REPUBBLICA DI SAN MARINO

REGOLAMENTO 30 dicembre 2015 n.20

Noi Capitani Reggenti
la Serenissima Repubblica di San Marino

Visto l'articolo 42 della Legge 27 novembre 2015 n. 174;
Vista la deliberazione del Congresso di Stato n.14 adottata nella seduta del 23 dicembre 2015;
Visti l'articolo 5, comma 5, della Legge Costituzionale n. 185/2005 e l'articolo 13 della Legge Qualificata n.186/2005;
Promulghiamo e mandiamo a pubblicare il seguente regolamento:

REGOLAMENTO TECNICO PER LA PROTEZIONE DEI DATI PERSONALI IN APPLICAZIONE DELLO SCAMBIO DI INFORMAZIONI IN MATERIA FISCALE

Art. 1
(Finalità e ambito di applicazione)

1. Il presente regolamento disciplina le regole tecniche di protezione dei dati personali ai fini dello scambio delle informazioni in materia fiscale secondo lo schema di cui all'Allegato "A".
2. Il regolamento definisce in particolare:
    1. le procedure per la valutazione del personale e dei collaboratori che possono venire a contatto con il trattamento dei dati in materia di scambio di informazioni in materia fiscale;
    2. le politiche di protezione dei siti e la sicurezza degli accessi fisici;
    3. la sicurezza logica dei sistemi e delle reti utilizzati nel trattamento dei dati;
    4. la gestione e configurazione dei controlli di sicurezza;
    5. i controlli interni e la gestione dei rischi;
    6. la protezione dei dati scambiati in ambito internazionale e le regole tecniche.

TITOLO I
DEL PERSONALE PREPOSTO AL TRATTAMENTO

Art. 2
(Figure preposte al trattamento e loro compiti)

1. L'Istituzione Finanziaria (brevemente IF) e l' Autorità Competente (brevemente AC) sono titolari del trattamento perché a capo effettivamente del trattamento dei dati personali e sono tenuti a svolgere i seguenti compiti:

a) assumere decisioni, per quanto di propria competenza, in ordine: alle finalità e alle modalità del trattamento dei dati personali, agli strumenti utilizzati nello scambio di informazioni in materia fiscale ivi compresi i profili della sicurezza, alle modalità di gestione e di controllo, quando queste non siano state delegate al responsabile del trattamento;
b) nominare il responsabile del trattamento;
c) nominare l'incaricato del trattamento;

d) notificare, la richiesta di autorizzazione per il trattamento dei dati ai fini del presente regolamento.

Qualora non venga nominato il responsabile del trattamento, le funzioni del responsabile rimangono in carico al titolare del trattamento ovvero ad una persona fisica che lo rappresenta.

2. Il responsabile del trattamento, quando nominato dal titolare del trattamento è tenuto a:

a) gestire il processo di formazione dei flussi per lo scambio di informazioni in materia fiscale;
b) effettuare i controlli formali e di completezza sul flusso dei dati raccolti;
c) gestire il sistema di crittazione e firma digitale delle informazioni;
d) effettuare i controlli sulle attività svolte dall'incaricato al trattamento dei dati in fase di trasmissione e ricevimento delle conferme di ricezione.

Per quanto riguarda il trattamento di documenti non elettronici, il responsabile del trattamento dell'AC è tenuto a:

a) redigere istruzioni scritte finalizzate al controllo ed alla custodia dell'intero processo di trattamento degli atti e dei documenti non elettronici relativi allo scambio di informazioni in materia fiscale;
b) redigere, mantenere ed aggiornare, con cadenza periodica almeno annuale, la lista degli incaricati e l'ambito di trattamento loro consentito.

3. L'incaricato del trattamento nelle IF, è nominato dal titolare del trattamento, ed è tenuto a:

a) firmare digitalmente il flusso pervenutogli dal responsabile del trattamento;
b) trasmettere il flusso all'AC;
c) ricevere le conferme di ricezione dall'AC;
d) eseguire l'archiviazione delle conferme di ricezione.

4. L'incaricato del trattamento nell'AC, è nominato dal titolare del trattamento. Per quanto riguarda la ricezione dei flussi provenienti dalle IF esso è tenuto a:

a) ricevere i flussi inviati dalle IF;
b) decrittare ogni flusso ricevuto;
c) effettuare i controlli formali e di completezza sul flusso dei dati raccolti dalle IF;
d) emettere ed inviare le conferme di ricezione alle IF;
e) archiviare i flussi pervenuti dalle IF;
f) ricevere le conferme di ricezione dall'AC;
g) eseguire l'archiviazione delle conferme di ricezione.

5. Per quanto riguarda la formazione dei flussi da inviare alle giurisdizioni estere (brevemente GE), in attesa di protocolli definiti in ambito internazionale, l'incaricato al trattamento della AC è tenuto a:

a) firmare digitalmente i flussi pervenutigli dal proprio responsabile del trattamento;
b) trasmettere ogni singolo flusso alle GE competenti;
c) ricevere le conferme di ricezione dalle GE;
d) eseguire l'archiviazione delle conferme di ricezione.

6. Per quanto riguarda la ricezione dei flussi provenienti dalle GE, in attesa di protocolli definiti in ambito internazionale, l'incaricato al trattamento della AC è tenuto a:

a) ricevere i flussi inviati dalle GE;
b) decrittare ogni flusso ricevuto;
c) effettuare i controlli formali e di completezza sul flusso dei dati raccolti dalle GE;
d) emettere ed inviare le conferme di ricezione alle GE;
e) archiviare i flussi pervenuti dalle GE.

7. Per quanto riguarda il trattamento di documenti non elettronici, l'incaricato al trattamento della AC è tenuto a:

a) seguire le istruzioni scritte per il trattamento dei documenti non elettronici;
b) controllare e custodire gli atti e i documenti non elettronici loro affidati;
c) restituire i documenti o gli atti esclusivamente a chi ne ha la titolarità di conservazione all'interno del processo.

Art. 3

(Procedure per la valutazione del personale e dei collaboratori)

1. Il personale preposto al trattamento delle informazioni deve essere in possesso di particolare esperienza professionale o capacità acquisita in materia.

2. Le IF e l'AC dovranno procedere ad apposito screening del personale preposto al trattamento dei dati, almeno annualmente:

a) nelle IF le figure professionali che saranno impiegate nel trattamento nello scambio di informazioni in materia fiscale, dovranno essere valutate e nominate con delibera degli organi di amministrazione (consiglio di amministrazione, amministratore delegato, ecc.).
b) l'AC è per definizione titolare del Trattamento. Nella AC le figure professionali che saranno impiegate nel trattamento nello scambio di informazioni in materia fiscale, sono agenti pubblici che sono soggetti al codice di condotta in base alla legge 141/2014, esse sono integrate nella pianta organica dell'AC. Al direttore dell'AC spetta il compito di nominare l'eventuale responsabile e gli Incaricati del trattamento, i quali sono figure obbligatorie.

3. L'AC nel trattare le informazioni ricevute dalle GE o dalle IF possiede una figura denominata "Punto di Contatto" rappresentata dal suo direttore.

Art. 4

(Formazione del personale preposto al trattamento delle informazioni confidenziali)

1. Il personale preposto deve seguire appositi corsi per il mantenimento della "formazione continua" in materia di trattamento dei dati e delle informazioni.
2. Sia le IF che l'AC debbono mantenere un apposito registro nel quale vengono trascritte le informazioni relative ai corsi effettuati. A titolo d'esempio non esaustivo, nome del corso, data di svolgimento, durata in giorni o ore, ragione sociale dell'organizzatore del corso, nominativo/i del personale coinvolto.

Art. 5

(Politiche di uscita del personale e dei collaboratori)

1. Il personale ed i collaboratori che sono stati impiegati nel trattamento dei dati sono soggetti anche a specifiche politiche di uscita, oltre alle normali attività di gestione amministrativa comuni a tutto il personale.
2. Al personale in uscita vengono disabilitate le credenziali di accesso ed autorizzazione e viene ritirata la smart-card od altri strumenti di accesso sia ai sistemi informativi che ai locali fisici.
3. Nel caso di trasferimento presso altri uffici o per l'espletamento di altre funzioni, le credenziali di accesso verranno immediatamente revocate e saranno riemesse in funzione del nuovo incarico.

TITOLO II
SICUREZZA DEGLI ACCESSI FISICI A LUOGHI E ARCHIVI PREVISTI NEL PERIMETRO DI PROTEZIONE

Art. 6

(Politiche di protezione dei siti e di accesso fisico agli stessi)

1. L'accesso sia ai locali che agli archivi contenenti dati relativi allo scambio di informazioni in materia fiscale è controllato. Il personale deve essere preventivamente autorizzato all'accesso, a qualunque titolo si svolga l'accesso. L'accesso può essere manuale o attraverso sistemi elettronici. In caso di accessi manuali, il personale è prima identificato e registrato. Se l'accesso è controllato da sistemi elettronici, la registrazione avviene contestualmente all'effettuazione dell'accesso.
2. L'accesso ai locali dei data center della Pubblica Amministrazione (brevemente PA) in cui sono installati i server utilizzati per lo scambio di informazioni in materia fiscale è controllato. Il personale, anche di terze parti, deve essere preventivamente autorizzato all'accesso a detti siti. L'accesso manuale è consentito solo ai responsabili della PA in caso di emergenza. L'elenco nominativo dei responsabili tecnici della PA o loro collaboratori di terze parti che possono accedere manualmente ed intervenire nei data center debbono essere iscritti in un apposito elenco conservato dall'AC. Per accesso manuale si intende un qualunque accesso che escluda il sistema di registrazione automatico. Nello svolgimento ordinario l'accesso è consentito solo attraverso dispositivi elettronici di registrazione degli accessi.

Art. 7

(Modalità di archiviazione dei documenti non elettronici)

1. Particolare importanza rivestono gli archivi cartacei soprattutto nei casi in cui, al loro interno, sono contenuti dati relativi allo scambio di informazioni in materia fiscale.
Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti i dati relativi allo scambio delle informazioni in materia fiscale.
2. L'AC, in qualità di titolare del trattamento, deve redigere una lista degli incaricati che possono trattare i documenti cartacei e/o ne sono responsabili per la conservazione e la tutela della riservatezza.
La lista degli incaricati può essere redatta anche per classi omogenee di incarico o per profili di autorizzazione.
Nell'aggiornamento periodico della lista degli incaricati, da effettuarsi con cadenza almeno annuale, va sempre individuato e riportato l'ambito del trattamento consentito ai singoli incaricati.
3. Quando gli atti e i documenti contenenti dati afferenti allo scambio di informazioni in materia fiscale siano affidati agli incaricati del trattamento, per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla loro restituzione in maniera che a tali documenti o atti non accedano persone prive di autorizzazione, ed essi siano restituiti a chi ne ha la titolarità di conservazione al termine delle operazioni di trattamento affidate.
4. Il personale preposto al trattamento degli atti e dei documenti deve mantenere il controllo costante sugli stessi e non lasciarli incustoditi sulla propria scrivania. In caso di allontanamento, anche temporaneo, gli atti ed i documenti cartacei devono essere riposti in luoghi sicuri e protetti, al fine di evitarne la sottrazione anche temporanea.

TITOLO III
SICUREZZA LOGICA DEI SISTEMI E DELLE RETI UTILIZZATI NEL TRATTAMENTO ENTRO IL PERIMETRO DI PROTEZIONE

Art. 8

(Protezione dei sistemi e delle comunicazioni)

1. L'AC, per il tramite dell'Ufficio Informatica, Tecnologia, Dati e Statistica (brevemente ITDS), è responsabile dell'intero canale di comunicazione con le IF ed, entro il perimetro giurisdizionale, anche con GE.
Qualsiasi dato che transita sulla rete di comunicazione tra AC, IF e GE, è crittografato.
2. L'AC sarà dotata di strumenti per la gestione ed il monitoraggio delle diverse fasi dello scambio di informazioni in materia fiscale.
3. Tutti gli accessi ai sistemi utilizzati ai fini del presente regolamento sono consentiti esclusivamente al personale autorizzato dotato di specifici dispositivi elettronici (smart-card) e credenziali di accesso.
4. La sicurezza informatica nell'area di lavoro dell'AC e degli uffici autorizzati agli accertamenti, come l'Ufficio Tributario, prevede: il confinamento e la crittazione delle comunicazioni in rete e l'installazione di periferiche di lavoro idonee al grado di sicurezza richiesto, come la virtualizzazione del desktop (terminali) ed esclusione di dispositivi locali di memorizzazione o trasferimento dei dati.
5. Sui dispositivi server centralizzati, è creata un' area di rete specifica, dove risiedono gli applicativi dedicati alle attività dell'AC Il personale autorizzato accede solo tramite dispositivi smart-card con certificato di riconoscimento a bordo. Il database, che contiene i dati soggetti a protezione secondo questo regolamento, è crittografato e l'accesso ai dati sarà inibito a tutto il personale, compreso quello tecnico e sistemistico, se non abilitati dal responsabile dell'AC che ne possiede il certificato di decrittazione.

Art. 9

(Integrità dei sistemi e delle informazioni)

1. Sono implementate procedure, processi, e sistemi atti a garantire la cosiddetta "Alta Affidabilità", tale per cui coesistono e sono pienamente funzionanti sistemi gemelli collocati in siti differenti che si replicano automaticamente e che, in caso di guasto o disastro in un sito, sono in grado di continuare l'operatività senza degrado sull'altro sito.
2. Sono comunque implementate apposite procedure tecnico-organizzative per la gestione dei salvataggi dei dati e delle applicazioni (c.d. backup) con una frequenza adeguata alle attività tecnico-operative e di gestione della sicurezza, stabilite dall'ITDS. Sono anche implementate procedure tecnico-organizzative di controllo dei salvataggi pregressi al fine di accertarne la bontà d'utilizzo in caso di ripristino.
3. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con le necessità operative e con il rispetto dei tempi stabiliti negli accordi internazionali.

Art. 10

(Pianificazione delle implementazioni, dello sviluppo e dell'aggiornamento dei sistemi di sicurezza delle informazioni)

1. Gli uffici preposti alla pianificazione dei sistemi informativi a disposizione dell'AC, definiscono un piano di implementazione con cadenza triennale.
2. In ogni caso si provvede ad effettuare aggiornamenti periodici, almeno annuali, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (a titolo esemplificativo e non esaustivo: Antivirus, Antispam, AntiMalware, Intrusion detection/prevention, Firewall software e/o Hardware ecc.) e a correggerne difetti.
3. Sono altresì stabilite apposite politiche di aggiornamento per quanto riguarda il software di base dei sistemi, al fine di garantirne la perfetta rispondenza ai prerequisiti di sviluppo del sistema per lo scambio di informazioni in materia fiscale.
4. Sono anche stipulati specifici contratti di assistenza, manutenzione ordinaria e straordinaria, e di piani di implementazione del software applicativo, sulla base di quanto richiesto nei trattati internazionali in materia di cooperazione fiscale internazionale.

Art. 11

(Gestione e configurazione dei controlli di sicurezza)

1. La gestione della sicurezza informatica del perimetro che contiene, o potenzialmente può contenere, dati relativi allo scambio di informazioni in materia fiscale, viene gestito internamente da ITDS , che periodicamente informa l'AC dei piani di sviluppo ed adeguamento in materia di sicurezza informatica. L'AC può richiedere ad enti terzi controlli sulla sicurezza del perimetro di competenza dello scambio di informazione in materia fiscale.

Art. 12

(Identificazione e autenticazione del personale preposto al trattamento)

1. I dati e le informazioni, raccolte nell'ambito dei processi tecnico-organizzativi afferenti allo scambio delle informazioni in materia fiscale, debbono soggiacere alle seguenti modalità tecniche di identificazione e autenticazione:

a) Sistema di autenticazione:
   La AC, per il tramite di ITDS, dota le risorse umane, coinvolte nel processo di scambio delle informazioni in materia fiscale, di idonei strumenti di autenticazione per svolgere una o più operazioni di trattamento dei dati.
   Lo strumento di autenticazione adottato nella Pubblica Amministrazione è la smart-card con certificato digitale a bordo. Il rilascio delle smart-card avviene previo riconoscimento e sottoscrizione delle clausole di utilizzo e responsabilità.
   Vengono rilasciate, su richiesta dell'AC, anche credenziali di autenticazione nominative per la creazione di canali di comunicazione sicura (VPN), che si compongono essenzialmente di un codice identificativo (Userid) e di una parola chiave (Password). Il codice associato

all'incaricato (Userid), una volta utilizzato, non può essere assegnato ad altri soggetti, neppure in tempi diversi.
Le credenziali di autenticazione non utilizzate dopo sei mesi dovranno essere disattivate.
La parola chiave (Password) deve essere composta da almeno otto caratteri. Non deve contenere riferimenti riconducibili all'incaricato e deve essere modificata dall'incaricato stesso al primo utilizzo dello strumento elettronico e, successivamente, almeno ogni tre mesi.
Sistemi di rilevazione come: token magnetici, badge con rfid o dispositivi biometrici verranno utilizzati per l'apertura di varchi, abilitazione allarmi, registrazione di accessi ai locali protetti.
Le risorse umane dovranno essere sensibilizzate ad adottare le necessarie cautele per assicurare la segretezza della credenziali di accesso, codice segreto o password, nonché la diligente custodia dei dispositivi loro assegnati e a non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento (i sistemi, a tal fine, permettono di predisporre uno screen saver con richiesta di password).
Processo di assegnazione delle credenziali:

1. Personale interno ad AC ed agli uffici PA
   Al personale interno viene fornito da ITDS una Identità Elettronica I.D. tramite smart-card personale contenente certificato di firma digitale e certificato di autenticazione, emessi da una Certification Autority riconosciuta a livello internazionale.
   Il processo di assegnazione dell'I.D. avviene tramite riconoscimento de visu presso la sezione RAO dell'ITDS.
   A seguito della consegna degli strumenti (smart-card e codici di sblocco) e delle istruzioni, le persone sono autonome e responsabili nei processi di firma (legalmente riconosciute) e di crittazione.
   I ruoli assegnati e le credenziali saranno individuati e comunicati dall'AC all'ITDS che abiliterà gli accessi sulla rete interna della PA verso le specifiche aree protette.
2. Soggetti esterni (Istituzioni Finanziarie)
   L'AC richiede all'ITDS le credenziali di accesso al sistema di trasmissione crittato (VPN) per gli incaricati di ogni IF Le credenziali sono nominative.
   L'ITDS a seguito di ogni singola richiesta crea l'Identità Elettronica fornendo credenziali di accesso temporanee.
   L'incaricato della IF ricevute le credenziali sarà obbligato a cambiare password al primo collegamento.
   Le IF sono tenute a fornire i certificati di firma digitale riconosciuti e legalmente validi (emessi da una Certification Autority riconosciuta a livello internazionale) ai propri responsabili interni preposti alla raccolta e alla compilazione delle informazioni e all'incaricato dell'invio dei flussi verso l'AC.
   L'AC è tenuta a fornire alle IF i certificati pubblici dei propri responsabili preposti a decrittare i flussi inviati. Per tutte le attività che prevedono operazioni di trattamento dei dati soggetti allo scambio di informazioni in materia fiscale, l'accesso agli stessi è consentito esclusivamente mediante uso delle credenziali o degli strumenti sostitutivi messi a disposizione. A tale fine sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento delle varie risorse umane coinvolte nelle operazioni di trattamento. In tali ultimi casi la procedura per la messa a disposizione di strumenti sostitutivi deve essere notificata al Garante per la tutela della riservatezza dei dati di cui al Capo V della Legge n. 70/1995.

b) Sistema di autorizzazione
Sono predisposti profili operativi che individuano le autorizzazioni concesse nel sistema in base ai ruoli che ogni utente coinvolto deve ricoprire.
I profili operativi sono predisposti per gruppi omogenei di utenti sulla base delle operazioni di trattamento che essi devo svolgere. I profili operativi sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque con cadenza annuale, occorre verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Art. 13
(Protezione dei dispositivi di archiviazione e memorizzazione)

1. Devono essere implementate e documentate apposite procedure tecnico-organizzative per la gestione della custodia dei supporti rimovibili su cui sono memorizzati i dati afferenti allo scambio delle informazioni in materia fiscale, compreso l'eventuale loro riutilizzo, al fine di evitare accessi non autorizzati, operazioni di trattamento non consentite o ricostruzione dei dati da supporti rimovibili già utilizzati.

Art. 14
(Politiche di distruzione smaltimento di documenti cartacei ed informatici)

1. I documenti cartacei che contengono informazioni ritenute sensibili dall'AC al termine del loro utilizzo, se non sono soggette ad archiviazione, devono essere distrutte e smaltite con adeguati sistemi, in modo tale che le informazioni contenute non possano essere ricostruite.
2. I supporti informatici che contengono informazioni sensibili, nel caso di dismissione, vanno adeguatamente cancellati e prima dello smaltimento resi inoperativi.

Art. 15
(Gestione della manutenzione dei sistemi)

1. La gestione e la manutenzione dei sistemi è di competenza e responsabilità dell'ITDS. Gli interventi tecnici sistemistici, impiantistici, ordinari e straordinari avvengono sotto autorizzazione dell'ITDS.
2. Ogni figura tecnica che potenzialmente possa venire a contatto con le aree che contengono informazioni riservate, deve essere preventivamente riconosciuta e dovrà firmare un accordo di non diffusione delle informazioni.
3. Per gli accessi fisici ai locali del centro di calcolo potrà essere demandato al personale che lo presidia, il riconoscimento e la registrazione delle persone che vi accedono.

TITOLO IV
CONTROLLI INTERNI E GESTIONE DEI RISCHI

Art. 16
(Gestione dell'audit)

1. All'AC vengono messi a disposizione sistemi di audit per il controllo degli accessi informatici nelle reti e nei server che contengono o che hanno contenuto per transito, dati rilevanti allo scambio di informazioni in materia fiscale.
2. AC può richiedere monitoraggi aggiuntivi in merito alle attività tecniche/sistemistiche.

Art. 17
(Valutazioni della sicurezza)

1. L'ITDS deve sviluppare ed aggiornare con periodicità almeno annuale, le politiche di processo atte a verificare, convalidare ed autorizzare i controlli di sicurezza per la protezione dei dati. A titolo puramente indicativo debbono essere curate le seguenti attività: standard di sicurezza applicabili, valutazione delle vulnerabilità e penetration test.

Art. 18
(Valutazioni dei rischi di trattamento)

1. Il titolare del trattamento, con l'ausilio delle proprie strutture organizzative o con quelle acquisite in outsourcing, deve definire la matrice "rischi/impatti" individuati in ambito di trattamento dei dati necessari per lo scambio di informazioni in materia fiscale. La matrice va accompagnata da un documento esplicativo in cui per ogni rischio individuato si espliciti l'impatto associato e le azioni di mitigazione necessarie al fine di minimizzare detti rischi. I rischi devono essere identificabili e su ciascuno di essi debbono essere applicate soluzioni tecniche

concretamente disponibili, la cui mancata adozione espone a responsabilità civile per danno qualora non si riesca a dimostrare di aver adottato tutte le misure idonee ad evitarlo.

2. Periodicamente, e preferibilmente nel corso del primo trimestre di ogni anno, o quando le condizioni operative cambiano introducendo nuovi rischi, il titolare del trattamento sottopone a revisione la matrice "rischi-impatti" ed il relativo documento esplicativo, al fine di mantenere un adeguato presidio sui rischi di trattamento.
3. Periodicamente, e comunque almeno annualmente, o quando le necessità tecnico-organizzative lo richiedano, il sistema di autorizzazione è rivisitato al fine di verificare la sussistenza delle condizioni per la conservazione dei profili operativi per ciascun utente.
4. I dati personali debbono essere protetti dal rischio di intrusione di cui all'articolo 190-Bis del codice Penale (Intercettazione o interferenze illecite in comunicazioni informatiche o telematiche), e dal rischio di danneggiamento di cui all'articolo 202-Bis del Codice Penale (Danneggiamento di informazioni, dati e programmi informatici), mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale. La mancata applicazione di misure minime di sicurezza tali da ridurre i rischi espone l'organizzazione a responsabilità oggettiva con rilevanza penale.

Art. 19

(Pianificazione delle emergenze sui sistemi, dati ed informazioni)

1. Il sistema informativo nelle sue macro componenti (ambienti, server, rete, software) deve essere sottoposto a test periodici, almeno annualmente.
2. Tali test devono essere pianificati in modo da non causare interruzione di servizi essenziali. I risultati devono entrare a far parte delle modalità operative di ripristino e di pianificazione degli investimenti.

TITOLO V
PROTEZIONE DEI DATI SCAMBIATI IN AMBITO INTERNAZIONALE E REGOLE TECNICHE

Art. 20

(Protezione dei dati scambiati in base ai trattati internazionali)

1. Verranno adottati i sistemi di protezione dei dati scambiati, in base ai trattati internazionali recepiti. In assenza di specifiche regole di protezione verranno adottati i livelli di protezione e sicurezza implementati per la protezione dei dati contenuti nel perimetro di sicurezza definito nel presente regolamento.

Art. 21

(Regole tecniche applicabili al flusso dei dati tra IF e AC)

1. Le Istituzioni finanziarie sono tenute a reperire le informazioni all'interno dei loro database privati e a predisporre un flusso che abbia la seguente struttura:
a) un blocco iniziale conforme allo standard XML dell'Allegato 3 del Common Reporting Standard OCSE (CRS);
b) un blocco finale che riporti le seguenti informazioni statistiche reperibili sulla base dei dati che hanno formato il blocco di cui al punto (a) precedente:
   - numero di Paesi rilevati nel periodo come residenze fiscali estere comunicate nel flusso all'AC;
   - per ogni sigla Paese rilevato, secondo lo standard ISO-3166-1 Alpha-2 (ES:IT):
     - Periodo di rilevazione (data minima–massima) AAAA-MM-GG-AAAA-MM-GG;
     - Numero di "Controlling Persons".
2. Il flusso dei dati va denominato con il seguente schema:
<CODICE-COE> + <AAAA-MM-GG>+<HH-MM-SS>.TXT, dove il COE è il Codice Operatore della IF, AAAA-MM-GG rappresenta la data nella forma anno, mese e giorno, HH-MM-SS rappresenta l'orario di elaborazione del flusso.

3. Il flusso dei dati, composto dalle tre sezioni, viene quindi sottoposto a crittografia con l'apposito programma approvato dall'AC ;
4. L'incaricato al trattamento, tramite l'accesso al portale della PA, per queste attività, che avverrà con l'uso di certificati digitali e autenticazione, trasmette il flusso, con la denominazione di cui al precedente punto 2, al sistema informatico dell'AC;
5. L'AC tramite i suoi incaricati al trattamento, deve eseguire le seguenti attività:

a) esegue la decrittazione del flusso;
b) esegue la verifica, tramite confronto dell'impronta digitale informatica (HASH), al fine di accertare che il flusso ricevuto non sia stato alterato nel tempo intercorso tra la trasmissione effettuata dall'IF e la ricezione dell'AC;
c) esegue un applicativo di "Validazione" al fine di verificare che la sezione dati, nello standard "XML", sia stata correttamente riempita sulla base della "User Guide" OCSE.
d) esegue il ricalcolo delle statistiche, al fine di verificare che il calcolo dei dati riassuntivi effettuate dalla IF sia avvenuto correttamente;
e) Se gli applicativi di validazione e verifica hanno dato risultato positivo, allora il flusso viene memorizzato nella Banca Dati predisposta a contenere il flusso di dati riservati. Successivamente dalla stessa Banca Dati verranno elaborati gli smistamenti per l'inoltro alle singole GE;
f) l'incaricato AC invia all'incaricato della IF, un messaggio di notifica di accettazione con gli elementi significativi a conferma di correttezza del flusso. Il messaggio viene firmato ed apposta una marca temporale.
   Se, viceversa, le validazioni e le verifiche effettuate dall'AC non avranno fornito una risposta positiva, allora il flusso viene scartato e salvato temporaneamente in una area dedicata per essere sottoposto a processo di distruzione dei dati. L'incaricato AC invia all'incaricato dell'IF, un messaggio di notifica di non accettazione con gli elementi significativi relativi alla non accettazione. Il messaggio viene firmato ed apposta una marca temporale.

Art. 22

(Riferimenti al "Common Reporting Standard for Automatic Exchange of Financial Account Information in Tax Matters")

1. Per quanto non indicato nel presente regolamento in materia di protezione dei dati, l'AC e l'ITDS, preposto alla gestione dei sistemi per conto della AC, debbono applicare quanto indicato nell'Allegato 4 del "Common Reporting Standard - OCSE", paragrafo 2 "Information Security Management".

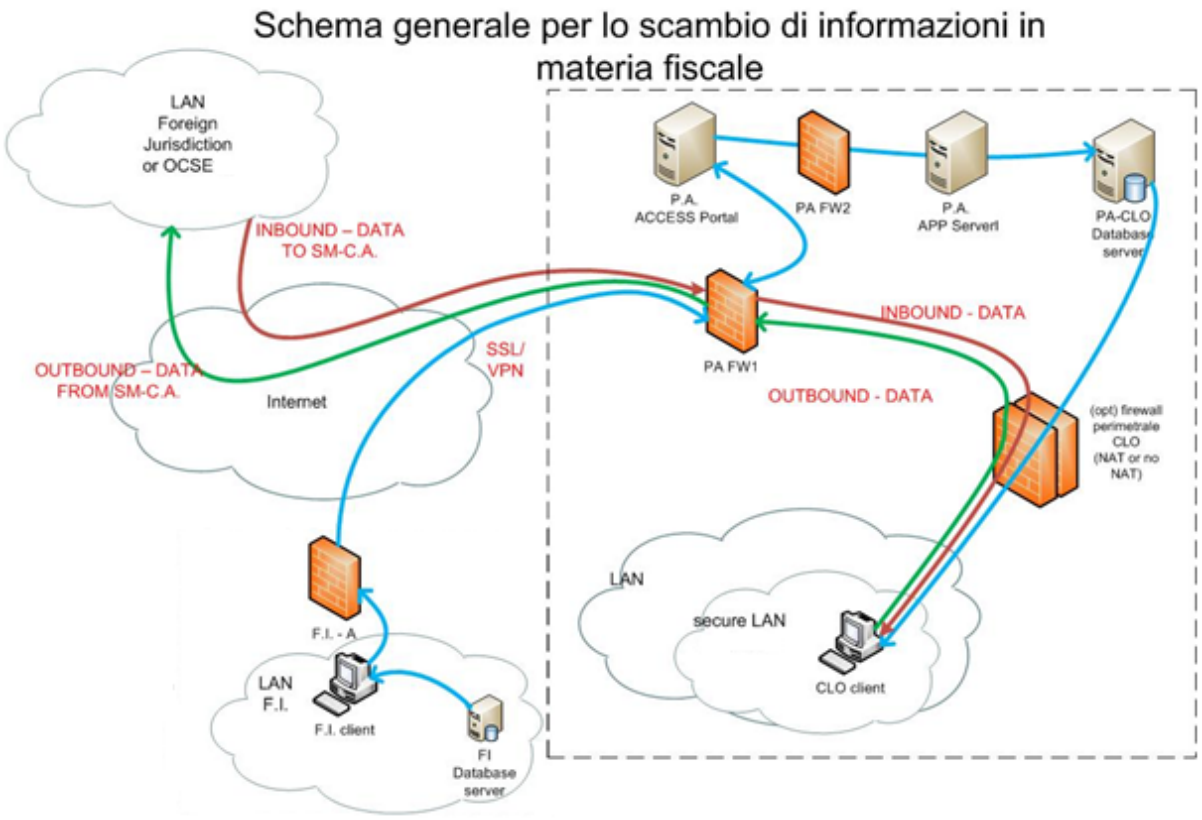
Dato dalla Nostra Residenza, addì 30 dicembre 2015/1715 d.F.R.

I CAPITANI REGGENTI
Lorella Stefanelli – Nicola Renzi

IL SEGRETARIO DI STATO
PER GLI AFFARI INTERNI
Gian Carlo Venturini

ALLEGATO "A"

Lo schema successivo illustra il quadro generale e il perimetro di applicazione del regolamento



L'area tratteggiata rappresenta il perimetro di protezione dei dati sottoposto al presente regolamento.

I soggetti esterni, istituti finanziari e giurisdizioni estere, sono coinvolti nel processo di protezione dei dati e sottoposti al presente regolamento relativamente ai dati che attraversano il perimetro di protezione.