THE PERIMETER OF NATIONAL CYBERSECURITY: STRATEGIC PRIVATE OPERATORS ON THE FRONT LINE.

Through the recent conversion into law[1] of the Italian law decree no.105 of 21 September 2019, setting forth urgent provisions on the perimeter of national cybersecurity (the "**Decree**"), the rules and obligations imposed upon **private parties that provide services of strategic importance at the national level** are confirmed. These parties will be required to ensure **high levels of security of IT systems and networks**. In the event of breaches, **sanctions of up to Euro 1.8 million will apply**. In the context of the protection of national security and strategic sectors, significant **reforms in the area of the "Golden Power"** have been introduced.

Key issues

- Private parties in strategic sectors are included within the perimeter of national cybersecurity
- Operators are bound by new obligations to transmit lists of IT networks to the Government
- Organisational measures are envisaged to guarantee high levels of cybersecurity
- Breaches of new obligations are punished with sanctions ranging from a minimum of Euro 200.00 to a maximum of Euro 1,800,000
- Coordination with the NIS legal framework is provided
- Golden Power: the Government's powers have been extended to also cover sectors featuring a "high technological density"

THE PERIMETER OF NATIONAL CYBERSECURITY

The Decree establishes the perimeter of national cybersecurity (the "**Perimeter**") in order to ensure a high level of security of the networks, IT systems and IT services (i) the malfunctioning, interruption or unauthorised/improper use of which may cause prejudice to national security and (ii) managed by parties that provide a service essential for maintaining civil, social or economic activities which are fundamental for the interest of the State.

Within four months of the date of entry into force of the conversion law (therefore, on 21 March 2020), a decree issued by the President of the Council of Ministers shall identify the **public and private national entities and operators with registered offices in the national territory to be included within the Perimeter**, which shall be under a duty to honor the obligations and provisions set forth in the Decree.

Criteria for identifying the parties included within the Perimeter:

- the party guarantees an essential service for the maintenance of civil, social or economic activities that are fundamental for the interests of the State;
- the exercise of such function or the performance of such service depends upon networks, IT systems and IT services;
- for purposes of such identification, attention is focused, following a criterion of significance/degree, on the prejudice for national security, **in relation to the specificity of the various sectors of activity,** which may derive from the malfunctioning or interruption, even on a partial basis, or unauthorised use of the networks, IT systems and IT services.

[1] Law no. 133 of 18 November 2019

THE OBLIGATIONS IMPOSED UPON PARTIES FALLING WITHIN THE PERIMETER

Notification of lists

Within six months of the entry into force of the degree for the identification of parties falling within the Perimeter, such parties shall be required to send to the Office of the President of the Council of Ministers and to the Ministry of Economic Development a list **to be updated at least once per year**, of the networks, IT systems and IT services respectively pertaining to them.

Obligation to report cyber incidents

A further requirement of considerable impact for parties included within the Perimeter is the obligation to report cyber incidents: indeed, specific procedures shall be defined, through a dedicated decree by the President of the Council of Ministers, to be issued **within ten months of the entry into force of the conversion law (therefore, by 21 September 2020)**, under which the parties included within the Perimeter shall be required to report to the Italian Computer Security Incident Response Team (CSIRT) any incident that has had an impact on the networks, IT systems or IT services respectively pertaining to them. The CSIRT, in turn, shall have the task of forwarding such reports in a timely manner to the Department of security information (*Dipartimento delle informazioni per la sicurezza*), including for the activities delegated to the cybersecurity Team/Department (*Nucleo per la sicurezza cibernetica*).

Measures for guaranteeing high levels of cybersecurity

Through the same implementing decree to be adopted by 21 September 2019, the Office of the President of the Council of Ministers shall also elaborate the **measures aimed at ensuring high levels of security** of the IT systems and IT services pertaining to the parties included within the Perimeter.

Such measures shall take into account the **standards defined at the international and European Union levels**, and shall concern the following areas:

- organisational structure dedicated to security management;
- security and risk management policies;
- mitigation, management and prevention of incidents, including through interventions on devices or products that are seriously inadequate from a security standpoint;
- logical and physical data protection;
- integrity of IT networks and systems;
- operational management, with specific regard to continuity of service;
- monitoring, testing and control;
- training and awareness;
- assignment of contracts for the supply of information and communication technology (ICT) goods, systems and services, including through the definition of general characteristics and requisites.

Contracts subordinated to the favorable outcome of hardware/software tests

The parties included within the Perimeter and belonging to the categories identified by a decree issued by the President of the Council of Ministers[2], that intend to outsource the supply of ICT goods, systems and services meant to be used on the IT networks and systems and the performance of IT services, will be required to process **a specific notification, complete with an assessment of the risk associated with the subject matter of the supply, to the Center for national assessment and certification (*Centro di valutazione e certificazione nazionale*** or CVCN) to be established with the Ministry of Economic Development.

Within 45 days of receipt of the notification, which term may be extended only once for an additional 15 days, the CVCN may conduct **verifications,** impose **conditions** and require the performance of **hardware and software tests**.

