate technical and organisational measures which are designed to:

- implement data protection principles (e.g. data minimisation)
- integrate necessary safeguards to meet the requirements of the GDPR and protect the rights of data subjects

Appointing a processor: Organisations must only use data processors that provide sufficient guarantees that the processing will meet the requirements of the GDPR and all processing by processors must be governed by a contract or other binding legal act which contains prescribed obligations on the processor. Additionally, processors cannot engage another processor (e.g. a sub-processor) without prior specific or general written authorisation of the controller and, in some cases, the processor must flow down the same provisions as it has in place with the controller

Security breach reporting: Organisations must provide notice of a security breach:

- in the case of controllers to (a) the regulator without undue delay but, in any event, within 72 hours of becoming aware of the breach; and (b) to individuals without undue delay where the breach is likely to result in high risk to individuals
- in the case of processors, to the controller without undue delay upon becoming aware of the breach

Data Protection Impact Assessments: Data protection impact assessments must be conducted where a type of processing (in particular using new technologies) is likely to result in a high risk to the rights and freedoms of natural persons

eversheds-sutherland.com

DTUK000565_05/18