

**ADVANT** Altana | Beiten | Nctm

[www.advantlaw.com](http://www.advantlaw.com)

## **CONTENT**

INTRODUCTION	<b>1</b>
CYBERSECURITY THREATS	<b>2</b>
VICTIMS, HACKERS AND AUTHORITIES	<b>3</b>
GDPR AND DATA BREACHES	<b>7</b>
THE ELECTRONIC COMMUNICATIONS CODE AND THE OBLIGATIONS IMPOSED ON PROVIDERS OF PUBLIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES	<b>14</b>
THE NIS DIRECTIVE AND THE OBLIGATIONS OF ESSENTIAL SERVICES OPERATORS AND DIGITAL SERVICES PROVIDERS	<b>20</b>
OTHER RELEVANT REGULATIONS	<b>24</b>

## **1. INTRODUCTION**

The subject of cybersecurity, previously confined to sectoral regulations, has been the focus of European, Italian, French and German lawmakers since around 2018.

The exponential increase in cyberattacks and the acquired awareness of the seriousness of their consequences to the detriment of the State, businesses and people have given a clear acceleration to the production of legislation.

From the GDPR to the European Electronic Communications Code, from the implementation of the NIS Directive to the perimeter of national cybersecurity, cybersecurity obligations now concern an increasingly wide range of subjects.

Let's start then by looking at the data.

## 2. CYBERSECURITY THREATS

According to the ENISA (European Union Agency for Network and Information Security) Threat Landscape 2022 Report, published on 3 November 2022, of the eight cybersecurity threat categories taken into account, ransomware continues to occupy the top positions in the period between July 2021 and July 2022 with regard to both the number of incidents and the volume of extortion.

The ransomware scheme is that of extortion: hackers encrypt the data of an organization and demand payment of a sum of money (usually in cryptocurrency) to restore access to it. In some instances, the attack is not limited to data encryption but also consists of data exfiltration, followed by the threat of disclosing the data to the public if the ransom is not paid.

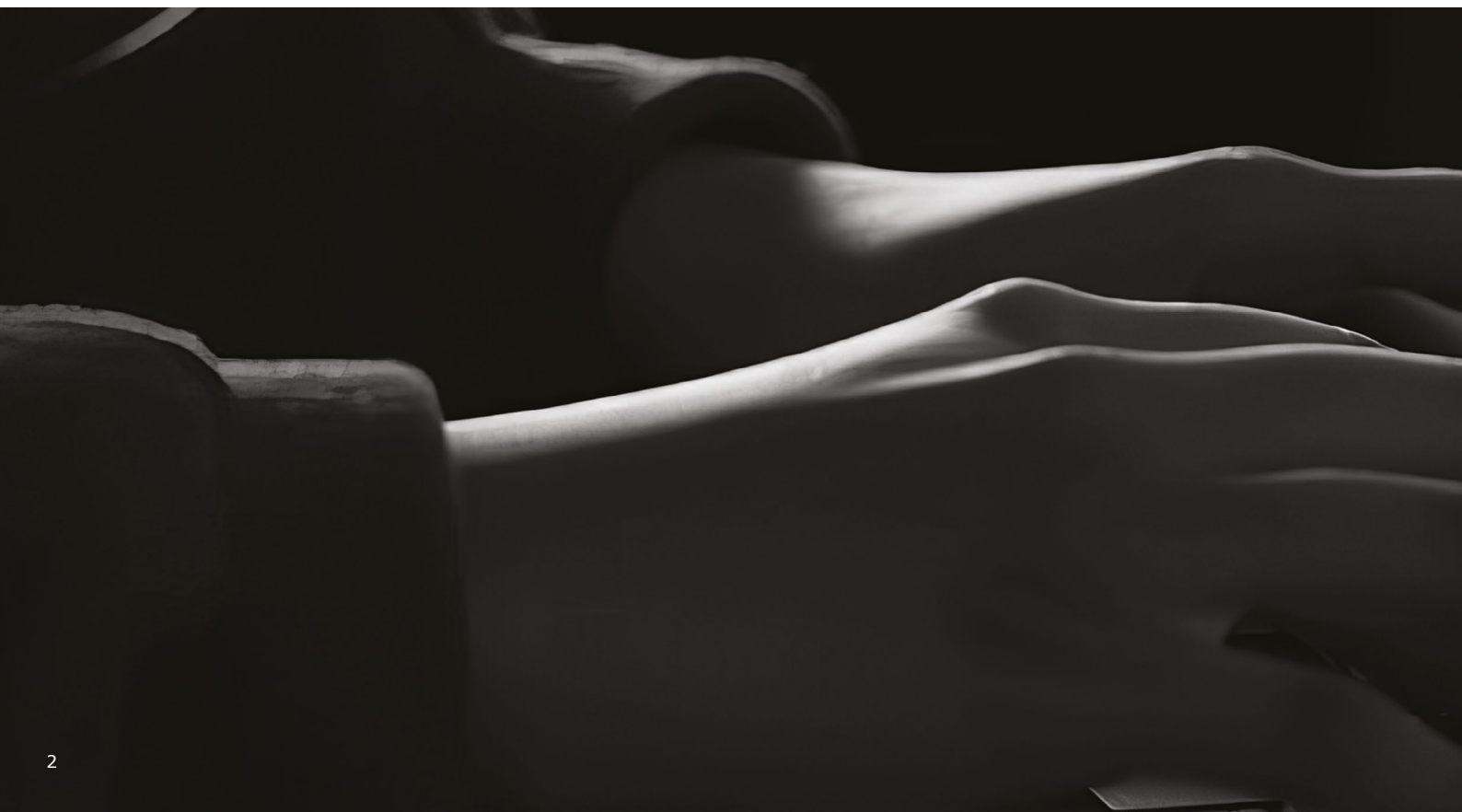
Another category of cybersecurity threats that does not know any setbacks is social engineering. These are attacks conducted mostly via email with which hackers attempt to exploit human error or with the aim of gaining access to information or services. Of these, phishing is the best known. In its simplest version, the hacker, pretending to be someone else, sends an email to the victim asking for information such as credit card numbers or passwords. The most sophisticated phishing technique that is becoming increasingly popular, at least in Italy, is called BEC (Business Email Compromise).

Typically, BEC is carried out in this way: the hacker steals the credentials to access the email account of an employee or a manager of an organization through a normal phishing action; then, pretending to be a senior manager, they ask their employee to make a payment to a certain bank account or, pretending to be a supplier, they ask the client to make the payment due using different bank details than those originally communicated by the legitimate supplier.

The number of malware and DoS (Denial of Service) attacks is also on the rise compared to 2021.

If those mentioned above are the primary cybersecurity threats to businesses generally, for providers of public communications networks and publicly available electronic communications services, security incidents caused by intentional external actions represent a relatively small percentage of the total.

The ENISA Telecom Security Incidents 2021 Annual Report, issued by ENISA on 27 July 2022, shows that, out of the total number of security incidents experienced by telecom operators in 2021, 59% were caused by system failures (mostly hardware failures and software bugs), 23% by human errors, 10% by natural phenomena (such as fires, floods, etc.) and 8% by cyber attacks (which doubled compared to the



### 3. VICTIMS, HACKERS AND AUTHORITIES

When a security incident occurs, there is always a victim.

Potentially, anyone can be a victim of a security incident.

However, as we will see below, some players are more involved than others, either because they operate in industrial sectors that are more exposed to the risk of cyberattacks or because they provide essential services whose failure can even jeopardize national security. From this perspective, according to the ENISA Threat Landscape 2022, the most affected sectors were public administration (24.21%), digital services (13.09%) and the banking and finance sector (8.64%), closely followed by the health sector (7.2%). Interestingly, the number of attacks on individual users has also grown in recent months (12.43%).

Incidents are almost always caused by individuals.

Although - as we have seen - not all security incidents are the result of intentional external actions, hackers certainly represent - at least in the collective imagination - the main protagonists of this phenomenon.

They are individuals or, most of the time, organized groups acting in their own or third parties' interest in order to obtain profits or other illegal advantages. In some cases, the activity of hackers is part of more complex geopolitical strategies of national states, which tolerate or even support their criminal activities. This became evident following the outbreak of the conflict between Russia and Ukraine, during which there was the simultaneous and concerted conduct of cyberattacks and military operations, as well as the spread of the phenomenon of so-called hactivism (i.e. the conduct of cyberattacks for ideological reasons). Last year, the most active hacker groups, in terms of both the number of attacks and the size of ransom demands, were Lockbit, Conti and ALPHV (BlackCat).

On the flip side, besides the police and judicial authorities, responsible for preventing and repressing cybercrime phenomena, there are several state authorities charged in various ways with handling security incidents.



