

# Embracing the Challenges of the Digital Transformation

Why Portugal's Data Protection and Cybersecurity Regimes  
Offer a Unique Opportunity for Hyperscalers

June 2022

Executive Summary .....	1
I. Powerhouse of Business and Innovation .....	2
II. Portugal's Action Plans To Keep Pace With The Digital Transformation.....	3
III. Mild and Resilient Geographical Climate and Superb Network Connectivity .....	4
IV. Adherence to EU Framework Without Additional Burdens on Data Processing .....	6
V. Domestic Laws Favour Hyperscalers .....	7
VI. Proportionate and Pragmatic Approach to Penalties .....	8
VII. Cnpd's Receptive and Cooperative Approach .....	10
VIII. Safety Net of Confidentiality.....	10
IX. The National Cybersecurity Centre: also Supportive and Collaborative .....	11
X. Paving the Way With International Best Practices in Cybersecurity .....	12
Conclusion .....	14

# Executive Summary

---

Since 2010, an unprecedented digital transformation has taken place globally: the integration of emerging technologies into all business areas and the digitalisation of society across all sectors. Internet traffic has increased reportedly 15-fold, with global internet traffic surging by over 40% in 2020 alone.<sup>1</sup> The digitalisation is set to continue with swelling amounts of data being consumed, for example, through video streaming services, machine learning, quantum computing, Internet-of-Things devices, expansion of services such as online banking, electronic commerce and virtual healthcare, the blockchain infrastructure, the 5-G wireless rollout and the metaverse. In parallel with the global digital transformation, European countries have placed increasing emphasis on the concept of personal data protection and the operationalisation of such concept through the adoption of new laws and regulations, which has resulted in various European countries embracing concepts akin to “data sovereignty”, i.e. keeping data within a state’s own borders. Since the introduction of the GDPR<sup>2</sup> in 2018, it has become more difficult than ever to transfer personal data outside of the European Union (EU), and companies must satisfy high hurdles in order to be permitted to do so. In addition, a number of European countries and their data protection authorities (DPAs) have made transfers of personal data outside these countries to non-EU states even more challenging than under the GDPR alone. These factors put increasing pressure on data centres, whose occupiers often require data to be processed and shared globally and moved among different jurisdictions, in order to function efficiently. The evolving sophistication of cyber threats, combined with the ability of EU DPAs to issue fines of up-to the higher of EUR20 million or 4% of worldwide annual turnover and the heightened risk of related private actions by individuals (including class actions), mean that controllers and processors handling EU data must be strategic when choosing a jurisdiction from which to operate.

Utilising a data centre in Portugal presents a unique solution to the challenges posed by the trend towards data sovereignty and the growing sophistication of

global cyber threats. Portugal is a welcoming hub for large technology companies and hyperscalers, with minimal restrictions on data processing within the EU framework. Portugal adheres to best practices in the law and regulation of data protection, yet at the same time it is consistently ranked as one of the most business-friendly, stable and open jurisdictions in the EU. Publicly recognised for fostering innovation, Portugal has taken concrete steps to embrace the digital transformation and encourage technological investment.

Portugal’s cybersecurity framework also aligns its laws with industry-leading international standards and certifications. While working within the high standards of the EU framework, Portugal maintains a sensible, secure and confidential privacy and cybersecurity enforcement regime.

These characteristics, coupled with the country’s strong network connectivity and favourable environmental conditions, position Portugal to be a highly desirable jurisdiction in which to establish and operate a data centre. This paper presents the advantages of developing and operating a data centre in Portugal from privacy, data protection and cybersecurity perspective.

This paper is structured as follows:

- I. Powerhouse of Business and Innovation
- II. Portugal’s Action Plans to Keep Pace with the Digital Transformation
- III. Mild and Resilient Geographical Climate and Superb Network Connectivity
- IV. Adherence to EU Framework Without Additional Burdens on Data Processing
- V. Domestic Laws Favour Hyperscalers
- VI. Proportionate and Pragmatic Approach to Penalties
- VII. CNPD’s Receptive and Cooperative approach
- VIII. Safety Net of Confidentiality
- IX. The National Cybersecurity Centre: Also Supportive and Collaborative
- X. Paving the Way with International Best Practices in Cybersecurity

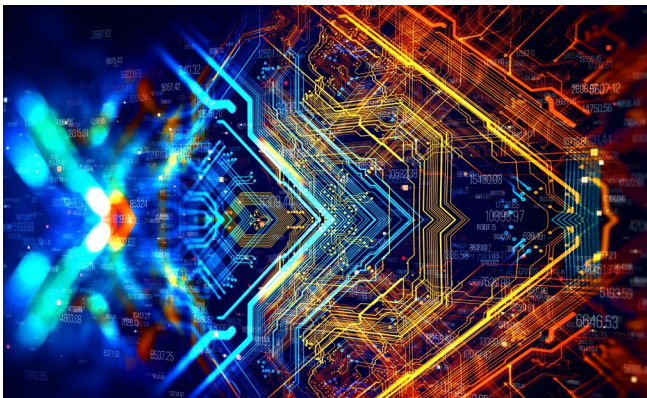
---

<sup>1</sup> [International Energy Agency, Data Centres and Data Transmission Networks Tracking Report](#), November 2021

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR).

