EU, Competition and Regulatory

July 2015

APPROACH AGREED ON NEW DATA PROTECTION REGULATION

On 15 June 2015, the EU Council agreed a general approach to the new data protection legislation. This means that the Council has a basis on which to negotiate with the European Parliament. The updated regime will be brought into law by a Regulation; therefore when it becomes law it will be directly effective in all Member States simultaneously. There is expected to be a two year transitional period.

The stated aims of this Regulation are to enhance the level of personal data protection for individuals and to increase business opportunities in the digital single market. It is hoped that this new Regulation will harmonise data protection procedures and enforcement across the EU. The Regulation will be applicable to non-EU companies who offer goods or services to data subjects (individuals) in the EU.

The significant changes and additions to the current regime will be:

Right to be forgotten

Citizens will have more control over their personal data and its processing by organisations. The "right to be forgotten" will enable a data subject, for example, to require that a service provider remove, without delay, personal data collected when that individual was a child.

One-stop-shop mechanism

The Regulation will create a "one-stop-shop" so that in international cases a single supervisory decision will be taken. This would help to reduce costs and also provide legal certainty and consistency between Member States.

Judicial review

A data subject will have the right to a judicial review of a legally binding decision of a supervisory authority. This review shall be brought in the courts of the Member State where the supervisory authority is established.

Territorial scope

Some of the most significant changes are in the territorial scope of the Regulation. In particular, it will apply to data controllers not established in the EU who offer goods or services to data subjects in the EU.

Application to data processors in the EU

In contrast to the current Data Protection Directive (**DPD**), the Regulation will apply to the processing activities of a data processor in the EU. Data processors in the EU will potentially have joint and several liability with data controllers for infringements of the legislation. Thus, new obligations on a data processor are expected to include:

- Ensuring the security of processing.
- Entering into data processing agreements.
- Enabling the data controller to comply with individuals' rights, perhaps by compliance with an approved code of conduct.
- Assisting the data controller on data breach notifications, data protection impact assessments and prior authorisations.
- Handing over results and no longer processing data at the end of processing for approved purposes.
- Maintaining records of processing operations.

European Data Protection Board (EDPB)

The EDPB will replace the Article 29 Working Party on the Protection of Individuals with regard to the processing of personal data. The European Commission will be able to request an opinion from the EDPB within a specific time limit.

Data protection officers (DPOs)

A requirement for a DPO in certain circumstances may be introduced in legislation by Member States. It could become mandatory for all public sector entities and for companies in the private sector with over 250 employees to have a DPO. Other companies, where the core activities of the data controller or data processor consist of processing operations which require regular and systematic monitoring of data subjects, would also be required to have a DPO. The DPO's contact details would be public and have to be lodged with the National Data Protection Authority (**NDPA**), i.e. in the case of the UK, the Information Commissioner's Office (**ICO**).

Requirement to notify breaches to the NDPA

The draft Regulation introduces a limited obligation on data controllers to notify the NDPA of data breaches. A notification to the NDPA would only be required if the data subject needed to be informed of the breach (see below). The Regulation includes a prescribed format for a NDPA notification.

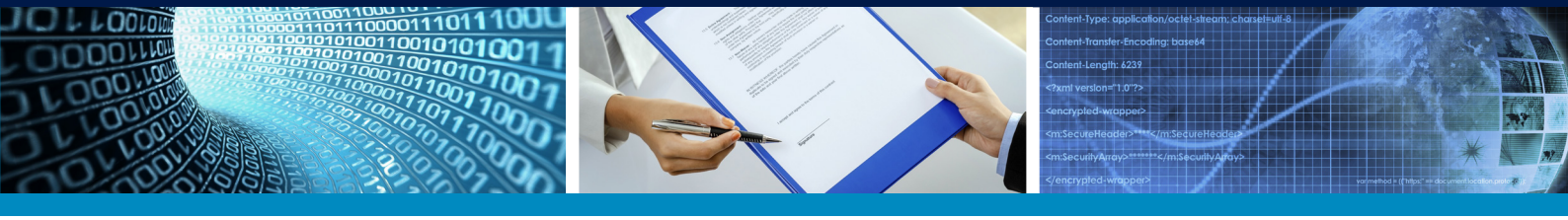
Requirement to notify breaches to data subjects

The draft Regulation provides that the data subject needs to be informed if the breach is likely to result in: *"a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to reputation, unauthorized reversal of pseudonymisation (a procedure where identifying data is replaced with pseudonyms or artificial identifiers in such a way that data can no longer be attributed to a specific data subject), loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage".*

There are exceptions to the requirement to notify breaches to data subjects, such as where:

- The data controller has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption.
- The data controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise.
- It would involve disproportionate effort, in particular owing to the number of cases involved. In such cases, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
- It would adversely affect a substantial public interest.

In spite of these limitations to the requirement to notify, the criteria for a "high risk" breach are fairly broad and it is likely that data controllers will be required to notify the NDPA/ data subject in a wide range of circumstances. The requirement is less stringent than it was in earlier drafts of the Regulation, but this provision is still significantly more onerous than under the DPD. There is no current obligation under the DPD to notify data breaches but there is an obligation under the E-Privacy Directive, which applies to electronic communications services, to notify the NDPA and, in some circumstances, an individual, of a breach.



