REPUBLIC OF SAN MARINO

REGULATION no. 20 of 30 December 2015

We the Captains Regent
of the Most Serene Republic of San Marino

Having regard to Article 42 of Law no. 174 of 27 November 2015;
Having regard to Congress of State Decision no. 14, adopted during its sitting of 23 December 2015;
Having regard to Article 5, paragraph 5 of Constitutional Law no. 185/2005 and to Article 13 of Qualified Law no. 186/2005;
Promulgate and order the publication of the following Regulation:

TECHNICAL REGULATION FOR THE PROTECTION OF PERSONAL DATA IN APPLICATION OF EXCHANGE OF INFORMATION IN TAX MATTERS

Art. 1
(Purpose and scope of application)

1. This Regulation shall apply to the technical rules of protection of personal data for the purposes of exchange of information in tax matters in accordance with the table in Annex "A".
2. This Regulation shall in particular establish:
   1. procedures for the assessment of staff and collaborators who may come in contact with the processing of data concerning exchange of information in tax matters;
   2. policies of protection of the sites and security of physical access;
   3. logical security of systems and networks used in data processing;
   4. management and configuration of security controls;
   5. internal controls and risk management;
   6. protection of data exchanged internationally and technical rules.

TITLE I
STAFF IN CHARGE OF THE PROCESSING

Art. 2
(Subjects responsible for data processing and relevant tasks)

1. The Financial Institution (hereinafter referred to as FI) and the Competent Authority (hereinafter referred to as CA) are data controllers since they effectively control personal data processing and are required to perform the following tasks:

a) to adopt decisions falling within their competence with respect to: the purposes and methods of processing personal data, the instruments used in the exchange of information in tax matters, including security profiles, the management and control methods, when these have not been entrusted to the data processor;
b) to appoint the data processor;
c) to appoint the person in charge of the processing;

d) to notify the request for authorisation for data processing for the purposes of this Regulation.
If the data processor is not appointed, his functions shall be performed by the data controller or by a natural person representing him.
2. The data processor, when appointed by the data controller, shall be required to:
a) manage the process of formation of flows for the exchange of information in tax matters;
b) perform formal and completeness checks on the flow of data collected;
c) manage the system of encryption and digital signature of information;
d) carry out checks on the activities performed by the person in charge of the processing in the transmission and receipt of acknowledgements.
With regard to the processing of non-electronic documents, the data processor of the CA shall be required to:
a) draw up written instructions aimed at the control and custody of the entire processing of non-electronic deeds and documents relating to the exchange of information in tax matters;
b) draw up, maintain and update, on a regular basis at least once a year, the list of persons in charge of the processing and the scope of their permitted processing.
3. The person in charge of the processing in the FIs shall be appointed by the data controller and shall be required to:
a) digitally sign the flow received by the data processor;
b) transmit the flow to the CA;
c) receive acknowledgements from the CA;
d) archive the acknowledgements of receipt.
4. The person in charge of the processing in the CA shall be appointed by the data controller.
With regard to the receipt of the flows coming from the FIs, he shall be required to:
a) receive the flows sent by the FIs;
b) decrypt any flow received;
c) perform formal and completeness checks on the flow of data collected by the FIs;
d) issue and send acknowledgements of receipt to the FIs;
e) archive the flows received from the FIs;
f) receive acknowledgements from the CA;
g) archive the acknowledgements of receipt.
5. With regard to the formation of flows to be sent to foreign jurisdictions (hereinafter referred to as FJs), pending protocols established at an international level, the person in charge of the processing in the CA shall be required to:
a) digitally sign the flows received from his data processor;
b) transmit every single flow to the competent FJs;
c) receive acknowledgements from the FJs;
d) archive the acknowledgements of receipt.
6. With regard to the receipt of flows coming from FJs, pending protocols established at an international level, the person in charge of the processing in the CA shall be required to:
a) receive the flows sent by the FJs;
b) decrypt any flow received;
c) perform formal and completeness checks on the flow of data collected by the FJs;
d) issue and send acknowledgements of receipt to the FJs;
e) archive the flows received from the FJs.
7. With regard to the processing of non-electronic documents, the person in charge of the processing of the CA shall be required to:
a) follow written instructions for the processing of non-electronic documents;
b) check and guard non-electronic deeds and documents entrusted to him;
c) return the documents or deeds exclusively to those who, in the process, are responsible for their keeping.