# I. Powerhouse of Business and Innovation

---



Portugal has been recognised as a trailblazer. It is consistently ranked as one of the most business-friendly jurisdictions in the EU in terms of innovation, digitalisation and technical expertise, which creates an attractive jurisdiction where a data centre and its occupants can flourish. The Portuguese Government has publicly declared its intentions for Portugal to become the digital hub of Europe.<sup>3</sup>

---

**“Ranked as one of the most business-friendly jurisdictions in the EU and becoming the digital hub of Europe”**

---

Portugal scores highly on the World Bank’s ‘Ease of Doing Business’ rankings.<sup>4</sup> In 2019, it was ranked as the world’s 39<sup>th</sup> most favourable jurisdiction for ease of doing business, higher than 14 other EU Member States including the Netherlands, Italy and Belgium<sup>5</sup>. Portugal also scores highly in Ernst & Young’s 2021 Attractiveness Survey, where it ranked as the 6<sup>th</sup> largest destination in Europe for software and IT services.<sup>6</sup> According to World Bank data, in 2019 the net inflow of foreign direct investment into Portugal was 4.3% of GDP compared to an EU average of

0.8%, meaning that Portugal ranks 6<sup>th</sup> in the EU for the level of foreign investment.<sup>7</sup>

In 2020, Portugal achieved recognition for its exceptional state of affairs in the European Commission’s European Innovation Scoreboard (EIS), with a score of 96.7 relative to the EU in 2019.<sup>8</sup> The EIS provides a comparative assessment of research and innovation performance in EU countries and other comparable jurisdictions. For 2020 Portugal was ranked as the EU’s leading jurisdiction for innovation in respect of small and medium-sized enterprises (SMEs) due to its high share of SMEs with innovative products and business processes. Portugal’s overall performance on the EIS scoreboard was also high, having been elevated from a “moderate innovator” in the 2019 rankings to a “strong innovator” in 2020, evidencing that its innovation performance was above or close to the EU average. Out of all EU countries and comparable jurisdictions which were monitored in the EIS, Portugal ranked fourth for an increase across the relevant “performance indicators” between 2012 and 2019 relative to that of the EU in 2012. Overall, 32 “performance indicators” were used to arrive at this conclusion, including indicators measuring each countries’ level of digitalisation, such as the level of broadband penetration among enterprises and the supply of individuals with above basic overall digital skills. For 2021, although there was a decline in Portugal’s ranking, the EIS specifically noted Portugal’s “*strong performance increases on Tertiary education, Government support for business R&D, ICT specialists, Job-to-job mobility of HRST, and Environment-related technologies*”<sup>9</sup>.

Portugal’s recognition as a business-friendly, innovative hub continues to take hold as the Government announces multiple plans of action to keep pace with rapid technological developments and growing threats resulting from the digital transformation.

---

3 [Inside Portugal’s bid to become a ‘startups factory’](#), November 2021. See also [With right policies, Portugal could spearhead Europe’s digital innovation](#), March 2021.

4 [World Bank Group, ‘Doing Business 2020: Comparing Business Regulation in 190 Economies’](#), October 2019.

5 Other EU Member States that rank lower than Portugal for ease of doing business include Poland, Czech Republic, Slovakia, Croatia, Hungary, Cyprus, Romania, Bulgaria, Luxembourg, Greece and Malta.

6 [Foreign investors back Europe, but is Europe back?](#), Ernst & Young, June 2021

---

7 The World Bank, [Foreign direct investment, net inflows \(% of GDP\) - European Union](#)

8 [European Innovation Scoreboard 2020](#), June 2020.

9 [Portugal Profile](#), European Innovation Scoreboard 2021, June 2021.

## II. Portugal's Action Plans to Keep Pace with the Digital Transformation



Global internet traffic reportedly more than doubled between 2017 and 2020, and if current trends are sustained, is expected to double again by 2023.<sup>10</sup> This growing demand for data services combined with rapidly evolving technological developments means that the best jurisdictions in which to develop and use data centres are those that are dynamic, innovative and invest heavily in their digital future. Portugal has several plans in place to ensure that it maintains and improves its already impressive international rankings.

### Action Plan for Digital Transition

From a forward-looking perspective, Portugal is investing heavily in its digital future. In April 2020, the Portuguese Ministry of Economy and Digital Transition published its Action Plan for Digital Transition (the "Action Plan"), which is based on three pillars: (i) capacity-building and the digital inclusion of people; (ii) the digital transformation of businesses; and (iii) the digitalisation of the State.<sup>11</sup>

One of the 12 measures set out in the Action Plan is the creation of Technology Free Zones (TFZs)<sup>12</sup>, which are physical spaces where new technologies can be tested and developed within a flexible regulatory regime specific to each TFZ. The Portuguese Government has adopted legislation regarding the framework and governance model for the creation of TFZs and such regimes are expected to promote a culture of experimentation. The Portuguese approach goes beyond the creation of "regulatory sandboxes", "innovation spaces", "experimental spaces" or "living labs" that have been set up in certain other

EU jurisdictions, as TFZs will not be confined to a particular sector or predefined area. Instead, TFZs provide for a coherent and aligned approach for testing products and services that are cross-sector and integrated (i.e. that span across more than one sector and may therefore be subject to different regulations and regulators). This promotes a culture of innovation in Portugal that is ripe for the establishment and operation of data centres within the jurisdiction.

The Action Plan also envisages the development of more Digital Innovation Hubs (DIHs), which are essentially one-stop-shops that provide businesses with access to technical expertise and experimentation, in addition to innovation services such as financing advice, training and skills development. At the time of writing, Portugal already has 14 DIHs which are operational, planned or in the process of being created, with reportedly further DIHs in the pipeline.<sup>13</sup>

---

**"Portugal has implemented solid steps to be at the forefront of the digital transformation"**

---

### AI Portugal 2030

In June 2019, the Portuguese Government presented its National Strategy on Artificial Intelligence (AI), which sets out a plan for the use of AI in the public and private sector over the coming years.<sup>14</sup> The plan envisages, among other things, Portugal's participation in European Networks (e.g. Big Data Value Public-Private Partnership), European AI excellence centres and other European DIHs (e.g. the DIH on cybersecurity at Leon, Spain or the DIH on Internet-of-Things (IoT) in Salamanca, Spain). The plan also sets out the development of new infrastructure, including the creation of a centralised repository for administrative data.

### Portugal's Recovery and Resilience Plan

Following the COVID-19 pandemic, Portugal developed a Recovery and Resilience plan which was endorsed by the European Commission.<sup>15</sup> The

<sup>10</sup> International Energy Agency, Data Centres and Data Transmission Networks Tracking Report, November 2021.

