Hogan Lovells

EU draft Data Protection Regulation: the LIBE Committee amendments

A Hogan Lovells Briefing Paper

2013

EU draft Data Protection Regulation: the LIBE Committee amendments

The EU Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") voted on Monday 21 October 2013 to adopt the amendments to the draft General Data Protection Regulation and the separate Directive for the law enforcement sector, which had been proposed by Raporteurs Mr Albrecht and Mr Droutsas.

What happens next?

In addition to approving the amendments proposed by the two Raporteurs, the LIBE committee also voted to grant them a negotiating mandate to enable discussions to be commenced with the Council of the EU. The vote permits the LIBE Raporteurs to begin trilogue discussions with the Council and Commission. Procedural rules allow such negotiations to start even where the Council has not itself reached an agreed position as between its Member State participants. Previously the high number of amendments (approximately 4,000) submitted by separate parliamentary committees had given rise to concerns that the Regulation would not be passed before the next European elections. Now that the European Parliament has simplified and made known its position, pressure will shift to the Member State governments to reach agreement on a position within the Council of the EU and to cooperate with the LIBE committee.

Unfortunately for the progress of the draft Regulation, there are still strong divisions within the Council. The much-reported compromise on the language used to refer to progress of data protection reform in the Conclusions, issued following the European Council meeting of Ministers on 24/25 October, provides an indication of the tussle ahead on the draft Regulation itself. The European Commission has indicated that it intends to continue to push for the adoption of the Regulation before the end of the current parliamentary session in June 2014.

Summary of the amendments

For a higher level summary of the key changes, visit our data protection blog http://www.hldataprotection.com/2013/10/articles/consumer-privacy/4258/

The report contains significant amendments compared with the original draft prepared by the European Commission in January 2012. Some of the changes are predictably consumer friendly, but the Parliament has also proposed amendments which are helpful to business.

- **Sanctions increase**. The Parliament's draft proposes that sanctions could be as high as €100 000 000 or 5% of annual global turnover (whichever is the greater), compared with the Commission's proposal of €1 000 000 or 2% of annual global turnover. Compliance programs and accountability will be taken into account when applying sanctions.
- Sanctions can include the obligation to perform periodic audits.
- The **one-stop shop mechanism** is maintained, although modified against the Commission's original draft. The original position was that where a data controller operated in a number of jurisdictions, the supervisory authority in the country of its main establishment would be responsible for supervising that controller's activities in all Member States. The Parliament takes an intermediary position by the concept of a "lead supervisory authority". The lead supervisory authority is the sole authority empowered to take legal decisions, but must consult with other authorities. Consumers may always complain to their local DPA, instead of being obligated to go to the main DPA responsible for the controller's activities.
- One of the shortcomings previously identified around the one-stop-shop mechanism was that the Regulation treated separate legal entities as separate controllers, so that corporate groups could not take advantage of it where they were

operating through separate legal entities. The Parliament's draft introduces a definition of **main establishment** which explicitly references the existence of a group of undertakings.

- The rules on **jurisdiction** are essentially unchanged from the Commission's proposal. A data controller located outside the European Union will be subject to the regulation if the data controller "offers goods or services" to data subjects in the EU, or "monitors" them. The new draft clarifies that it is irrelevant (i) where the processing takes place (within or outside the Union) and (ii) that the goods and services may be offered for free.

- The draft clarifies that the "**domestic purposes" exemption** applies to a publication of personal data where it can be reasonably expected that it will be accessed only by a limited number of persons. In other words the application of the exemption will be limited where personal data is disseminated through the Internet.

The **principles according to which any processing of data should occur** have evolved on a number of issues. The main elements of evolution include:

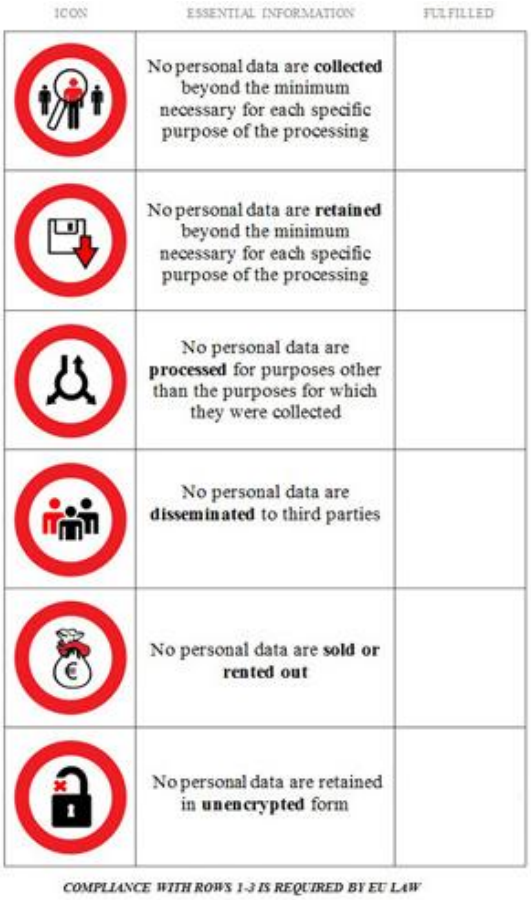
- the amendments suggest **the creation of two new principles**: (i) data should be processed in a fashion which allows data subjects to effectively exercise their rights (so-called principle of "effectiveness") and (ii) a principle of integrity which results from prior requirements of security as it requires that data be processed in a way which protects against unauthorized or unlawful processing and against accidental loss, etc.

