Via Giuseppe Grezar, 14
00142 Roma – RM
Tel. 06 98 9581
www.agenziaentrateriscossione.gov.it

Direzione Internal audit
Settore Protezione dati e qualità

Prot n. 1582637 del 25/03/2020 Progetto tecnico ai sensi art. 23 comma 15 D. Lgs. 50/2016

Protezione dati – Revisione ed integrazione del Catalogo delle misure di sicurezza ed assessment delle soluzioni applicative

Sommario

Premessa 3
Descrizione del fabbisogno 5
Dimensionamento ed analisi dei costi 5
Modalità di acquisizione 6
Conclusioni 10

Premessa

L'Agenzia delle entrate-Riscossione (di seguito per brevità Agenzia o AdeR) tratta, in qualità di Titolare, i dati personali necessari alla realizzazione delle proprie finalità istituzionali connesse alla riscossione nazionale dei tributi.

Ai fini dell'adeguamento alle previsioni del Regolamento UE 679/2016 (GDPR) e della normativa nazionale di riferimento aggiornata in materia di protezione dati, Agenzia delle entrate – Riscossione ha introdotto uno specifico Sistema di Gestione per la Protezione dei dati (più oltre anche GDPR).

Quest'ultimo ricerca il miglioramento continuo del modello operativo e organizzativo di *data protection* adottato dall'Agenzia supportando, con l'introduzione di processi e procedure documentate, la realizzazione degli obiettivi di compliance e di migliore diffusione a tutti i livelli dell'Organizzazione di comportamenti adeguati agli standard attesi.

Il GDPR introduce, per le organizzazioni Titolari, il Principio di "*Accountability*", tradotto in italiano con "Responsabilizzazione", secondo il quale il Titolare del trattamento deve poter dimostrare di aver adottato misure di sicurezza (tecniche e organizzative), adeguate rispetto ai rischi per i diritti e delle libertà degli interessati e per la sicurezza dei dati trattati.
Tali misure e la loro adeguatezza, inoltre, devono essere verificate e aggiornate in maniera costante.

Al fine della corretta valutazione dei rischi in materia di *data protection,* AdeR ha adottato una propria Metodologia per l'analisi del rischio e la valutazione di impatto in relazione ai trattamenti per i quali possono sussistere dei rischi legati alla tutela dei diritti e delle libertà delle persone fisiche ed alla sicurezza dei dati. Tale approccio metodologico è stato condiviso ed adottato da tutti i componenti del Sistema Informativo della Fiscalità (SIF), con riferimento al Documento di sintesi concordato con il Comitato di Governo delle Agenzie fiscali/Enti del MEF.

A supporto di tale metodologia AdeR e Ade (Agenzia delle entrate) hanno progettato, con il partner tecnologico Sogei S.p.A., una soluzione applicativa denominata DIANA (Data Impact ANAlysis) che ha l'obiettivo di supportare le competenti strutture dei Titolari nella valutazione dei rischi sottesi ai trattamenti.

Per quanto rappresentato, è di fondamentale importanza per AdeR condurre un *assessment* delle componenti informatiche sottese ai trattamenti di dati personali, al fine di disporre di una efficace rappresentazione dello stato dell'arte tecnologico e procedere ad un migliore coordinamento delle informazioni esposte nel Registro delle attività di trattamento e delle misure di sicurezza tecniche e organizzative disponibili.

In particolare, attraverso l'*assessment* richiesto, è necessario approfondire il contenuto informativo (categorie di dati personali) e le modalità di funzionamento dei servizi, applicazioni e infrastrutture informatiche (basi dati), con le connesse misure di sicurezza disponibili per i trattamenti censiti nel Registro dell'Agenzia.

Detto *assessment* inoltre è necessario per la migliore specificazione degli elementi che definiscono il perimetro e le modalità di svolgimento di ciascun trattamento realizzato.

In riferimento alle misure di sicurezza tecniche e organizzative richieste al Titolare per la mitigazione dei rischi AdeR ha adottato, in condivisione con le amministrazioni del SIF, il *framework multicompliance* FOURSe*c,* definito dal partner tecnologico Sogei S.p.a.

Tale *framework* propone le misure di sicurezza da applicare in ragione del livello di rischio rilevato per ciascun trattamento e/o servizio/applicazione informatica.
In relazione all'esigenza di standardizzazione delle misure di sicurezza da applicare ai trattamenti, AdeR ha la necessità di consolidare la classificazione/tassonomia di quelle presenti, anche in considerazione delle attività di trattamento realizzate attraverso Responsabili esterni.

