February 9, 2012

New EU Data Protection Regulations Could Mean Hefty Fines for US Companies: How You Should Prepare

As business continues to expand globally, the European Union is taking affirmative steps to enhance and consolidate its already strict privacy laws and regulations. Under the EU Data Protection Directive 95/46/EC3 ("Directive 95/46'"), each EU Member State establishes, implements and enforces its own regulatory structure consistent with guidance provided in Directive 95/46. In November 2011, a draft version of proposed changes to Directive 95/46 was circulated within the Commission, and was leaked widely (the "Draft Version"). In late January 2012, the European Commission formally announced proposed revisions to Directive 95/46 that centralize rule making and enforcement activity, and imposes new administrative sanctions and fines. Any organization that conducts business in the EU, and/or removes personal data from the EU or among its Member States, should be aware of these important developments.

New EU Data Protection Framework

Intense negotiations by the European Commission over the last two years culminated on January 23, 2012 with the release of proposed revisions to Directive 95/46 (the "Proposed Regulation"). Supporters and critics alike agree that, in over 600 pages of detailed text, the European Commission is recommending radical steps including the following key points:

- One Set of Consistent Rules. The Proposed Regulation would repeal the existing Directive 95/46, and replace it with a single set of regulations that specifically overrides national laws of the EU Member States. Policymaking power would be shifted away from the Data Processing Authorities ("DPA") of the EU Member States to the European Commission in Brussels. The Article 29 Working Party would cease to exist, and a European Data Protection Board ("EDPB") would be established to help guide the Member States as they adjust to operating under one set of rules and one supervisory authority. There are also consistency rules designed to prevent the Member States from going back to diverging sets of rules. As an example, if a DPA takes an action that has an impact outside of its territory, the DPA will take a draft measure to the EDPB. The EDPB can render an opinion on it, and DPA would be urged to take their opinion into consideration. If the DPA ignores it, then it may be escalated up to the European Commission, which may suspend the measure.

- "One Stop Shop Rule." The Proposed Regulation would apply to companies that have their "main establishment" in the EU, and also to non-EU based companies that process personal data about EU residents. Instead of reporting directly to the DPAs in each Member State where the company has a physical establishment, the One Stop Shop Rule allows the company to report only to the DPA in the Member State where the company has its "main establishment." Interestingly, the "main establishment" is defined as the location where primary decisions are made regarding the purposes, conditions, and means of data processing, and not necessarily where the processing

Contact Us

Mary J. Hildebrand, Esq.
973.597.6308
mhildebrand@lowenstein.com

Katherine Anne Varker, Esq.
973.422.6430
kvarker@lowenstein.com

Related Services

Privacy Law

actually occurs.

- Data Protection Officers Required. Companies would also be required to appoint a Data Protection Officer ("DPO") if (i) there are more than 250 employees in the enterprise worldwide; or (ii) the company is a data controller or processor and one of its core activities consists of regular monitoring of persons. Only one DPO is required per "undertaking," so if there is a parent company with divisions or subsidiaries, only one DPO is necessary.

- New Definition for "Personal Data." The Proposed Regulation expands the definition of Personal Data to include online identifiers such as IP addresses and cookie identifiers, but then goes on to say that such information need not always be considered personal data. We predict that this apparently inconsistent definition will be a source of much discussion, and will likely be refined through the review process.

- Clear and Plain Language; Explicit Consent. In response to increasing concern among DPAs with respect to misuse of consent, under the Proposed Regulation statements in a privacy policy or an implied consent will likely not be sufficient. In addition to advising data subjects what kind of data is being collected and what will be done with it, the Proposed Regulation requires additional transparency in the form of using clear and plain language that is adapted to the data subject. Under the Proposed Regulation, Companies must also disclose the name of the DPO, the period of retention of the data, the nature of the company's legitimate business interest in the data, the complaint process, and more information about non-EU countries that the data may be transferred to, including adequacy analysis of those countries. Consent from the data subject must be explicit, by a statement or clear affirmative action (like an opt-in), and it may not be considered proper consent if the parties are in an unequal bargaining position (like an employer and employee). We expect additional guidance is still to come.