- the principle of **processing for "legitimate interests" remains** and even appears to be broader than the existing provision as it also covers the legitimate interests of recipients of data in case of disclosure of the data – there is however now a requirement of processes meeting the "reasonable expectations of the data subject based on his or her relationship with the controller". This will not constitute a substantial modification for a number of jurisdictions which already conducted this "reasonable expectations" test.

- the **importance of consent is strengthened** by specifying that provisions on data subject consent which do not meet the requirements of the regulation shall be deemed "fully void". This may have a substantial effect on information society service providers, notably with regards to the changes in the terms of their privacy policies. The amended version of the Regulation also requires that withdrawing consent should be as easy as to grant it and that data subjects should be made fully aware of the risk of termination of the services if they withdraw their consent to processing. The most fundamental amendment to the consent provisions provides for the automatic "termination" of the validity of consent granted by a data subject once the purpose for which it was granted has been achieved or when the data is no longer necessary to achieve this purpose. The same new article 7.4 also prohibits making the performance of a contract or provision of a service dependent on consenting to the processing of data where that data is not strictly necessary to such performance or provision of service.

- The original draft Regulation was criticised for the number of delegated acts and powers given to the Commission. The LIBE committee clearly wanted to **reduce the role of the European Commission** and has transferred such "powers" to the new European Data Protection Board which will only have, however, the power to issue "recommendations, guidelines and best practices".

- Changes are made to the requirements relating to the **information to be provided to data subjects**. Data controllers must use standardized symbols to tell consumers how their data are handled before providing the other information required:



ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing	
	No personal data are **processed** for purposes other than the purposes for which they were collected	
	No personal data are **disseminated** to third parties	
	No personal data are **sold or rented out**	
	No personal data are retained in **unencrypted** form	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

- **Additions to the information to be provided** to data subjects include:
    - where applicable, that the controller intends to transfer the data to a third country or international organisation and the reference to the appropriate decision or safeguards relied on;
    - information about the existence of profiling and related measures and effects;
    - meaningful information about the logic involved in any automated processing;
    - information about whether personal data was provided to public authorities during the last consecutive 12-month period; and
    - where appropriate, the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk.

If the controller cannot specify the data retention period (a requirement of the original draft), the notice shall include the criteria used to determine such period.

- The "**right to be forgotten**" is relabelled "right to erasure," but its provisions are for the most part unchanged.
- The "**right to data portability**" has been merged with the right to access. Individuals have a right to a copy of personal data "in an electronic and interoperable format which is commonly used and allows for further use by the data subject".
- The **right to object** also remains, but the explicit reference to marketing purposes has been dropped.

There are a number of clarifications and amendments to the **responsibilities of data controllers**:

- **Controllers may transmit personal data inside the European Union within the group of undertakings of the controller**, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of data subjects are safeguarded by internal data protection provisions or codes of conduct;
- The Regulation now states more clearly that joint controllers must enter into an arrangement which reflects the responsibilities, effective roles and relationships vis-à-vis data subjects. **In case of unclarity, the controllers shall be jointly and severally liable.**
- The **requirement for foreign controllers** established in a third country not providing for an adequate level of data protection to **designate a representative in the Union** has been revised so that the obligation is linked to the volume and sensitivity of the data processed, instead of the size of the enterprise.
- Accountability, privacy by design and data protection impact assessments all remain. In addition there are obligations around risk analysis and data protection compliance reviews. A **data protection risk analysis would become obligatory** for any processing involving more than 5000 data subjects during any consecutive 12-month period, or any other kind of risky processing.

- The Regulation sets out more detailed requirements in relation to security policies and measures to be adopted. The **data breach notification** obligation remains but the reporting obligation has been softened from "24 hours" to "without undue delay", with a presumption that 72 hours is "without undue delay." The information to be included in a notification to the authority may, if necessary, be provided in phases.
- The **data protection officer** ("DPO") remains an important role:
    - the data protection officer shall directly report to the executive management of the controller or the processor;
    - the appointment of a DPO is required where:
        - the processing carried out by a legal person relates to more than 5000 data subjects in any consecutive 12-month period (instead of referring to an enterprise employing 250 persons or more).
        - the core activities of the controller or the processor consist of processing special categories of data, location data or data on children or employees in large filing systems.
    - A main responsible data protection officer may be appointed for a group of undertakings (this had been limited to specific cases in the original draft), provided the DPO is easily accessible from each establishment.
    - The DPO must be appointed for a period of at least four years in case of an employee and for two years in case of an external service contractor. The recitals have been amended to state further principles regarding the appointment of a data protection officer, his/her position in the company and the required qualification.

