



the global voice of  
the legal profession®

IBA Intellectual Property, Communications  
and Technology Law Committee

## Digital Regulations in the Metaverse Era **SÃO TOMÉ AND PRÍNCIPE**

Regional coordinator:

Docia Agyemang Boakye *technology and innovation lawyer, Accra*



# Data

Magda Cocco *Vieira de Almeida, Lisbon*Iakovina Kindylidi *Vieira de Almeida, Lisbon*

---

## 1. Are there any data (personal and non-personal) policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Although São Tomé and Príncipe (STP) currently lacks specific data protection policies, strategies or regulations explicitly addressing the metaverse, the existing legal framework for data protection applies.

The Personal Data Guarantee and Protection Law (Law 03/2016) in STP closely mirrors the European Data Protection Directive (Directive 95/46/EC) and aims to safeguard privacy and individual liberties concerning personal data by promoting transparent processing practices. This law boasts a wide-ranging scope of application, extending protection to all types of personal data of individuals. It applies to the processing of personal data, whether paper-based or through digital means, in the following circumstances:

- concerning the involvement of a data controller headquartered in STP;
- when processing occurs within a controller's establishment in STP;
- when the application of STP law applies due to international public law, even if the processing occurs outside the country; and
- when the utilisation of equipment, whether automated or not, is located in STP by a controller not based in the country, with the exception of equipment used solely for transit purposes.

STP has recently tackled data sharing and governance in public institutions, through the National Framework for Interoperability (Law 1/2024).

Furthermore, STP is a signatory to the African Union Convention on Cyber Security and Personal Data Protection. The convention establishes a framework for addressing cybersecurity, cybercrime and data protection across Africa, offering guidelines to safeguard personal data from privacy infringements related to activities such as the collection, processing, transmission, storage and utilisation of data.

In relation to non-personal data, without prejudice to the specific responses provided in the questions below, the protection of non-personal data is not specifically addressed in the STP legal framework. Moreover, there are no policies or strategies addressing non-personal data in the context of the metaverse.

---

## 2. How is the various personal and non-personal data associated with the metaverse protected in your jurisdiction?

Although not specifically referring to data in the metaverse or to novel data categories, the Personal Data Guarantee and Protection Law is applicable to personal data processing activities concerning the metaverse, involving data such as user or third-party data collected through devices and peripherals, inferred data or avatars. Consequently, the relevant provisions concerning the principles of data processing, data subject rights, the responsibilities of controllers and processors, and the relevant obligations are fully applicable in this context.

However, it should be noted that novel types of data, such as synthetic data, raise new regulatory challenges, since the current framework does not address them adequately.

Moreover, intellectual property (IP) rights may apply to certain non-personal data, subjecting it to the protection of the applicable legal regime. For more complete analysis of IP law in the metaverse, please refer to the chapter on intellectual property.

---

### **Q 3. Who are the different stakeholders are involved in the data value chain in the metaverse and, in the case of personal data, what are their data protection roles? How are their activities regulated under regional/national policies, strategies or regulations?**

Due to the diverse technologies and activities within the metaverse, the data value chain can be complex, involving various stakeholders who support and engage with the metaverse. These stakeholders may include content creators, platform and service providers, data intermediaries, analysts, regulators, researchers and users.

Accordingly, depending on the nature of their activities, they may be subject to different rules and obligations. Given that the same stakeholder may assume multiple data-related roles, a case-by-case analysis and clear mapping of the data flows is necessary.

---

### **Q 4. In relation to personal data, what are the data protection principles (eg, transparency) applicable to the metaverse? What are the most common types of infringement of data protection principles in relation to the metaverse (eg, data minimisation) in your jurisdiction?**

The STP constitution enshrines the principle of the protection of private life, under which all citizens are entitled to the protection of their personal identity, private and family life.