<sup>11</sup> [Portugal's Action Plan for Digital Transition](#), 21 April 2020.

<sup>12</sup> Addressed in the Resolution of the Council of Ministers no. 29/2020.

<sup>13</sup> European Commission, [Digital Innovation Hubs](#).

<sup>14</sup> [AI Portugal 2030](#)

<sup>15</sup> [NextGenerationEU: European Commission endorses Portugal's](#)

plan is an important step so that Portugal can benefit from the EU disbursing EUR13.9 billion in grants and EUR2.7 billion in loans over the period 2021-2026.<sup>16</sup> This financing will support the implementation of new investments in the fields of digital and green transition. Portugal is planning to allocate 22% of its funds particularly to measures that support the digital transition.<sup>17</sup>

---

€16.6 billion recovery and resilience plan, 16 June 2021.

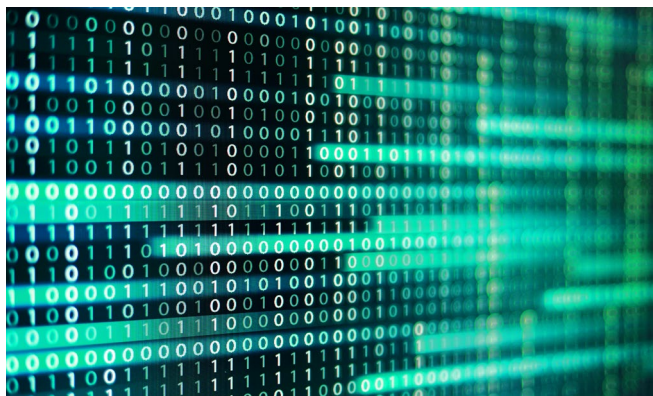
16 [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_4025](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4025)

17 [https://ec.europa.eu/commission/presscorner/detail/bg/ip\\_21\\_2985](https://ec.europa.eu/commission/presscorner/detail/bg/ip_21_2985)

As Portugal continues to position itself as the future digital hub of Europe, the country has taken steps to strengthen vital characteristics attractive to data centre operators, including in the areas of connectivity, sustainability, data protection and cybersecurity while capitalising on its ideal geographical climate.

### III. Mild and Resilient Geographical Climate and Superb Network Connectivity

---



Portugal benefits from existing dark fibre connections to Europe, North America, South America, Africa, Middle East and Asia, with more developments reportedly planned in the near future next to the Sines 4.0 Hyperscaler Data Centre. Under its Action Plan for Digital Transition, Portugal has implemented the Building Europe Link to Latin America programme, under which the consortium EllaLink deployed a submarine cable system connecting Latin America and Europe.<sup>18</sup>

From a geographical perspective, Portugal is well positioned to be the “connecting hub” for undersea cables which span the South Atlantic, offering a unique opportunity for exploring alternative routes to Africa, the Americas and further afield. Portugal is part of the Community of Portuguese Language Countries,

also known as the Lusophone Commonwealth (“CPLP”), whose members include Brazil, one of the largest ICT markets in the world, as well as Angola and Cape Verde, both of which are currently investing significantly in the deployment of undersea cables. CPLP is a political project founded on the historical link, common heritage and language of its member states, and focuses on diplomatic coordination as well as cooperation in a number of areas such as the economy, energy, social affairs and the environment.<sup>19</sup>

Against that background, Portugal is well connected (network-wise and otherwise) to CPLP’s member states, including through already existing subsea cables from Portugal to Angola. This is significant because the world’s first submarine cable system across the South Atlantic (the “South Atlantic Cable System” or “SACS”) has been deployed in Angola, connecting Angola’s capital Luanda to Fortaleza, Brazil and offering the lowest latency cable between Africa and the Americas.<sup>20</sup> SACS in turn connects to the Monet subsea cable system, which is itself operated by Google, Angola Cables (Angola), Algar Telecom (Brazil) and Antel (Uruguay) and connects Santos (São Paulo) and Fortaleza in Brazil to Boca Raton (Florida) in the USA. As a result, Portugal is well positioned to promote the exchange of internet traffic

---

18 Action Plan for Digital Transition, 21 April 2020. See also Digital Economy and Society Index Report 2021, Portugal, page 9.

19 See further details at <https://portaldiplomatico.mne.gov.pt/en/foreign-policy/community-of-portuguese-speaking-countries#key-areas-of-action>

20 See further details at <https://www.angolacables.co.ao/en/sacs/>

between the African continent and the Americas via the South Atlantic, including the further development and deployment of subsea cables. Notably, this configuration of cables provides an alternative route for the transfer of information between Europe and the Americas, aiming to offer redundancy in the global undersea cables system and to alleviate concerns associated with threats to that system in the modern world. In addition, the digital transition in the African continent is of particular interest to a number of stakeholders, and Portugal's good connectivity to Africa makes it one of the frontrunners for the EU's contribution to that digital transition and an attractive jurisdiction to develop commercial operations.

Further, Portugal has recently also been improving its own network connectivity by replacing outdated submarine cables such as the Atlantic submarine cable ring linking mainland Portugal to its various islands, including Madeira and Azores (CAM submarine cables).<sup>21</sup> According to the 2021 Digital Economy and Society Index Report<sup>22</sup>, published by the EU every year, Portugal ranks 15<sup>th</sup> out of the 27 EU Member States in terms of its connectivity. The report notes that total and rural fibre to the premises (FTTP) coverage continued to increase from five percentage points in total FTTP coverage to two percentage points in rural FTTP coverage. Further details about Portugal's robust network connectivity are set out in detail in *Portugal: A Hidden Gem of Connectivity*.

**Figure 1.**



Source: Deloitte sponsored by Start Campus.

