COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Privacy & Data Security

October 24, 2013

WHAT COMPANIES NEED TO KNOW ABOUT THE EUROPEAN PARLIAMENT'S PROPOSED AMENDMENTS TO THE DRAFT EU GENERAL DATA PROTECTION REGULATION

On Monday, the LIBE Committee of the European Parliament adopted proposed amendments to the Commission's legislative proposal for a General Data Protection Regulation (the "Proposal"). Earlier this week, we summarized the vote and procedural details (here). In this alert, we provide more detail on the actual amendments and discuss next steps in the legislative process.

OVERVIEW OF THE PROPOSED AMENDMENTS

All of the proposed amendments will be subject to negotiation during the next phases of the legislative process. The following are likely to be of most interest to companies:

- **Sanctions.** Companies that do not comply with the Regulation could be fined up to *€100 million or five percent of the annual worldwide turnover*, whichever is greater. Although the approach to fines has been simplified compared to the Proposal, now any violation of the Regulation will trigger at least one of three types of administrative sanctions (a written warning, regular period data protection audits or a fine). The list of criteria that national data protection authorities should consider when determining a sanction is more detailed. Further, individuals would now be entitled to claim compensation for non-pecuniary damages.
- **Expanded territorial scope.** The Regulation would apply to processing irrespective of whether it takes place in the EU or whether data subjects reside in the EU. Non-EU controllers or processors would be covered if their processing activities relate to the offering of goods or services or the monitoring of data subjects.
- **Lead authority.** The concept of a one-stop shop for the supervision of controllers or processors remains intact. The amendments clarify that the same authority would act as lead authority regardless of whether a company processes data as a controller or a processor. However, the lead authority (based on the main establishment criterion) would now be required to consult all other competent supervisory authorities to try to reach a consensus. Data subjects would be able to complain to the supervisory authority of their choice and the lead authority must coordinate its work also with this authority.
- **Standardised information policies and extended information requirements.** In addition to furnishing notice, controllers would be required to provide certain essential basic information in a prescribed standardized format, using various predefined icons. The standard notice has to include information about the security of the processing, criteria to determine the retention period (if that period cannot be specified), data transfers and profiling, as well as disclosure of personal data to public authorities.

- **Consent.** The requirement in the Proposal that consent must be "explicit" has not been changed. New language states consent is "purpose limited" and may lose "its validity." Recitals also list specific scenarios (modifying pre-ticked boxes or mere use of a service) that do not constitute consent.
- **Legitimate interests.** The "legitimate interests" ground remains in place, but such interests must now also "meet the reasonable expectations of the data subject."
- **Transfers.** In response to the revelations surrounding the surveillance activities of U.S. intelligence agencies, companies must notify the supervisory authority of any request for data transfers or disclosures by a third country court or administrative authority, obtain prior authorization and also provide certain information to the data subjects concerned. Any adequacy decisions taken under the existing framework — i.e., in relation to countries and the U.S. Safe Harbor self-certification scheme and the European Commission's standard contractual clauses — would only remain in force for a maximum of five years after the Regulation enters into force (unless amended, replaced or repealed by the Commission before then). Authorizations of national data protection authorities in relation to transfer mechanisms would only remain valid for two years after the Regulation comes into force (unless the authorization is amended or replaced before the end of that period). The possibility to transfer personal data outside of the EU on the basis of a legitimate interest as suggested in the Proposal has been deleted.
- **Profiling.** The new definition of "profiling" covers a broad range of processing activities intended to evaluate certain personal aspects or to analyze or predict performance at work, economic situation, location, health, personal preferences, reliability or behavior — regardless of whether or not such processing produces legal effects or significantly affects or harms data subjects. Data subjects have the right to object to any form of profiling and must be informed about that right in a highly visible manner. Where profiling does produce legal effects or significantly affects a data subject, companies must obtain the data subject's consent or show that the processing is necessary for entering into or performing a contract or is expressly authorized under national law.
- **Data breach notification.** The 24 hour deadline for data breach notifications to the supervisory authority contained in the Proposal has been replaced by the requirement to notify "without undue delay." A recital states that notification "should be presumed to be no later than 72 hours," but the European Data Protection Board can issue guidelines, recommendations and best practices determining what undue delay means; this potentially leaves room for a shorter time frame. As was the case in the Proposal, the European Commission may lay down standard forms for breach notifications and the documentation to be kept by controllers (the new ePrivacy related Regulation (here) is likely to serve as a model).
- **European Data Protection Seal.** This new certification would allow controllers and processors to have their data processing activities certified by supervisory authorities or accredited third parties; in return, certified entities would be subject to reduced fines and could transfer data outside the EU and receive data from the EU more easily.

