DATA AND SECURITY INCIDENT REPORTING – STRESS TEST ON RISK GOVERNANCE HAS BEGUN

Duties to report personal data and security incidents under the GDPR[1] and the NIS Directive[2] are now in force. The Italian Data Protection Authority reports: (i) a 500% increase in data breach reporting has been recorded since 25 May 2018[3], (ii) 140 data breaches were recorded only in May 2018 and (iii) 330,000 individuals were affected by data breaches from March to May 2018. Failure to notify exposes businesses to the risk of penalties, claims for damages and reputational damage. Prevention is the key.

Key issues

- Personal data breaches under GDPR must be notified within 72 hours
- Security incidents under NIS Directive must be notified without undue delay
- Penalties up to EUR 10 million or 2% of global turnover for failure to notify personal data breaches
- Penalties from EUR 25,000 to EUR 125,000 for failure to notify security incidents under Italian law
- Personal data breaches treated as security and cyber security incidents
- All businesses should assess risk in their organisations
- Preventing incidents through an appropriate response plan is vital

NOTIFICATION REQUIREMENTS

Under the GDPR

Data controllers (i.e. any organisation that determines why and how personal data are processed) **must (i) notify a personal data breach to the supervisory authority[4] within 72 hours after becoming "aware" of it and (ii) communicate the personal data breach to the data subject without undue delay**, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

Data processors (i.e. any third party that processes personal data on behalf of the controller customer, *e.g.* service providers) must notify the controller without undue delay after becoming "aware" of a personal data breach. **Legal responsibility to notify the supervisory authority continues to rest with the controller**.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR").
[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive").
[3] On 25 May 2018 the GDPR came into force.
[4] In Italy, the Data Protection Authority to notify is the *Garante per la Protezione dei Dati Personali*.

Personal data breaches are security incidents which according to the Article 29 Working Party[5] ("29WP") may fall in these categories:

- "**Confidentiality breach**", in case of unauthorised or accidental disclosure of personal data or unauthorised access to such data;
- "**Integrity breach**", in case of unauthorised or accidental alteration of personal data;
- "**Availability breach**", in case of accidental or unauthorised loss of access to personal data or destruction of such data.

…and under the NIS Directive, now implemented in Italy

Under the NIS Directive, operators of essential services[6] and digital service providers[7] must notify, without undue delay, the NIS competent authority of any security incidents with significant/substantial impact on, (i) in the case of operators of essential services, the continuity of the essential services provided or, (ii) in the case of the digital services providers, the provision of ecommerce, search engines and cloud services.

The NIS Directive has been recently implemented in Italy with Legislative Decree no. 65 of 2018 (the "Decree"). The Decree clarifies that **security incidents must be notified to the Italian computer security incident response teams (CSIRT)**, set up at the Presidency of the Council of Ministers, and to the NIS competent authority for the purpose of information. **Penalties from Eur 25,000 to EUR 125,000 apply in case of failure to notify the CSIRT of a security incident.**

Under the Decree, the Ministry competent for the operator's business sector is the NIS authority competent to adopt specific security measures, supervise the operators of essential services and impose penalties. Each NIS competent authority identifies the operators of essential services based in Italy for its respective sector by **9 November 2018**.

The table below lists the Italian NIS competent authorities for each business sector.

Sector	Italian NIS competent authority
Energy, oil and gas	Ministry of Economic Development
Transport (air, rail, water, road)	Ministry of Infrastructure and Transport
Banking	Ministry of Economy and Finance
Financial market infrastructures	Ministry of Economy and Finance
Health sector	Ministry of Health
Drinking water supply and distribution	Ministry of Environment
Digital Infrastructure	Ministry of Economic Development

[5] The Article 29 Working Party is composed, among others, of representatives of the supervisory authorities of each EU Member State (the Guidelines). This working party has advisory status and acts independently. After the entry into force of the GDPR, the European Data Protection Board replaced the Article 29 Working Party.
[6] Providers of services with remarkable impact over social community, such as services in the banking, energy, transport and health sectors.
[7] Providers of on-line services such as e-commerce, on-line search engines and cloud services.

Personal data breaches are a cyber security issue

The Italian Data Privacy Authority highlighted the significant symmetry between data protection and cyber security. The 29WP also alerted that data protection requirements may overlap with cyber security requirements.

In particular, the 29WP noted that **Digital Services Providers may have to (separately) report the same incident under both the GDPR and the NIS Directive**. In this regard, the Decree (article 13) expressly provides that in case of incidents involving personal data breaches the NIS competent authority cooperates closely with the Italian Data Protection Authority.

The 29WP provides the following **examples of personal data breaches arising out of cyber security violations**:

- a controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated;
- a controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system;
- a controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.

For an overview on data/security breach notification duties, please refer to our briefing on Data and security incident reporting under GDPR, PSD2, NISD and eIDAS Regulation.

Actions

Organisations that have already implemented appropriate measures to face new requirements should monitor their reliability and keep their legal risk assessments up-to-date. All organisations should make an effort to prevent data breaches and, in any case, minimise their consequences, once occurred.

The 29WP clarifies that controllers should adopt measures to immediately establish that personal data breaches have occurred and act to avoid or contain their effects, such as encrypting personal data, ensuring that processing systems (e.g. data storage tools) are resilient, timely restoring availability and access to personal data after incidents, regularly testing the security system adopted.

In particular, with regard to data and security incidents, any organisations should have a security breach readiness strategy, to meet the 72-hour breach notification requirement and remember that, for security incidents under the NIS Directive, notification is mandatory without undue delay.

In all cases, a preliminary risk assessment is vital to take appropriate action and prevent incidents.

CONTACTS

KEY CONTACTS FOR THIS BRIEFING

Carlo Felice Giampaolino
Partner
Italy

T +39 064229 1356
E carlofelice.giampaolino @cliffordchance.com

Alessandro Sciarra
Associate
Italy

T +39 064229 1384
E alessandro.sciarra @cliffordchance.com

OUR DATA PROTECTION AND CYBER SECURITY EXPERTS NETWORK

Jonathan Kewley
Partner
London

T +44 20 7006 3629
E jonathan.kewley @cliffordchance.com

Samantha Ward
Partner
London

T +44 20 7006 8546
E samantha.ward @cliffordchance.com

Megan Gordon
Partner
Washington

T +1 202 912 5021
E megan.gordon @cliffordchance.com

Daniel Silver
Partner
New York

T +1 212 878 4919
E daniel.silver @cliffordchance.com

Alice Kane
Counsel
New York

T +1 212 878 8110
E alice.kane @cliffordchance.com

Dessislava Savova
Partner
Paris

T +33 1 4405 5483
E dessislava.savova @cliffordchance.com

Grégory Sroussi
Avocat
Paris

T +33 1 4405 5248
E gregory.sroussi @cliffordchance.com