In addition, 5G technology has been launched in Portugal. Such technology benefits from faster connectivity speeds, ultra-low latency, improved reliability, and greater network capacity. The 5G

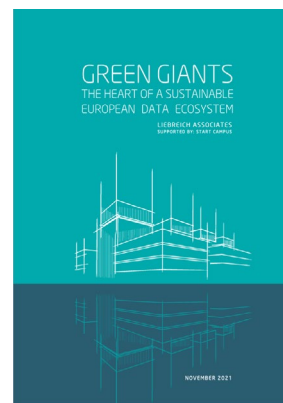
21 Digital Economy and Society Index Report 2021, Portugal, page 4.

22 Digital Economy and Society Index Report 2021, Portugal.

rollout and the ability for large volumes of data to be transferred quickly and reliably will enable Portugal to maintain its place as an important international "connecting hub".

In light of the connectivity details outlined above, the Sines 4.0 Hyperscaler Data Centre is therefore well positioned. Its location presents a physically safe and secure environment which in turn improves its cybersecurity posture. The area around the city of Sines, located 150km south of Portugal's capital Lisbon, has a mild climate due to ocean proximity and is not subject to extreme weather conditions. Such a climate is very suitable for a data centre, and the further unique environmental advantages of the Sines 4.0 Hyperscaler Data Centre are discussed in detail in *Green Giants: The Heart of A Sustainable European Data Ecosystems*.

**Figure 2.**



Source: Liebreich Associates supported by Start Campus.

Against the backdrop of a clear commitment by the Portuguese Government to propel further the country's role in the digital transformation and assisted by external factors such as its mild climate, Portugal's favourable legal framework relevant to data protection, privacy and cyber matters stands out as another stark advantage of the jurisdiction when one considers where to operate a data centre.

## IV. Adherence to EU Framework Without Additional Burdens on Data Processing

---



Handling personal data of EU individuals, whether as controller or processor, requires compliance with the EU legal standards on data privacy. Portugal maintains these high standards whilst ensuring that its laws do not become over-burdensome on businesses.

In contrast to other European countries, aside from implementing the GDPR, Portugal is committed to the concept of “data mobility,” meaning that it has not enacted any additional laws prohibiting the transfer of data outside of its territory or restricting the processing of such data (sometimes known as “data sovereignty laws”). Accordingly, Portugal has minimal laws restricting the use, processing and transfer of personal data outside of the GDPR. Similarly, Portugal does not impose any additional restrictions on the use of cookies and e-marketing in addition to those set out at EU level under the e-Privacy Directive<sup>23</sup>. The absence of Portuguese-specific data sovereignty laws means that the jurisdiction imposes the fewest restrictions on the transfer of personal data that it possibly could, as an EU Member State.

---

“The absence of Portuguese-specific data sovereignty laws means that the jurisdiction imposes the fewest restrictions on the transfer of personal data that it possibly could, as an EU Member State.”

---

By way of contrast, some other Member States have imposed restrictions on the processing and transfer of personal data, over and beyond the GDPR, including in certain sectors and/or industries. Such measures often result in the unintended but inevitable risks of stifling innovation, technology and Big Data developments.

For example, in France new certification regimes are being imposed on cloud providers despite reported acknowledgements from the Director General of France’s National Cybersecurity Agency (ANSSI) that such measures are likely to limit the possibilities for certain international technology companies to operate within the jurisdiction.<sup>24</sup> The French legislature has set out plans requiring cloud service providers who store health data to be certified under the ‘Hébergeurs de Données de Santé’ scheme, which imposes advanced security and privacy requirements.

---

<sup>23</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

---

<sup>24</sup> [France wants cyber rule to curb US access to EU data](#), Politico.eu, accessed on 13 January 2022.

## V. Domestic Laws Favour Hyperscalers



As described in section IV, in contrast to other comparable EU jurisdictions, Portugal's legal framework does not burden businesses with significant additional obligations, over and beyond what is required at EU level. Indeed, Portugal's legal framework goes further than this by actively supporting hyperscalers in various ways.

Firstly, Portugal has maintained a general liability exemption in relation to intermediary service providers ("ISPs"), including hyperscalers that operate data centres. Under the E-Commerce Directive<sup>25</sup>, implemented by Portugal under Decree-Law no. 7/2004, of 7 January 2004, ISPs are not subject to a general surveillance obligation or to an obligation to investigate illegal activity relating to information which they transmit or store, save for if ISPs become aware of manifestly unlawful activities carried out through their services with respect to protected content. In such a case ISPs are obligated to inform Portugal's Inspeção-Geral das Atividades Culturais (a branch of the Ministry of Culture). ISPs must also remove or block access to protected content within 48 hours of being notified, or within the shortest possible time where this period would substantially reduce the usefulness of the removal or prevention of access.

ISPs that have failed to comply with their ordinary duties or liability under Decree-Law no. 7/2004 may be fined between EUR2,500 to EUR100,000. Failure to comply with the obligations and procedures set out in Law 82/2021 regarding unlawful access to protected content may constitute a violation subject to fines between EUR5,000 and EUR10,000.

In practice, the Portuguese courts have taken a reasonable approach towards imposing any liability on ISPs. For example, in the Supreme Court of Justice's judgment of 10 December 2020, application no. 44/18.6YHLSB.L1.S2, the Court decided not to hold a Spanish web hosting company liable for the use, on a website it owns, of the distinctive signs owned by the claimant without the necessary legal authorisations. The Court found that the web hosting company would only be liable if it had in some way participated or interfered with the content of the information transmitted or stored. The Court stated that such participation or interference was not proven.

Secondly, in comparison with various other European jurisdictions, Portuguese law is relatively permissive in allowing contracting parties to exclude or limit liability under a contract. Therefore, under Portuguese law, unless there is gross negligence or wilful misconduct, a contract may generally contain exclusion or limitation clauses, for example: (i) excluding liability entirely; (ii) limiting liability to a certain amount or exempting some debtor's assets from the scope of financial liability; (iii) excluding liability in respect of acts of third parties appointed by the parties; (iv) excluding liability relating to force majeure events; (v) excluding indemnity claims when penalties had been agreed; and/or (vi) excluding incidental, indirect and consequential damages, provided that the clauses are not considered contrary to the public order.

