

EU Gives Further Guidance on Personal Data Breach Reporting Obligations

APRIL 8, 2014

The Article 29 Data Protection Working Party recently issued its “[Opinion](#) 03/2014 on Personal Data Breach.” The Opinion interprets the ePrivacy Directive (2002/58/EC), which requires electronic service providers to notify competent authority for all personal data breaches as well as the individual where there is likely to be adverse effects to personal data or privacy. The Opinion is meant to “provide guidance to [data] controllers in order to help them to decide whether to notify data subjects in case of a ‘personal data breach.’” The Working Party notes that while this is an issue right now for the electronic service provider sector, it provides examples from other sectors as well, “in the context of the draft data protection regulation,” which has data breach notification obligations for all entities.

The Opinion gives a series of examples of personal data breaches requiring notification to data subjects and, critically, a non-exhaustive list of what the controllers could have done to avoid the breach in the first place. Preventive measures include: having sufficiently up-to-date, secure back-up data available; protecting the data using encryption methods; continuously monitoring potential vulnerabilities of the technologies used; code reviewing and having a security incident management policy in place; limiting access to databases by applying need-to-know and least-privilege principles; and using an office shredder to destroy physical files before throwing them away. The Opinion also noted instances in which notification is unnecessary, for example, where the data has been rendered unintelligible to any person not authorized to access it. The Opinion makes clear that in cases of doubt, controllers should err on the side of notifying affected individuals.

Tip: This Opinion gives guidance to a limited group of companies and electronic service providers. However, it serves as useful foreshadowing of what might be expected of all entities if the draft regulations go into effect.

1 Min Read

Related Locations

Chicago

Related Topics

Data Breach

Europe Privacy

Related Capabilities

Privacy & Data Security

Related Regions

Europe

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.