Privacy impact assessments

The draft Regulation requires that where a type of processing is likely to result in a high risk for the rights and freedoms of individuals then the data controller shall carry out an impact assessment prior to processing. This particularly applies to the use of new technologies. The ICO has previously promoted this approach, under the Data Protection Act, as indicative of good practice but under the new Regulation this will be required by law in all Member States.

Data portability

This is a controversial area that several of the Member States, including the UK, France and Germany, believe is outside the scope of data protection. The right will enable a data subject to receive personal data concerning him, which has previously been provided to a data controller and to transmit that data to another data controller.

Automated individual decision making or "profiling"

Data subjects will have the right not to be subject to a decision, which produces legal effects or significantly affects them which is based solely on automated processing. The notable exceptions to this provision are: when such "profiling" is necessary for entering into or performance of a contract and also where the data subject has provided "explicit" consent. In practice, this right already exists under the DPD but there are some differences such as: the Regulation now specifically refers to profiling and businesses will need individuals' explicit rather than unambiguous consent.

Fines

The draft Regulation provides for a range of sanctions, including written warnings and fines at different levels depending on the severity of the breach and whether it was intentional or negligent. The highest bracket is planned to be up to €1 million or 2% of annual worldwide turnover (whichever is greater). By contrast, under the current UK data protection regime, the Information Commissioner only has the power to impose a fine up to a maximum of £500,000 for serious contraventions. The higher penalties are intended to result in a higher profile for compliance.

Next steps

The next step is the start of negotiations with the European Parliament with a view to reach an overall agreement. The discussions began on 24 June 2015. The current aim is to have a completed reform package by the end of the year.

No final Regulation has been approved. However, it is worth bearing in mind the general principles that the final version of the Regulation is likely to include such as a greater focus on the rights of data subjects and the responsibilities of data controllers and data processors. The EU Council is very keen for the Regulation to be brought into law as soon as possible so that citizens can enjoy the benefits of the reform as soon as possible. Therefore, it would be best to start thinking about adjustments that can be made to improve compliance sooner rather than later, for example by having clear guidance about the procedure to follow in the case of a data breach. In addition, given prospective joint and several liability between data controllers and EU data processors, they should consider allocating responsibilities contractually and the negotiation of liability and indemnity provisions relating to privacy and data protection is likely to become more significant and complex.

Final thoughts – data breach v cyber attack

A recent UK Government report has emphasised that the threat from cyber attacks is often conflated with data breaches. It is important for businesses to understand the risks that either present and be sufficiently insured:

"At present, within the insurance sector, the cyber threat is not well defined, with confusion surrounding definitions based on different causes and consequences. Insurers tend to conflate cyber with data breach given the well-developed demand for that cover driven by US Regulation; however, UK firms have broader concerns about possible damage from cyber risk, including business interruption, damage to property, and theft of intellectual property.

The Government hopes that insurers will help businesses to cope with the many and varied threats to data privacy and network security - both with financial support and application of expertise. However, whilst insurance should be considered as part of the solution, it is not a panacea and it remains the responsibility of each individual or entity to take such reasonable steps as are necessary to comply with the UK DPA and related legislation and to prepare for the implementation of the EUDPR."

For more information, please contact the authors of this briefing:

Anthony Woolich
Partner, London
T: +44 (0)20 7264 8033
E: anthony.woolich@hfw.com

Felicity Burling
Associate, London
T: +44 (0)20 7264 8057
E: felicity.burling@hfw.com

HFW's London office is part of an international network of 13 offices in 11 countries. For further information about EU, Competition and Regulatory related issues in London or any other jurisdiction, please contact:

Daniel Martin
Partner, London
T: +44 (0)20 7264 8136
E: daniel.martin@hfw.com

Edouard Taÿ Pamart
Partner, Paris
T: +33 1 44 94 40 50
E: edouard.taypamart@hfw.com

Konstantinos Adamantopoulos
Partner, Brussels
T: +32 2 643 3401
E: konstantinos.adamantopoulos@hfw.com

Jeremy Davies
Partner, Geneva
T: +41 (0)22 322 4810
E: jeremy.davies@hfw.com

Jasel Chauhan
Partner, Piraeus
T: +30 210 429 3978
E: jasel.chauhan@hfw.com

Ian Chung
Partner, Dubai
T: +971 4 423 0534
E: ian.chung@hfw.com

Brian Gordon
Partner, Singapore
T: +65 6411 5333
E: brian.gordon@hfw.com

Guy Hardaker
Partner, Hong Kong
T: +852 3983 7644
E: guy.hardaker@hfw.com

Julian Davies
Partner, Shanghai
T: +86 21 2080 1188
E: julian.davies@hfw.com

Aaron Jordan
Partner, Melbourne
T: +61 (0)3 8601 4535
E: aaron.jordan@hfw.com

Stephen Thompson
Partner, Sydney
T: +61 (0)2 9320 4646
E: stephen.thompson@hfw.com

Simon Adams
Partner, Perth
T: +61 (0) 8 9422 4715
E: simon.adams@hfw.com

Fernando Albino
Partner, São Paulo
T: +55 (11) 3179 2900
E: fernando.albino@hfw.com

Lawyers for international commerce hfw.com

São Paulo London Paris Brussels Geneva Piraeus Dubai Shanghai Hong Kong Singapore Melbourne Sydney Perth