By way of contrast, many other European regimes contain stricter rules in this regard. For example, the German legal regime precludes parties from enforcing exclusion clauses that limit or exclude liability for certain types of damages like loss of profit<sup>26</sup>, and under English law, parties are prohibited from enforcing so-called "penalty clauses" which place an obligation upon the party who has breached the contract to provide compensation to the aggrieved party where such compensation amounts to a "penalty". The advantage of Portugal's permissive attitude towards exclusion and limitation of liability clauses is that the contracting parties' risk can be significantly limited.

<sup>25</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

<sup>26</sup> Although clauses limiting or excluding liability for "loss of profit" are not expressly prohibited under Portuguese law, there is some debate as to whether provisions that exclude or limit liability for wilful misconduct and negligence are valid. These provisions are often included in contracts although it is possible that they may be declared void by the courts.

Against that background of a favourable legal framework, the bodies responsible for upholding that framework in relation to privacy and cybersecurity have a marked reasonable and pragmatic approach, as

discussed in the next sections, which further entices data centre operators to carry out their business in Portugal.

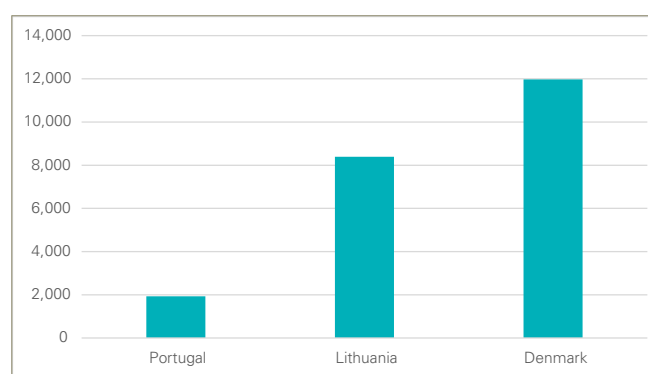
## VI. Proportionate and Pragmatic Approach to Penalties



Over the last few years, the EU has seen record breaking fines being imposed on controllers and processors across various industries for non-compliance with EU data protection laws. The EU data protection regulators, the “DPAs”, are able to issue fines of up-to the higher of EUR20 million or 4% of worldwide annual turnover. These substantial sums, combined with the increasing sophistication of cyber-criminals, make the threat of regulatory fines an alarming prospect.

By contrast, at the time of writing, Portugal is one of the EU countries that has opened the fewest number of cases, in comparison with countries such as France, Germany, Ireland, Luxembourg and the UK. Portugal’s DPA, Comissão Nacional de Proteção de Dados (CNPd), opened a total of 1,839 cases during 2019 and a total of 1,926 cases during 2020. By way of comparison, DPAs in many countries with population sizes smaller than Portugal have opened far more cases, including Denmark’s DPA which opened 11,972 enforcement cases in 2020 and Lithuania’s DPA which opened 8,388 enforcement cases in 2020.

**Figure 3. EU DPA Enforcement Cases Snapshot, 2020**

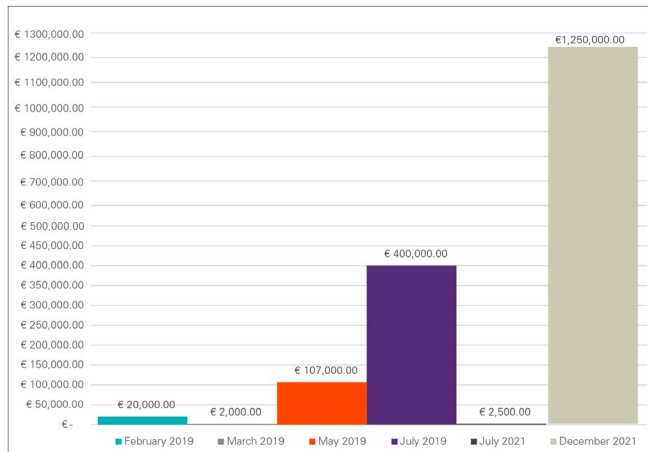


When the CNPD imposes a fine, the value of any such fine is usually relatively low. The largest fine that the CNPD has issued publicly<sup>27</sup> was for EUR1.25 million on the Municipality of Lisbon for sending sensitive personal data of political protest organisers to external third parties (including foreign diplomats whose countries were the targets of those political demonstrations), internal services and advisors of the City Council; such sharing of personal data was held to be in violation of the GDPR rules, including on lawfulness, transparency and fairness, data minimisation, storage limitation, and handling of special category of data. Other fines that have been made public and that have been issued by the CNPD include: (i) a EUR400,000, levied on a public hospital for breach of the GDPR obligations of integrity and confidentiality (Article 5(1)(f)) and security of processing (Article 32). The hospital, however, sought and was granted relief in the form of a waiver of the fine, under a mechanism available to public bodies in certain circumstances under the Portuguese Data Protection Law (Law no. 58/2019, of 8 August); (ii) a fine for EUR20,000 on an unknown entity for violations of the right of access (Article 15 GDPR); (iii) a fine for EUR107,000 on an unknown entity for

<sup>27</sup> Portugal does not release the value of all its fines to the public, this is the largest value fine that has been made public.

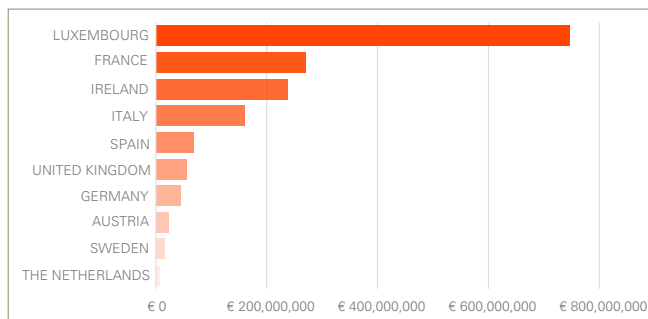
sending direct marketing messages without adequate consent from the data subject; (iv) a fine for EUR2,000 on an unknown entity for breach of the information provision requirements (Article 13 GDPR); and (v) a fine for EUR2,500 on a Portuguese municipality for breach of the lawfulness, fairness and transparency obligation (Article 5(1)(a)).

