OLSWANG

Security and breach notification: draft NIS Directive compared to Data Protection Regulation

This table provides a quick comparison of the obligations proposed under the draft Directive on Network and Information Security and the draft Regulation on Data Protection. References to the Regulation reflect the original text and where relevant proposed amendments by the EP's LIBE Committee.

	Draft NIS Directive	**Draft DP Regulation**
Who is subject to the rules?	"Public administrations" "Market operators" providing services within the EU including: • ecommerce platforms • Internet payment gateways • Social networks • Search engines • Cloud computing services • Application stores Operators of infrastructure relating to: • energy • transport • banking • financial markets • health care. *Article 3(8) and Annex II*	All data controllers, regardless of sector. *Articles 30, 31 and 32* Data processors are also subject to a number of obligations directly. *Articles 30 and 31* Continued…/

	Draft NIS Directive	Draft DP Regulation
Security obligations	"Appropriate technical and organisational measures to manage the risks posed to security of the networks and information systems which they control and use in their operations." "Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems". *Article 14(1)*	"Appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation." "The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data." *Article 30*
Will standards apply?	Standards are likely to be key. Member States shall encourage technical standards and specifications, to promote convergent approaches. *Article 16*	Yes: Commission may adopt delegated acts and implementing acts specifying criteria and conditions for the "technical and organisational measure" including what constitutes the state of the art, for specific sectors and in specific data processing situations. *Article 30(3)* Continued…/

	Draft NIS Directive	Draft DP Regulation
What triggers notification?	"Incidents having a significant impact on the security of the core services they provide". *Article 14(2)*	No materiality threshold for notification to the Regulator. *Article 31*
	Commission may define circumstances triggering by "delegated acts" *Article 14(5)*	Notification to individuals if privacy likely to be adversely affected. *Article 32*
Who to notify?	"The competent authority" – a new NIS authority to be established by each Member State. *Article 14(2)*	Data protection regulator. *Article 31*
	The public, if required to do so by the competent authority, in the public interest. *Article 14(4)*	Individuals**,** if privacy likely to be adversely affected. (The EP's changes would clarify this test by reference to ID theft, fraud, physical harm, significant humiliation or damage to reputation). *Article 32*
Notification deadlines?	No deadlines specified	Notification to regulator "without undue delay" and, where feasible, not later than 24 hours (72 hours, if the EP's changes are adopted) after having become aware of it. *Article 31(1)*
		Notification to individuals "without undue delay". *Article 32(1)* Continued…/

	Draft NIS Directive	Draft DP Regulation
Powers and sanctions?	National cybercrime authorities to have power to investigate non compliance and to issue "binding instructions". *Article 15* Member States to provide "effective, proportionate and dissuasive" sanctions. *Article 17*	Fines of up to 2% of annual worldwide turnover. *Article 79*
When will rules be in force?	Unclear – formal legislative process has not yet begun. Member States would have 18 months from date of adoption to bring requirements into force.	Likely to be in force by mid 2016 (Commission aims to adopt Regulation by mid 2014; then directly effective within two years).
Next steps?	Timetable awaited – see EP procedure fiche.	Key LIBE Committee vote expected April 2013.

This comparison is provided as a high level guide to the two proposed regimes, based on draft proposals as at February 2013. Both the draft NIS Directive and draft Data Protection Regulation are still subject to negotiation and the detailed obligations which may eventually be adopted are subject to change. For more information please contact Ross McKean, Head of Privacy and Data Protection (ross.mckean@olswang.com) or Claire Walker, Head of Commercial Group Know How (claire.walker@olswang.com).