L'insieme delle misure di sicurezza associate e/o associabili ai trattamenti e/o ai servizi/applicazioni/infrastrutture utilizzate dal titolare del trattamento AdeR definisce il cd. Catalogo delle misure di sicurezza. Quest'ultimo dovrà essere oggetto di aggiornamento periodico, mediante specifici adeguamenti/interventi di revisione (anche evolutiva), in ragione dell'evoluzione degli scenari di rischio in materia di protezione dati. Quanto fin qui descritto allo scopo di consentire il corretto presidio e l'adeguata manutenzione da parte delle competenti strutture ICT in qualità di owner dell'attività.

L'esigenza di disporre di un adeguato *assessment* e del Catalogo delle misure di sicurezza è inoltre funzionale:

- alla predisposizione degli elementi richiesti per l'introduzione di una soluzione informatica capace di integrare i processi di *data protection* identificati da AdeR nel modello operativo del proprio Sistema di Gestione per la protezione dati, in coerenza con le previsioni del Regolamento 2016/679;
- alla necessità di far convergere nel modello di *data protection* dell'Ente i requisiti e le misure richieste in ambito *cybersecurity* anche relativi all'applicazione della recente normativa europea (Regolamento sulla *cybersicurezza* – Regolamento (UE) 2019/881 del 17 aprile 2019). Al riguardo, infatti, si specifica che il GDPR considera la sicurezza un requisito di liceità che ciascun Titolare, a norma dell'art.32 dello stesso Regolamento, è tenuto ad assicurare nel trattamento di dati personali;
- allo sviluppo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) dell'Ente;
- alla corretta progettazione di servizi ai cittadini-contribuenti e agli Enti.

La realizzazione di quanto esposto richiede l'acquisizione dell'insieme di servizi professionali necessari a supportare AdeR nell'attuazione dell'iniziativa descritta.

Descrizione del fabbisogno

In considerazione di quanto sopra rappresentato, l'intervento richiesto deve condurre a:

- definire un complessivo Catalogo delle misure di sicurezza di AdeR (tecnologiche, organizzative e logistiche) da applicare in riferimento alle esigenze di mitigazione dei rischi in materia di protezione dati;
- un *assessment* che preveda:
    - Il censimento puntuale:
        - dei servizi/soluzioni applicative/basi di dati che gestiscono trattamenti di dati personali da confrontare con quelli censiti nel registro dei trattamenti;
        - delle categorie di dati personali trattati attraverso le stesse;
        - delle misure di sicurezza previste dall'esercizio in produzione delle soluzioni informatiche anche con il contributo di fornitori esterni (es. Sogei);
    - l'identificazione, a partire dai requisiti di sicurezza sottesi all'applicazione del *framework* FOURSec in uso:
        - di eventuali gap di sicurezza presenti per le soluzioni in esercizio, di ulteriori misure di sicurezza non adottate e la definizione di piani di *remediation*;
        - di possibili standard minimi di sicurezza (*privacy by default/design*) da applicare durante la progettazione di trattamenti di dati personali.

Modalità di acquisizione

Dall'analisi dei servizi disponibili nell'ambito del Contratto Quadro SPC – Lotto 2 relativo alla fornitura di servizi di Identità Digitale e Sicurezza Applicativa, stipulato da Agid/Consip ed il RTI composto da:

- Leonardo S.p.A. (mandataria)
- IBM Italia S.p.A.
- Sistemi Informativi S.r.l.
- Fastweb S.p.A

è stata individuata la soluzione basata sul servizio avente codice L2.S3.9 – "Servizi professionali".

Le esigenze riguardano, in particolare, l'attivazione dei servizi volti ad innalzare il livello di protezione dei dati personali trattati dall'Agenzia e di seguito elencati:

L2.S3.9 - Servizi professionali finalizzati a supportare l'Amministrazione:

- nella definizione di un *Catalogo delle Misure di Sicurezza* associate a requisiti di sicurezza GDPR già definiti dall'Amministrazione (**SP1**);
- nello svolgimento di un'attività di *assessment applicativo* volta a mappare la tipologia di dato personale presente sulle applicazioni utilizzate per i trattamenti ed effettuare una *gap analysis* alle Misure di Sicurezza di cui al punto precedente (**SP2**).

Il servizio individuato come **SP1** è finalizzato a supportare l'Amministrazione a definire un *Catalogo di Misure di Sicurezza* associate ai requisiti GDPR.

In particolare, l'Agenzia ha definito circa 250 requisiti di sicurezza e per ognuno di detti requisiti si richiede che siano individuate una o più Misure di Sicurezza, intese come gli interventi operativi (di tipo organizzativo e/o tecnologico) la cui implementazione è necessaria a mitigare i rischi legati alla protezione dei dati.

