ITALIAN ACADEMY OF THE INTERNET CODE

POSITION PAPER

DEFINIZIONE DELLE INFORMAZIONI DA TRASMETTERE E DELLE SPECIFICHE TECNICHE PER LA REALIZZAZIONE, APPROVAZIONE E RILASCIO DELLE SOLUZIONI SOFTWARE DI CUI ALL'ARTICOLO 24 DEL DECRETO LEGISLATIVO 8 GENNAIO 2024, N. 1, AI FINI DELLA MEMORIZZAZIONE ELETTRONICA E DELLA TRASMISSIONE TELEMATICA DEI DATI DEI CORRISPETTIVI GIORNALIERI DI CUI ALL'ARTICOLO 2, COMMA 1, DEL DECRETO LEGISLATIVO DEL 5 AGOSTO 2015 N. 127

Summary: 1. Premise – 2. Equal treatment between RT suppliers and SSW producers and providers – 3. Burdens for operators – 4. Security and inalterability of data – 5. Compatibility with eIDAS regulation on advanced electronic seals and electronic registers – 6. Protection of personal data.

1. PREMISE

Pursuant to Article 2, paragraph 3, of Legislative Decree No. 127 of August 5, 2015 ("*Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'articolo 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23*"), the electronic storage and telematic transmission to the Italian Revenue Agency (AdE) of daily transaction data for tax purposes is carried out using technological tools (telematic registers, or RT) that ensure the inalterability and security of the data, including those enabling payments by debit and credit cards.

The new Article 24 of Legislative Decree No. 1 of January 8, 2024 ("*Memorizzazione elettronica e trasmissione telematica dei corrispettivi mediante apposite procedure software*") provides that the electronic storage and telematics transmission of the total amount of anonymous daily receipts may also be carried out through software solutions (SSW) that ensure the security and inalterability of the data. These SSW must comply with specific technical specifications defined by a Provision of the Director of the Italian Revenue Agency, notified to the European Commission, and referenced in this contribution.

Reference regulations:

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

- **Legislative Decree No. 1 of January 8, 2024 (“***Memorizzazione elettronica e trasmissione telematica dei corrispettivi mediante apposite procedure software*”);
- **draft provision of the Director of the Italian Revenue Agency**, concerning the “*Definizione delle informazioni da trasmettere e delle specifiche tecniche per la realizzazione, approvazione e rilascio delle soluzioni software di cui all’articolo 24 del decreto legislativo 8 gennaio 2024, n. 1, ai fini della memorizzazione elettronica e della trasmissione telematica dei dati dei corrispettivi giornalieri di cui all’articolo 2, comma 1, del decreto legislativo del 5 agosto 2015 n. 127*” (hereinafter, the “**Draft Provision of the Director of the Italian Revenue Agency”**);
- **draft technical specifications** implementing Article 24, paragraph 3, of Legislative Decree No. 1 of January 8, 2024 (Draft version of July 2024) – hereinafter, “**Draft Technical Specifications”**;
- **Legislative Decree No. 127 of August 5, 2015** (“*Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'articolo 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23*”)
- **provision of the Director of the Revenue Agency of October 28, 2016 –** which regulates (according to Article 2, paragraph 4, of Legislative Decree No. 127 of August 5, 2015) the information to be transmitted, the technical rules, the deadlines for telematic transmission, and the technical characteristics of the telematic registers (RT).
- **Technical specifications for the electronic storage and telematic transmission of daily transaction data as per Article 2, paragraph 1, of Legislative Decree No. 127 of August 5, 2015** (version 11.1) – hereinafter, “**Technical Specifications”**;

2. EQUAL TREATMENT BETWEEN RT SUPPLIERS AND SSW PRODUCERS AND PROVIDERS

The new Article 24 of Legislative Decree No. 1 of January 8, 2024, states that the electronic storage and telematic transmission of the total amount of anonymous daily receipts may also be carried out through software solutions that ensure the security and inalterability of the data. This provision adds a new tool alongside the traditional telematics registers (RT) rather than replacing them, and both must guarantee the security and inalterability of the data to be stored and transmitted. Although the new software solutions (SSW) have been explicitly designed to simplify and reduce the burden for VAT operators required to electronically store and transmit receipts using solely software solutions, the option remains for operators to choose between adopting an RT or an SSW.

In any case, the need for operators to be simplified, should not lead a Member State to establish market entry conditions for SSW producers that are more favourable and less burdensome than those imposed on RT producers, as this would undermine the principle of free competition. Instead, a comparison of the regulations with the Provision of the Director of the Revenue Agency and the

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

Technical Specifications governing the RT suggests that there appear to be fewer constraints for the producers and providers of SSW.

RTs, equipped with a fiscal module, consist of both hardware and software components. The definition of RT in the Technical Specifications refers to "a device equipped with a fiscal module and telematic transmission capability," where "fiscal module" is defined as "the hardware and software component that manages the fiscal part of the Telematic Register" (see Glossary of Technical Specifications).

Fiscal data is stored in a "non-volatile memory" (read-only) containing a program (fiscal firmware) for the exclusive management, logically and functionally separated from management software, and a "permanent memory" that is non-rewritable, designed to hold fiscal data (as well as a "working memory" that holds temporary data before it is consolidated into the permanent memory). The "permanent memory" is divided into two components: "summary memory" and "detail memory," both allocated within the enclosure containing the fiscal module, which is protected by a fiscal seal to ensure its inaccessibility. The "summary memory" is fixed immovably to the structure of the Telematic Register and is protected by thermosetting resin that ensures its inaccessibility and immovability (see Paragraph 2.1 of the Technical Specifications).

The fiscal seal is a physical seal consisting of a self-adhesive label made from material destroyed upon removal. Additionally, the central part must be transparent to make visible the closure system (e.g., screw) that secures the enclosure housing the fiscal module. The label features the RT symbol followed by the manufacturer's logo. The fiscal seal is affixed by the manufacturer. By applying the fiscal seal, the manufacturer certifies that the RT unit conforms to the model approved by the Italian Revenue Agency (AdE). For the approval process, AdE relies on the Commission to approve fiscal measuring devices, as per Article 5 of Ministerial Decree No. 23 of March 23, 1983 (see Paragraph 2.1 of the Technical Specifications).

Thanks to the presence of the fiscal seal, the access to the fiscal module is allowed only for authorized technicians (in compliance with the UNI EN ISO 9001:2015 standard) or personnel from the Revenue Agency for periodic checks and maintenance and/or repair interventions. The installation and activation of the RT at the operator's premises are carried out by laboratories and technicians authorized by the Revenue Agency, whose list is published on the Agency's website (see Glossary of Technical Specifications).

Within the aforementioned physical device, there is also a unique key that identifies the device, which must be included in the XML file containing the fiscal data to be transmitted. Specifically, the manufacturer verifies the correspondence between the device's serial number and the public key. For each RT, a key pair is generated. The private key, corresponding to the public key, is stored within the summary permanent memory, along with the device certificate issued by the Revenue Agency

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

(AdE) for signing the transaction data, which contains the unique identifier of the device (see Paragraph 2.3 of the Technical Specifications).

In the case of the SSW pursuant to Legislative Decree No. 1 of January 8, 2024, there are two fiscal modules (see Par. 2 of the Draft Technical Specifications):

- Fiscal Module 1 (MF1), defined as the Point of Emission (PEM), which can be an integral part of an app or management software and must be installed on a hardware device or system;
- Fiscal Module 2 (MF2), which must be installed on a hardware system capable of interfacing in web service mode with the AE system, defined as the processing point (PEL).

The software solutions referred to in Legislative Decree n. 1 of January 8, 2024, therefore, do not depend on a specific hardware device, the choice of which falls to the operator (unlike traditional RTs). It is stated that the MF1 must be installed on a hardware device or system (such as SmartPOS, PC, Tablet, or others), which, with its MF1 component, is defined as the Point of Emission (PEM) and is used for the secure recording of fiscal data related to the commercial transaction (for 48 hours from the cash register opening and, in any case, until complete transmission of the data to the PEL if it occurs after 48 hours), including electronic payment data; the issuance of the corresponding commercial document; the management of lottery flows (both deferred and instant); the transmission of data to the PEL; and the consultation of stored data. As for the hardware on which to install the software component MF2, it is stated that this hardware system must be capable of interfacing in web service mode with the reception system of AdE and is defined as the Processing Point (PEL) with its MF2 component. The PEL must ensure the proper functioning of the Fiscal Module 1 of the connected PEMs; prepare and transmit the daily XML file of operational reports; fiscally store the detailed data of individual transactions (digitally preserving them over time); prepare and transmit the XML file of daily telematic transaction data; manage lottery flows (both deferred and instant); and allow, upon request from auditors (Revenue Agency or Guardia di Finanza), the querying and extraction of detailed data on individual transactions conducted at the PEMs (see Par. 2 of the Draft Technical Specifications).

The approval phase by the Commission on Fiscal Measuring Devices is intended solely for the software components (see Par. 2 of the Draft Technical Specifications), not for the hardware device (or devices, considering that PEM and PEL can also be physically distinct). Furthermore, for the installation and configuration of the Point of Emission (which aims to uniquely associate a Serial Number of the PEM with the physical device, in the absence of a unique hardware identifier), the intervention of authorized parties is not required (see Par. 5.2 of the Draft Technical Specifications).

Just like the RTs, the PEM and PEL also have a dual public/private key system necessary for signing the fiscal data generated and to be transmitted to the PEL (in the case of the PEM) or to AdE (in the case of the PEL), equipped with appropriate certifications. In the absence of RTs, the storage of the

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

private keys related to the certificates used within the PEMs and PELs is regulated in a secure area that prevents extraction from that area and their duplication (while still allowing for the need to provide appropriately regulated backup procedures). For example, certified Smart Card solutions for CNS or Digital Signature and Hardware Security Modules or equivalent systems are mentioned. No specific certifications or minimum requirements are prescribed (see Par. 9.2 of the Draft Technical Specifications).

In summary, the separation between hardware and software that characterizes the new SSWs allows for greater freedom in choosing the physical devices on which to install the PEM and PEL, as well as the secure areas in which to store the private keys related to the certificates used within the PEMs and PELs. This difference effectively relieves producers and providers from the obligations imposed on RT suppliers, potentially resulting in a disparity of treatment.

3. BURDENS FOR OPERATORS

It is noted that the reduced obligations for the producers and providers of SSWs correspond to more significant exposure to liability and legal uncertainty for the operators.

As specified above, with traditional RTs, the hardware and software components are closely interconnected, forming a single unit. The compliance of the RT with the technical specifications is guaranteed by the manufacturer of the RT itself. In fact, the models of RT presented by manufacturers to AdE must be approved by them based on certification from the manufacturer attesting to conformity with the technical and functional characteristics specified in the Technical Specifications (par. 2.2 of the Technical Specifications); the application of the fiscal seal by the manufacturer then certifies the compliance of the RT specimen with the model approved by AdE (par. 2.1 of the Technical Specifications).

In this way, the operator can rely on certified devices; moreover, as noted, the operator has access to laboratories and technicians authorized by the Agency of Revenue, whose list is published on the AdE website, who carry out the installation and activation of the RT (par. 2.4 of the Technical Specifications), periodic verification activities, and interventions in case of malfunction or irregular operation (par. 2.5 and 2.6 of the Technical Specifications).

The new SW, on the other hand, does not rely on a specific hardware device. The responsibility of the Provider pertains to the software but not to the device, the choice of which falls to the Operator.

Consequently, it is stated in the draft technical specifications that the installation and configuration (on the device) of the PEM is the responsibility of the operator, with the support of the provider in communicating to AdE the identifying details that uniquely identify the installation of the approved MF1 software component on a specific device (par. 5.2 and 3.1.2 Draft Technical Specifications).

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

Additionally, the operator remains responsible for the security of the signed files residing in the memory spaces of the PEM, unless this hardware device is also provided by the provider (par. 9.3 Draft Technical Specifications). Another consequence is the absence of laboratories and technicians authorized by AdE.

A system designed in this way evidently exposes the operator to greater risk compared to traditional RTs, due to the responsibilities assigned regarding the security of the signed files residing in the memory spaces of the PEM and in the absence of laboratories and technicians specifically authorized to support it.

Therefore the result is contrary to the goal of simplifying and making less burdensome for VAT operators the electronic storage and transmission of daily takings through the use of exclusively software solutions.

4. SECURITY AND INALTERABILITY OF DATA

The issues described raise doubts about the ability of the new software solutions (SSW) to ensure an equivalent level of security and data inalterability, as required by the regulations. Specifically, **the new SSW exhibits a lower level of assurance regarding the security and inalterability of both the fiscal data stored in the PEM and PEL and the private keys related to the certificates used within the PEM and PEL**, especially when compared to traditional electronic cash registers (RT). This is primarily due to the lack of specification regarding technical characteristics and/or approval procedures to safeguard the inaccessibility of the hardware devices used for storing fiscal data and the private keys associated with the certificates used within the PEM and PEL, as well as the absence of provisions for personnel specifically authorized to access and intervene on the PEM and PEL.

IN LIGHT OF THE ABOVE, IT IS CONSIDERED NECESSARY TO PROVIDE CLARIFICATIONS AND ASSURANCES REGARDING THE MAINTENANCE OF EQUAL MARKET ACCESS CONDITIONS FOR BOTH RT SUPPLIERS AND SSW PRODUCERS AND PROVIDERS, WITHOUT BURDENING THE OPERATORS AND ENSURING AN EQUAL LEVEL OF SECURITY AND DATA INALTERABILITY BETWEEN THE TWO SOLUTIONS.

5. COMPATIBILITY WITH EIDAS REGULATION ON ADVANCED ELECTRONIC SEALS AND ELECTRONIC REGISTERS

The Electronic Cash Register (RT) transmits tax data to the Revenue Agency (AdE) at the end of each day through an XML file that is electronically sealed (par. 3.2 of the Provision of the Director of the Revenue Agency dated 28/10/2016). The authenticity, integrity, and confidentiality of the

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

transmitted information are ensured by the advanced electronic seal affixed to the file sent to the Revenue Agency's system and by a secure connection to that system via web service on an encrypted TLS channel (par. 7.1 of the Director's Provision). The Technical Specifications explicitly reference the definition of an advanced electronic seal as outlined in EU Regulation No. 910/2014 concerning electronic identification and trust services for electronic transactions in the internal market (eIDAS), which guarantees the origin and integrity of the transmitted file (see Glossary of Technical Specifications). The advanced electronic seal is produced using a signing certificate (in PKCS#10 format) issued by the Revenue Agency's Certification Authority, which is recorded in the permanent memory of the Electronic Cash Register, along with the private key generated during the production of the Register (par. 2.3, 2.4, and 5 of the Technical Specifications).

For the new Software Solutions (SSW), there is a dual transmission of tax data: from the Point of Emission (PEM) to the Point of Processing (PEL), and from the PEL to the Revenue Agency (AdE). **In this regard, a discrepancy is noted between what is outlined in the draft provision from the Director of the Revenue Agency and the draft Technical Specifications attached to the provision, which should be clarified.**

Indeed, in point 10.1 of the Draft Provision of the Director of the Revenue Agency, it is prescribed that "*L'autenticità, la inalterabilità e la riservatezza nella memorizzazione e trasmissione delle informazioni di cui al punto 6.1, è garantita dalle misure di sicurezza e dal sigillo elettronico avanzato apposto al file inviato al sistema dell'Agenzia delle entrate e dalla connessione protetta verso tale sistema in modalità web service su canale cifrato TLS, secondo le disposizioni delle specifiche tecniche*". This formulation, which generically refers to the fiscal data to be transmitted, appears to extend these measures (advanced electronic seal and secure connection in web service mode over a TLS-encrypted channel) to both the transmission from the PEM to the PEL and from the PEL to the AdE system.

On the contrary, in the Draft Technical Specifications, there is no reference to the advanced electronic seal mentioned above. It is exclusively specified that, concerning the transmission from the Point of Emission (PEM) to the Point of Processing (PEL), the XML files of individual transactions are sent in real-time to the PEL after being signed with the PEM certificate (in PKCS#10 format and uniquely associated with the PEM). Additionally, during cash closing, the Journal file of daily operations is also signed with the PEM certificate (see paragraphs 3.2.5 and 9.1 of the Draft Technical Specifications).

Furthermore, for the communication between the Point of Emission (PEM) and the Point of Processing (PEL) a "*protocollo di scambio dati privato in grado di garantire un adeguato livello di inalterabilità dei dati scambiati*" is required. The responsibility of ensuring "*il massimo livello di sicurezza che sia sufficiente a tutelare l'integrità, l'autenticità e il non ripudio*" of what is sent by the operator through the PEM lies with the Operator. In contrast, the secure communication between the

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

PEL and the AdE System is guaranteed by the use of the TLS 1.2 communication protocol and mutual authentication via X.509 certificate (see paragraph 9.3 of the draft Technical Specifications).

It would therefore be useful to rectify these discrepancies and specify the security measures required for data transmission from the Point of Emission (PEM) to the Point of Processing (PEL) and from the PEL to the AdE system. In any case, it is deemed necessary to extend the use of the advanced electronic seal and specific certified communication protocols to avoid disparities, not only concerning the level of integrity and security of stored and transmitted data but also between RT suppliers and producers and providers of Software Solutions (SSW).

In order to "make the management of commercial documents produced by the PEM more secure", a link is established between the various documents using a hash algorithm and the construction of chains of these hashes. For each commercial document produced and signed, the SHA256 hash is calculated and transformed into base 64. This also includes the hash of the immediately preceding document, "securely and immutably ensuring the concatenation of the various documents." Each Journal file must therefore contain the data of the recently issued commercial document, the hashes of the documents issued throughout the day, as well as the link to the previous Journal file and the file of daily receipts from the previous day. "To mitigate the risk of alterations" in the hash chain, the solution must include a specific component of the PEM capable of performing a verification within the open Journal of the chain in the blocks preceding the one to be inserted, and only if the result is positive can the new block be created. A negative result cannot be accepted as valid, and the Point of Emission must be blocked (par. 7.2 Draft Technical Specifications).

The mention of "*catene di hash*" is a technological tool lacking recognized legal and probative value. Upon further analysis, the concept of concatenating documents through the use of hash functions (such that the block of data contains an associated hash and also references the hash of the previous block) may evoke blockchain technology. It is worth noting that the recent eIDAS 2 Regulation (EU Regulation 2024/1183), which amends the eIDAS Regulation, has introduced specific rules regarding electronic registers, formulated in a technologically neutral manner with the clear intent of recognizing legal efficacy for blockchain. According to Article 3, no. 52, an electronic register is a sequence of recordings of electronic data that ensures the integrity and accuracy of the chronological order of such recordings. These guarantees are presumed in the presence of a qualified electronic register (Article 45-duodecies), which qualifies as such in the presence of specific requirements as per Article 45 *terdecies*. A qualified electronic register provided in one Member State is recognized as a qualified electronic register in all other Member States, in accordance with the principle of mutual recognition (Article 24-bis, no. 11).

The definition of an electronic register in the eIDAS 2 Regulation could abstractly encompass the hash chains introduced in the Draft Technical Specifications. This aspect should be clarified, both to provide assurances to the market regarding the actual legal effects recognized

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

for the tool used to consider the necessity of not hindering the implementation of the principle of mutual recognition among Member States that governs qualified electronic registers.

6. PROTECTION OF PERSONAL DATA

The regulations concerning the new software solutions (SSW) as per Article 24 of Legislative Decree No. 1 of January 8, 2024, require a prior consultation with the Italian Data Protection Authority in accordance with Article 36 of Regulation (EU) 2016/679 before proceeding with the processing of personal data (hereinafter, GDPR).

In this regard, compared to the traditional cash registers (RT), it is clear that the data controller is the Merchant. Specifically, concerning the RT, the Italian Data Protection Authority, in its measure No. 221 of December 18, 2019 (document web No. 9217337), expressed a favourable opinion on the document "*Specifiche tecniche per la memorizzazione elettronica e la trasmissione telematica dei dati dei corrispettivi giornalieri di cui all'art. 2, comma 1, del decreto legislativo 5 agosto 2015, n. 127*", stated that "*l'esercente in quanto TITOLARE DEL TRATTAMENTO dei dati presenti nelle memorie del registratore telematico (o del server RT) deve mettere in atto adeguate misure tecniche e organizzative al fine di garantire la conformità del trattamento al Regolamento".* Considerations that have been included in the latest version of the Technical Specifications related to the RT, where in paragraph 2.1 it states that *"L'esercente in quanto TITOLARE DEL TRATTAMENTO dei dati presenti nelle memorie del Registratore Telematico ai sensi dell'art. 24 del Regolamento Generale sulla protezione dei dati 2016/679 deve mettere in atto adeguate misure tecniche organizzative al fine di garantire la conformità del trattamento al Regolamento stesso".*

On this matter, concerning the new SSW, it is noted that there is an interposition between the Producer and the Merchant by the figure of the Provider, as "*soggetto, opportunamente qualificato, che rende disponibile all'esercente la soluzione software approvata dall'Agenzia nella sua interezza e assicura l'assistenza tecnica/operativa necessaria a gestire la stessa"*, nonché *"soggetto responsabile del corretto funzionamento e del rispetto dei vincoli della soluzione software nella sua interezza*" (Par. 3.1.2 Draft Technical Specifications).

The Draft Technical Specifications do not clarify the roles and respective responsibilities of the Merchant and Provider in the context of data protection regulations. Similarly to what is prescribed for the RTs, it could be inferred that the role of data controller belongs to the Merchant, as the entity responsible for processing data to fulfil the purposes related to their business activities, while the Provider can be classified as a data processor, defined under Article 3, No. 8, GDPR, as "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*").

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584

This clarification is essential because the introduction of the Provider, given the current wording of the Draft Technical Specifications, reduces the Merchant's ability to control the management of personal data that may be processed. In fact, once the data is transmitted from the PEM to the PEL, the Merchant effectively loses all control over the data, especially considering that the responsibility for storing and preserving the data produced by the PEM lies with the Provider (see paragraphs 3.1.2, 9.7, and 9.8 of the Draft Technical Specifications).

This framework, despite the provision that responsibility lies with the Provider, does not reconcile well in terms of liability arising from the processing of personal data. Article 82 of the GDPR establishes a general civil liability for the data controller, while the data processor assumes liability only if they fail to perform the specific tasks assigned to them by the Regulation or if they act contrary to the instructions of the controller.

Based on the above considerations, a scenario emerges in which the Merchant passively endures the choices of the Provider, unable to exercise any form of control, while being exposed to liability under the GDPR. The principles of accountability, privacy by design, and privacy by default that apply to the data controller (Articles 24 and 25 of the GDPR) indeed require the controller to carefully evaluate, ex ante, the capability of the tools used for storing and transmitting receipts to meet the GDPR requirements. This is especially true considering that the relationship between the controller and the processor is contractually regulated (Article 28 of the GDPR), making it increasingly common for data processors to configure their relationships with data controllers based on standardized contracts and adherence, effectively rendering the controller the weaker party in the relationship.

From this perspective, the considerations made earlier regarding a potentially lower level of assurance, compared to traditional RTs, about the security and immutability of stored and transmitted data are also relevant. This is because the data controller/Merchant is responsible for implementing appropriate technical and organizational measures to ensure a level of security commensurate with the risk and must be able to demonstrate this (see Articles 24 and 32 of the GDPR).

These considerations naturally affect not only the software aspect but also the hardware component. As previously highlighted, for the new tools, the choice of devices on which to install the software components or hold the private keys, unlike traditional RTs, is entirely the merchant's responsibility, in the absence of specific technical guidelines, certifications, and support from dedicated personnel. Therefore, **there is a reduced protection for the merchant in ensuring an adequate level of security for the processed data, as required by the relevant legislation, resulting in a plausible increase in costs for the merchant to compensate for the lack of guidance on this matter.**

Accademia Italiana del Codice di Internet
Via dei Tre Orologi 14/a 00197 Roma (RM)
Mail: italianacademyinternetcode@gmail.com
C.F. 97811820584