The Personal Data Guarantee and Protection Law serves as the primary legal instrument embodying the principles on data protection. These principles include:

- lawfulness, necessitating that personal data processing adhere to lawful and fair practices, in accordance with the principle of good faith;
- transparency, requiring personal data processing to occur transparently, while respecting individuals' right to privacy;
- proportionality, dictating that processed personal data should be relevant, adequate and not excessive, concerning the purposes that justified its collection and processing;
- minimisation, mandating that personal data collection and processing occur for specific, explicit and legitimate purposes, as outlined in defined legal or statutory bases, while ensuring that the data is retained only for the necessary period to achieve the purposes of its collection and processing, followed by erasure or anonymisation; and
- veracity, requiring that processed personal data remains accurate and up to date, with necessary measures taken to rectify or erase inaccurate or incomplete data.

The law establishes a range of fines and criminal sanctions for various breaches, including violations of the data protection principles, obligations and rights, as well as unauthorised data communication or transfer.

The Data Protection Agency (Agência Nacional de Proteção de Dados Pessoais or ANPD) is tasked with imposing fines, as well as ancillary measures, such as data cessation, blocking, deletion or destruction.

A failure to properly notify or the provision of fraudulent information to the agency can result in fines ranging from STN 50m to STN 120m for individuals and from STN 250m to a maximum of STN 500m for legal entities.

Regarding criminal liability, most intentional data protection-related violations can be punished with fines of upwards of 120 days' salary and/or one year imprisonment. For unlawful access to personal data, the sanctions are the same, with the possibility of being doubled if certain factors are verified. The destruction of personal data can be sanctioned with fines of up to 150 days' salary or two years imprisonment.

The number of days in a fine is set following criteria that considers the circumstances and gravity of the crime. Afterwards, the value of the days is calculated according to the economic situation of the defendant. Each day may be valued between STD 10,000 and STD 100,000 (approximately between €0.40 and €4.06).

There is no case law or any decisions by a regulator regarding infringements of these rules in regard to the metaverse, as this is a new and evolving phenomenon.



## **5. In relation to non-personal data: how is data sharing/licensing regulated in your jurisdiction? Is data ownership recognised? How is proprietary information, including any rights to datasets, regulated in your jurisdiction? What are the most common types of infringement of these rules in regard to the metaverse (eg, unlawful use of proprietary information) in your jurisdiction?**

The sharing and licensing of non-personal data is not specifically regulated in STP.

The Law on the National Framework for Interoperability aims to create, among other things, a data governance framework to facilitate data sharing by public authorities. Despite encompassing various goals and objectives in alignment with international standards, specific measures have yet to be implemented due to its recent publication.

Data ownership is not explicitly recognised by STP law, as information is not protected by a property right. However, data may be subject to other types of rights or interests, such as IP rights and contractual rights.

There is no information on any infringements of these rules in the metaverse in STP.

There is no case law or any decisions by a regulator regarding infringements of these rules in the metaverse, as this is a new and evolving phenomenon.



## **6. Are there any policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?**

There are no specific policies, strategies or regulations applicable to digital marketing in the metaverse in STP.

Nonetheless, without prejudice to the rights recognised in regard to data subjects in STP under the Personal Data Guarantee and Protection Law, specifically in relation to digital marketing, data subjects may exercise their right to object to the processing of their personal data for direct marketing or any other form of commercial communication and their right to be informed, at no additional cost, before their personal data is communicated to or used on behalf of third parties for direct marketing purposes, as well as their right to object.

Failure to comply with these requests constitutes a violation of the law, potentially leading to administrative fines and further sanctions if non-compliance persists, as mentioned above.

There is no case law or any decisions by a regulator regarding infringements of these rules in regard to the metaverse, as this is a new and evolving phenomenon.

---

**Q 7. Are there any policies, strategies or regulations in your jurisdiction focused on ensuring the protection of minors' data? What is the age of consent for data protection purposes? Is it necessary to verify the consent provided by a responsible adult?**

STP's Personal Data Guarantee and Protection Law does not contain specific provisions addressing the protection of minors' personal data. Consequently, concerning data protection matters, the age of consent is governed by the overarching legal framework, which stipulates that only individuals aged 18 or above can lawfully provide consent.