## THE AUTHORITIES INVOLVED IN ITALY

The Italian Data Protection Authority (the **"IDPA"**) is the authority responsible for receiving reports of personal data breaches. It has both inspective and sanctioning powers.

The Italian National Cybersecurity Agency (the **"Italian Agency"**), set up by Law Decree No. 82/2021, is the authority that, inter alia, helps and supports national public and private subjects providing essential services, in preventing and mitigating incidents as well as in restoring systems. The Computer Security Incident Response Team (**"Italian CSIRT"**), the National Evaluation and Certification Centre for technological scrutiny of national strategic digital assets and the National Coordination Centre for cybersecurity in turn operate within the Italian Agency to which cybersecurity functions previously attributed to the Ministry of Enterprise and Made in Italy were recently

transferred. Like the IDPA, the Italian Agency has inspection and sanctioning powers.

The Prime Minister's Office and certain internal bodies such as the Interministerial Committee for Cybersecurity (Comitato Interministeriale per la Cybersicurezza, **"CIC"**) and the Interministerial Committee for the Security of the Republic (Comitato Interministeriale per la Sicurezza della Repubblica, **"CISR"**), the Department of Information for Security (Dipartimento delle Informazioni per la Sicurezza, **"DIS"**) and five Ministries (Ministry of Enterprise and Made in Italy, Ministry of Infrastructure and Sustainable Mobility, Ministry of Economy and Finance, Ministry of Health and Ministry of Environment and Energy Security) acting as NIS authorities are likewise charged with handling security incidents.

## THE AUTHORITIES INVOLVED IN FRANCE

The French Network and Information Security Agency (ANSSI) was created in 2009 and is the national cybersecurity authority. First responder in French cyber space, ANSSI is responsible for preventing (including from a normative perspective) and reacting to IT incidents affecting sensitive institutions. It also organizes crisis exercises at a national level.

The French data protection authority, named "Commission Nationale de l'Informatique et des Libertés (CNIL)" was created by the Data Protection Act of 6 January 1978 ("Loi Informatique et Libertés"). The CNIL is an independent administrative authority (AAI) which is now the French supervisory authority under the GDPR. It has a role of alerting, advising, informing the public, controlling and sanctioning.

The French Ministry for the Armed Forces has a two-fold mission to ensure the protection of the networks underpinning its action and integrating digital warfare into military operations. In order to consolidate the Ministry's work in this field, a cyber defence operational chain of command (COMCYBER), under the orders of the Armed Forces Chief of Staff, was created in early 2017.

Furthermore, the role of France's Ministry of the Interior is to protect from all forms of cybercrime national institutions and interests, economic stakeholders and individuals. To this end it mobilizes specialized central services, the local networks of the national police, national "gendarmerie" and internal security forces. These forces are responsible for investigations aimed at identifying and prosecuting cyber criminals. They also contribute to the prevention and information of the public.

Besides, the ARCEP (Regulation Authority for Electronic Communications, Posts and Press Distribution) was created on January 5, 1997. The ARCEP is an independent administrative authority (AAI). It ensures the regulation of the electronic communications and postal sectors, on behalf of the State but independently of political power and economic stakeholders.

## THE AUTHORITIES INVOLVED IN GERMANY

Germany has a federal system of data protection supervision consisting of **data protection supervisory authorities** at the federal and state levels.

The responsibility of the Federal Commissioner ("**BfDI**") extends, on the one hand, to data protection supervision at federal public bodies. On the other hand, the BfDI supervises data privacy compliance at companies that provide telecommunications or postal services or are subject to the Security Review Act. By contrast, the BfDI is not responsible for the majority of companies in the private sector, as well as for clubs, associations or freelancers, but rather the supervisory authorities in the 16 federal states.

There are a large number of authorities at federal and state level in Germany dealing with cybersecurity. The most important ones are mentioned below:

The tasks of the Federal Office for Information Security ("**BSI**") is defined by the "Act to Strengthen Federal Information Security" ("**BSI Act**"). The objective of the BSI is the preventive promotion of information and cybersecurity in order to enable and advance the secure use of information and communication technology in society. With the support of the BSI, IT security is to be perceived as an important topic in administration,

business and society and implemented independently. The BSI is also responsible for protecting the federal government's IT systems. This involves defending against viruses, Trojans and other technical threats against the federal administration's computers and networks.

The National Cyber Defense Center ("**Cyber-AZ**") is not an independent agency, but represents a joint platform that spans agencies and institutions. It was founded in 2011 as part of the implementation of the German government's Cyber Security Strategy ("**CSS**"). The central task of the Cyber-AZ is to identify IT security incidents at an early stage, assess them quickly and comprehensively, and develop coordinated recommendations for action. This is done on the basis of a holistic approach that brings together the various threats in cyberspace.

In addition to the Federal Ministry of Defense, the following agencies, among others, are involved in the Cyber-AZ: Federal Office for Information Security, Federal Office for the Protection of the Constitution, Federal Office of Civil Protection and Disaster Assistance, Federal Criminal Police Office, Federal Intelligence Service, Federal Police, Customs Criminal Police Office and the Federal Financial Supervisory Authority.







## 4. GDPR AND DATA BREACHES

Article 4(12), of Regulation (EU) 2016/679 (hereinafter, the "GDPR") defines "*personal data breach*" as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

Personal data breaches can therefore be categorized into:

- confidentiality breach, where there is an unauthorized or accidental disclosure of, or access to, personal data;
- availability breach, where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
- integrity breach, where there is an unauthorized or accidental alteration of personal data.

There are two main obligations that the GDPR imposes on a data controller in the event of a personal data breach.

The first, under Article 33(1) of the GDPR, is that of notifying the breach to the competent supervisory authority; the second, under Article 34(1) of the GDPR, is that of communicating the breach to data subjects.

Data breach notification to supervisory authorities is always mandatory, unless the breach is "*unlikely to result in a risk for the rights and freedoms of individuals*".

There is a risk for the rights and freedoms of individuals when the breach is even only potentially capable of causing material or immaterial damage to the data subject.

As concerns the notification timeframe, notification must be made "*without undue delay and, where feasible, within 72 hours after [the controller] having become aware of it*", that is to say, from the time when it is reasonably certain that a security incident resulting in compromising the personal data has occurred. In instances of notifications made after 72 hours, the controller shall be under an obligation to give reasons for the delay. A processor who becomes aware of a breach shall on the other hand notify the controller without undue delay and, therefore, as soon as possible.

As for the form, content and methods of transmission of the notification to the supervisory authority, it is the supervisory authority itself that establishes the relevant requirements, which may also go beyond the minimum requirements set out in the GDPR.

## THE PROCEDURE FOR NOTIFYING DATA BREACHES IN ITALY

In Italy, from 1 July 2021, the notification to the IDPA may be made exclusively via the online procedure available in the IDPA's online services portal and accessible at <https://servizi.gdpd.it/databreach/s/>.

Notification may be made directly by the controller, through a legal representative, or a proxy acting on the controller's behalf, authorized by a power of attorney to act in the procedure in the name and on behalf of the controller.

The notifying person (whose identity is established at the time of accessing the service via SPID (Public Digital Identity System), CIE (Electronic Identity Card) or CNS (National Service Card), or at the time of signing the notification by digital signature) is required to provide a certain amount of information.

The information requested can be classified as follows:

- A) Data of the notifying person;
- B) Type of notification;
- C) Data controller;
- D) Contact details for information relating to the breach;
- E) Any further persons involved in the processing;
- F) Information concerning the breach;
- G) Likely consequences of the breach;
- H) Measures taken to address the breach;
- I) Assessment of risk to data subjects;
- J) Communication of the breach to data subjects;
- K) Other information;
- L) Information on cross-border violations;
- M) Information on breach concerning processing carried out by a controller established outside the European Economic Area.



It should be noted that the rules described above, introduced and fully regulated by the GDPR, now also apply, pursuant to the IDPA's order of 30 July 2019, to personal data breach notification obligations imposed on providers of electronic communication services under Directive 2002/58/EC (so-called "e-Privacy Directive") and the relevant national implementing legislation (Legislative Decree 69/2012, which in turn amended, in that regard, Legislative Decree 196/2003), as well as to communication obligations regarding health records, biometrics, circulation of information in the banking sector and the exchange of personal data between public administrations.

# THE PROCEDURE FOR NOTIFYING DATA BREACHES IN FRANCE

A CNIL teleservice is dedicated solely to data controllers (private or public bodies) wishing to notify the Commission of a breach affecting the personal data they process:

<https://notifications.cnil.fr/notifications/index>

In case of such an event, the organization must inform the CNIL via the teleservice of the following elements:

- a description of the nature of the personal data breach;
- the categories of data;
- the approximate number of people affected by the breach;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer or other point of contact from whom further information can be obtained;
- a description of the likely consequences of the data breach;
- and the measures taken or to be taken to remedy the personal data breach, including measures to mitigate any negative consequences.

