

ALLEN & OVERY



Radical changes to European data protection legislation

January 2012

A new European data protection landscape

The stage has been set for significant changes to data protection legislation in the EU. On 25 January, the Commission released proposed draft amendments to the European data protection framework. If these remain materially intact through the legislative process, the impact on organisations both within and outside the EU will be substantial.

As anticipated, the draft amendments focus on increased harmonisation and bolstering rights for data subjects. They also claim to reduce red tape across the EU. They take the form of a Regulation which will replace the current Directive and will be directly applicable in all member states without the need for national implementing legislation. Alongside this will be a Directive which sets out rules on protecting personal data processed to prevent, investigate or prosecute criminal offences etc.

While the proposed Regulation will take a while to become law (two years after adoption), we expect that organisations will start to move towards compliance in advance.

This note summarises some highlights from the draft Regulation. With the increase in potential fines and tighter controls, ignoring data protection responsibilities is not an option.

EXPANDED TERRITORIAL REACH

Data controllers outside the EU whose processing activities relate to the **offering of goods and services to, or monitoring the behaviour of**, data subjects residing in the EU are caught by the Regulation, and many will need to appoint a representative in the EU.

Recital 21 clarifies that the monitoring of behaviour will occur where individuals are tracked by applying a profile to enable decisions to be made/predict personal preferences etc (eg using cookies).

ACCOUNTABILITY AND PRIVACY BY DESIGN

The Regulation places onerous accountability obligations on data controllers, eg by requiring them to (i) **maintain documentation** of all processing operations (which shall be made available on request to their supervisory authority) with minor exceptions for certain small organisations, (ii) **conduct a data protection impact assessment** for more risky processing, eg using new, large-scale filing systems, and (iii) **implement data protection by design** and by default, eg data minimisation.

24-HOUR DATA BREACH NOTIFICATION

Data controllers must notify any personal data breach to the DPA **without undue delay and, where feasible, within 24 hours** of awareness.

If the delay is beyond 24 hours, they must explain the reasons when notifying. In some cases, data controllers must also notify the affected data subjects without undue delay.

This will be burdensome on both data controllers and DPAs and does not sit well with the desire to cut red tape. However it will be popular with data subjects.

SANCTIONS

The Regulation establishes a tiered approach to penalties for breach which enables DPAs to impose fines of up to **2% of annual worldwide turnover**. This represents a dramatic change which seems to be designed to attract the attention of board-level executives.

EXPLICIT CONSENT

As well as requiring that a data subject's consent to processing of its personal data is freely given, specific and informed, the Regulation requires that consent be *explicit*, shown either by a **statement or by a clear affirmative action**, which signifies agreement to the processing; the burden of proof is on the data controller.

Consent does not provide a valid legal ground for processing where there is a **significant imbalance** between the data subject and the data controller (Recital 34 gives the example of a clear imbalance in the employment context). Where personal data is processed for **direct marketing**, the data subject shall have the right to object, which shall be explicitly offered.

RIGHT TO BE FORGOTTEN

Individuals can require *the erasure of personal data relating to them and the abstention from further dissemination of such data*, by the data controller in certain situations, eg they withdraw consent and no other legal ground for processing applies.

Where data has been made public, the controller shall take **all reasonable steps to inform third parties** to erase links to, or copies of, the data, and where the controller authorised the publication, it remains responsible. While attractive to users of social networks, this will be difficult and costly to implement.

REMOVAL OF NOTIFICATION REQUIREMENT

A welcome change for data controllers is the removal of the current requirement to notify the DPA in many circumstances. The aim appears to be to alleviate the associated administrative and financial burden.

This has been **replaced with an obligation** to maintain documentation of processing operations and conducting impact assessments (which may include consulting DPAs) for more risky processing. The effort required and potential fine for failure is likely to outweigh this benefit.

DATA PROTECTION OFFICERS

Data controllers and processors that employ **250 employees or more**, or whose core activities involve *regular and systematic monitoring of data subjects*, must appoint a Data Protection Officer.

This person must be **independent** and must report to the management. They may be employed or under a service contract. A group of undertakings may appoint a single DPO, as may certain groups of public authorities.

INTERNATIONAL TRANSFERS

This is essentially the same toolkit. However, in certain member states (eg Spain, the Netherlands and Poland) the process has been improved by the removal of the need for authorisation for model clauses.

The **legitimate interests** concept has been introduced as a new derogation, applicable to transfers which are not frequent or massive – in some countries this represents a useful broadening of the derogations; in others, this is more restrictive, eg in the UK.

BINDING CORPORATE RULES

The Regulation expressly recognises binding corporate rules for controllers **and processors** as a means of legitimising international data transfers outside the EEA. This may be less attractive to global organisations as it must cover **every member of the group**.

The approach will be more streamlined with one supervisory authority taking the lead (subject to complying with a consistency mechanism).

NEW EUROPEAN DATA PROTECTION BOARD

An independent EDPB is to **replace the Article 29 Working Party** and will comprise of the EDP Supervisor and the heads of the DPAs. Its obligations include issuing opinions, ensuring EU-wide data protection harmonisation and reporting to the Commission.

ROLE OF DATA PROCESSORS

Data processors have many **direct obligations** under the Regulation, eg assisting with impact assessments, implementing technical and organisational measures, maintaining documentation on processing activities and informing the controller immediately after establishing that there has been a data breach. Data processors also need the **controller's prior permission to appoint a sub-processor**.

MORE POWER TO BRUSSELS?

The Commission's efforts to harmonise data protection legislation across the EU has made things better for some and worse for others, with a **generally higher standard imposed**.

The Regulation proposes that the Commission be empowered to **adopt delegated acts** to further specify certain criteria and conditions in the Regulation.

ONE LEAD SUPERVISORY AUTHORITY

The DPA in the member state in which a multi-jurisdictional data controller has its **main establishment** shall supervise processing activities of the data controller across all member states, applying various obligations to cooperate with other authorities. This "one stop shop" is a significant change to the current position, and may lead to disputes between DPAs.

Companies may find it difficult in practice to agree on the location of their main establishment. If no decisions on processing are taken in the EU, the main establishment is where the main processing activities take place. For a processor, it is the **place of central administration** in the EU.

