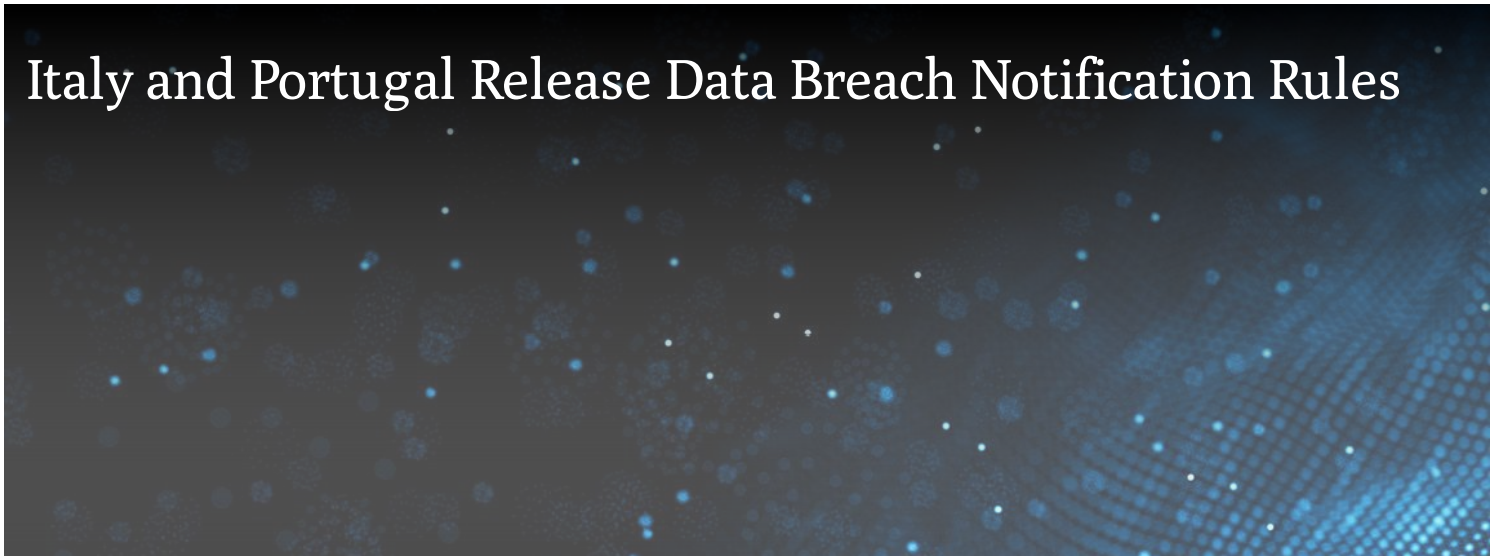
WINSTON & STRAWN LLP

BLOG

Italy and Portugal Release Data Breach Notification Rules



SEPTEMBER 17, 2012

The Garante per la Protezione dei Dati Personali (the Italian data protection authority) has released a new set of data breach notification rules that implement the European Union's 2009 amendments to the existing privacy laws (2009/136/EC). These amendments, among other things, require notification by providers of "publicly available electronic communication services" in the event of data breaches. The new Italian rules will require that all telecommunications and Internet service providers give the Guarante notice within 24 hours of discovering a breach. The rules clarify that company network operators (for employee use), public internet access points, search engines, and internet content providers are exempt from the notification requirements. Covered entities, though, must not only notify the Guarante, but must provide a later, more detailed notification within 72 hours of the first. In more serious cases, individual users also must be notified within 72 hours, unless the data was unintelligible and/or anonymous. In general, telecoms and ISPs must maintain records of any breach and remedial actions taken, and then allow privacy authorities to access these records at any time. Covered entities that fail to notify will be fined anywhere from €25,000 to €150,000 ($31,000 - $186,000). The new rules go into effect immediately, although enforcement is reportedly going to begin gradually within the next 90-120 days. Portugal has also recently announced a new law transposing the same e-Privacy Directive and requiring electronic communication service companies to similarly notify the National Data Protection Commission (the country's data protection authority) "without unjustified delay." Covered entities must also notify end users when the breach could negatively affect them, unless the entity can show that it has adopted "adequate technological protection measures." Violations can lead to significant fines of between € 5,000 and € 5 million ($6,274 – 6.3 million). In November 2011, both countries were among the 16 EU Member States notified by the European Commission that they had failed to fully bring into effect the provisions of the breach requirements (and other requirements under Directive 2009/136/EC) within the May 25, 2011 deadline. The other non-compliant countries included Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, France, Germany, Greece, Hungary, the Netherlands, Poland, Romania, Slovenia and Spain. All have since communicated provisions to the EU Commission, although the Commission has not yet determined whether they satisfactorily transpose the Directive.

Tip: These new breach notification laws are the most recent from EU member states implementing national legislation regarding data breach notifications by providers of "electronic communication services." Covered entities that have breach plans in place under U.S. laws, should be well prepared for EU requirements, although they should keep in mind the tight notification time frames in places like Italy.

2 Min Read

Related Topics

Data Breach | Europe Privacy

Related Capabilities

Privacy & Data Security

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.