**Figure 4: Portugal – Published Fines for GDPR Breaches**



By way of comparison, other European jurisdictions have issued significantly larger fines, as Figure 5 indicates.

**Figure 5: EU Member States - Published Fines for GDPR Breaches, Top 10 by Value**



Country	Sum of Fines
LUXEMBOURG	€ 746,267,200 (at 19 fines)
FRANCE	€ 269,694,300 (at 25 fines)
IRELAND	€ 243,510,900 (at 15 fines)
ITALY	€ 137,547,096 (at 150 fines)
SPAIN	€ 55,525,370 (at 426 fines)
UNITED KINGDOM	€ 53,961,800 (at 9 fines)
GERMANY	€ 52,105,753 (at 84 fines)
AUSTRIA	€ 24,774,550 (at 17 fines)
SWEDEN	€ 16,232,230 (at 27 fines)
THE NETHERLANDS	€ 14,594,500 (at 20 fines)

Source: Underlying figures from <https://www.enforcementtracker.com/insights>  
Figures as of 15 June 2022

The sums comprising Figure 5 are telling – as it is telling that Portugal is not in that list, since the fines it imposes are significantly less in value than these figures. Luxembourg’s DPA, Commission Nationale pour la Protection des Données (CNPd), issued a EUR877 million fine against Amazon. France’s DPA, the Commission Nationale de l’Informatique et des Libertés (CNIL), has issued fines against Google: EUR100 million for breach of the cookie requirements and EUR50 million for lack of transparency; as well as against Amazon: EUR35 million for breach of the cookie requirements. The ICO’s largest fines to date include, for example, a EUR22 million fine on British Airways, UK’s flag carrier airline, a EUR23.8 million fine on Marriott, the hotel chain, and a EUR1.39 million fine on Ticketmaster, the tickets marketplace. In Germany, the Hamburg Commissioner for Data Protection and Freedom of Information issued a fine against H&M, the clothing retailer, in the amount of EUR35 million and a EUR10.4 million fine against Notebooksbilliger, an electronics retailer. Elsewhere in the EU, other high value fines have been imposed, including a EUR225 million fine against WhatsApp by the Irish DPA, a EUR27.8 million fine against TIM, a telecommunications operator, by the Italian DPA, a EUR8.15 million fine against Vodafone, another telecommunications operator, by the Spanish DPA, and a EUR7 million fine against Google by the Swedish DPA.

The Portuguese CNPD’s reluctance to issue large value fines, such as those seen across many EU Member States, is a notable advantage to locating a data centre in Portugal.

## VII. CNPD's Receptive and Cooperative Approach

---



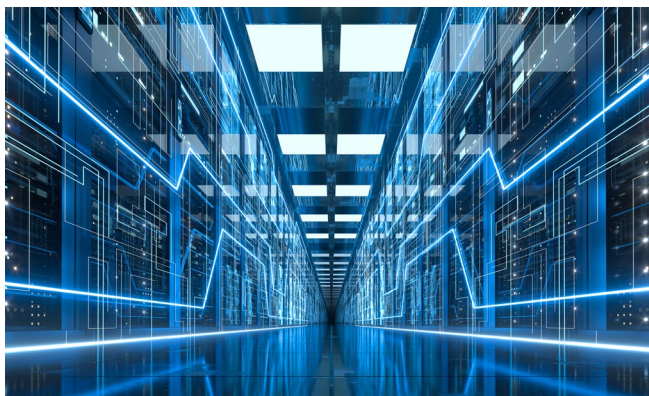
As discussed throughout this paper, Portugal adheres to best practices in data protection and cybersecurity matters, and aligns its laws with industry-leading international standards and certifications; at the

same time, it is consistently ranked as one of the most business-friendly jurisdictions in the EU. The Portuguese regulators in data protection and cybersecurity are pragmatic in their approach, and have historically been willing to engage in negotiations and discussions in order to work alongside hyperscalers and other businesses.

The CNPD has shown a comparatively reasonable approach to enforcement, relative to other European DPAs such as the German, French, UK and Irish DPAs. The CNPD is both supportive and collaborative with private stakeholders, including hyperscalers, and is shaping up as a reasonably approachable DPA.

## VIII. Safety Net of Confidentiality

---



In addition to the CNPD's approach in general, the practicalities of the regime in Portugal result in the CNPD presenting favourably in relation to a further important point: reputational risk following substantial fines. The number of eye-watering fines issued by various EU DPAs discussed above have been making the headlines in the international press, often causing reputational damage. However, Portugal's CNPD is not obliged to publish all the fines it imposes.

Portuguese national law provides that deliberations on administrative offences may only be published

after they have been anonymised. This factor is an attractive feature of the Portuguese landscape, as businesses can have a greater level of confidence that in case there are fines or rulings against them, these are likely to remain confidential, which would usually assist with managing any reputational risks.

By way of contrast, many European DPAs routinely publish the fines they issue along with explanations of each decision. The UK's ICO releases details of the fines it has issued, on occasions with additional information: for example, the penalty notices against British Airways and Marriott (both fines mentioned above) spanned over 114 pages and 91 pages respectively. The ICO also publishes a dedicated "Action we've Taken" newsletter.