International data transfers are attracting a great deal of attention at the moment and it is unsurprising that the LIBE committee proposes the restriction of the grounds for transfer of personal data to countries outside the EEA previously contemplated by the draft Regulation:

- As envisaged in the draft Regulation, adequacy decisions can be made by the Commission in respect of a third country, a territory or a processing sector within that third country, or an international organisation.
- As regards new adequacy decisions, the LIBE committee proposes that the sufficiency of sanctioning powers held by an independent supervisory authority and the existence of legally binding conventions/instruments with respect to the protection of data within the third country also be taken into account by the Commission. The existence, however, of any legislation in a third country which provides for extra-territorial access to personal data processed in the Union, without authorisation under Union or Member State law, would be considered as an indication of lack of adequacy.
- Existing adequacy decisions will remain in force for 5 years after the entry of the Regulation into force, unless amended, replaced or repealed by the Commission prior to that. New adequacy decisions in respect of a processing sector within a third country would also expire after 5 years.
- Transfers based on binding corporate rules, a valid "European Data Protection Seal" for the controller and the recipient, standard clauses adopted by a supervisory authority, or contractual clauses authorised by a supervisory authority shall not require any specific authorisation. Existing approvals of contracts for international data transfers granted by supervisory authorities will expire 2 years after the introduction of the Regulation, unless amended or replaced.
- A key change in respect of binding corporate rules is the removal of an express reference to processor binding corporate rules, although it is anticipated that controller binding corporate rules could extend to cover external subcontractors.

- A new Article 43a states that **no judgment/decision of a court, tribunal or an administrative authority of a third country requiring a controller or a processor to disclose personal data shall be recognized or be enforceable**, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State. Following any such request, the controller or processor must notify the supervisory authority and obtain their prior authorisation for transfer or disclosure.
- In cases where controllers/processors are confronted with conflicting compliance requirements between the jurisdiction of the EU on the one hand, and that of a third country on the other, **the Commission should ensure that EU law takes precedence at all times**. The Commission should seek to resolve the jurisdictional conflict with the third country in question.
- The possibility of relying on legitimate interest as a basis for the transfer of data in the absence of an adequacy decision or appropriate safeguards has been dropped.
- The Commission is required to report to the European Parliament and the Council at regular intervals on the application of the international transfer provisions.
- **Supervisory authorities are now entitled to**:
    - order the controller to communicate a personal data breach to the data subject;
    - put in place mechanisms to encourage confidential reporting of breaches taking into account guidance issued by the EDPB; and
    - investigate the controller and processor without prior notice (including all necessary documents, and by accessing their premises, data, equipment and means (in this regard, the reference to "where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there" has been deleted)).
- The EDPB has an expanded role:
    - It "may decide on the identification of the lead authority" where it is unclear or the supervisory authorities do not agree.
    - It plays a greater role with regard to the consistency mechanism in individual cases. In particular, it regulates the cooperation obligations between the lead authority and the relevant supervisory authorities, and may get involved if a consensus is not reached between the lead authority and the relevant supervisory authorities.
    - The Commission is required to seek an opinion from the EDPB before adopting any implementing acts of general application.

If you have any questions relating to any of the content of this document please contact:

Mac Macmillan
Of Counsel, London
T +44 20 7296 5745
mac.macmillan@hoganlovells.com

Chris Wolf
Partner, Washington
T +1 202 637 8834
christopher.wolf@hoganlovells.com

Marco Berliri
Partner, Rome
T +39 (06) 675823 29
marco.berliri@hoganlovells.com

Gonzalo Gallego
Partner, Madrid
T +34 (91) 3498 257
gonzalo.gallego@hoganlovells.com

Stefan Schuppert
Partner, Munich
T +49 (89) 29012 240
stefan.schuppert@hoganlovells.com

Winston Maxwell
Partner, Paris
T +33 (1) 5367 4847
winston.maxwell@hoganlovells.com

Elisabethann Wright
Partner, Brussels
T +32 2 505 0926
ea.wright@hoganlovells.com

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Jeddah*
London
Los Angeles
Luxembourg
Madrid
Miami
Milan
Moscow
Munich
New York
Northern Virginia
Paris
Philadelphia
Prague
Rio de Janeiro
Riyadh*
Rome
San Francisco
Shanghai
Silicon Valley
Singapore
Tokyo
Ulaanbaatar
Warsaw
Washington DC
Zagreb*

*Associated offices