Furthermore, in the event of a high risk to the persons concerned, the controller must also inform, in clear and simple terms, the users affected by the breach, unless the controller has taken appropriate technical or organizational measures before or after the breach. If communicating to the persons concerned would require disproportionate efforts, a public communication or other similar equally effective measure may be carried out.

The notification must be sent to the CNIL within 72 hours following the discovery of the data breach.

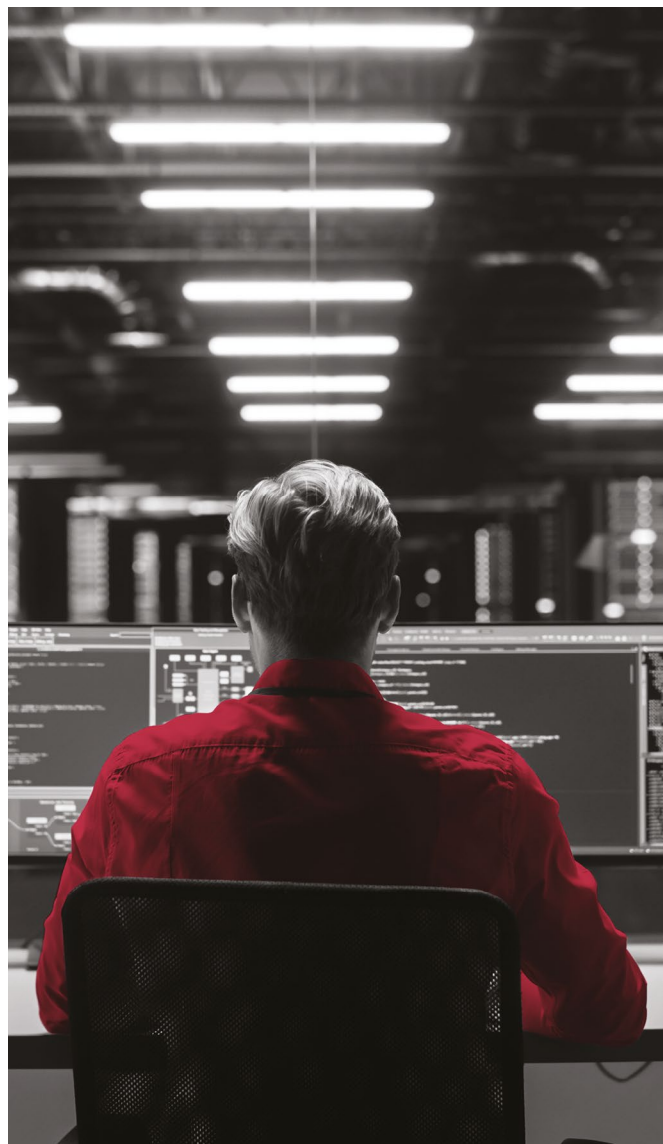
If the data controller is unable to provide all the information required within 72 hours because further investigations are necessary, it is possible to submit a notification in two stages: an initial notification within 72 hours, followed by a supplementary notification as soon as the additional information is available.

The procedure relating to the notified violation may be closed if the CNIL consider that:

- The violation does not affect personal data or does not present a risk for the rights and freedoms of individuals;
- The data controller has correctly informed the persons concerned;
- The data controller has put in place, prior to the breach, appropriate technical protection measures.

The CNIL may require the data controller to inform the persons concerned if:

- The information to the persons concerned has not been made properly;
- The technical protection measures put in place prior to the breach are not appropriate.



# THE PROCEDURE FOR NOTIFYING DATA BREACHES IN GERMANY

In Germany, almost all data protection authorities in the 16 federal states provide online reporting forms on their websites. However, the notification can also be made in another form, e.g., by mail, although online reporting is preferred.

Notification may be made directly by the controller, through a legal representative, or a proxy acting on the controller's behalf, but this depends on the authority concerned.

Article 33 (3) GDPR sets out specific requirements regarding the minimum content of the notification to the supervisory authority. In their notification forms, the data protection authorities of the federal states usually request the following information:

- A) Controller as defined in Art. 4 No. 7 GDPR
- B) The point in time at which the responsible entity or the responsible employee or representative body became aware of the data breach
- C) The time at which the person making the notification became aware of the data breach and, if applicable, the reasons why the notification was not made within 72 hours
- D) Description of the specific incident
- E) Nature of the data breach
- F) Naming of other parties involved
- G) Description of the measures in place to protect the data concerned
- H) Category/ies of data affected
- I) Approximate number of data sets and individuals affected
- J) Description of the possible consequences of the data breach
- K) Description of the measures already taken to remedy the data breach
- L) Name and contact details of the data protection officer or other contact person for further information
- M) Name and contact details of the person making the notification



Communication to data subjects is, on the other hand, mandatory "when the breach of personal data is likely to result in a high risk to the rights and freedoms of natural persons". The risk threshold required for disclosure is therefore higher than that required for notification; not all breaches notified to the supervisory authority therefore need to be communicated to data subjects.

As concerns the timeframe for communication, communication must be made "*without undue delay*", i.e. as soon as possible.

The main purpose of such requirement is to provide data subjects with detailed information as to the measures they can take to protect themselves against any detrimental consequence of a breach.

There are no specific procedures or formalities for making the communication.

Article 34 (2) GDPR requires only that the communication, besides identifying the name and contact details of the Data Protection Officer (DPO) or other contact point, describe, in clear and simple terms, the nature of the personal data breach, the likely consequences of the breach and the measures taken or proposed to be taken to address the breach.

There is, however, no obligation to communicate when:

- the data controller has implemented, in relation to the data breach, appropriate technical and organizational measures, in particular those that render the data unintelligible to anyone who is not authorized to access it (such as encryption or tokenization);
- immediately after the breach, the data controller has taken steps that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize (e.g., the data controller has taken prompt action against the individual who gained unauthorized access to the data before the latter being able to use it); or when
- contacting data subjects would involve a disproportionate effort (e.g., contact information was lost due to the breach); in such case, a public communication or similar measure may be taken.

In consideration of the above, it is clear that the assessment of the existence of a risk (or a high risk), as soon as one becomes aware of a breach, is essential to understand whether to make the notification to the competent supervisory authority and the communication to data subjects as well as, of course, to take effective measures to limit and resolve the breach.

In this regard, the WP29, with its "*Guidelines on Personal data breach notification under Regulation 2016/679 (WP250)*", subsequently adopted by the European Data Protection Board, lists and describes seven risk factors

to consider, referring to the document of December 2013 "*Recommendations for a methodology of the assessment of severity of personal data breaches*" adopted by ENISA, containing a methodology for data breach severity assessment, as a useful tool allowing controllers to prepare an action plan. Such factors include:

- type of breach;
- nature, sensitivity and volume of personal data;
- ease of identification of individuals;
- severity of consequences for individuals;
- special characteristics of the individual;
- special characteristics of the data controller;
- the number of affected individuals.

By way of example, based on the aforementioned guidelines, a cyberattack making a hospital's medical records unavailable for a period of 30 hours should be notified to the supervisory authority and communicated to the data subjects, involving a high risk for the patients' health and privacy.

By contrast, a brief power outage lasting a few minutes at a controller's call centre, preventing customers from calling the controller and accessing their records, would not amount to breach subject to notification or communication.

There is, moreover, a further requirement placed on the data controller in case of breach, regardless of whether or not the breach is notified and communicated to the supervisory authority and to data subjects.

The data controller is indeed required to document any personal data breach, including the circumstances surrounding the breach, its consequences and any remedial action taken. Also in respect of such activity, there are no specific procedures or formalities; in practice, companies have set up a data breach register completed with the above information. This is obviously a tool that allows the controller to demonstrate for accountability purposes (and the supervisory authority to verify) compliance with the applicable legislation.

Finally, a few pieces of statistical information.