Art. 3
(Procedures for assessing staff and collaborators)

1. The staff responsible for the processing of information shall have specific professional experience or skills acquired in this field.

2. The FIs and the CA shall carry out specific screening of the staff in charge of data processing, at least annually:

a) in the FIs, professionals in charge of the processing with respect to exchange of information in tax matters shall be assessed and appointed by means of a decision of the management bodies (board of directors, CEO, etc.).
b) The CA shall be by definition the data controller. In the CA, the professionals in charge of the processing with respect to exchange of information in tax matters shall be public officials subject to the code of conduct under Law no. 141/2014 and shall be included in the staffing plan of the CA. The Director of the CA shall be responsible for the appointment of any data processor and of the persons in charge of the processing, the latter being compulsory.

3. In processing the information received from the FJs or from the FIs, the CA shall rely on a "Contact Person", i.e. its Director.

Art. 4

(Training of the staff responsible for the processing of confidential information)

1. The staff responsible for the processing of confidential information shall follow special on-going training courses in the field of data and information processing.
2. Both the FIs and the CA shall keep a special register in which information on organised courses are transcribed. Such information shall include, but is not limited to, the name of the course, its date and duration in days or hours, the business name of the organiser, the name/s of the staff involved.

Art. 5

(Policies concerning the termination of service of the staff and collaborators)

1. The staff and collaborators in charge of data processing shall also be subject to specific policies concerning the termination of service, in addition to ordinary administrative management activities common to all staff.
2. Leaving staff members shall have their login and authorisation credentials disabled and their smart card, or other means of access to both information systems and physical premises, shall be withdrawn.
3. In case they are transferred to other offices or to perform other functions, their login credentials shall be immediately revoked and shall be newly issued for the new position.

TITLE II
SECURITY OF PHYSICAL ACCESS TO PLACES AND ARCHIVES ENVISAGED IN THE PROTECTION PERIMETER

Art. 6

(Policies for the protection of the sites and physical access thereto)

1. Access both to premises and to archives containing data relative to exchange of information in tax matters shall be controlled. Any access by the staff for any purpose shall be previously authorised. Access can take place manually or through electronic systems. In case of manual access, the staff shall be first identified and registered. If access is controlled by electronic systems, staff members shall be registered upon access.
2. Access to local data centres of the Public Administration (hereinafter referred to as PA), where the servers used for exchange of information in tax matters are installed, shall be controlled. The staff, including of third parties, shall be previously authorised to access said sites. Manual access shall be allowed only to officials of the PA in emergency cases. The list of technical officials of the PA or their collaborators of third parties who can manually access and intervene in data centres shall be entered in a specific list kept by the CA. Manual access shall mean any access that excludes automatic registration system. With regard to ordinary activities, access shall be permitted only through electronic registration of access.

Art. 7
(Non-electronic document archives)

1. Particularly important are paper archives, especially where they contain data relating to exchange of information in tax matters.
The persons in charge of the processing shall be given written instructions concerning the control and custody, during the entire period of time necessary for the processing operations, of deeds and documents containing data relating to exchange of information in tax matters.
2. In its capacity as data controller, the CA shall draw up a list of persons in charge of the processing who can process paper documents and/or are responsible for their conservation and confidentiality protection.
The list of persons in charge of the processing may be drawn up according to homogeneous position classes or to authorisation profiles.
In the periodic updating of the list of persons in charge of the processing, to be carried out at least annually, the scope of processing allowed to each of them shall always be identified and indicated.
3. When deeds and documents containing data relative to exchange of information in tax matters are entrusted to the persons in charge of the processing for the performance of their tasks, such deeds and documents shall be checked and guarded by said persons until they are returned, so that these documents or deeds are not accessed by unauthorised persons and are returned to those responsible for their conservation upon completion of processing operations.
4. The staff responsible for the processing of deeds and documents shall maintain constant control over them and shall not leave them unattended on their desks. In case the staff leaves the working station, even temporarily, deeds and documents shall be stored in safe and protected places so as to avoid their taking, even temporarily.