---

**"The Portuguese regulators in data protection and cybersecurity are pragmatic, reasonable and cooperative in their approach"**

---

## IX. The National Cybersecurity Centre: Also Supportive and Collaborative



Similar to the CNPD, the Portuguese National Cybersecurity Centre (the CNCS), which is the competent authority responsible for supervising compliance with the cybersecurity legislation in the country, is also both receptive to and collaborative with private stakeholders. For instance, the CNCS has reportedly cooperated with certain hyperscalers for the issuance of seals. The issuance of a seal by the CNCS requires significant effort and cooperation on the part of businesses, which evidences Portugal's commitment to a strong cybersecurity framework. However, the CNCS has a keen interest in encouraging adherence to best practices and will collaborate with the private sector to meet those standards. To that end, Portugal is also developing a digital maturity certification scheme, covering four aspects, namely sustainability, cybersecurity, privacy and accessibility, and including three levels of digital maturity: bronze, silver, and gold. The cybersecurity component of the seal is already fully operational.

The CNCS also supports businesses by regularly publishing guidance and information notes. For example, the CNCS released a Roadmap for Minimum Cybersecurity Capabilities, which sets out a cybersecurity training model in five phases aimed at improving processes, people and technologies in the cybersecurity field.<sup>28</sup> It also launched the Cybersecurity Capabilities Assessment Framework, an assessment document that classifies an organisation's compliance with five national cybersecurity objectives, namely identify, protect, detect, respond and recover, in order to enable organisations to comply better with the National Cybersecurity Reference Framework, and aligns with the five functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.<sup>29</sup>

<sup>28</sup> CNCS Press Release, [The Roadmap for Minimum Cybersecurity Capabilities is now available](#), October 2019.

<sup>29</sup> CNCS Press Release, [The Cybersecurity Capabilities Assessment Framework is now available](#), January 2020.

## X. Paving the Way with International Best Practices in Cybersecurity

---



### Adherence to highest international cybersecurity standards

Portugal is highly attuned to the ever-growing threat posed by cyber-criminals globally and adopts cybersecurity standards aligned with international best practices. Between 2018 and 2020, Portugal's ranking for cybersecurity has increased exponentially according to the International Telecommunication Union's "Cybersecurity Maturity Index". During that period, Portugal rose from 25<sup>th</sup> to 8<sup>th</sup> place in the EU rankings and from 44<sup>th</sup> to 14<sup>th</sup> place globally. The ranking is developed based on 82 indicators, including the number of attacks, the country's public policies, and how the countries' cybersecurity strategies are ultimately executed. In addition, in the National Cybersecurity Index, developed by the e-Governance Academy Foundation, Portugal occupies the 7<sup>th</sup> position globally, scoring 89.61 and ranking just after Germany at 6<sup>th</sup> place with 90.91, and in front of many other European countries such as France (at 11<sup>th</sup> place with 84.42), UK (at 22<sup>nd</sup> place with 77.92) and Ireland (at 40<sup>th</sup> place with 63.64).<sup>30</sup> The CNCS credited Portugal's significant success to the set of legislative, technical, organisational, capacity development and cooperation initiatives that have been defined and implemented with the aim of strengthening the cybersecurity framework at the national level in recent years.<sup>31</sup>

Portugal has also implemented the NIS Directive,<sup>32</sup> which is the first piece of EU-wide legislation on

cybersecurity and provides legal measures to boost a country's overall level of cybersecurity. Such legal measures include, for example, requiring EU Member States to be equipped with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority, which, similar to the EU's Agency for Cybersecurity, oversees compliance over the cybersecurity laws and issues guidance and best practices. Further, the NIS Directive is compatible with other cybersecurity standards, including the NIST standard and the industry ISO 2700X family.

---

**"Portugal's cybersecurity framework aligns its laws with industry-leading international standards and certifications"**

---

### Determined raising of cyber awareness across the board

In terms of the workforce, the 2021 Annual Internal Security Report published by the Cybersecurity Observatory, a service of Portugal's CNCS (the CNCS Observatory), notes that the number of cyber awareness raising courses has steadily increased over the years.<sup>33</sup> Such training initiatives ensure that the country's population is aware of the risks of cyberspace and cybersecurity best practices in order to mitigate the effects of existing threats and vulnerabilities. The activities include the National Cybersecurity Exercise<sup>34</sup>, which is organised and promoted by the CNCS. The exercise involves various stakeholders and national officials being placed before a simulation of a cyberattack or cybersecurity incident in order to (i) develop the prevention, monitoring, detection, reaction, analysis and correction of incidents by entities in the area of cybersecurity; (ii) promote training and qualification of employees; and (iii) promote cooperation between participants. The National Cybersecurity Exercise is just one of the numerous and varied cybersecurity awareness

---

30 [National Cyber Security Index](#)

31 CNCS Press Release, [The ITU's Global Cybersecurity Index 2020 is now available](#), June 2021

32 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

33 [Annual Internal Security Report](#).

34 CNCS Press Release, [National Cybersecurity Exercise](#)

initiatives.<sup>35</sup> Another such initiative is, for example, the launch of a nationwide project aimed at creating a National Cybersecurity Academy. In association with Portugal's universities and other academic institutions, the Academy will deliver courses in various areas of cybersecurity, for both citizens in general and cybersecurity professionals in particular.

## Continuous enhancement of defences

Similar to other states, Portugal carefully monitors cybersecurity threats and has a Computer Emergency Response team which is an important element of an active national 53-member strong CSIRT network. The network is made of both public and private CSIRTs who routinely exchange cybersecurity information. Further, in its Annual Report on Internal Security 2020 the CNCS Observatory identified cybercrime as one of the top priorities for Portugal to focus on and committed to continue to implement new criminal policy guidelines addressing the issue.<sup>36</sup>

The CNCS Observatory's 2021 Report on Cybersecurity Risks and Conflicts demonstrates Portugal's preparedness for the growing threats of cybercrime.<sup>37</sup> The detailed report, which spans over 120 pages, outlines various cyber threats facing the world, including a breakdown by sector, cyber-crime tactics and cyber-threat agents. Portugal aims to combat such threats using advanced digital technologies such as AI and quantum computing. The report recognises that developing Portugal's cloud computing infrastructure is of paramount importance for the country, with the report ranking cloud computing as the highest perceived emerging technology set to improve cybersecurity operations in 2020/2021.