- The Right to be Forgotten. In this highly controversial provision, the Proposed Regulation would allow a data subject to require the data controller to erase the data relating to that individual under certain circumstances. Significant penalties may apply if the data controller fails to act promptly, and requires the data controller to inform third parties processing the data that the data subject has requested that they be erased.

- Data Portability. Under the Proposed Regulation, a data subject may transfer its data to another service provider's system upon request to its data controller. In turn, the data controller would be required to accommodate such a request without hindrance. In practice, the costs of allowing data subjects to move their own data from one system to another could vary significantly, and this could be very burdensome for cloud providers and social networks.

- Security Breaches MUST be Reported within 24 Hours. Any breach of the security of any personal data MUST be reported to the DPA within 24 hours—there is no standard of harm and no carve out if the company takes protective measures. Interestingly, "serious" breaches have to be reported to the data subject "without undue delay," but are not required if the company has "implemented appropriate technological protection measures." As even the drafters acknowledge, these requirements could result in an avalanche of breach notifications.

- New Sanctions and Fines. Each DPA will have the power to ban processing by a company, suspend data flows, and impose administrative sanctions and fines up to 2% of the company's worldwide gross revenue. The Draft Version provided for fines up to 5% of the company's worldwide gross revenue but, not surprisingly, met with negative publicity. Additionally, under the Proposed Regulation individual organizations have the right to bring complaints and start court proceedings on behalf of data subjects.

- Model Contracts and Other Provisions Survive. In its current form, the Proposed Regulation leaves intact the model contracts and the U.S. Safe Harbor system which permit organizations to transfer personal data from the EU to countries

that are deemed not to have “adequate” security, such as the United States. This language was not in the Draft Version. Thus, data transfers under adequacy mechanisms that have already been approved, standard contractual clauses, and data transfer arrangements approved by DPAs can continue. Also, Business Continuity Rules (“BCRs”) are explicitly welcomed, and remaining barriers to their use under Member State laws will be removed.

What Happens Next?

The Proposed Regulation will now enter an evaluation and discussion phase by the European Parliament and Member States. We should expect significant negotiation among the various stakeholders, and it may take a year or more to achieve agreement. The Proposed Regulation is set to take effect two years after that.

Many of the Proposed Regulations are viewed as positive efforts to standardize the “rules of the road” in the EU, especially for companies located in foregoing jurisdictions that desire to conduct business there. However, the benefits of predictability across Member States must be measured against the increased accountability demanded by the Proposed Regulation, in addition to hefty fines for non-compliance, data breach notification requirements, data portability and the right to be forgotten. In order to avoid potential liability, companies will be compelled to enhance procedures, monitor compliance and be prepared to take quick action as necessary. In recent years, the insurance industry has introduced new policies that may help to mitigate these risks including certain privacy and network insurance products that protect against the costs of defending regulatory actions wherever they are brought, and also the fines and penalties imposed (where the law allows).

What should organizations be doing to prepare?

First, do an assessment of your data collection, storage, use and processing activities in the EU, and any such activities that involve personal data provided by data subjects that reside in the EU.

Second, take steps to ensure that you are in compliance with Directive 95/46 in each of the Member States where you conduct business. If you are located in a foreign jurisdiction, such as the US, and transfer personal data from a third party in the EU, then ensure that you have executed Model Contracts to protect such data, that you are certified as Safe Harbor compliant, or that you have obtained express consent to the transfer of the data. If your company has business operations in the EU and in foreign jurisdictions such as the US, you may need to establish Binding Corporate Rules to allow for the international transfer of data within the organization. Remember that even if you have no physical presence in the EU, if your business collects and transfers personal information out of or among EU Member States, you must comply with Directive 95/46.

Third, develop and implement a compliance monitoring program that will alert management to potential violations in sufficient time to implement corrections before sanctions or fines are imposed.

For more information on our Privacy Law practice, please contact:

Mary J. Hildebrand
Chair, Privacy Practice Area
973-597-6308
mhildebrand@lowenstein.com

Kathy Varker
Counsel
973-422-6430
kvarker@lowenstein.com

www.lowenstein.com

New York
1251 Avenue of the Americas
New York, NY 10020
212.262.6700

Palo Alto
390 Lytton Avenue
Palo Alto, CA 94301
650.433.5800

Roseland
65 Livingston Avenue
Roseland, NJ 07068
973.597.2500