ALERT MEMORANDUM

Cybersecurity in the EU – The New Regime under the GDPR and NISD

May 3, 2017

From May 2018, organizations established or providing services in the EU will be subject to new national and EU-wide cybersecurity legislation, as regulators in EU Member States begin to apply both the General Data Protection Regulation (the "**GDPR**")[1] and national legislation implementing the Network and Information Security Directive (the "**NISD**").[2] These new laws will significantly increase the territorial and sectoral scope of organizations subject to EU cybersecurity obligations and introduce strict data security and breach disclosure obligations with potentially severe penalties for non-compliance.

This tightening of the EU cybersecurity regime coincides with similar developments in other jurisdictions worldwide and reflects a global trend for legislators and regulators to require organizations to observe increasingly stringent cybersecurity practices. This memorandum considers the key components of the new EU laws and outlines a number of recent cybersecurity developments in other key jurisdictions.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

LONDON

Colin Pearson
+44 20 7614 2390
cpearson@cgsh.com

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

PARIS

Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

BRUSSELS

Christopher Cook
+32 22872137
ccook@cgsh.com

Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

ROME

Francesco de Biasi
+39 06 6952 2254
fdebiasi@cgsh.com

FRANKFURT

Thomas Kopp
+49 69 97103 246
tkopp@cgsh.com

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

[1] Regulation (EU) 2016/679.
[2] Directive (EU) 2016/1148.

I. The current EU regime

The current cybersecurity regime in the EU comprises a collection of sector-specific and data protection legislation, which has been implemented differently in different Member States.

All organizations established in the EU must implement appropriate technical and organizational measures to ensure the security of the personal data that they control.[3] Rules on data breach notification differ between Member States and, while notification to data protection authorities and affected individuals is not mandatory across the board, it is generally recommended for significant breaches.

On top of this obligation to safeguard personal data, organizations operating in specific sectors are subject to overarching obligations to safeguard the security of their networks and services and to report security breaches more generally. For example, providers of public electronic communications services and networks must take appropriate technical and organizational measures to manage the risk of security incidents affecting their networks and services, guarantee network integrity and service continuity, and report security breaches to relevant authorities.[4] A number of other sector-specific laws impose similar cybersecurity obligations on organizations operating in the payment services and electronic trust services sectors.[5]

II. GDPR

The GDPR strengthens the cybersecurity obligations currently contained in the Data Protection Directive and national implementing laws.[6] From May 25, 2018, all organizations offering goods and services or monitoring individuals in the EU (including service providers processing data on behalf of other companies) will be required to:

- implement appropriate technical and organizational measures to protect personal data against the risk of destruction, loss, alteration, and unauthorized disclosure or access;[7]
- use only third party processors providing sufficient contractual guarantees to do the same;[8]
- conduct a data protection impact assessment before undertaking any data processing which, by its nature, is likely to result in a high risk to the rights and freedoms of individuals;[9]
- notify the relevant supervisory authority of any personal data breach, except breaches unlikely to result in any risk to individuals' rights and freedoms, without undue delay and, where feasible, within 72 hours of becoming aware of the breach;[10] and
- notify any affected individual without undue delay where a breach is likely to result in a high risk to individuals' rights and freedoms.[11]

With respect to the first requirement, what technical and organizational measures are "*appropriate*" must be assessed on an ongoing basis, taking into account the state of the art, costs of implementation, and, most importantly, the risks posed to individuals by the processing activity. In general, organizations should:

- pseudonymize and encrypt personal data;
- be able to (i) ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, and (ii) restore availability and access to personal data in a timely manner in the event of a security incident; and

[3] *See* Directive 1995/46/EC (Data Protection Directive). Organizations established outside the EU but using "*means*" located in the EU to process personal data are also subject to the legislation.

[4] Directive 2002/21/EC, as amended by Directive 2009/140/EC (Framework Directive, as amended). These organizations are also subject to particularly stringent data protection laws, under Directive 2002/58/EC as amended by Directive 2009/136/EC (E-Privacy Directive), including mandatory breach notification requirements.

[5] *See* Directive (EU) 2015/2366 (Payment Services 2 Directive) and Regulation (EU) 2014/910 (Electronic Identification Regulation).

[6] The GDPR also contains wider reforms to the EU data protection regime. *See* our alert memorandum "The General Data Protection Regulation: Key Changes and Implications", published on May 13, 2016, available at https://clients.clearygottlieb.com/rs/alertmemos/2016-50.pdf for more information.

[7] *See* GDPR Article 32.

[8] *Ibid*., Article 28.

[9] *Ibid.*, Article 35.

[10] *Ibid.*, Article 33(1). Notifications made later than 72 hours after the organization becoming aware of a data breach must be accompanied by reasons for the delay in notifying.

[11] *Ibid*., Article 34(1). Exceptions apply where (i) the data were rendered unintelligible by encryption prior to the breach, (ii) the organization has subsequently taken measures that ensure the high risk to individuals is no longer likely to materialise, or (iii) individual notification would involve disproportionate effort, in which case a public communication regarding the breach will suffice.

- have in place a process to regularly test, assess, and evaluate the effectiveness of the security measures in place.[12]

The GDPR places importance on organizations not only complying with data security requirements but being able to demonstrate their compliance. This can be achieved by means of approved codes of conduct or certification mechanisms.[13] Becoming ISO 27001 certified, for example, demonstrates that an organization is following international best practices on data security.