In 2021 the CNCS Observatory also published its Report on Public Policies in the Area of Cybersecurity.<sup>38</sup> The report aims to describe Portugal's landscape of public policies in this area, recognising that such policies must also take into account the international state of play, so as to account for the transnational nature of cyber-threats. The report sets out a consolidated list of Portugal's policies that are relevant to the cybersecurity landscape, including the Recovery and Resilience Plan, the Action Plan for Digital Transition and the National Strategy for AI (all described in more detail above).

<sup>35</sup> For further examples see section H.9.3 of the Report on Public Policies in the Area of Cybersecurity.

<sup>36</sup> [Annual Internal Security Report, 2020](#)

<sup>37</sup> [Report on Cybersecurity in Portugal, Risks and Conflicts](#), May 2021.

<sup>38</sup> [Report on Public Policies in the Area of Cybersecurity](#)

## National Strategy for Cyberspace Security 2019-2023

Portugal's National Strategy for Cyberspace Security, adopted in June 2019, acknowledges that "[t]he trend towards a growing increase of the dependence on information and communication technologies and the emergence of new phenomena with a direct impact on social development have also brought about, in connected societies like ours, significant opportunities for those wishing to compromise our network and information systems for potentially harmful purposes on the well-being of the Portuguese society".<sup>39</sup>

The country has also recognised the impact of the COVID-19 pandemic on this trend: for example, it was reported that there was a 25% increase in notifications of personal data breaches to the CNPD, going up to 301 from 240 in 2019.<sup>40</sup> The Strategy is aimed at deepening the security of network and information systems and ensuring a free, safe and efficient use of cyberspace by all citizens and businesses. It sets out three high-level strategic objectives: (i) maximising digital resilience by enhancing the country's networks, in order to safeguard against threats that may compromise or cause the disruption of network and information systems; (ii) fostering and enhancing national innovation by affirming the cyberspace as a domain for the economic, social and cultural development and prosperity; and (iii) generating and guaranteeing the allocation of adequate resources for building and sustaining the national capacity on cyberspace security. The Strategy sets out six practical steps (known as "intervention axes") that Portugal will take to achieve its goals. These include supporting the public bodies which attack cybercrime, such as the CNCS, as well as promoting national and sectoral cyberspace protection cooperation structures, including within the private sector.

## An ethics-focused approach

Portugal has an impressive reputation for applying an ethics-based approach when dealing with cybersecurity issues and threats. In 2021, the CNCS Observatory published the Report on Cybersecurity, Ethics and Law which sets out the main ethical and legal risks associated with cyber-security, including those which may relate to cloud service providers.<sup>41</sup> The report aims to ensure that policymakers take an ethical and transparent approach when drafting new action plans and implementing new laws to promote cybersecurity.

<sup>39</sup> Portugal's Resolution of the Council of Ministers No. 92/2019

<sup>40</sup> [Report on Cybersecurity in Portugal, Risks and Conflicts](#), May 2021

<sup>41</sup> [Report on Cybersecurity, Ethics and Law](#), December 2020.

In January and February 2022, the Agency for Modernization of Public Administration (AMA) carried out a public consultation on the 'Guidelines for Ethical, Transparent and Responsible AI'. The Guidelines, proposed by AMA, presents a framework for the responsible use of AI and acts as a reference point for the implementation of ethical, transparent and responsible AI. The principles are to be based on five pillars of accountability, transparency, explainability, fairness and ethics. Although the focus of the Guidelines is on the public sector, if approved, the Guidelines may also be used as a tool for development of AI projects by the private sector.

Such policies ensure that Portugal will continue to strike the right balance between creating a secure and robust cyber-landscape whilst maintaining the interests and fundamental rights of businesses, other stakeholders and individuals.

## Conclusion

---

Portugal offers an unparalleled location in which to establish a data centre, by striking a unique and unmatched balance between adherence to best practices in the law and regulation of data protection, whilst consistently ranking as one of the most business-friendly, stable and open jurisdictions in the EU. Portugal already benefits from an abundant, and ever expanding, network of fibre optic cables which position it as the "European gateway" country to Africa, the Americas and further afield. In terms of data protection, the country's legal framework and enforcement regime is notably attractive to large technology companies and hyperscalers, by providing a collaborative, confidential and supportive approach to setting and enforcing data protection standards. In terms of cybersecurity, Portugal's ranking has increased exponentially under international scoreboards since 2018, as evidenced through the Portuguese Government's commitment to

enhancing cybersecurity preparedness and increasing cybersecurity awareness. Moreover, over the next few years, Portugal is expected to go from strength to strength in establishing itself as the leading hub for large technology companies and hyperscalers. Through new policies and initiatives such as its Action Plan for Digital Transition and its National Strategy on Artificial Intelligence, Portugal is well-positioned not only to keep pace with the digital transformation but also to continue its journey as one of the European frontrunners for technological innovation.

All of these characteristics make Portugal a highly desirable jurisdiction in which to establish and operate a data centre, and ensure that Portugal is likely to develop further its position as a trailblazer for innovation, cybersecurity standards and data protection for the foreseeable future.



Transformative  
Legal  
Experts



Akin Gump has prepared this paper at the request of a consultant for Start Campus. Akin Gump's contributions herein are limited to Akin Gump's particular expertise. Akin Gump is not licensed to practice law in Portugal, and it is not opining on Portuguese law, regulatory activity, or government planning. References herein to network connectivity and geographic features are based on public source materials, and Akin Gump is not expressing conclusions on scientific and engineering topics.

This paper was prepared for information purposes only. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No reliance may be placed on this paper or any part thereof by you. No representations or warranties, express or implied, have been made as to the accuracy, completeness or sufficiency of this paper, or for any errors, omissions or misstatements, negligent or otherwise, relating thereto and no duty has been formed or obligation owed regarding this paper or to provide any updates with respect to information set forth in this paper.