masuda funai

News & Types: Client Advisories

The New EU Data Protection Regulation - A Global Standard For Data Privacy

5/10/2018

Practices: Commercial, Competition & Trade

Authors: Reinhold Krammer
Co-Author: Caroline Kaeb (Foreign Legal Adviser)

The new EU General Data Protection 2016/679 regulation (the "GDPR") is scheduled to enter into force on May 25th. It is considered the most significant change in data privacy regulation worldwide in 20 years. GDPR, which supersedes the EU Data Protection Directive of 1995, "applies to the processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the Union, where the processing activities are related to […] the offering of goods or services." This is true regardless of whether or not your company has an establishment in the EU, whether you do data processing as part of your core business or merely by means of operating a commercial website to sell your goods or services in the EU, and—for the most part— irrespective of the size of your business operations. In short, it will likely apply to your business in some way. The EU regulator has set out to protect the personal data of its residents within the EU as well as globally wherever the data might be transferred to or stored.

The fines are steep, with up to 4% of annual global revenue or $20 million, whichever is greater. But can the EU really enforce the new regulation against U.S. companies without any physical presence in the Union? The U.S. Department of Commerce and the Federal Trade Commission ("FTC") are standing ready to enforce data protection standards against those U.S. companies under the EU-U.S. Privacy Shield agreement and likely also under other cooperation treaties between the U.S. and EU. The FTC has an active history of enforcing the previous EU data protection law under U.S. consumer protection rules and there is no reason to anticipate any change in that trend. The Acting FTC Chairman recently reaffirmed "the FTC's commitment to aggressively enforce the Privacy Shield frameworks, which are important tools in enabling transatlantic commerce." Thus, the message of U.S. authorities seems loud and clear.

Overall, the new EU regulation has significantly extended the extraterritorial reach to non-EU companies. At the same time, it also marks a step towards streamlining the process and increasing companies' ownership and freedom to devise a unique GDPR compliance system, which works for their business. Doing away with the general notification requirements for data processing activities, the new regulation provides more flexibility for companies, but it also demands more stringent due diligence on the part of the data controller. It is critical to realize that GDPR is just one part of the equation, serving as a floor, not a ceiling, for data protection in the

EU. Companies and their legal counsel will have to monitor closely the evolving national implementation laws across EU member states in order to have a full picture of the EU data protection landscape. Expert legal advice will be imperative, not just as GDPR enters into effect, but well into the future.

Here are a few practical pointers that you should keep in mind while you are getting ready for May 25, 2018, when the GDPR will go into force.

PRACTICAL POINTERS

- Determine whether GDPR applies to you.
- If so, appoint a "representative" in the EU if you have no presence there.
- Institute adequate record-keeping and perform impact assessments of your data processing activities. If a high risk is detected, EU supervisory authorities need to be consulted.
- Review and update your company's policies and procedures for data privacy.
- Obtain consent that is freely given by clear affirmative action for each specific purpose of data processing, but do not rely on consent as the sole basis for lawful processing. Also, note that obtaining consent does not waive the controller's obligation to comply with the general data protection principles.
- Review and update any relevant contract language to protect your company.
- If you are transferring personal data outside of the EU, you will need to show that you ensure adequate safeguards.
    - Consider self-regulating your cross-border data transfers through your own Code of Conduct or Binding Corporate Rules (within corporate groups)—both to be approved by European data protection authorities.
    - Consider using Standard Model Clauses by the EU for your transfers, especially if you have a place of main establishment in the EU.
    - Consider self-certifying under the EU-U.S. Privacy Shield, especially if you are transferring large amounts of data in a frequent manner.
- Determine which Data Protection Agency(/ies) among EU member states is (/are) responsible for your business.
- Monitor national implementation laws in all EU countries of your operations since they can—and have—set more stringent data protection standards.

The independent European Union advisory body on data protection cautions that consent is far from the most desirable basis for legitimizing data processing.

While GDPR provides for a One-Stop-Shop enabling companies to deal with only one Lead DPA for all your operations across all EU member states, this only applies to companies with an administrative seat or place of data processing decision-making in the EU.