TITLE III
LOGICAL SECURITY OF SYSTEMS AND NETWORKS USED IN THE PROCESSING WITHIN THE PROTECTION PERIMETER

Art. 8
(System and communications protection)

1. The CA shall be responsible, through the IT, Technology, Data and Statistics Office (hereinafter referred to as ITDS), for the entire communication channel with the FIs and, within the jurisdiction's perimeter, also with FJs.
Any data transiting through the communication network among CA, FIs and FJs shall be encrypted.
2. The CA shall be equipped with instruments for the management and monitoring of the various stages of exchange of information in tax matters.
3. Any access to the systems used for the purposes of this Regulation shall be allowed exclusively to authorised staff provided with specific electronic devices (smart cards) and login credentials.
4. IT security in the CA's working environment and in the offices authorised to perform assessments, such as the Tax Office, shall provide for the following: the confinement and encryption of networked communications and the installation of the working peripheral devices suitable to the degree of security required, such as desktop virtualisation (terminals) and exclusion of local storage or data transfer devices.
5. A specific network area shall be created on centralised server devices, where the applications dedicated to the CA's activities are located. Authorised staff shall have access only via smart card devices with a certificate of recognition on board the card. The database, which contains the data subject to protection in accordance with this Regulation, shall be encrypted and data access shall be prohibited to all staff, including technical and system experts, unless authorised by the official of the CA in possession of the relevant decryption certificate.

Art. 9
(System and information integrity)

1. Procedures, processes and systems to ensure the so-called "High Reliability" shall be implemented. For this reason, twin systems located in different sites shall coexist and be fully operational; they shall automatically replicate and, in case of failure or disaster in a site, they shall continue to guarantee operations without damaging the other site.
2. However, appropriate technical and organisational procedures shall be implemented for managing data and application backups at a frequency adequate to technical and operational activities and to security management, as established by the ITDS. Technical and organisational procedures to control past backups shall also be implemented in order to verify their proper use in case of recovery.
3. Appropriate measures shall be adopted to ensure recovery of access to data in case of damage of such data or of electronic instruments, in good time, meeting operational needs and in compliance with the time limits established in international agreements.

Art. 10
(Planning of implementation, development and updating of information security systems)

1. The offices responsible for planning the information systems available to the CA shall establish an implementation plan every three years.
2. In any case, periodical updates shall be made, at least yearly, of computer programs aimed at preventing the vulnerability of electronic instruments (including, but not limited to: Antivirus, Antispam, AntiMalware, Intrusion detection/prevention, Firewall software and/or Hardware etc.) and at correcting their deficiencies.
3. Moreover, specific upgrade policies shall be established with respect to the basic software of the systems, in order to ensure perfect compliance with the prerequisites of development of the system for exchange of information in tax matters.
4. Specific contracts of assistance, ordinary and extraordinary maintenance shall be concluded, as well as of plans to implement the application software, based on the requirements of international treaties on international tax cooperation.

Art. 11
(Management and configuration of security controls)

1. The IT security of the perimeter that contains, or may potentially contain data related to exchange of information in tax matters shall be managed internally by the ITDS, which shall periodically inform the CA of the plans of development and adjustment in the field of IT security. The CA may require third parties to check the security of the perimeter involved in exchange of information in tax matters.

Art. 12
(Identification and authentication of the staff responsible for the processing)

1. The data and information collected during the technical and organisational processes involved in exchange of information in tax matters shall be subjected to the following technical procedures of identification and authentication:

a) Authentication system:
   Through the ITDS, the CA shall provide human resources involved in the process of exchange of information in tax matters with appropriate authentication instruments to perform one or more of the data processing operations.
   The authentication instrument adopted in the Public Administration shall be the smart card with digital certificate on board the card. The smart card shall be issued upon recognition and signing of the terms of use and liability waiver.
   Upon request of the CA, nominal authentication credentials for the creation of secure communication channels (VPN) shall also be issued. These credentials shall be essentially composed of an identification code (Userid) and a Password. Once used, the code associated with

the person in charge of the processing (Userid) shall not be assigned to other persons, not even at different times.
After six months, the authentication credentials that have not been used shall be deactivated.
The Password shall be at least 8 characters. It shall not contain references related to the person in charge of the processing and shall be changed by him on first use of the electronic instrument and, thereafter, at least every three months.
Detection systems such as magnetic tokens, badges with RFID or biometric devices shall be used to open doors, activate alarms, register access to protected premises. Human resources shall be encouraged to take the necessary precautions to ensure the secrecy of access credentials, secret codes or passwords, as well as to properly guard the devices assigned to them and not to leave the electronic instrument unattended and accessible during a processing session (to this end, the systems shall enable the creation of a screen saver with password request).
Assignment process of credentials:

1. Internal staff of the CA and of PA offices
   The ITDS shall provide internal staff with an Electronic Identity (eID) via personal smart card containing the certificate of digital signature and the certificate of authentication, issued by an internationally recognised Certification Authority.
   The eID shall be assigned through visual recognition at the RAO of the ITDS.
   Following the delivery of the instruments (smart card and unlock codes) and instructions, persons shall be autonomous and liable with respect to signature (legally recognised) and encryption processes.
   The roles assigned and the credentials shall be identified and communicated by the CA to the ITDS, which shall enable access on the internal network of the PA to the specific protected areas.
2. External parties (Financial Institutions)
   The CA shall ask the ITDS for login credentials to the encrypted transmission system (VPN) for the persons in charge of the processing in each FI. The credentials shall be nominal.
   Following each single request, the ITDS shall create the Electronic Identity by providing temporary login credentials.
   Once he receives the credentials, the person in charge of the processing in the FI shall be obliged to change the password on the first access.
   FIs shall be required to provide recognised and legally valid digital signature certificates (issued by an internationally recognised Certification Authority) to their internal staff responsible for the collection and compilation of information and to the person in charge of transmitting the flows to the CA.
   The CA shall be required to provide the FIs with the public certificates of its staff responsible for decrypting the flows sent. For all activities involving data processing operations subject to exchange of information in tax matters, access to such data shall only be allowed by using the credentials or substitute instruments made available. To this end, appropriate and preventive written instructions shall be provided to clearly identify the ways in which the data controller may ensure the availability of data or electronic instruments in case of prolonged absence or inability of the various human resources involved in the processing operations. In these latter cases, the procedure for the provision of substitute instruments shall be notified to the Guarantor for the protection of the confidentiality of personal data referred to in Chapter V of Law no. 70/1995.

b) Authorisation system
Operational profiles identifying the authorisations granted in the system shall be established according to the roles to be performed by each user involved.
The operational profiles shall be established according to homogeneous groups of users on the basis of the processing operations that they have to perform. The operating profiles shall be preventively established and set up at the beginning of the processing, in order to limit access exclusively to data necessary to carry out the processing operations.
Periodically, and in any case on an annual basis, it shall be verified whether the conditions for the maintenance of the authorisation profiles are met.

Art. 13
(Protection of archiving and storage devices)

1. Appropriate technical and organisational procedures shall be implemented and documented for the management and custody of removable storage devices containing data relating to exchange of information in tax matters, including their possible re-use, in order to prevent unauthorised access and processing operations or reconstruction of data from removable devices already used.

Art. 14
(Paper and electronic document destruction and disposal policies)

1. At the end of their use, if not archived, paper documents containing information considered sensitive by the CA shall be destroyed and disposed of through adequate systems, so that the information contained cannot be reconstructed.
2. In case a storage device containing sensitive information is no longer used, it shall be adequately deleted and disabled before disposal.

Art. 15
(Management and maintenance of systems)

1. Maintenance and management of systems shall be the responsibility and liability of the ITDS. Ordinary and extraordinary technical interventions to systems and plants shall be authorised by the ITDS.
2. Any technical expert who can potentially come into contact with the areas containing sensitive information shall be preventively recognised and sign an agreement not to disseminate information.
3. For physical access to the premises of the data centre, the recognition and registration of persons accessing it may be entrusted to the staff responsible for monitoring the centre.

TITLE IV
INTERNAL CONTROLS AND RISK MANAGEMENT

Art. 16
(Auditing management)

1. Auditing systems shall be made available to the CA to control IT access in the networks and servers that contain data relevant to exchange of information in tax matters, or through which such data have transited.
2. The CA may require additional monitoring concerning technical/system activities.

Art. 17
(Security assessments)

1. The ITDS shall develop and update, at least annually, policies to verify, validate and authorise security controls for data protection. Purely for illustrative purposes, the following activities shall be guaranteed: applicable security standards, vulnerability assessment and penetration testing.

Art. 18
(Processing risk assessments)

1. The data controller, assisted by its organisational structures or by outsourced ones, shall define the "risks/impacts" array identified in the processing of data necessary to exchange of information in tax matters. The array shall be accompanied by an explanatory document indicating for each risk identified the associated impact and the mitigation actions necessary to minimise said risks. Risks shall be identifiable and effectively available technical solutions shall be applied to each of them.

Failure to adopt such solutions shall entail civil liability for damage if it is not demonstrated that all appropriate measures to avoid it have been taken.

