This is one of ten monthly alerts, counting down to the date when GDPR applies. 6 months to go

WOMBLE BOND DICKINSON

GDPR Breach Notification Checklist

U.S. companies already face a panoply of data breach notification laws enacted by 48 States and numerous regulators. Those subject to the GDPR may soon have yet another breach notification requirement to worry about.

Follow our chart below to determine if and when you must provide notice, who you must notify, and what your notice should include.

Who Required	When Obliged	Who to Notify	How Quickly	What Notice Must Include
Controller	**"Personal data breach"** that is likely to result **in a risk** to the rights and freedoms of natural persons	**"Competent supervisory authority"**	**"Without undue delay"** once the controller **"becomes aware"** of the personal data breach *Under 72 hours where feasible* *Can be done in phases if necessary*	• Nature of the breach (including types and approximate number of individuals and records) • Name and contact details for the data protection officer or alternate point of contact • Likely consequences of it • Measures taken or proposed by the controller to address it • (Reason for delay if notifying after 72 hours)
	"Personal data breach" that is "likely to result **in a high risk** to the rights and freedoms of natural persons" *But not if data was encrypted, or the controller made that high risk "no longer likely to materialize"*	Affected individuals *If such notice would involve "disproportionate effort," then controller may notify via "public communication or similar measure"*	**"Without undue delay"**	• Nature of the breach • Name and contact details for the data protection officer or alternate point of contact • Likely consequences of it • Measures taken or proposed by the controller to address it • Recommendations for the affected individual to mitigate any potential adverse effects
Processor	**"Personal data breach"**	Controller	**"Without undue delay"**	(Unspecified) *NOTE: controllers can address this as a matter of contract and should consider specifying the content to be included in these notices in their contracts with processors*

This text leaves open plenty of questions. However, on October 3, 2017, the Article 29 Working Party issued guidelines interpreting these data breach notification requirements. Here are some of the answers:

What is a "personal data breach"?	"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"
When could a breach be "unlikely to result in a risk to the rights and freedoms of natural person"?	For example, where the data was already publicly available, or where the data was encrypted and remains accessible to the controller (or adequately backed-up); however, each personal data breach will need to be assessed on its facts
What is the difference between "risk" and "high risk" to persons' rights and freedoms?	"High risk" would exist where "the breach may lead to physical, material or non-material damage for the individuals whose data have been breached," such as "discrimination, identity theft or fraud, financial loss and damage to reputation"
When does the controller become "aware" of the breach?	"When that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised," depending on the circumstances, this may allow for "a short period of investigation in order to establish whether or not a breach has in fact occurred"
What is "without undue delay"?	"As soon as possible" (or immediately, in the case of a processor giving notice to a controller)
Who is the "competent" supervisory authority" when a personal data breach affects individuals in more than one EU Member State?	The "lead supervisory authority," i.e., "the supervisory authority of the main establishment or of the single establishment of the controller or processor"

Key Contacts

Allen O'Rourke
Of Counsel
t: 704.350.6357
e: allen.orourke@wbd-us.com

Peter Given
Legal Director
t: +44 (0)238 020 8194
e: peter.given@wbd-uk.com

Contact Us

If you have any questions about the checklist above, contact Allen O'Rourke at 704.350.6357 or allen.orourke@wbd-us.com or any member of our GDPR Compliance Task Force.