In this case, the Decree imposes that clauses are inserted into the **supply contracts** (or invitations to tender, in the case of administrations) **subordinating the effectiveness of the same, in the form of either conditions precedent or conditions subsequent, upon fulfillment of the conditions and the favorable outcome of tests ordered by the CVCN.**

SANCTIONS

Unless such breaches amount of a criminal offense, art. 1, paragraph 9, of the Decree introduces significant administrative sanctions for breaches of the new obligations. In particular, the Ministry of Economic Development may apply the following sanctions to private parties:

- **from Euro 300,000 to Euro 1,800,000** for the failure to report to the CVCN or use of products or services on the IT networks or systems, or for the performance of IT services in breach of the conditions or without passing the tests imposed by the CVCN;
- **from Euro 250,000 to Euro 1,500,000** for the failure to fulfill the reporting obligation in a timely manner, the failure to comply with the security measures mentioned above and the failure to collaborate in the performance of the tests imposed by the CVCN, the failure to fulfill the requirements imposed by the Ministry of Economic Development or the Office of the President of the Council of Ministers upon the completion of inspections, the failure to honor the requirements imposed by the CVCN;
- **from Euro 200,000 to 1,200,000**, for the breach of obligations to prepare and update the list of IT networks, systems and services.

The new legal framework has also introduced criminal sanctions consisting of **imprisonment from one to three years** for anyone who, in order to hinder or influence the performance of the above-mentioned processes aimed at the verification of IT security of the parties falling within the Perimeter or the performance of inspection or oversight activities, provides untruthful information, data or factual elements or fails to report them within the required terms. **The criminal offense is included within the category of wrongful acts/offenses leading to a presumption of liability on the part of entities pursuant to legislative decree 8 June 2001, no. 231.**

[2] Also to be adopted within ten months of the entry into force of the conversion law.

COORDINATION WITH THE "NIS" LEGAL FRAMEWORK

The **operators of essential services** (OES), **digital service providers** identified under the Italian legislative decree no. 65 of 18 May 2018, issued in accordance with the NIS directive[3], and the **businesses providing public communications networks or electronic communication services accessible to the public,** referred to in the electronic communications code (Italian legislative decree 259/2003), **included within the national cybersecurity perimeter,** will also be required:

- To honor the cybersecurity measures provided under the respective legislative decrees of reference indicated above, **if such measures are of a level at least equivalent to those adopted in accordance with the Decree**. The Ministry of Economic Development has the task of identifying, for **private parties, any additional measures that may be necessary in** order to achieve the security levels provided under the Decree.
- The notification of the cyber incidents made in accordance with the Decree **serves to fulfill the obligation of reporting incidents having a material impact on the service provided, within** the meaning set forth in arts. 12-14 of legislative decree 65/2018 (NIS notification) and art. 16-*ter* of the Electronic Communications Code. To such end, the Italian CSIRT has the task of forwarding the notifications to the competent Ministry.

CHANGES IN THE "GOLDEN POWER" REGIME

The Decree also extends the Government's powers on the matter of the so-called Golden Power provided under the Italian law decree no. 21/2012, which refers to the Government's special powers with regard to acquisitions of national companies in areas of strategic importance in the energy, transport and communications sectors. Under the Decree:

- through specific implementing measures, to be adopted within one hundred twenty days of the entry into force of the Decree, the so-called "**sectors characterised by high technological intensity**" subject to the application of the Golden Power legal framework will be identified, taking into account the technologies, critical production factors and sensitive information indicated in art. 4, par. 1, regulation (EU) 2019/452.
- The Government now has **up to 45 days of the notification of the transaction falling within the scope of the "Golden Power" to exercise its powers**. If it requests additional information from the reporting parties, the term of 45 days is suspended, until receipt of the information, **to be notified within 10 days of the request**. Such latter term **is extended to 20 days** if the recipient of the request for information is a third party with respect to the transaction.
- The legal framework also introduces an additional **threshold of 50% of the shareholdings in companies that conduct business operations that are strategically important for the national defense and security system, which triggers the Government's special powers.**

[3] Directive (EU) 2016/1148 of 6 July 2016 setting forth measures for a common high level of security of IT networks and systems of the Union ("**NIS Directive**"). With regard to the NIS legal framework, see our previous briefing available here.

- Prior to the entry into force of the Regulation (EU) 2019/452[4], implementation provisions are already introduced, which entail, *inter alia*, **a possible increase in the term of 45 days within which the Government may exercise its special powers,** if a Member State, or the European Commission, notifies its intention to formulate observations or to issue an opinion on a transaction.

[4] Regulation (EU) 2019/452 of 19 March 2019 which establishes a framework for oversight on foreign investments to be made in the Union.

AUTHORS

Carlo Felice Giampaolino
Partner, Rome

T +39 064223 1356
E carlofelice.giampaolino@cliffordchance.com

Alessandro Sciarra
Associate, Rome

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

NETWORK

Jonathan Kewley
Partner, London

T +44 207006 3629
E jonathan.kewley@cliffordchance.com

Dessislava Savova
Partner, Paris

T +33 14405 5483
E dessislava.savova@cliffordchance.com

Richard Jones
Director of Data Privacy, London

T +44 207006 8238
E Richard.jones@cliffordchance.com

Megan Gordon
Partner, Washington DC

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

Grégory Sroussi
Counsel, Paris

T +33 14405 5248
E gregory.sroussi@cliffordchance.com

Maxime D'Angelo Petrucci
Avocat, Paris
T +33 14405 5167
E maxime.dangelopetrucci@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Via di Villa Sacchetti, 11, 00197 Rome, Italy

Clifford Chance Studio Legale Associato

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.