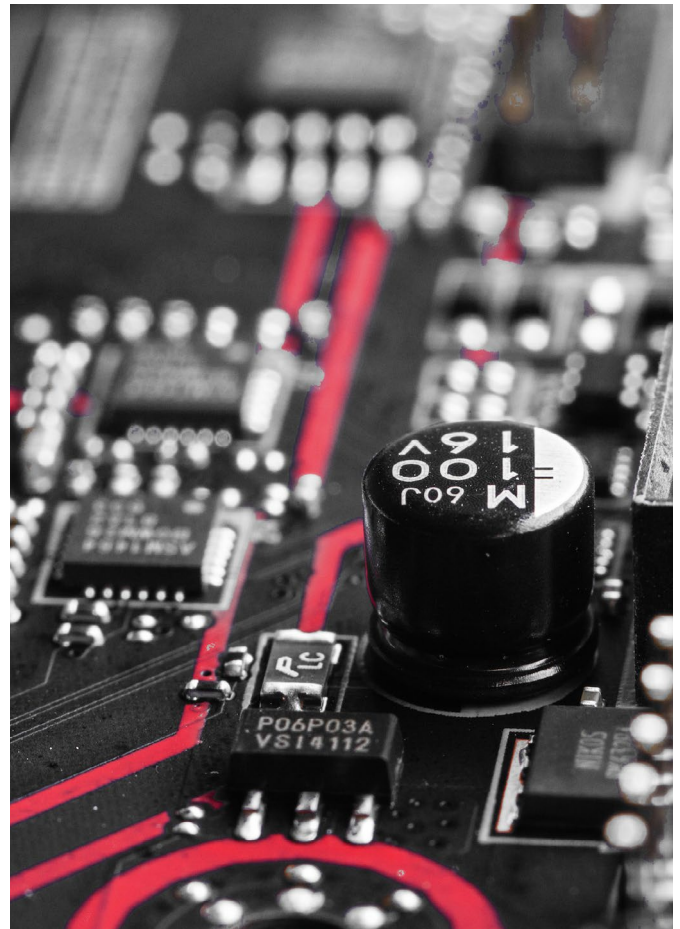
## DATA BREACH NOTIFICATIONS IN ITALY AND SANCTIONS APPLIED

In terms of breaches notified to the IDPA, 1,443 cases were recorded in 2019, 1,387 cases in 2020 and 2,071 in 2021; by contrast, in 2018 there were 650 cases only.

Out of the approximately 60 measures published by the IDPA on the matter in the last year (April 2021-January 2022), almost all of them targeted actions connected with internal incidents (e.g., incidents of erroneous transmission/sharing of data with unauthorized parties), while in the other cases said measures addressed external intentional actions associated with ransomware attacks.

With regard to the type of sanctions applied, the IDPA issued warnings or administrative fines to the persons involved.

Among the highest sanctions, the IDPA sanctioned a credit institution for EUR 1,650,000, not for a specific breach under Articles 33 and 34 of the GDPR, but for its failure to adopt technical and organizational measures capable of ensuring a level of security adequate to the risk, a circumstance that in fact emerged in the course of the IDPA's investigation.



## DATA BREACH NOTIFICATIONS IN FRANCE AND SANCTIONS APPLIED

The CNIL reports 5,037 notifications of breaches received in 2021, compared with 2,821 notifications in 2020. This sharp increase of 79% can be explained by a very strong growth in cyberattacks, especially ransomware attacks, which are the main cyber threat to companies, local authorities and public bodies in France (43% of notifications).

As in previous years, the CNIL mainly receives breach notifications related to a loss of confidentiality of personal data (around 80%). Nearly 3,000 notifications result from hacking, which represents around 59% of notifications.

Regarding sanctions, 2021 was an unprecedented year, both in terms of the number of measures adopted and the cumulative amount of fines. The CNIL issued 135 formal notices and 18 sanctions, for a cumulative

amount of historic fines that exceeded 214 million euros. Twelve of them have been made public.

These 18 sanctions include notably 15 fines (including five with injunctions under penalty) and two calls to order, with injunctions. Among the most frequent breaches are the lack of information of persons and excessive data retention periods. Out of these 18 sanctions, half involve a violation related to the security of personal data. Finally, four sanctions relate to poor management of cookies and other tracers.

Finally, among the 18 sanctions imposed by the CNIL, four were adopted in cooperation with European counterparts, within the framework of the one-stop shop of the GDPR, for example the sanction adopted against Slimpay.

## DATA BREACH NOTIFICATIONS IN GERMANY AND SANCTIONS APPLIED

In 2021, significantly fewer data breaches were reported to the German supervisory authorities pursuant to Article 33 GDPR 2020. While more than 26,000 reports were registered at that time, these only amounted to 13,890 in 2021 (as statistics on reported data breaches were not available from all supervisory authorities this number should also be understood as a lower limit).

Over the course of 2021, 373 fines were imposed by German authorities with a total amount of more than EUR 2.11 million (as not all authorities have commented on the amount of the fines, this figure is also to be understood as a lower limit).

Comparing these figures with those of the previous year, it becomes clear that although the number of German fines has increased, their total amount has decreased notably. The 284 sanctions from 2020 still amounted to more than 48 million euros. It is also remarkable that in 2021, there have been no spectacular decisions from the German supervisory authorities, such as the fines against H&M (EUR 33.5 million) and notebooksbilliger.de (EUR 10.4 million) in 2020.

Most of the fines in 2021 were in the four- or low five-digit range. The most frequently punished violations included the unlawful processing of data (Articles 5 and 6 GDPR), for example through unauthorised video recordings, database queries or transfers to third parties, violations of the obligations to provide information (Articles 12 to 15 GDPR) and inadequate technical and organizational security measures (Article 32 GDPR).



## 5. THE ELECTRONIC COMMUNICATIONS CODE AND THE OBLIGATIONS IMPOSED ON PROVIDERS OF PUBLIC COMMUNICATIONS NETWORKS AND PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES

Certain companies have cybersecurity obligations beyond those imposed on them under the GDPR.

This is the case, for example, of companies providing public communications networks or publicly accessible electronic communications services. These include telecommunications operators, providers of Internet messaging services and of VoIP services and providers of other Internet communications services.

Specific cybersecurity obligations have been provided for these latter by Directive (EU) 2018/1972 (the “**EECC Directive**”).





## THE TRANSPOSITION IN ITALY OF THE EEC DIRECTIVE

In Italy, the EEC Directive has been transposed into Legislative Decree no. 259/2003 (the so called Italian Electronic Communications Code) by Legislative Decree No. 104/2022.

Articles 40 and 41 of Legislative Decree no. 259/2003 provide for two obligations on providers of public communications networks or publicly available electronic communications services.

The first obligation is to take the (technical and organizational) measures identified by the Italian Agency to manage the risks posed to the security of publicly accessible electronic communications networks and services (e.g. the use of encryption technologies). Furthermore, the Italian Agency may issue binding instructions to providers of public communications networks or publicly available electronic communications services to remedy a security incident or prevent one from occurring when a significant threat has been identified.

To date, the Italian Agency has not yet established such measures. Therefore, reference must still be made to the measures set out in Article 4 of Decree of the Ministry of Economic Development (now Ministry of Enterprise and Made in Italy) of 12 December 2018 in relation to critical assets.

The measures identified by the Decree include, in particular:

- definition and updating over time of security policies, approved by the company Management;
- identification of the main risks to the security and integrity of networks and services and definition of the methods for managing them;
- definition of roles and assignment of responsibilities to employees, whose availability in the event of security incidents must be ensured;
- definition (and verification of compliance) of the requirements to be met by services and products provided by third parties and definition of the methods for managing security incidents relating to or caused by third parties and affecting the network or the service provided;
- provision of training courses to staff, rotation of staff with positions of responsibility and definition of

intervention procedures in case of breach of security policies;

- adoption of physical and logical security measures (e.g. procedures for assigning and revoking access rights; authentication mechanisms gauged on the basis of the type of access; protection mechanisms against unauthorized physical access or unexpected events; monitoring and recording of accesses, etc.);
- implementation of protection systems and malware detection systems and adoption of measures to prevent the tampering or alteration of software used in the network and in information systems, as well as the disclosure of critical security data, such as passwords and private keys;
- adoption (and verification of compliance) of operating procedures relating to the operation of critical systems and preparation and updating over time of a database of system configurations to enable their possible recovery, as well as an inventory of critical assets;
- assignment of a technical structure with adequate competence and availability to manage security incidents, as well as adoption of procedures for the detection, management and resolution of incidents;
- development of a contingency plan and adoption of disaster recovery procedures;
- periodic performance of tests, checks and other monitoring activities.

The second obligation is to notify the Italian Agency and the Italian CSIRT of security incidents that are considered significant for the proper functioning of networks and services.

The identification of significant security incidents is the responsibility of the Italian Agency, the law only indicating the parameters that the Italian Agency must consider in order to identify them, namely:

- a) the number of users affected by the security incident;
- b) the duration of the security incident;
- c) the geographical spread of the area affected by the security incident;
- d) the extent of the impact on the operation of the network or service;
- e) the extent of the impact on economic and social activities.

## THE TRANSPOSITION IN ITALY OF THE EEC DIRECTIVE (CONTINUED)

While waiting for the Italian Agency to identify significant security incidents, the criteria set out in Article 5 of the Decree of Ministry of Economic Development (now Ministry of Enterprise and Made in Italy) of 12 December 2018 shall apply, whereby a security incident - meaning "a breach of security or loss of integrity that results in a malfunction of electronic communications networks and services" - is significant when:

- a) its duration exceeds one hour and the percentage of users affected is higher than fifteen percent of the total number of domestic users of the service concerned;
- b) its duration exceeds two hours and the percentage of users affected is higher than ten percent of the total number of domestic users of the service concerned;
- c) its duration exceeds four hours and the percentage of users affected is higher than five percent of the total number of domestic users of the service concerned;
- d) its duration exceeds six hours and the percentage of users affected is higher than two percent of the total number of domestic users of the service concerned;
- e) its duration exceeds eight hours and the percentage of users affected is higher than one per cent of the total number of domestic users of the service concerned.

The communication to the Italian CSIRT exempts the obliged party from the burden of making a separate communication to the Italian Agency, the Italian CSIRT being a body of the Italian Agency. The deadline for notification is 24 hours from the detection of the incident. The notification made within 24 hours must include at least information about:

- a) the service concerned;
- b) the duration of the incident, if concluded, or the estimated conclusion if still ongoing;
- c) the estimated impact on the users of the service concerned expressed as a percentage of the national user base for said service.

In addition, within five days of notification, a report must be submitted which contains:

- a) a description of the incident;
- b) the cause of the incident such as, by way of example only and without limitation, human error, failure, natural phenomenon, malicious action, failure caused by a third party;
- c) the consequences on the service provided;

- d) the infrastructures and systems affected;
- e) the impact on interconnections at national level;
- f) the response actions to mitigate the impact of the incident;
- g) the actions to reduce the risk of recurrence of the incident or similar incidents.

In order to verify compliance with the obligations described above, the Italian Agency may request from network and service providers any and all information necessary for assessing the security of networks and services (in particular, documents relating to security policies), as well as carry out audits and inspections, either directly or through an appointed third party.

Sanctions in case of breach of the obligations described above are quite high.

Failure to comply with security measures shall be punished with an administrative fine between EUR 250,000 and EUR 1,500,000 and failure to report significant security incidents with an administrative fine between EUR 300,000 and EUR 1,800,000. Finally, failure to provide the information necessary to assess security shall be punished with an administrative fine between EUR 200,000 and EUR 1,000,000.

However, sanctions may be reduced by up to one third, taking into account the minor nature of the breach, any efforts made by the party in question to eliminate or mitigate the consequences of the breach, and the economic importance of the operator.

## THE TRANSPOSITION IN FRANCE OF THE EECC DIRECTIVE

Directive (EU) 2018/1972 of December 11, 2018 implementing the European electronic communications code has been transposed into French legislation by Ordinance No. 2021-650 of May 26, 2021 relating to measures for adapting the powers of the Regulatory Authority for Electronic Communications, Posts and Press Distribution.

Indeed the provisions of the transposition ordinance diversify the ARCEPS's means of action for a more agile regulation.

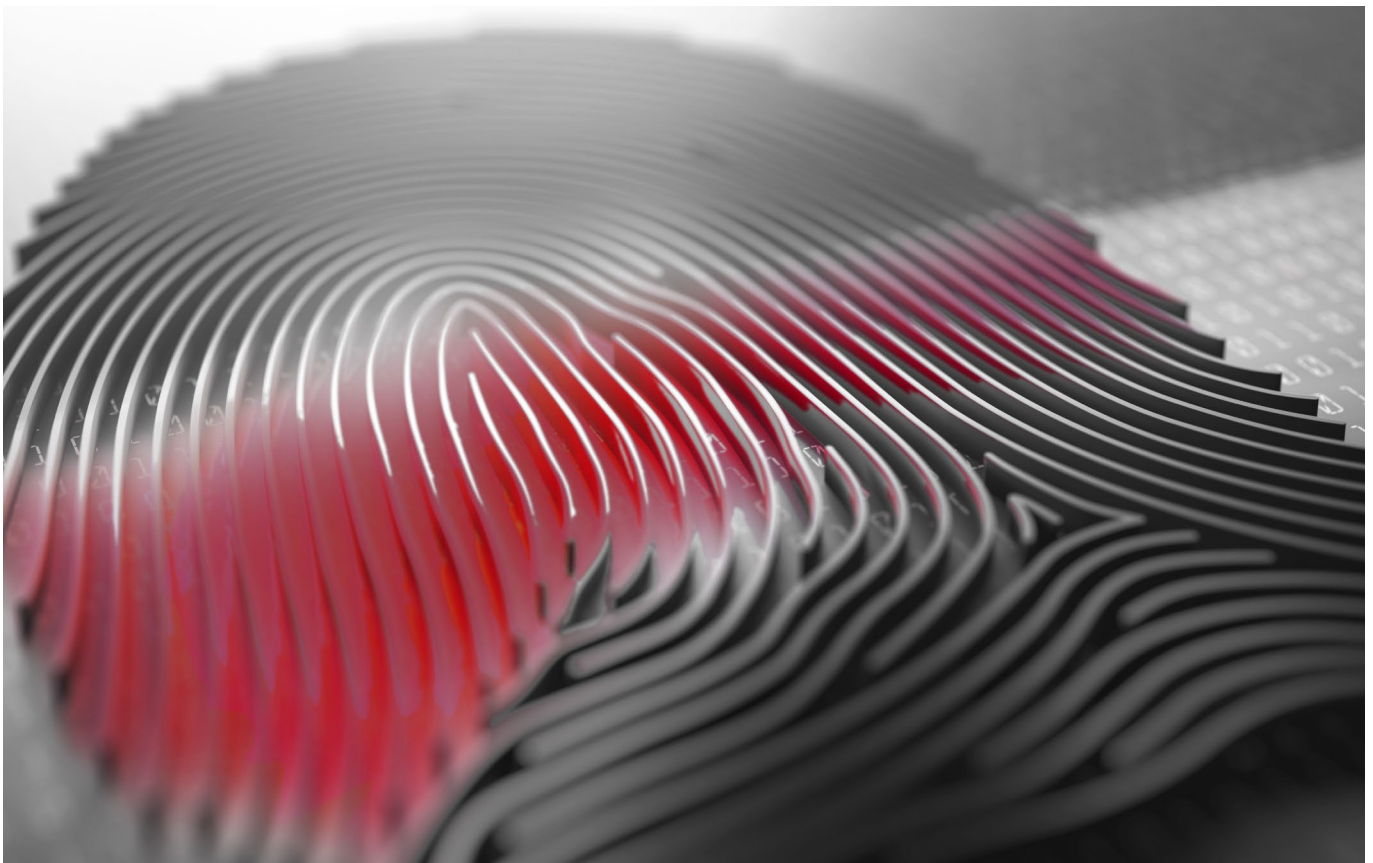
The transposition of the European Electronic Communications Code reinforces the role and action of ARCEP, in particular through consolidated and enriched regulatory tools. For example, Arcep's power to collect information has notably been extended to actors other than operators (other companies active in the electronic communications sector or in sectors closely related to it).

In addition, the transposition ordinance introduces a mechanism allowing operators designated as powerful on a market to submit to the Authority proposals for commitments relating to the conditions of access or co-investment, which the ARCEP can make enforceable.

Article L.33-1 of the Post and Electronic Communications Code (CPCE) provides that the establishment and operation of networks open to the public and the provision of electronic communications services to the public are free, but subject to compliance with notably the rules relating to the permanence, quality, availability, security and integrity of the network and the service, which include obligations to notify the competent authority of security incidents that have had a significant impact on their operation.

Article L39 of the Post and Electronic Communications Code (CPCE) as modified by the ordinance, punishes by one year of imprisonment and a fine of EUR 75,000 the fact of:

- Maintaining a network open to the public in violation of a decision to suspend or withdraw the right to establish such a network;
- Maintaining an electronic communications service in violation of a decision to suspend or withdraw the right to provide the public or to market such a service.



# THE TRANSPOSITION IN GERMANY OF THE EEC DIRECTIVE

In Germany, the EEC Directive was transposed into national law as part of a major amendment to the Telecommunications Act ("TKG"). This was adopted in mid-December 2020.

Pursuant to section 165 (1) TKG, anyone who provides telecommunications services or is involved in providing telecommunications services shall take appropriate technical precautions and other measures to protect

1. the secrecy of telecommunications and
2. against breaches of the protection of personal data.

Pursuant to section 165 (2) TKG, anyone operating a public telecommunications network or providing publicly accessible telecommunications services shall take appropriate technical and organizational precautions and other measures in the telecommunications and data processing systems operated for this purpose

1. to protect against disruptions that lead to significant impairments of telecommunications networks and services, also insofar as these disruptions may be caused by external attacks and the effects of disasters, and
2. to manage the risks to the security of telecommunications networks and services.

The Federal Network Agency may order operators of public telecommunications networks or providers of publicly available telecommunications services to undergo an inspection by a qualified independent body or a competent national authority to determine whether the statutory requirements have been met.

Any person operating a public telecommunications network or providing publicly available telecommunications services shall designate a security officer, appoint a contact person established in the European Union and draw up a security policy stating,

- a) which public telecommunications network is operated and which publicly accessible telecommunications services are provided,
- b) which hazards are to be assumed and
- c) which technical precautions or other protective measures have been taken or are planned.

Anyone who operates a public telecommunications network or provides publicly accessible telecommunications services must immediately notify the Federal Network Agency and the Federal Office for Information Security of a security incident with significant effects pursuant to section 168 TKG.

The extent of the impact of a security incident shall be assessed in particular on the basis of the following criteria:

1. the number of users affected by the security incident,
2. the duration of the security incident,
3. the geographical extent of the area affected by the security incident,
4. the extent of the degradation of the telecommunications network or service,
5. the extent of the impact on economic and social activities.

The notification must contain the following information:


1. details of the security incident,
2. information on the above mentioned criteria,
3. information on the affected systems as well as
4. information on the suspected or actual cause.

In the event of a breach of the protection of personal data pursuant to section 169 TKG, anyone providing publicly accessible telecommunications services shall immediately notify the Federal Network Agency and the Federal Commissioner for Data Protection and Freedom of Information of the breach. If the personal data breach is likely to seriously affect the rights or legitimate interests of end-users or other persons, the provider of the telecommunications service shall also notify the persons concerned of the breach without delay.

Violations of the above-mentioned provisions of the TKG can be punished with fines of between EUR 10,000 and 300,000.



## 6. THE NIS DIRECTIVE AND THE OBLIGATIONS OF ESSENTIAL SERVICES OPERATORS AND DIGITAL SERVICES PROVIDERS



Directive (EU) 2016/1148 on security of network and information systems (the “NIS Directive”) provides for measures for a high common level of security of network and information systems used by essential services operators (“ESOs”) and digital services providers (“DSPs”).

### THE TRANSPOSITION IN ITALY OF THE NIS DIRECTIVE

The NIS Directive has been transposed in Italy by Legislative Decree No. 65/2018.

Under Legislative Decree No. 65/2018, ESOs are those operators that provide a service essential to the maintenance of key social and/or economic activities in the areas of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution as well as digital infrastructure. They are identified by NIS authorities by their own measures. The list with the names of ESOs is kept at the Ministry of Economic Development (now Ministry of Enterprise and Made in Italy) and is updated every two years.

DSPs include entities providing digital e-commerce, cloud computing and search engine services, having their principal place of business, registered office or appointed representative in the national territory. Unlike ESOs, DSPs are not identified by the NIS authorities. The onus is therefore on the company to determine

whether or not it falls within the definition of DSP under Article 3 of Legislative Decree No. 65/2018, i.e. any legal person providing any information society service (i.e. any service normally provided for remuneration, remotely, electronically and at the individual request of a recipient of services) falling within the types set out in Annex III of the decree (online marketplace, online search engine, cloud computing services).

Pursuant to Article 12 of Legislative Decree No. 65/2018, ESOs are required to:

- a) adopt, on the basis of the guidelines prepared by the Cooperation Group (European body composed of representatives of the Member States, the European Commission and ENISA) and any guidelines prepared by the NIS authorities, appropriate and proportionate technical and organizational measures to manage the risks posed to the security of the network and information system they use in their operations;

- b) adopt, again on the basis of the above-mentioned guidelines, appropriate measures to prevent and minimise the impact of incidents on the security of the network and information systems used for the provision of essential services, in order to ensure the continuity of these services;
- c) notify the Italian CSIRT (Computer Security Incident Response Team) of any incidents having a significant impact on the continuity of the essential services they provide.

Similar obligations are provided for by Article 14 of Legislative Decree No. 65/2018 on the part of DSPs, which are required to:

- a) identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services within the Union (taking into account elements such as network and facility security, incident handling, business continuity management, monitoring, audits and testing, and compliance with international standards);
- b) take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services offered within the Union, with a view to ensuring the continuity of such services;
- c) notify the Italian CSIRT of any incident having a substantial impact on the provision of a service offered by them within the Union.

Notifications of the relevant incidents must be made “without undue delay”, according to the terms set out by the Italian CSIRT and, where appropriate, by each sectoral NIS authority according to own guidelines.

Furthermore, any entities that cannot be classified as ESOs or DSPs are entitled to make notifications on a voluntary basis according to the terms of Article 17 of Legislative Decree No. 65/2018.

Finally, both ESOs and DSPs are required to provide the information necessary to assess the security of their network and information systems and to remedy any failure or deficiency identified.

The Italian Agency (which includes the Italian CSIRT, as mentioned above) is the authority responsible for monitoring the application of the NIS Directive, designated by Article 7 of Legislative Decree No. 65/2018 as the national competent NIS authority and single point of contact for network and information systems security. The following authorities (cooperating with the national competent NIS authority) are on the other hand designated as sectoral authorities:

- a) the Ministry of Enterprise and Made in Italy for the digital infrastructure sector, IXP, DNS, TLD sub-sectors, and for digital services;
- b) the Ministry of Infrastructure and Sustainable Mobility, for the transport sector, air, rail and road sub-sectors;
- c) the Ministry of Economy and Finance, for the banking and financial market infrastructure sectors;
- d) the Ministry of Health, for health assistance activities provided by the operators employed, appointed or entrusted by, or having an agreement with, the same, and the Regions and the Autonomous Provinces of Trento and Bolzano, either directly or through the competent local health authorities, for health assistance activities provided by operators authorised and accredited by the Regions or Autonomous Provinces in the respective local areas of competence;
- e) the Ministry of Environment and Energy Security for the energy sector, electricity, gas and oil subsectors; and
- f) the Ministry of Environment and Energy Security and the Regions and the Autonomous Provinces of Trento and Bolzano, either directly or through the competent local authorities, for the drinking water supply and distribution sector.

In case of non-compliance with the obligations under the NIS Directive, administrative sanctions of up to EUR 150,000 shall apply, to be imposed by the competent national NIS authority.

## THE TRANSPOSITION IN FRANCE OF THE NIS DIRECTIVE

Law No. 2018-133 of February 26, 2018 about the security of networks and information systems, published in the Official Journal on Tuesday February 27, 2018 transposes the NIS directive.

It incorporates into French law the two new categories developed by the NIS directive:

Essential Service Operators (ESO): the law provides that operators will be appointed in France by the Prime Minister, in various sectors such as Energy, Transport, Banking, Financial Market Infrastructures, etc. (see application decree below) and that this list will be updated every two years.

The ESOs must take technical measures in order to manage the risks threatening the security of the networks upstream, to prevent incidents compromising security and to ensure that they notify the ANSSI of incidents having a significant impact on network security.

Digital Service Providers (DSPs): DSPs are subject to obligations similar to those of ESOs.

DSPs that employ at least 50 employees and have more than ten million euros in annual turnover must guarantee a satisfactory level of security for information systems by identifying risks to avoid incidents and implement preventive measures. DSPs must also notify ANSSI of network security incidents that have a significant impact on the provision of the service they provide.

Decree No. 2018-384 of May 23, 2018 relating to the security of networks and information systems of essential services operators and digital service providers, establishes the list of services essential to the functioning of French society and economy.

A fine of EUR 100,000 is imposed if the ESOs managers fail to comply with the safety rules upon issuance of the deadline set by a formal notice.

A fine of EUR 75,000 is imposed if the ESOs managers fail to comply with the obligation to report an incident. A fine of EUR 125,000 is imposed if the ESOs managers obstruct the control operations carried by the ANSSI.





## THE TRANSPOSITION IN GERMANY OF THE NIS DIRECTIVE

The act on the implementation of the NIS Directive was promulgated on 29 June 2017.

In Germany, a uniform legal framework for cooperation between the state and companies for more cybersecurity in critical infrastructures (CRITIS) has already existed since July 2015 with the IT Security Act. This requires CRITIS operators to implement IT security according to the "state of the art" and to report significant IT security incidents to the Federal Office for Information Security ("**BSI**"). The law to implement the NIS Directive expands the BSI's supervisory and enforcement powers vis-à-vis CRITIS operators.

The only completely new regulations to be created in Germany were those for digital service providers. The regulations were implemented in the BSI Act.

Operators of critical infrastructure are obliged to take appropriate organizational and technical precautions to prevent disruptions to the availability, integrity, authenticity and confidentiality of their information

technology systems, components or processes that are essential to the functioning of the critical infrastructures they operate. The BSI can check the operator of critical infrastructures for compliance with the requirements.

Digital service providers shall take appropriate and proportionate technical and organizational measures to manage risks to the security of the network and information systems they use to provide digital services. The providers shall report any security incident that has a significant impact on the provision of a digital service they provide within the European Union to the BSI without delay.

In the event of violations of the BSI Act requirements, the BSI can impose fines of up to EUR 2 million.

Remarkably, in light of some critical issues that have emerged in these first years of implementation of the NIS Directive, on 16 December 2020 the European Commission presented a proposal for its revision (called the NIS 2 Directive) on which provisional agreement was reached between the European Council and the European Parliament on 13 May 2022. The European Parliament approved the text of the directive at its sitting on 10 November 2022. The NIS 2 Directive provides, *inter alia*, for: notification of major accidents within 24 hours; the broadening of the scope of the Directive to cover medical device manufacturers, waste management operators and postal and courier services operators; identification of ESOs directly by the Directive and not by Member States; obligation on Member States to impose administrative fines, in any event increased up to €10 million or 2% of the total worldwide annual turnover of the undertaking concerned.

## 7. OTHER RELEVANT REGULATIONS

In addition to European-derived regulations, there are a number of other national regulations that govern aspects relevant to cybersecurity. Below are the most relevant ones for each country.

### THE ITALIAN NATIONAL CYBERSECURITY PERIMETER

The national cybersecurity perimeter was established by Article 1 (1) of Decree Law No. 105/2019 *"in order to ensure a high level of security of the networks, information systems and IT services of public administrations, public and private bodies and operators headquartered in the national territory, that are instrumental to the exercise of essential functions of the State, or the provision of a service essential for the maintenance of civil, social or economic activities that are fundamental to the interests of the State, and whose malfunctioning, interruption, whether partial or not, or improper use, could be prejudicial to national security"*.

Decree Law No. 105/2019 delegates to subsequent Decrees of the President of the Council of Ministers the function of defining:

- a) the criteria and methods for identifying the entities included in the national cybersecurity perimeter and the rules governing the obligations resulting from the inclusion in the national security perimeter;
- b) the procedures for reporting incidents occurring on networks, information systems and IT systems included in the perimeter and the relevant security measures;
- c) the procedures, methods and deadlines to be complied with by public administrations, national bodies and operators, both public and private, included in the national cybersecurity perimeter, planning to award contracts for the supply of ICT goods, systems and services to be used on the networks, information systems and for the performance of the IT services identified in the list sent to the Presidency of the Council of Ministers and the Ministry of Enterprise and Made in Italy.

Moreover, Decree Law No. 105/2019 identifies the tasks of the National Assessment and Certification Centre (Centro di Valutazione e Certificazione Nazionale, "CVCN"), with reference to the procurement

of ICT products, processes, services and associated infrastructure - if intended for networks, information systems, IT systems included in the national cybersecurity perimeter. The CVCN is entrusted with the task of ensuring security (and the absence of vulnerabilities) of products, hardware and software intended to be used in networks, information systems and IT services of the entities included in the perimeter.

Moving on to the analysis of the implementing decrees, Decree of the President of the Council of Ministers No. 131 of 30 July 2020 (the so-called **"DPCM 1"**) laid down the criteria and procedural methods for the identification of the entities included in the national cybersecurity perimeter and defined the criteria for the preparation and updating of the list of the networks, information systems and IT services relevant to them.

The entities included in the perimeter are identified in Article 2 of DPCM 1, which distinguishes between entities exercising "essential functions" of the State and entities exercising "essential services" for the maintenance of civil, social or economic activities fundamental to the interests of the State.

The first category includes all those entities entrusted by law with tasks aimed at ensuring continuity of government action and of constitutional bodies, internal and external security and defence of the State, international relations, security and public order, administration of justice and functionality of economic, financial and transport systems.

The second category includes those (public or private) entities carrying out: activities instrumental to the exercise of essential State functions; activities necessary for the exercise and enjoyment of fundamental rights; activities necessary for the continuity of supplies and the efficiency of infrastructures and logistics: research activities and activities relating to production environments in the field of high technology and in any



other sector, where they are of economic and social importance, also for the purposes of ensuring national strategic autonomy, competitiveness and development of the national economic system.

Article 3 defines the sectors of activity included in the perimeter: priority is given to entities operating in the government sector, which concerns the activities of the CISR (Interministerial Committee for the Security of the Republic) administrations; it also includes other entities engaged in activities related to the interior, defence, space and aerospace, energy, telecommunications, economy and finance, transport, digital services, critical technologies, and social security/labor institutions.

The list of entities included in the perimeter is contained in an administrative act, adopted at the proposal of the CISR by the President of the Council of Ministers.

On the other hand, Decree of the President of the Council of Ministers No. 81 of 14 April 2021 (the so-called **"DPCM 2"**) defines the modalities for the notification of incidents affecting networks, information systems and IT services related to the national cybersecurity perimeter.

In particular, Article 2 of DPCM 2 provides for the obligation, for entities included in the perimeter, to notify security incidents affecting their ICT goods.

The taxonomy of incidents is provided by Tables 1 and 2 of Annex "A" to DPCM 2, which classify events on the basis of their severity. Less serious incidents are listed in Table 1, and can be classified in the following categories: (i) infection; (ii) failure; (iii) installation; (iv) lateral movements; (v) actions on targets, including cases of unauthorized exfiltration of data. The most serious cases are instead identified by Table 2, which identifies the following categories: (i) "actions on targets", which include cases of inhibition of response functions, impairment of control processes and intentional disservice; (ii) "disservice", which includes

cases of breach of the expected service level, defined by the entity included in the cybersecurity perimeter pursuant to the provisions of the security measures contained in Annex B, especially in terms of availability of ICT goods, as well as cases of breach of corrupted data or execution of corrupted operations through the ICT good and unauthorized disclosure of digital data related to ICT goods.

Said distinction is functional to the different timing established by DPCM 2 for fulfilling the notification obligation: incidents indicated in Table 1 must be notified to the Italian CSIRT within six hours, whereas most serious incidents - indicated in Table 2 - must be notified within one hour, starting from the moment in which the entities included in the Perimeter became aware thereof, including by means of monitoring, testing and control activities.

Notification to the Italian CSIRT shall be made through appropriate communication channels, in the ways published on the Italian CSIRT website. At the specific request of the Italian CSIRT, the entity included in the perimeter shall update the notification within six hours of such request.

Once the plans for the implementation of the activities to restore ICT goods affected by the notified incident have been defined, the entity included in the perimeter that made the notification shall promptly notify the Italian CSIRT and shall submit, at Italian CSIRT's request and within 30 days, a technical report illustrating the significant elements of the incident, including the consequences of the impact of the incident on ICT goods and the remedial actions taken, unless the relevant judicial authority has previously communicated the existence of specific investigation secrecy requirements.

## THE ITALIAN NATIONAL CYBERSECURITY PERIMETER (CONTINUED)

Entities included in the perimeter may also notify, on a voluntary basis, incidents relating to ICT goods not included in the tables under Annex A or incidents included in said tables but relating to non-ICT networks and systems.

The body in charge of managing notifications received by the Italian CSIRT is the Security Intelligence Department (Dipartimento delle informazioni per la sicurezza - DIS), which forwards them to the competent authorities (to the office of the Ministry of the Interior in charge of security and regularity of telecommunication services; to the department of the Presidency of the Council of Ministers in charge of technological innovation and digitalization, if notifications come from a public entity; to the Ministry of Enterprise and Made in Italy, if notifications come from a private entity; to the competent NIS Authority if the notification is made by entities falling within the scope of the NIS legislation).

With regard to the notification of incidents, we would like to point out that Article 37-*quater* of Decree Law No. 115/2022 (the so-called *Aids bis* Decree) extended the scope of the notification obligation to incidents occurring on networks, information systems and IT services that are outside the perimeter (i.e., other than ICT assets), but pertaining to entities included in the perimeter. In this case, notification must be made within 72 hours. The taxonomy of incidents and any specific notification modalities will be determined by the Deputy Director General of the Italian Agency.

DPCM 2 also identifies the security measures that entities included in the perimeter are required to adopt with respect to the relevant ICT goods and services.