Other important changes in the proposed amendments concern:

- **Mandatory appointment of a data protection officer.** The number of employees is no longer the decisive criterion in whether a company must appoint a data protection officer. This would now be determined by the number of data subjects (more than 5,000) whose personal data is processed in any consecutive 12-month period and the level of risk involved. The designation period of *internal* data protection officers has been increased from two to four years.

- **Data protection by design.** The data protection by design obligation has been extended to processors. Controllers are obliged to take the results of any data protection impact assessment (see below) carried out into account when developing those measures and procedures. Data protection by design shall be a prerequisite for public procurement tenders.
- **Data portability.** The right to obtain data from the controller covers all personal data that a data subject has provided, irrespective of the legal basis on which the data is processed (in the Proposal this was limited to cases where the data is processed on the basis of consent or a contract). Moreover, the data must be provided in an *interoperable* format and the data subject may even request that the data be transferred directly by the controller to another controller (where technically feasible and available).
- **Risk analysis and data protection impact assessment.** For certain processing operations that are deemed to present a higher risk, controllers and processors would first have to carry out a risk analysis (which the controller must review at least annually or immediately in case of significant changes to the processing operations). Depending on the result, controllers may be obliged to designate a data protection officer (and non-EU controllers a representative) or to carry out a full-fledged data protection impact assessment ("DPIA"). The list of elements to be contained in a DPIA has been extended compared to the Proposal (for instance, now requiring an assessment of the necessity and proportionality of the processing operations in relation to the purposes). The controller must carry out a compliance review periodically at least every two years and document the outcome.
- **Sensitive data.** Genetic and biometric data, gender identity, administrative sanctions and suspected offences have been expressly included in the special categories of data that are subject to a stricter set of rules as compared to personal data generally.
- **Processing of personal data concerning health.** In particular, the requirements regarding anonymization, pseudonymization and consent have been further developed. Member States have the possibility to provide for exceptions to the requirement of consent for research, which will lead to a patchwork of national rules. The rules regarding processing for historical, statistical and scientific research have also been amended.

Several provisions have clearly been inspired by German data protection law, for instance:

- the inclusion of a provision on **intra-group data transmissions**, including for employee data, specifically setting out under which conditions such transmissions are allowed, and on minimum standards for processing data in the **employment context**;
- consultation obligations with the **data protection officer** (in case one has been appointed) instead of the supervisory authority and
- the recognition of **works council** agreements and references to employee representatives.

NEXT STEPS

The LIBE Committee also approved a mandate to start negotiations with the Council (the EU institution representing the EU Member States' governments) and the Commission — the so-called trilogue process. It is clear that the Parliament will push for rapid negotiations with the Council and the Commission in order to obtain a full vote on the final text of the proposed Regulation before the Parliament elections in May 2014. The Commission is equally determined to get the proposed Regulation adopted within this time frame.

As we described earlier this week in more detail, the ball is now in the court of the Council, which still needs to agree on a negotiating mandate, known as the "general approach." (Informal negotiations may begin earlier, however.) Given the lack of agreement among Member States, it looks increasingly unlikely that the Council will be able to reach a general approach this year. This would leave very little time for the trilogue process next year before the current term of the Commission and Parliament expire.

In any event, further changes can be expected to any compromise text regardless of whether the negotiations conclude during this legislative period or the next.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Privacy & Data Security Practice Group:

Daniel Cooper	+44.(0)20.7067.2020	dcooper@cov.com
Jetty Tielemans	+32.(0).25495252	htielemans@cov.com
Monika Kuschewsky	+32.(0).25495249	mkuschewsky@cov.com
Mark Young	+44.(0)20.7067.2101	myoung@cov.com

Covington has set up a Working Group to analyze the proposed amendments and assess possible consequences for industry, closely follow and contribute to the trilogue process and observe the ongoing work of the Council. If you are interested to learn more about this Working Group and how you can get involved, please contact:

Jetty Tielemans	+32.(0).25495252	htielemans@cov.com
Wim van Velzen	+32.(0).25495250	wvanvelzen@cov.com