---

**Q 8. How are international data transfers regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of these rules in your jurisdiction?**

International transfers of data are regulated by STP's Personal Data Guarantee and Protection Law. The law stipulates that transfers of data must only occur if the laws of the destination country guarantee an adequate level of protection. In cases where this is not assured, exceptions may be made, such as for the purposes of contractual obligations or to safeguard the vital interests of the data subject.

Prior to commencing any processing activities, the data controller is required to notify the ANPDP or obtain authorisation for specific types of data processing. The ANPDP maintains a public register of all authorised data processing activities and issues reports detailing its decisions and opinions regarding legal matters.

---

**Q 9. How is automated decision-making regulated in your jurisdiction? Is there any case law or are there any decisions by a regulator regarding infringements of the rules applicable to automated decision-making in your jurisdiction?**

Under STP's data protection framework, individuals have the right not to be subject to decisions that have a significant impact on them, or produce legal effects, solely based on automated data processing designed to assess aspects of their personality, such as their professional capacity, creditworthiness, trustworthiness or behaviour. Nonetheless, exceptions exist in cases where decisions are made within contractual obligations or are authorised by law, provided that appropriate measures are implemented to protect the interests and rights of the data subject.

There is no case law or any decisions by a regulator regarding infringements of these rules in regard to the metaverse, as this is a new and evolving phenomenon.

---

**Q 10. What rights are granted to individuals for protecting their rights in the metaverse and how can they be exercised? What is the level of enforcement based on private claims in your jurisdiction?**

Although not explicitly referring to the metaverse, the law on data protection sets out the following rights for data subjects:

- right of access: individuals have the right to obtain confirmation as to whether or not personal data concerning them is being processed and, if so, be given access to that data and certain information about how it is processed;

- right to object: individuals have the right to object to the processing of their personal data in certain situations, such as for direct marketing purposes;
- right to not be subject to decisions based on automated processing: individuals have the right not to be subject to a decision based solely on automated processing which evaluates aspects of their personality, like their professional capacity or trustworthiness, and impacts their legal standing or significantly impacts their wellbeing; and
- right to compensation: individuals have the right to claim compensation for losses arising from illegal data processing or a breach of data protection laws. However, data controllers may be exempt from some or all liability if they can prove that the damage was caused by factors beyond their control.

To exercise these rights in the context of the metaverse, individuals would likely need to engage with the platforms or service providers operating within the metaverse environment, as well as lodge a complaint with the ANPDP.

The level of enforcement of these rights in STP is not clear.

In relation to non-personal data, without prejudice to specific rules, especially in relation to trade secrets, such rights are usually regulated contractually.

---

## 11. Are there any upcoming policies, strategies or regulations that will impact the use of data in the metaverse?

There are no announced or forthcoming policies, strategies or regulations that might affect the utilisation of data within the metaverse. Additionally, there have been no new policies or regulations introduced to amend the existing personal data protection framework. However, in the 2020 National Strategy for Digital Governance, a new initiative was included for a legal framework aimed at encouraging data sharing in the delivery of public services.

# Cybersecurity

## 1. Are there any cybersecurity policies, strategies or regulations applicable to the metaverse in your jurisdiction?

There are no specific policies, strategies or regulations addressing cybersecurity within the metaverse in STP.

However, there are various strategies and regulations addressing cybersecurity in STP.

In the *National Sustainable Development Plan for São Tomé and Príncipe 2020–2024*, there is a focus on enhancing e-government services, which involves the development of policies within the legal framework for data protection and cybercrime.

Furthermore, the *2020 National Strategy for Digital Governance* outlines objectives at the legislative level, including the implementation of a data governance framework to enhance data sharing for improved public services and increased transparency around the provision of government information, such as public procurement.

STP's commitment to cybersecurity is evident through its participation in the African Union Convention on Cyber Security and Personal Data Protection (Resolution 42/XII/2023 and Presidential Decree 24/2023), which entails the adoption of legislative measures on cybersecurity and personal data protection.

Cybercrime in STP is regulated by the Criminal Code (Law 6/2012), the Cybercrime Law (Law 15/2017), while the Personal Data Guarantee and Protection Law includes some provisions that penalise the unauthorised destruction of personal data.

Moreover, there is not a formally recognised national computer incident response team in STP.

## 2. What are the security by design principles applicable to the metaverse in your jurisdiction?

There is currently no implementation of security-by-design principles in regard to both physical and digital interfaces within the metaverse in STP.

Notwithstanding, the Personal Data Guarantee and Protection Law requires data controllers to implement suitable technical and organisational measures to safeguard personal data from accidental or unlawful destruction, unauthorised access, alteration, dissemination or loss. Data controllers are responsible for ensuring that the data processors that they engage also adhere to these measures.

Despite the recognition of cybersecurity legislation as essential for digital transformation in the 2020 National Strategy for Digital Governance, STP has not yet ratified an officially approved national or sector-specific cybersecurity framework aligned with globally accepted standards. Additionally, there is no formally recognised national computer incident response team in STP.

## 3. Have there been any cyber incidents in the metaverse in your jurisdiction? How do the applicable policies, strategies or regulations deal with cyber-incidents?

There have been no reported cyber incidents within the metaverse in STP. However, in the event of such occurrences, the country possesses legislation on cybercrime that could be applicable to address such actions.



STP's Cybercrime Law encompasses provisions covering various cybercrimes, including:

- computer falsehood;
- damage to computer programs or other data;
- computer sabotage;
- unlawful access;
- unlawful interception;
- unlawful reproduction of a protected program; and
- insertion of false data.

Violations of these provisions can result in penalties of imprisonment for up to ten years and/or fines.

Additionally, the Cybercrime Law includes procedural provisions to facilitate the adequate access, seizure and preservation of data, such as traffic data, emails, communication records and general computer data. These measures are crucial for investigating crimes and utilising evidence in criminal proceedings.

Moreover, STP's Criminal Code also addresses computer and communications fraud, punishable with imprisonment ranging from three to eight years, along with fines, depending on the aggravating circumstances. Furthermore, devastation caused through information technology is punishable with imprisonment ranging from one to two years, again depending on the aggravating circumstances.

In addition to criminal penalties, perpetrators may also face civil liability, which may include obligations to repair or compensate the injured parties for the damage incurred.



#### **4. Are there any cybersecurity standards in your jurisdiction specifically applicable to the metaverse? What are the main obligations they set out?**

STP does not have in place a comprehensive framework that establishes cybersecurity standards. As such, there are no cybersecurity measures applicable to the metaverse.



# Digital identity and authentication

## 1. Are there any digital identity and authentication policies, strategies and regulations applicable to the metaverse in your jurisdiction?

There are no specific policies, strategies or regulations addressing matters related to digital identity specifically within the metaverse in STP.

STP has longstanding civil registration and identification systems. In 2018, the Computerisation and Simplification of Civil Registration and Identification Acts and Procedures aimed to streamline and modernise these processes. This decree included provisions for digitising certain acts and procedures, as well as approving new models for certificates and personal identifiers (IDs).

Despite these efforts, there may still be uncertainties regarding the full implementation of digital processes for all civil registration and identification acts, including requests concerning a person's nationality.

Currently there is no official database for civil identification, residence visas, certificates or nationality documentation. Moreover, there are no clear linkages between the registration and identification databases and any other database systems, such as SIGA (the integrated system for the management of certificates/inscriptions).

Although biometric data is collected in STP, specific details about the types of data collected are not readily available.

## 2. What are the different types of digital identity in the metaverse: what are the different tiers and types of ID and what are the different levels of protection in your jurisdiction?

In STP, there are currently no distinct types of digital identity that are specifically applicable to the metaverse.

The country employs several government-issued civil identification systems for individuals, serving various purposes. These systems can generally be categorised into two main groups:

- foundational systems, which encompass civil registration, civil identification and identification systems for foreigners; and
- functional identification systems, which include identification for social security, labour and employment, taxation, voting, passports, education, health and other purposes.

However, the laws governing these identification systems lack provisions for utilising electronic means, including remote access.

Furthermore, the utilisation of these identification systems for e-commerce and e-government purposes still lacks comprehensive legal frameworks and implementation measures. However, recent changes have been made in the realm of data sharing between public entities, notably through the introduction of the National Framework for Interoperability. These changes aim to enhance connectivity and cooperation between different systems within government infrastructure.

## 3. How is self-determination exercised and protected in the metaverse in your jurisdiction?

There are no specific policies or regulations directly addressing self-determination within the metaverse in STP.



However, it is important to note that the Constitution of the Democratic Republic of SPT safeguards the self-determination of its people and residents, guaranteeing their fundamental rights, including the freedom of speech and expression. These constitutional protections extend to the online presence of individuals, which encompasses digital platforms such as the metaverse.

---

**Q 4. How is the role of intermediary ID providers regulated in your jurisdiction? What are some of the main obligations?**

The role of intermediary ID providers is not regulated in STP.

---

**Q 5. Are there any upcoming policies, strategies or regulations that will impact the digital identity and authentication processes in the metaverse?**

There are no upcoming policies, regulations or strategies impacting digital identity in the metaverse in STP.

# Intellectual property

## 1. What public policies, strategies or regulations are applicable to intellectual property in the metaverse in your jurisdiction?

There are no specific policies, strategies or regulations addressing matters related to IP in the metaverse in STP.

STP acknowledges the protection of IP as a fundamental right in its constitution. Additionally, the country has been a member of the World Intellectual Property Organization (WIPO) since 1998 and is a party to several treaties and conventions on IP, including the WIPO Convention, the Berne Convention, the WIPO Copyright Treaty, the WIPO Performances and Phonograms Treaty, the Paris Convention and the Patent Cooperation Treaty.

The Law on Copyright and Related Rights Code (Decree Law 2/2017) and the STP Industrial Property Code (Decree Law 23/2016), which addresses patent law, trademarks, designs and designations of origin, have a broad scope of application and could encompass works created in the metaverse.

## 2. How are intellectual property rights concerning ‘virtual objects’, ‘buildings’ and ‘avatars, etc, protected in your jurisdiction?

‘Virtual objects’, ‘buildings’ and ‘avatars’ may be eligible for protection, depending on their specific characteristics. The most significant forms of protection that may apply include:

- copyright and related rights: copyright protection does not require the fulfilment of administrative requirements or formalities and is automatically granted upon creation of the work; and
- designs (*desenho industrial*): protection is subject to registration.

## 3. How are digital replicas of physical objects protected in your jurisdiction?

STP does not have a specific legal framework protecting digital replicas of physical objects. Notwithstanding, depending on the specific characteristics of the replica, it may be subject to protection under STP’s IP framework.

## 4. How is user-generated content and other derivative works protected in your jurisdiction?

STP’s Copyright and Related Rights Code aligns with the principles and standards outlined in the WIPO treaties and the Berne Convention, protecting various forms of literary and artistic works in all mediums. Therefore, in the metaverse and on other online platforms, copyright protection can be extended to most user-generated content if it meets both subjective and objective criteria. These criteria require the presence of an author and that the content qualifies as an original work, representing the intellectual expression of the author.

While the Copyright and Related Rights Code may not explicitly address the existence of derivative works, they can still be protected by copyright if authorised by the rightsholder of the original work, or if an exception or limitation to copyright protection applies.



## **Q 5. Are there any collective rights management organisations active in your jurisdiction that also manage intellectual property rights in the metaverse?**

Collective rights management organisations are regulated under Decree Law 12/2022 and must be registered with the National Service of Intellectual Property and Quality of São Tomé and Príncipe (Serviço Nacional da Propriedade Intelectual e Qualidade de São Tomé or SENAPIQ-STP), the competent authority for IP in STP. However, there are no collective rights management organisations currently operating in STP for copyright in general, and IP in the metaverse in particular.

## **Q 6. How are intellectual property rights protected and enforced in the metaverse in your jurisdiction?**

STP's Copyright and Related Rights Code establishes both civil and criminal liability for infringements of copyright and related rights. In relation to criminal sanctions, the law criminalises various acts of infringement, with special provisions covering the usurpation of other works, counterfeiting and infringement of moral rights. Offenders can face fines ranging from 150 to 250 days' salary or imprisonment for up to three years.

Crimes may be punishable by fines in 'days', which are valued between STD 10,000 and STD 100,000 (approximately between €0.40 and €4.06). Moreover, in criminal proceedings, illicit copies or counterfeits can be seized. Civil liability is applicable independently of criminal liability or any ongoing criminal proceedings.

The Copyright and Related Rights Code also establishes administrative fines and procedures for various infringements related to a lack of identification of rightsholders. Such infringements may be subject to fines ranging from STD 2m to STD 20m (approximately €81.35 to €813.89). The Industrial Property Code sets out criminal sanctions for violations of industrial property rights, including patents, designs and trademarks. Offenders can face fines of up to 360 days or imprisonment for up to three years, as explained above. Criminal proceedings for these infringements are often dependent on a complaint or participation. Finally, the unfair competition and/or the use of privileged information and trade secrets are subject to administrative procedures, with fines ranging from STD 5m to STD 50m (approximately €203.39 to €2,032.79) for legal entities (ie, not natural persons).

In criminal proceedings, illicit copies or counterfeits can be seized. Civil liability is applicable independently of criminal liability or any ongoing criminal proceedings.

The Copyright and Related Rights Code also establishes administrative fines and procedures for various infringements related to a lack of identification of rightsholders. Such infringements may be subject to fines ranging from STD 2m to STD 20m.

The Industrial Property Code sets out criminal sanctions for violations of industrial property rights, including patents, designs and trademarks. Offenders can face fines of up to 360 days' salary or imprisonment for up to three years. Criminal proceedings for these infringements are often dependent on a complaint or participation.

Unfair competition and/or the use of privileged information and trade secrets are subject to administrative procedures, with fines ranging from STD 5m to STD 50m for individuals and STD 25m to STD 250m for legal entities.

There is no case law or any decisions by a regulator regarding infringements of these rules in regard to the metaverse, as this is a new and evolving phenomenon.

## **Q 7. Are there any intellectual property strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote interoperability in the metaverse?**

There are no IP policies, strategies or regulations in STP with the aim of promoting interoperability in regard to the metaverse.

---

**Q 8. Are there any competition strategies, policies or regulations in your jurisdiction applicable to the metaverse that aim to promote standardisation and access to fair and non-discriminatory licences?**

While there may not be specific strategies, policies or regulations aimed at promoting competition and standardisation, there are provisions within the Industrial Property Code that address access to licences over critical patents through a mandatory licensing scheme.

This mechanism allows for the imposition of licences if the patent holder is deemed to be insufficiently exploiting the patent or if there are valid reasons based on the public interest to ensure access to the licence. In other words, if a patent holder is not utilising its patent effectively or if granting licences would serve the broader public interest, such as promoting innovation or ensuring access to essential technologies, then mandatory licensing may be imposed.

---

**Q 9. What are the different roles of metaverse providers?**

STP law does not have a legal framework that clearly defines roles that can be applicable to metaverse providers. Under the Copyright and Related Rights Code in STP, it is highly unlikely that metaverse providers are considered as co-authors, publishers or editors of user-generated content.

---

**Q 10. How does your jurisdiction moderate content and how does it balance this with freedom of expression?**

There is currently no specific legal framework addressing the liability of intermediary service providers, such as hosting services and online platforms, for content provided by their users. Consequently, there are no rules regarding content moderation and potential conflicts with the freedom of expression and other fundamental rights.

---

**Q 11. Are there any by-design notice mechanisms?**

There are no by design notice mechanisms stipulated in the current legal framework in STP.

---

**Q 12. Are there any upcoming policies, strategies or regulations relating to intellectual property in your jurisdiction?**

There are no upcoming policies, strategies or regulations impacting IP in STP.



# Digital marketing and consumer protection

## **Q 1. Are there any relevant policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?**

There are no specific policies, strategies or regulations addressing matters related to digital marketing in the metaverse in STP.

Moreover, please note that there is no advertising law in STP. However, there is a general obligation under the Consumer Protection Law (Law 9/2017) to ensure that any advertising is lawful and clearly defined as such. However, the means of such identification is not specified.

Additionally, please refer to the chapter on intellectual property, regarding the sanctions applicable to unfair competition practices related to industrial property.

Please refer to the chapter on data for the data protection-related implications of digital marketing.

## **Q 2. Are there any relevant policies, strategies or regulations regarding misleading advertising or other unfair commercial practices in regard to the metaverse in your jurisdiction?**

There are no specific policies, strategies or regulations addressing matters related to misleading advertising or other unfair commercial practices in the metaverse in STP.

Under the Consumer Protection Law, there are several information duties applicable to traders, producers, distributors and packagers. If the information provided about a good or service is inadequate, illegible, ambiguous or missing, and this affects the consumer's ability to use it properly, the consumer has the right to cancel the contract within seven working days of receiving the goods or signing the service provision contract.

While the Consumer Protection Law does not impose criminal or administrative penalties for violating these provisions, any damage caused may lead to civil liability. Additionally, consumer rights associations are authorised to request the correction or removal of any misleading or abusive advertising.

Additionally, please refer to the chapter on IP regarding the sanctions applicable to unfair competition practices related to industrial property.

Please refer to the chapter on data for the data protection-related implications of digital marketing.

There is no case law or any decisions by a regulator regarding infringements of these rules.

## **Q 3. Are there any relevant policies, strategies or regulations aiming to promote consumer protection in the metaverse in your jurisdiction?**

There are no specific policies, strategies or regulations addressing matters related to consumer protection specifically in the metaverse in STP.

STP's Consumer Protection Law regulates various aspects of consumer rights and protections. This law addresses information requirements, consumer rights, prohibitions against abusive contract clauses and the involvement of public entities in promoting consumer protection. It also outlines the establishment and functions of the National Council for

Consumers (Conselho Nacional do Consumo) and recognises the role of consumer rights associations in advocating for consumer interests.

---

#### **4. What is the minimum information that should be provided to consumers? Who are the stakeholders responsible for providing this information?**

STP's Consumer Protection Law outlines general and mandatory information disclosure requirements for suppliers and service providers. These requirements aim to ensure that consumers receive comprehensive and transparent information about the goods, services or rights being offered on the market. Suppliers and service providers must furnish clear and objective information regarding the products or services they offer. This information should cover the essential aspects of the product or service, such as the characteristics, composition, pricing, guarantees and post-purchase assistance. The obligation to provide adequate information extends to all actors involved in the production–consumption cycle, including manufacturers, importers and distributors.

Consumers retain the right to withdraw from a service or sales contract if they find that the information provided is inadequate or misleading.

Any party failing to fulfil the duty of adequately informing consumers may be held liable for damages. This liability extends to manufacturers, importers, distributors and other relevant parties involved in the supply chain.

Please refer to our response above regarding the possible sanctions.

There is no case law or any decisions by a regulator regarding infringements of these rules.

---

#### **5. Are there any relevant policies, strategies or regulations applicable to platform-to-consumer relationships in your jurisdiction? What are the main obligations of platform providers?**

There are no specific policies, strategies or regulations addressing matters related to platform-to-consumer relationships in the metaverse in STP.

Notwithstanding, the Consumer Protection Law is applicable. In addition to the information-related obligations outlined above, terms in contracts that create a significant imbalance between the parties to the detriment of the consumer are prohibited.

Please refer to our response above regarding the possible sanctions.

There is no case law or any decisions by a regulator regarding infringements of these rules.

---

#### **6. Are there alternative dispute resolution mechanisms available for consumers in your jurisdiction? How are they implemented in the metaverse?**

In STP, there is a legal framework for voluntary arbitration of disputes, as well as the establishment of arbitration centres. One such centre is the arbitration centre within the Chamber of Commerce, Industry, Agriculture and Services, established in 2020 (Decree Law 26/2020). However, this arbitration centre is limited in terms of its jurisdiction to disputes arising from commercial relationships or investment agreements.

Under Law 9/2016 governing voluntary arbitration, various aspects of the arbitration process are addressed, including the inclusion of arbitration clauses in contracts and the selection of arbitrators. While STP does have national jurisdiction for arbitration, its scope is confined to commercial and investment-related disputes. Additionally, Decree Law 5/2017 provides for the potential establishment of additional arbitration centres in the future.





Moreover, voluntary arbitration, including matters related to arbitration clauses and the selection of arbitrators, is regulated by Law 9/2016. Notwithstanding, mediation, conciliation and negotiation are not specifically regulated in STP.



**7. Are there any upcoming policies, strategies or regulations that will impact digital marketing in regard to the metaverse in your jurisdiction?**

There are no upcoming policies, strategies or regulations impacting digital marketing in STP.



**8. Are there any upcoming policies, strategies or regulations that will impact consumer protection in the metaverse in your jurisdiction?**

There are no upcoming policies, strategies or regulations impacting consumer protection in the metaverse in STP.

# Jurisdiction and governance

## 1. Are there any upcoming policies, strategies or regulations setting out rules on how to identify the governing law in the metaverse?

While STP does not currently have any explicit policies, regulations or strategies focused on governing laws pertaining to the metaverse, there are some existing international private law rules within STP's legal system that are relevant.

The STP Civil Code contains conflict of laws rules. Under STP's conflict of laws rules, contracting parties have the freedom to select the applicable law for the contract, subject to certain limitations. The chosen law must not be fraudulent or aimed at circumventing the obligations, and it cannot contravene the fundamental human rights or principles of STP's legal system. Additionally, the selected law must be reasonably connected to either the parties or the contract's subject matter, within certain parameters.

In cases where no law has been explicitly chosen or if the choice is deemed invalid under specific conditions, the STP Civil Code provides two supplementary criteria: the habitual residence of both parties and the place where the contract was concluded. However, these criteria might not be easily identified in certain metaverse disputes.

## 2. What are the regulators and government bodies for ensuring compliance with the applicable laws in the metaverse in your jurisdiction?

In STP, there are no regulatory bodies and government entities with enforcement powers dedicated specifically to enforcing compliance with the laws that govern the metaverse. However, as previously mentioned in other sections, such as the chapter on data, there are regulators responsible for specific affairs and sectoral activities that may have the authority to ensure compliance within the metaverse.

## 3. Are there any available dispute resolution mechanisms in your jurisdiction?

Please refer to our response on the matter in the chapter on digital marketing and consumer protection.

## 4. How is arbitration implemented in the metaverse in your jurisdiction?

Please refer to our response on the matter in the chapter on digital marketing and consumer protection.

## 5. Are there any upcoming policies, strategies or regulations on determining the governing law and jurisdiction in the metaverse in your jurisdiction?

There are no upcoming policies, strategies or regulations impacting the governing law and jurisdiction in regard to the metaverse in STP.