Failure to ensure appropriate security of personal data can attract a fine of up to the higher of EUR 20 million or 4% of an organization's total worldwide annual turnover.[14] Failure to adequately notify a data breach can attract a fine of up to the higher of EUR 10 million or 2% of total worldwide annual turnover.[15]

III. NISD

The NISD broadens the scope of organizations that must, in addition to complying with the GDPR, take measures to protect the security of their networks and services more broadly. Its measures apply to operators of essential services ("**OESs**") and digital service providers ("**DSPs**") that are established in the EU or, in the case of DSPs, offer services to persons within the EU.[16] The NISD also contemplates that other types of organization should be given the facility to notify security incidents on a voluntary basis.[17]

- OESs include providers of certain energy, transport, banking, financial market infrastructure, healthcare, drinking water, and digital infrastructure services, which are identified as OESs by the Member State in which they are established.[18]
- DSPs include providers of online market places, online search engines, and cloud computing services.[19]

Member States must require both OESs and DSPs to:

- take appropriate and proportionate technical and organizational measures to secure the network and information systems that they use, taking into account the state of the art and the risk of those systems being compromised;
- take appropriate measures to prevent and minimize the impact of security incidents affecting those systems with a view to ensuring service continuity; and
- notify the relevant supervisory authority of any security incident having a significant impact on service continuity without undue delay.[20]

Once the relevant authority has been notified, it may inform the authorities in other affected Member States of the security incident. It may also inform the public, or encourage the compromised organization to do so.[21]

Member States have a measure of discretion in implementing the NISD, including in identifying operators of essential services, adopting rules that require a higher level of cybersecurity than those set out in the NISD,[22] and defining national enforcement powers and penalties.[23] The new cybersecurity laws, when implemented nationally, will therefore differ to some extent between Member States, although the NISD does encourage a harmonized approach.[24]

[12] *Ibid.*, Article 32.

[13] *Ibid*., Article 24.

[14] *Ibid.*, Article 83(5). While the lesser fine of up to EUR 10 million or 2% of total worldwide annual turnover applies to breaches of the granular requirements for maintaining data security that are set out in Article 32 (*see* Article 83(4)), more egregious instances of processing personal data in a manner that does not ensure appropriate security would likely be treated as a breach of the data processing principles set out in Article 5 of the GDPR and thereby attract a higher fine.

[15] *Ibid.*, Article 83(4).

[16] *See* NISD, Articles 5(1) and 18, and Recital 65. There are exceptions for (i) organisations subject to equivalent sector-specific cybersecurity obligations (including the Framework Directive and Electronic Trust Regulation) and (ii) digital service providers that employ fewer than 50 people and have annual turnover and assets not exceeding EUR 10 million. *See* NISD Articles 1(3), 1(7), and 16(11).

[17] NISD, Article 20.

[18] *Ibid*., Article 5 and Annex II.

[19] *Ibid*., Article 4 and Annex III.

[20] *Ibid*., Articles 14 and 16. The significance of a security incident should be assessed on the basis of factors including the number of users affected by, duration, and geographical spread of the incident.

[21] *Ibid.*

[22] This applies in relation to operators of essential services, but not digital service providers. *See* NISD Article 16(10).

[23] NISD, Articles 3, 5(1), 15, 17, and 21.

[24] NISD, Article 19.

Cybersecurity in the UK post-Brexit

A report published by the UK government in December 2016 confirmed that both the GDPR and the NISD will come into force in the UK as planned, despite current uncertainty surrounding the terms of the UK's departure from the EU.

Extra-territoriality provisions in both the GDPR and the NISD will in any event require UK organizations providing services or monitoring the behaviour of persons within the EU to comply with their requirements, regardless of their implementation in UK law.

IV. Other recent cybersecurity developments

The entry into force of the new cybersecurity regime in the EU coincides with similar developments in the United States and China.

- The New York Department of Financial Services' Cybersecurity Regulations (the "**New York Regulations**")[25] came into effect on March 1, 2017. The scope and key terms of the New York Regulations are discussed in our alert memorandum "New York Cybersecurity Regulations for Financial Institutions Enter Into Effect", published on March 3, 2017.[26] Organizations subject to the New York Regulations are currently working towards achieving compliance before expiry of the 180 day transition period that applies to the majority of its requirements.
- Initiatives at a federal level are also under discussion in the United States. In October 2016, three federal banking regulators put forward a joint advance notice for "*Enhanced Cyber Risk Management Standards*" to apply to large entities in the financial sector.[27] The public consultation period in respect of the proposal expired in January 2017.
- A new Cybersecurity Law is also scheduled to come into force in China on June 1, 2017, which will require all "*network operators*", which is broadly defined to potentially cover any organization using a network in its operations, to protect the security of personal data. In addition, organizations that operate "*critical information infrastructure*" will be subject to additional requirements in respect of the storage and transfer of personal information and "*important data*" collected or generated within China, including obligations to store in-scope information and data within China and observe stringent restrictions on data export including, in certain circumstances, submitting to a security assessment by a Chinese regulator. These requirements are developed in more detail in the draft Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data released for public comment by the Cybersecurity Administration of China on April 11, 2017. Notably, the draft measures extend the onshore storage requirement and security assessment procedures for data export beyond operators of "*critical information infrastructure*" (as stipulated by the Cybersecurity Law) to all "*network operators*". The public consultation on the draft measures will end on May 11, 2017.

These developments are indicative of a general trend for legislators and regulators around the world to seek to reinforce the rigor of private organizations' cybersecurity practices, particularly in essential industries, as the threat and reality of cyber-attacks and personal data loss continue to loom large.

…

CLEARY GOTTLIEB

[25] New York Department of Financial Services, 23 NYCRR 500.

[26] *See* https://clients.clearygottlieb.com/rs/alertmemos/2017-29.pdf.

[27] Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, *Enhanced Cyber Risk Management Standards*, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf.