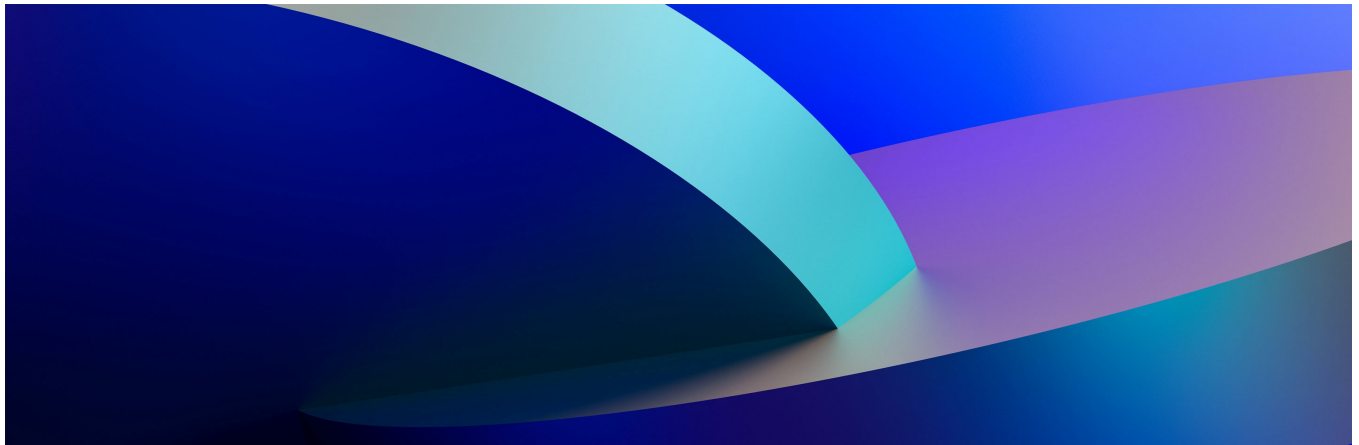




Data protection and cybersecurity laws in Portugal

Data protection

1. Local data protection laws and scope

In addition to the GDPR, the Portuguese legal framework comprises specific local legislation on data protection, namely:

- **Law no. 58/2019 of 8 August**, Portuguese Data Protection Law on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (transposing Directive 2016/679 of the European Parliament and of the Council of 27 April 2016);
- **Law no. 59/2019 of 8 August**, which approves the rules on the processing of personal data for prevention purposes, detection, investigation or prosecution of criminal offences or the enforcement of penalties (transposed Directive (EU) 2016/680 of the European Parliament and the Council, of 27 April 2016);
- **Law no. 41/2004 of 18 August**, amended by the Law no. 46/2012 of 29 August, concerning the processing of personal data and privacy in electronic communications sector (Directive 2002/58/EC on privacy and electronic communications);
- **Law no. 32/2008 of 17 July**, concerning the retention of data generated or processed in the context of electronic communications services (Directive 2006/24/EC);

The Portuguese framework also comprises a set of legal diplomas that foresee multiple legal provisions regarding data protection, such as:

- **Constitution of the Portuguese Republic**, sets forth the main principles and fundamental rights regarding privacy and data protection;
- **Law no. 7/2009 of 12 February**, (Portuguese Labour Code), that includes provisions on data protection regarding employees;
- **Law no. 34/2013 of 16 May**, regarding the use of video surveillance systems by private security entities and auto protection;
- **Law no. 1/2005 of 10 January**, which establishes the provisions concerning the use of video surveillance means by public authorities in public places;

- **Decree-Law no. 207/2005 of 29 November** , on electronic surveillance used by public authorities in traffic control.
- **Regulation no. 798/2018**, approved by the Portuguese Data Protection Authority regarding the List of Personal Data Processing Activities subject to Data Protection Impact Assessment.
- **Decree-law no. 2/2025 of 23 January** , which executes the Data Governance Act (Regulation (EU) 2022/868).

2. Data protection authority

Comissão Nacional de Proteção de Dados (CNPd) <https://www.cnpd.pt/>

3. Anticipated changes to local laws

Policy bodies have not announced upcoming changes, however given the recently approved Data Act, Data Governance Act and the AI Act, future amendments may take place.

4. Sanctions & non-compliance

Administrative sanctions:

The CNPD under the current law has administrative supervision and enforcement powers. According to Portuguese Law, the CNPD has the power to impose administrative.

- Accordingly, administrative fines set forth in Law 58/2019, sanctions against data controllers and data processor, thus, against the company, and will mostly depend on the seriousness of the considered offence, as such:
 - Very serious administrative offences:
 - From EUR 5,000 to EUR 20,000.00 or 4% of annual worldwide turnover, depending on the whichever is higher, being a large company;
 - From EUR 2,000 to EUR 2m or 4% of annual worldwide turnover, as appropriate. Whichever is higher, in the case of SMEs;
 - from EUR 1,000 to EUR 500,000 in the case of natural persons.
 - Serious administrative offences:
 - From EUR 2,500 to EUR 10,000.00 or 2% of the annual worldwide turnover according to whichever is higher, being a large company;
 - From EUR 1,000 to EUR 1m or 2% of annual worldwide turnover, as appropriate whichever is higher, in the case of SMEs;
 - From EUR 500 to EUR 250,000 in the case of natural persons.
- Further to the above, Law no. 41/2004, of 18 August (Processing of personal data and privacy in electronic communications sector) also penalises the breach of data protection-related duties and obligations, establishing the corresponding penalties for (i) serious administrative offences between EUR 1,500 to EUR 25,000 when committed by natural persons; or between EUR 5,000 to EUR 5m when committed by legal persons; and (ii) very serious administrative offences from EUR 500 to EUR 20,000 when committed by natural persons; or EUR 2,500 to EUR 2.5bn when committed by legal persons.
- Law no. 32/2008, of 8 August (retention of data generated or processed in the context of electronic communications services), administrative offenses will be (i) from EUR 1,500 to EUR 50,000 when committed by natural persons; and (ii) from EUR 5,000 to EUR 10m, when committed by legal persons.

Criminal sanctions:

Law no. 58/2019, of 8 August encompasses the following administrative sanctions:

- Incompatible use of data with the purpose of processing: subject to prison sentence of up to one year or a fine of up to 120 days;
- Inappropriate access: subject to imprisonment of up to one year or a fine of up to 120 days;
- iii. Misappropriation of data: subject to imprisonment of up to one year or a fine of up to 120 days;
- Tampering or destruction of data: subject to a prison sentence of up to two years or a fine of up to 240 days;
- Falsifying data: subject to a prison sentence of up to two years or a fine of up to 240 days;
- Breach of confidentiality: subject to imprisonment of up to one year or a fine of up to 120 days;
- Disobedience: subject to imprisonment of up to one year or a fine of up to 120 days.

Additionally, Law no. 32/2008, of 8 August (retention of data generated or processed in the context of electronic communications services), establishes that crimes related to the violation of the security of personal data, non-blocking of data or the access by unauthorised persons in punishable with imprisonment of up to two years or a fine of up to 240 days. This penalty may be doubled if the action is premeditated.

5. Registration / notification / authorisation

With the application of the GDPR there is no obligation to notify the CNPD as a legal requirement to begin processing activities/operations. Hence, data controllers may carry out processing activities without the need of a prior authorisation and/or inform/registry before the CNPD.

6. Main obligations and processing requirements

There are no substantive derogations from the GDPR.

7. Data subject rights

There are no substantive derogations from the GDPR. Notwithstanding the Portuguese Law sets specific provisions regarding the processing of genetic, biometric, and health data, accordingly:

- The Portuguese Law permits access to genetic, biometric, and health data only on a need to know basis in line with 29(1) of the Law no. 58/2019. Specifying they only a professional bound by secrecy or another person bound by a duty of secrecy or confidentiality may process personal data based on GDPR Articles 9(2)(h) and (i) (see GDPR Exceptions Permitting Processing). The person carrying out the processing must guarantee appropriate information security measures. (Article 29(2), Portuguese Law.);
- In addition, the Portuguese Law also binds individuals who access health-related data (controllers, workers and service providers, DPOs, researchers and healthcare providers) for healthcare monitoring or funding activities, to a duty of confidentiality and secrecy;
- Further to this, employers may only process this data for either: (i) attendance control, and (ii) controlling and/or limiting entrances to the employers' premises, in line with Article 28(6) Law no. 58/2019.

8. Processing by third parties

There are no substantive derogations from the GDPR.

9. Transfers out of country

There are no substantive derogations from the GDPR.

10. Data Protection Officer

Pursuant to Portuguese Data Protection Law (Law no. 58/2019, of 8 August), the designation of data

protection officers in public authorities is mandatory.

Additionally, it states the designation of Data Protection Officers in private entities is mandatory when the data controller and the data processor shall appoint a data protection officer whenever the principal private activity involves:

- Processing operations which require regular and systematic control of large-scale data subjects, because of their nature, scope and or purpose; or
- Large-scale processing of special categories of data according to Article 9 of the GDPR, or personal data related to criminal and offense convictions under Article 10 of the GDPR.

11. Security

The GDPR clearly provides that data controllers and data processors must implement appropriate technical and organisational measures to safeguard the data processing risks. Data controllers and data processors should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.

More recently, the CNPD adopted a Guidance (2023/1) on organisational and security measures applicable to the processing of personal data, and which, clarifies that controllers adapting their business or public management models and their technical and organisational means to ensure effective compliance with the law and due protection of personal data and the interests, rights and freedoms of data subjects, namely through the following measures:

- Regularly evaluating processing operations and the impact that technologies have on the functioning of their organisations and, in the case of their organisations and, in the case of personal data, the risks to the rights and freedoms of individuals. of natural persons;
- The controller must have an internal policy in place to detect and manage security incidents with an impact on the protection of personal data and, when data processing is processing is carried out by subcontractors, have effective control mechanisms in place regarding the actions of subcontractors, ensuring that they do not jeopardise the fulfilment of the controller's obligations in this area. in this area.
- Further to the above, the following organizational measures must be implemented:
 - define and regularly exercise the incident response and disaster recovery plan, providing for the necessary mechanisms to guarantee information security and the resilience of resilience of systems and services, as well as ensuring that data availability is re-established after an incident;
 - analysis procedures for monitoring network traffic flows;
 - define secure password management policies, imposing requirements for the size, composition, storage and frequency with which a password needs to be changed;
 - create a user lifecycle management policy to ensure that each worker only has access to the data needed to perform their duties and frequently review the permissions of the various user profiles, if possible, as well as deactivating/revoking inactive profiles;
 - alarm systems to identify situations of access, attempts or misuse;
 - define, at an early stage, the best information security practices to be adopted;
 - carry out IT security audits and vulnerability assessments tests;
 - checking that the security measures defined are in place, ensuring that they are effective and updating them regularly, especially when processing or circumstances change circumstances change, including those implemented by data processing subcontractors;
 - periodically assess internal technical and organisational security measures and update and revise them whenever necessary. update and revise them whenever necessary.

- Further to the above, the following technical measures must be implemented:
 - for authentication: (i) strong credentials with long (at least 12 characters), unique passwords, complex and with numbers, symbols, uppercase and lowercase letters, changing them frequently; (ii) considering the sensibility of the information multi-factor authentication;
 - for infrastructures and systems: (i) Ensure that server and terminal operating systems are up to date, as well as all applications (e.g. browser and plugins); (ii) Keeping network equipment firmware up to date; (iii) Design and organise systems and infrastructure in such a way as to segment or isolate systems and networks to prevent the spread of malware within the organisation and to external systems; (iv) Systems Strengthen the safety of workplaces by restricting and blocking access;
 - electronic mail: Clearly and unequivocally define internal policies and procedures on the specific sending of email messages containing personal data, introducing the necessary additional checks;
 - protection against malware: (i) Use secure encryption, especially in the case of access credentials, special data highly personal data⁸ or financial data; (ii) Create an up-to-date, secure and tested backup system, completely separate from the main databases and without external access; (iii) Reinforce the system with anti-malware tools that include the ability to scan and detect it, as well as real-time blocking of ransomware-type threats;
 - use of equipment in an external environment: (i) Storing data in internal systems, protected with appropriate security measures, and accessible remotely via secure access mechanisms (VPN); (ii) Only allow access via VPN; (iii) Block accounts after several invalid login attempts; (iv) Activate multi-factor authentication for equipment users; (v) Apply data encryption to the operating system; (vi) Automatically back up work folders when the equipment is connected to the organisation's network; (vii) Define clear and appropriate rules for using equipment in an external environment.
 - storage of paper documents containing personal data: (i) Use paper and printing that is durable; (ii) Keep documents in a place with humidity and temperature control; (iii) Store documents containing sensitive personal data in a closed, fire- and flood-resistant place, properly organised; (iv) Control access, recording the date and time, who accesses them and the specific document(s) accessed; (v) Destroy documents using specific equipment that guarantees "secure" destruction.
 - transport of information containing personal data: (i) Adopt measures to prevent the unauthorised reading, copying, alteration or deletion of information containing personal data when it is transported. read, copied, altered or deleted in an unauthorised way; (ii) Use secure encryption when transporting, on mass devices or potentially permanent archives (CD/DVD/USB devices (CD/DVD/USB stick).

12. Breach notification

There are no substantive derogations from the GDPR.

13. Direct marketing

Regarding advertising and marketing matters, Portugal has Law no. 41/2004 of 18 August on Personal Data Protection and Privacy in Telecommunications. Article 13-A on Unsolicited Communications, provides that communications for direct marketing purposes require the individual's consent and the disclosure of adequate information to the data subject.

For this purpose, data controllers normally rely on an opt-in solution, considering that in some cases there can also be a soft opt-in option (particularly in cases where the data subject is already in a contract with the respective data controller).

General data protection laws (including the GDPR) also give the data subject the right to object at any time to direct marketing purposes, namely through an opt-out option.

We also underline that for marketing purposes the consent must be explicit.

14. Cookies and adtech

Portugal has no particular rule regarding the use of Cookies so we currently use the rules stated in the GDPR and Directive 2002/58/EC (ePrivacy Directive).

The use of cookies requires the individual's explicit consent and the disclosure of adequate information to the data subject. Currently, data controllers need to rely on consent to secure the adequate legal basis for the processing of personal data. Notwithstanding, the CNPD is expected to issue specific guidance on this matter.

Law no. 41/2004, of August 18, transposes into national law Directive 2002/58/EC on privacy and the protection of personal data in electronic communications. This law regulates, among other things, the use of cookies, allowing their use only with the prior informed consent of the user, except when strictly necessary for the provision of a service requested by the user. It also imposes an obligation to provide clear information about the purpose of cookies and ensures users the right to refuse them, in particular through browser settings.

15. Risk scale

Medium (moderate)

16. Useful links

- <https://www.cnpd.pt/>

Cybersecurity

1. Local cybersecurity laws and scope

- Law 46/2018, of 13 August establishes the legal framework for cyberspace security, transposing 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 European Union.
- Decree-Law no. 65/2021, of 30 July, which regulates the legal framework for cyberspace security and defines the obligations in terms of cybersecurity certification in implementation of Regulation (EU) 2019/881 of the European Parliament, of 17 April 2019.

Further to these, the Portuguese legal framework also comprises local legislation on cybersecurity, namely:

- Law no. 16/2019, of 22 August, which transposes Directive 2017/541 of March, on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA;
- Decree-Law no. 69/2014, of 9 May, approving the constitution of the National Cyber Security Centre (CNCS), establishing the terms of its institutional operations, amended by Decree-Law no. 136/2017 of 6 November.
- Decree-Law no. 62/2011, of 9 May, on the identification and protection proceedings to essential infrastructure (Directive 2008/114/EC of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection).
- Decree-Law no. 116-A/2006, of 16 July, amended by the Decree-Law no. 161/2012 of 31 July, on the

electronic information systems certification for public essential infrastructure.

- Resolutions and Decisions regarding National Cyber Security policies and strategies (namely, the Resolution of the Council of Ministers no. 12/2012 of 16 January, no. 19/2013 of 5 April, no. 7-A/2015 of 20 February, no. 41/2018 and no. 92/2019 and Decision of the Defence Minister no. 13692/2013 of 28 October).
- The eIDAS Regulation (EU) 910/2014), which is directly applicable in Portugal without the need for transposition and establishes a wide range of trusted services, as well as the cross-border mutual recognition of electronic means of identification (eID).

Notwithstanding this legislation, the Portuguese framework also comprises a set of legal diplomas that includes dispositions at the level of personal data protection, such as:

- Law no. 109/2009, of 15 September, implementing the Council Framework Decision 2005/222/JHA, of 24 February 2005, and the Budapest Convention on Cybercrime on the national framework (“Cybercrime Law”);
- Portuguese Criminal Code (Decree-Law no. 48/95 of 15 March, amended by Law no. 16/2018 of 27 March;
- Law no. 52/2003, of 22 August (Law on the Fight Against Terrorism), implementing the Council Framework Decision 2002/475/JHA of 13 June, with the more recent amendments of Law no. 60/2015 of 24 June.

2. Anticipated changes to local laws

On July 3, 2025, the Portuguese Government proposed a draft bill to transpose the Directive (EU) 2022/2555 (NIS2), which is currently under discussion.

3. Application

- **Law no. 46/2018, of 13 August**, establishes the legal framework of cyberspace security, by transposing Directive 2016/1148 of 6 July, concerning measures for a high common level of security of network and information systems across the Union. This Law applies to organisations within the following sectors/infrastructures: drinking water, energy (electricity and gas), nuclear, finance, telecom, transportation and water-control.
- **Decree-Law no. 65/2021**, defines the obligations in terms of cybersecurity and certification, establishing a set of minimum requirements that must be met by the organisations covered by Law no. 46/2018;
- **Law no. 16/2019, of 22 August**, formally modifies Law no. 52/2003 (counter-terrorism), of 22 August, by transposing Directive 2017/541 of 15 March, on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA;
- **Decree-Law no. 62/2011, of 9 May**, sets forth the main proceeding to the identification and protection (security) of essential infrastructure, particularly on health, security and economic and social wellbeing in the energy and transport sectors;
- **Decree-Law no. 116-A/2006, of 16 July**, amended by the Decree-Law no. 161/2012 of 31 July, on the electronic information systems certification for public essential infrastructure;
- **Resolution of the Council of Ministers no. 12/2012**, that proceeds to revise the National Information Security structure and, among others, to establish the basis for the formation of the CNCS;
- **Decree-Law no. 69/2014 of 9 May**, approving the constitution of the CNCS and establishing the terms of its institutional operations;
- **Resolution of the Council of Ministers no. 19/2013 of 5 April**, sets forth the strategic concept of national defence, taking into consideration the risks of cyberterrorism and cybercrime.
- **Resolution of the Council of Ministers no. 41/2018 of 28 May**, approves minimum

requirements for information systems used by the State administration.

- **Resolution of the Council of Ministers no. 92/2019 of 5 June** , defines the first national strategy on the security of network and information systems (2019-2023).
- **The decision of the Defence Minister no. 13692/2013 of 28 October** that with regard to national defence strategy, establish the main lines of Cyberdefence Policies.
- **Resolution of the Council of Ministers no. 36/2015** provides the National Security Strategies for Cyberspace.
- **Resolution of the Council of Ministers no. 7-A/2015 of 20 February** , regarding National Security on the fight against terrorism, particularly implementing the National Plan of Action against Cyberthreats.

4. Authority

- National Cyber Security Centre (CNCS): <https://www.cncs.gov.pt>
- Computer Security Incident Response Team (CERT)

5. Key obligations

- **Law no. 46/2018, of 13 August :**
 - sets forth the obligation to ensure appropriate and proportional technical and organisational security measures taken in response to evaluated risk level of security of network and information systems for public administrations.
 - The obligation to communicate any incident with substantial impact to the Upper Council of Cyberspace Security for digital service providers, operators of essential services and public administrations.
- **Decree-Law no. 65/2021:**
 - It defines the obligations in terms of cybersecurity and certification, establishing a set of minimum requirements that must be met by the organisations covered by Law no. 46/2018. It focuses in particular on (i) the obligation to create the two figures for business cooperation (Security Officer and Permanent Point of Contact) and periodic risk analysis and respective documentation in order to strengthen collaboration between the entities concerned, and supervisory bodies; (ii) the creation of a security plan that is appropriate and proportional to the size and risk exposure of the company in question; (iii) drawing up an inventory of captives; (iv) specialisation of incident reporting deadlines and the introduction of an incident taxonomy that harmonises and simplifies the risk assessment process.
- **Decree-Law no. 62/2011, of 9 May :**
 - The obligation to make a security plan and to review it annually (the review must be conducted by the competent national authorities);
 - The need to designate an agent to be a point of contact in matters related to the security of Critical European Infrastructures (ICT), particularly in the exchange of information with the competent authorities concerning related risks and threats;
 - There is an obligation to conduct an annual assessment of the threats across ICT sub-sectors.
- **Decree-Law no. 116-A/2006, of 16 July :**
 - The law establishes an obligation to certify electronic information systems for public essential infrastructure;
 - GNS is the public entity that is responsible for accrediting natural and collective persons to access and handle classified information, as well as authorities for the accreditation and oversight of entities that operate within the scope of the Certification System State Electronic - Public Key Infrastructure (SCEE).

6. Sanctions & non-compliance

Administrative sanctions:

- **Law no. 46/2018, of 13 August**
 - Very serious administrative offences:
 - From EUR 5,000 to EUR 5,000 when committed by natural persons;
 - From EUR 10,000 to EUR 50,000, when committed by legal persons.
 - Serious administrative offences:
 - From EUR 1,000 to EUR 3,000 when committed by natural persons;
 - From EUR 3,000 to EUR 9,000 when committed by legal persons.
- **Decree-Law no. 65/2021, broadly** refers to the sanctioning regime of Law 46/2018, and adds that in case of (i) the use of an invalid, expired or revoked cybersecurity certification mark;(ii) the use of expressions or graphics that expressly or tacitly suggest the cybersecurity certification of a product, service or process that is not certified; (iii) maliciously omitting information or providing false information that is relevant to the ongoing cybersecurity certification process, under the terms defined in each certification scheme. constitute an administrative offence punishable by a fine of (euro) 1000.00 to (euro) 3740.98, in the case of a natural person, or (euro) 5000.00 to (euro) 44 891.81, in the case of a legal person

Administrative offences due to negligence:

- Negligence is punishable, with minimum and maximum fines being reduced by half

Criminal sanctions:

- Law no. 109/2009, of September 15
 - **IT fraudulent misrepresentation**
 - Prison sentence of up to five years or a fine from 120 up to 600 days.
 - If the damage caused is considered high value, the prison sentence is up to ten years.
 - **Damage to programmes or other computer data**
 - Prison sentence of up to three years or an application of a fine;
 - If the damage caused is of high value, the prison sentence is up to five years or a fine up to 600 days;
 - If the damage caused is of very high value, the prison sentence is from one year up to 10 years.
 - **Computer sabotage**
 - Prison sentence of up to five years or a fine up to 600 days
 - **Illegal access**
 - Prison sentence of up to five years or a fine up to 120 days
 - **Unlawful interception**
 - Prison sentence up to three years or an application of a fine
 - **Illegal reproduction of protected programme**
 - Prison sentence of up to three years or an application of a fine.

Note: The attempt of any of the above-mentioned crimes is punishable

- **Law no. 52/2003, of 22 August**
 - Crimes against communications or acts that destroy or render impossible the functioning of

channels of communication or divert from their normal purpose, either definitively or temporarily, totally or partially, are punishable by prison sentence from two to ten years.

- Anyone broadcasting a message to the public inciting the practice of the acts mentioned above through electronic communication media will be punished with a prison sentence from one to six years.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

CERT.PT is a service within the CNCS that coordinates responses to incidents involving State entities, critical infrastructure, operators of essential services, digital service providers and, in general, the national cyberspace, including any device belonging to a network or address block attributed to an operator of electronic communications, institution, collective or individual person based, or physically located, in Portuguese territory.

Also, there is a National Network of CSIRTs that provides a set of services to its members, coordinating any situations with the CNCS.

8. National cybersecurity incident management structure

The CNCS provides a response structure for handling cybersecurity crises and incidents that require national-level coordination and/or management (see the response above).

9. Other cybersecurity initiatives

The CNCS is cooperating with international entities regarding cybersecurity matters (i.e. European Commission, ENISA, ISAC, NATO, OSCE and Project “No more Ransom”).

10. Useful links

- <http://www.redecsirt.pt/#objetivos>

Key Contacts



José Luís Arnaut
Lisbon
Managing Partner
Managing Partner

Authors



José Luís Arnaut
Lisbon
Managing Partner
Managing Partner



João Leitão Figueiredo
Lisbon
Partner



Sara Rocha
Lisbon
Senior Associate



Ricardo Pintão
Lisbon
Senior Associate