BRYAN CAVE
A Broader Perspective
Bulletin

Data Privacy and Security Team

To: Our Clients and Friends February 6, 2012

Deciphering Proposed Changes to EU Data Protection

The ongoing revision of EU data privacy rules will likely affect business in Europe...but not yet.

On January 25, 2012 the EU Commission published the details of a long-awaited proposal for a renewed data privacy concept that would be applicable to EU member states. While law firms and news sources immediately reported on the proposal, many of the headlines and stories exaggerated the proposal's direct impact unnecessarily raising concerns among businesses that operate in the EU or that sell products to EU consumers. This alert attempts to dispel confusion surrounding the proposed change by summarizing the proposal and the law making process, which, in of itself, may help explain when businesses might need to take action to comply with any changes.

Status Quo

The data protection rules in the EU are based on a directive drafted in 1995. The directive instructed each member state to pass a data protection law that comprehensively regulated the handling of personal data about the residents of that state. Many businesses view the EU directive as unnecessarily strict (particularly when compared to non-EU legislation), and compliance with sometimes diverging member state legislation as unnecessarily confusing and burdensome.

Reform Proposal

The EU Commission's proposal provides for significant changes to the structure and substance of data protections in the EU. For example:

- **"Regulation" vs. "Directive"** – The proposal envisions a single set of privacy rules that would be valid across the entire EU (the "Regulation"). The Regulation would replace the current patchwork of national rules in 27 Member States. As a result, passage of the Regulation could theoretically lower some compliance costs for some businesses by eliminating the need to comply with the 27, sometimes divergent, member state laws.
- **Higher Penalties** - The proposed Regulation provides for sanctions that are believed to impose a deterrent value. For serious violations supervisory authorities could impose penalties of up to €1 million ($1.3 million) or up to 2% of the global annual turnover of a company. For less serious offences fines could start out at €250,000 ($330,000) or up to 0.5% of turnover.
- **Explicit Consent** – Whenever an individual's consent is required for its data to be processed, such consent would have to be express (i.e., not implied).

- **Notification** - Companies would be required to notify the national supervisory authority of serious data breaches as soon as possible (if feasible, within 24 hours). The individuals whose personal data could be adversely affected by the breach would also have to be notified without undue delay.
- **Data Protection Officer** – For companies employing 250 persons or more, the Regulation would require that they employ an internal data protection officer.
- **Scope of Application** – The Regulation could apply even if personal data is processed abroad.
- **Enforcement** – Individuals would be able to refer cases to the data protection authority in their home country if their data is breached, or they believe that the Regulation had been violated. Cases could be referred to home countries even if data is processed by a company based outside the EU.
- **Extended Damage Responsibility** - Any person who suffered damage as a result of an unlawful processing operation could receive compensation from the data controller or the data processor.

Reform Status

The proposal has been passed to the European Parliament and all EU Member States for discussion and potential amendment. Although it is difficult to estimate how long it might take the proposal to be considered, typically proposals of this significance are considered for two or more years before being adopted.

If adopted in its current state, the Regulation would go into force two years after it was adopted. In short, four or more years could pass before the proposal would directly affect business in Europe. As a result, for most businesses it may be premature to take action based on the proposal. Instead, businesses should continue to focus on ensuring that they are compliant with the national rules in the 27 Member States.

Bryan Cave Data Breach Hotline

If you experience a data security breach and are not able to contact a member of the Team directly, you can call Bryan Cave's Data Breach Hotline *24 hours a day, 7 days a week* at +1 202 508 6136 (international) or +1 888 474 9743 (toll free – US only).

For further information on this topic, please contact Jana Fuchs on +49 40 30 33 16 136 or any member of the Bryan Cave Data Privacy and Security Team.

Bryan Cave's Briefings are available online at www.bryancave.com/bulletins.