2. Periodically, and preferably during the first quarter of each year, or when operating conditions change by introducing new risks, the data controller shall review the "risks/impacts" array and the relevant explanatory document, in order to maintain adequate control of processing risks.
3. Periodically, and at least annually, or when so required for technical and organisational reasons, the authorisation system shall be reviewed in order to verify whether the conditions for the maintenance of the operational profiles for each user are still met.
4. Personal data shall be protected from the risk of intrusion under Article 190 bis of the Criminal Code (unlawful interception or interference in IT or telematic communications) and from the risk of damage referred to in Article 202 bis of the Criminal Code (Damage to IT information, data and programs), through activation of appropriate electronic instruments to be updated at least once every six months. In case of failure to apply minimum security measures mitigating risks, the organisation shall be subject to objective criminal liability.

Art. 19
(Planning of emergencies concerning systems, data and information)

1. Macro components of the information system (environments, server, network, software) shall undergo periodic tests, at least annually.
2. These tests shall be scheduled so as not to cause disruption of essential services. The results shall be part of the operational processes of recovery and investment planning.

TITLE V
PROTECTION OF DATA EXCHANGED INTERNATIONALLY AND TECHNICAL RULES

Art. 20
(Protection of data exchanged in accordance with international treaties)

1. Data protection systems shall be adopted, in accordance with the international treaties incorporated. In the absence of specific rules of protection, the levels of protection and security implemented for the protection of data contained in the security perimeter defined in this Regulation shall be adopted.

Art. 21
(Technical rules applicable to data flows between FI and CA)

1. Financial Institutions shall be required to find information within their private databases and to prepare a flow having the following structure:
a) an initial block compliant with the XML standard of Annex 3 to OECD's Common Reporting Standard (CRS);
b) a final block containing the following statistical information to be found on the basis of the data which formed the block referred to in letter (a) above:
   - number of countries detected in the period as foreign tax residences reported in the flow to the CA;
   - for each symbol of the country detected, according to ISO-3166-1 Alpha-2 (ES:IT):
     - Detection period (minimum–maximum date) YYYY-MM-DD-YYYY-MM-DD;
     - Number of "Controlling Persons".
2. The data flow shall be named with the following scheme:
<COE-CODE>+ <YYYY-MM-DD>+<HH-MM-SS>.TXT, where COE is the Economic Operator Identification Code of the FI, YYYY-MM-DD is the date in the form of year, month and date, HH-MM-SS is the time of the flow processing.

3. The data flow, consisting of the three sections, shall then be encrypted through the appropriate programme approved by the CA.
4. The person in charge of the processing, by accessing the PA portal for these activities through the use of digital certificates and authentication, shall transmit the flow, with the name referred to in paragraph 2 above, to the IT system of the CA.
5. Through its persons in charge of the processing, the CA shall perform the following tasks:

a) decrypt the flow;
b) verify, by comparing the digital fingerprint (HASH), that the flow received was not altered in the time between the transmission by the FI and the receipt by the CA;
c) verify, through a "Validation" application, that the data section, in the “XML” standard, was properly filled in on the basis of the OECD’s "User Guide";
d) recalculate statistics, in order to verify that the calculation of summary data by the FI was correct;
e) if the result of validation and verification applications is positive, the flow shall be stored in the Database designed to contain the flow of confidential data. Subsequently, from the same Database, the data to be transmitted to individual FJs shall be processed;
f) the person in charge of the processing of the CA shall send to that of the FI a notification of acceptance, with the significant elements to confirm correctness of the flow. The message shall be signed and provided with a timestamp.
On the contrary, if the result of validations and verifications carried out by the CA is not positive, the flow shall be discarded and temporarily saved in a dedicated area to undergo a process of data destruction. The person in charge of the processing of the CA shall send to that of the FI a notification of non-acceptance, with the significant elements relative to the non-acceptance. The message shall be signed and provided with a timestamp.

Art. 22
(References to the Common Reporting Standard for Automatic Exchange of Financial Account Information in Tax Matters)

1. For anything not specified in this Regulation with regard to data protection, the CA and the ITDS, responsible for managing systems on behalf of CA, shall apply what indicated in Annex 4 to the Common Reporting Standard - OECD, paragraph 2 "Information Security Management".

Done at Our Residence, on 30 December 2015/1715 since the Foundation of the Republic.

THE CAPTAINS REGENT
Lorella Stefanelli - Nicola Renzi

THE MINISTER OF
INTERNAL AFFAIRS
Gian Carlo Venturini