Said measures are listed in Annex B to DPCM 2, with respect to the categories identified by Decree Law No. 105/2019, and must be implemented according to a specific timeline. At each update of the list of ICT goods, entities included in the perimeter shall adjust the security measures, with the same timing provided for the first adoption.

The third decree implementing the Decree Law establishing the security perimeter is the DPCM of 15 June 2021 (the so-called "**DPCM 3**") which, together with Presidential Decree No. 54 of 5 February 2021, identifies the categories of ICT goods, systems and services to be used in the national cybersecurity perimeter and the methods and procedures relating to the functioning of the CVCN.

In particular, DPCM 3 defines the procedures, methods and deadlines to be complied with by public administrations, national bodies and operators, both public and private, included in the perimeter of national cybersecurity, planning to award contracts for the supply of ICT goods, systems and services, intended to be used on networks, information systems and for the performance of IT services identified in the list sent to the Presidency of the Council of Ministers and the Ministry of Enterprise and Made in Italy.

Of significant importance is the obligation for entities included in the cybersecurity perimeter to notify the CVCN of their intention to initiate procurement procedures in relation to such ICT goods, systems and services.

DPCM 3 identifies, on the basis of the technical criteria set out in Article 13 of Presidential Decree 54/2021, four categories of ICT goods, systems and services subject to prior assessment by the CVCN, namely (i) hardware and software components providing telecommunications network functionalities and services (access, transport, switching); (ii) hardware and software components providing functionalities for the security of telecommunications networks and the data processed by them; (iii) hardware and software components for the acquisition of data, monitoring, supervision, control, implementation and automation of telecommunications networks and industrial and infrastructure systems; (iv) software applications for the implementation of security mechanisms.

The same DPCM provides that the categories identified be updated at least once a year by decree of the President of the Council of Ministers, taking into account technological innovation and changes in technical criteria.

Lastly, the DPCM of 18 May 2022 (the so-called "**DPCM 4**") was issued, which establishes the procedures, requirements and terms for the authorization of accredited testing laboratories (the so-called LAPs) to support the CVCN in carrying out technology assessment activities on specific categories of ICT assets used within the perimeter. Worthy of note is the obligation for CVCNs, LAPs and CVs to notify the Italian CSIRT within 6 hours (and provide timely updates) of incidents on the networks, information systems and IT services pertinent to the performance of the functions covered by the accreditation, in terms of compromising the integrity or confidentiality of the data and information processed.

## OTHER RELEVANT REGULATIONS IN FRANCE

Law n°2013-1168, 18 Dec. 2013 relating to military programming for the years 2014 to 2019 has put in place various mechanisms in terms of cybersecurity. First of all, in terms of State organization, the responsibility of the Prime Minister in terms of coordination and the recognition of ANSSI as a national defense authority have been confirmed.

Then the operators of vital importance (OIV) are subject to specific safety rules as well as audits and controls. In the event of an incident, the OIVs have an obligation to notify and must follow the technical requirements of ANSSI. The ANSSI can, in the event of a cyberattack, access the information system, collect useful data and even neutralize the attack.

This law has also increased the means of information by authorizing specially designated agents to access identity and connection data held by operators for geolocation purposes.

This law has been followed by law n° 2018-607 of July 13, 2018 relating to military programming for the years 2019 to 2025.

Article 34 of Law No. 2018-607 amends several articles of the Post and Electronic Communications Code (CPCE) and the Defense Code in order to strengthen the capabilities for detecting, characterizing and preventing cyberattacks. In particular, this law grants more resources to ANSSI and mandates close collaboration between ANSSI and electronic communication operators.

Article L.33-14 al.1 to 4 of the Post and Electronic Communications Code (CPCE) regulates the possibility for electronic communications operators (OCE) to have supervision capabilities and to implement event detection devices likely to affect the security of their subscribers' information systems and allows ANSSI to rely on these capabilities.

Article L. 2321-2-1 of the Defense Code authorizes ANSSI to deploy, for threat characterization purposes, a detection device on the network of an electronic communications operator, or on the information system of an access provider or a host.

Articles L. 33-14 al.5 of the CPCE allows ANSSI to rely on the OCEs to transmit messages reporting vulnerability or suspicion of compromise to their subscribers.

Furthermore in France, the means of cryptology are subject to specific regulations. The use of a means of cryptology is free. On the other hand, the supply, import, intra-community transfer and export of a means of cryptology are subject, with some exceptions, to a declaration or an authorization request. These steps are the responsibility of the supplier of the cryptology means and must be carried out with the ANSSI. The applicable regime (declaration or authorization request) depends on the technical functionalities of the means and the planned commercial operation (supply, import, etc.).

## OTHER RELEVANT REGULATIONS IN GERMANY

In Germany, the police forces of the federal states are initially responsible for prosecuting and combating cybercrime. This stems from the **federal structure** of Germany. This means that on a basic level all 16 federal states are responsible themselves and independently for the implementation of cybersecurity issues. It should come as no surprise that this structure may well cause problems in terms of competence and cooperation with other authorities, especially when it comes to cross-state issues.

The structure in one federal state is to be exemplified by the federal state of Baden-Württemberg.

The Cyber Security Agency Baden-Württemberg ("**CSBW**") is the core of the state's new cybersecurity architecture. The CSBW was founded with the promulgation of the law to improve cybersecurity in Baden-Württemberg. A key objective is to protect the state's information technology by strategically managing and monitoring state-wide security measures.

The CSBW is a higher state authority, meaning it has state-wide responsibility and is the central coordination and reporting office in the area of cybersecurity in Baden-Württemberg. It constantly collects data on security vulnerabilities, malware, and attacks or attempted attacks on cybersecurity. For this purpose, it also accepts reports directly from those affected. It documents everything relevant and evaluates the data. The CSBW uses the situation report to inform other authorities. It also issues explicit warnings in the event of particular dangers. In addition, the CSBW networks the state, administrations, municipalities, business, science and research in the area of cybersecurity as well as all relevant cybersecurity organizations in the country, such as law enforcement agencies, security institutions, etc. For state authorities and organizations connected to the state administrative network, the CSBW can also issue orders and take measures to protect them.

In the event of cyberattacks or other incidents, the CSBW can assist authorities, cities and municipalities, in the recovery of systems after an attack. In justified individual cases, other organizations with important significance for the public community can also receive assistance.

Citizens as well as persons in the fields of business, science and administration are sensitized by the CSBW on the topic of cybersecurity. However, the CSBW does not perform police tasks such as law enforcement.

As the central office of the German police, the Federal Criminal Police Office ("**Bundeskriminalamt**" or "**BKA**") also assumes coordinating tasks in the area of combating cybercrime, provides information and tools and is the hub of international cooperation. Furthermore, the BKA conducts investigations in the area of cybercrime within the scope of its original competences, if, for example, federal authorities or institutions or security-sensitive agencies of vital institutions are affected or the BKA is commissioned with the investigations (section 4 BKAG). The Cybercrime Division at the BKA is primarily responsible for fulfilling these tasks.

**YOUR CYBER ADVANTAGE:**  
A MULTI-NATIONAL, MULTI-DISCIPLINARY TEAM

**A DEDICATED TEAM**



**Mickaël  
d'Allende**  
Partner  
**ADVANT Altana**



**Valérie  
Lafarge-Sarkozy**  
Partner  
**ADVANT Altana**



**Jean-Guy  
de Ruffray**  
Partner  
**ADVANT Altana**



**Philippe  
Goossens**  
Partner  
**ADVANT Altana**



**Susanne  
Klein**  
Partner  
**ADVANT Beiten**



**Dr. Andreas  
Lober**  
Partner  
**ADVANT Beiten**



**Dr. Gerald Peter  
Müller-Machwirth**  
Partner  
**ADVANT Beiten**



**Dr. Jochen  
Pörtge**  
Partner  
**ADVANT Beiten**



**Paolo  
Gallarati**  
Partner  
**ADVANT Nctm**



**Michele  
Bignami**  
Partner  
**ADVANT Nctm**



**Roberta  
Guaineri**  
Of Counsel  
**ADVANT Nctm**



**Giulio  
Uras**  
Counsel  
**ADVANT Nctm**

# ADVANT

Your European advantage



[www.advantlaw.com](http://www.advantlaw.com)

[ADVANT-ALTANA.COM](http://ADVANT-ALTANA.COM) | [ADVANT-BEITEN.COM](http://ADVANT-BEITEN.COM) | [ADVANT-NCTM.COM](http://ADVANT-NCTM.COM)

ADVANT member firm offices: BEIJING | BERLIN | BRUSSELS | DUSSELDORF | FRANKFURT  
FREIBURG | GENOA | HAMBURG | LONDON | MILAN | MOSCOW | MUNICH | PARIS | ROME | SHANGHAI