Si richiede, inoltre, di:

- verificare che le Misure individuate, a copertura dei requisiti di sicurezza, inerenti i servizi applicativi già definiti dall'Agenzia, siano completi e, ove necessario, definire le Misure aggiuntive;
- definire i criteri di prioritizzazione delle Misure di Sicurezza;
- definire, tramite una procedura documentale, il flusso informativo degli avvisi di sicurezza tra tutti gli attori coinvolti (ad es. funzione ICT, SGSI, DPO).

Nell'ambito dell'analisi e della verifica delle misure di sicurezza per i trattamenti dovranno essere previste:

- la classificazione delle stesse, in relazione alle minacce identificate dalla Metodologia di gestione dei rischi, sulla base del grado di efficacia e dell'idoneità di mitigazione;
- l'identificazione delle misure di sicurezza associate ai singoli trattamenti e alle componenti IT che li supportano;
- la valutazione del rischio residuo per le componenti ICT che supportano i trattamenti.

Il servizio individuato come **SP2** risponde all'esigenza di dover realizzare un processo di verifica, tramite interviste e/o analisi della documentazione esistente, della mappatura applicazioni/tipologia del dato personale trattato, al fine di verificare la coerenza con quanto censito nel Registro dei trattamenti.

L'Agenzia ha redatto, ai sensi dell'art. 30 del GDPR, il Registro delle attività di trattamento censendo circa 150 trattamenti afferenti a circa 260 applicazioni.

Inoltre, si richiede su un set di applicazione (pari ad n° di circa 40 applicazioni) strettamente connessi ai trattamenti di dati personali rientranti nella titolarità dell'Agenzia, di effettuare una *gap analysis* ai Controlli di Sicurezza definiti nell'ambito del servizio SP1 in precedenza descritto.

Per quanto concerne l'*assessment* richiesto sono da prevedere le seguenti macro fasi:

- Avvio attività – costituzione del team di progetto, condivisione degli obiettivi, individuazione del perimetro applicativo di riferimento, presentazione della metodologia e pianificazione degli interventi;

- Esecuzione – ricerca e raccolta delle informazioni necessarie per il censimento rappresentato in precedenza, verifica della struttura Owner del trattamento, censimento dei fornitori esterni e/o Responsabili del trattamento;

- Analisi – verifica della completezza e della coerenza della documentazione raccolta, dell'adeguatezza in relazione ai requisiti definiti, valutazioni ed eventuali integrazioni con il supporto delle strutture competenti;

- Conclusione – sintesi e presentazione dei risultati raggiunti al team di progetto.

Consip SpA, ai sensi dell'art. 54 del D.Lgs. n. 163/2006, ha indetto una gara a procedura ristretta, suddivisa in 4 lotti, come da bando pubblicato sulla Gazzetta Ufficiale dell'Unione Europea n. S251 del 28/12/2013 e sulla Gazzetta Ufficiale della Repubblica Italiana n. 151 del 27/12/2013.

A valle della conclusione delle procedure della gara di cui sopra, in luglio 2016 è stato stipulato e pubblicato il Contratto Quadro SPC per i "Servizi di gestione delle identità digitali e sicurezza applicativa". Tale Contratto Quadro offre la possibilità alle Amministrazioni Beneficiarie,

attraverso la stipula di singoli contratti esecutivi, di accedere ad un listino di servizi che ricomprende in particolare il codice L2.S3.9 – "Servizi professionali" riportati nei paragrafi precedenti.

Tanto ciò premesso, risulta necessario stipulare un nuovo contratto esecutivo con l'aggiudicatario del Contratto Quadro SPC Cloud – Lotto 2 con massimale di spesa pari a € 192.211,50 oltre IVA.

*Si segnala che, in aggiunta alla suddetta spesa, dovranno essere considerati:

- il contributo da corrispondere a Consip SpA pari a € 1.537,69 fuori campo IVA, conformemente a quanto previsto nel D.P.C.M. 23 giugno 2010[1];
- la quota del 5% di IVA indetraibile pari a € 2.114,33, calcolata applicando il 5% dell'IVA al 22% sull'importo complessivo del massimale di spesa[2].

[1] Il calcolo del contributo dovuto a Consip sarà effettuato nei termini di legge sulla base delle seguenti indicazioni, conformemente al DPCM 23 giugno 2010:

1. importo senza IVA del nuovo contratto esecutivo (ovvero contratto di fornitura) <= € 1.000.000,00 - contributo dovuto a Consip, 8‰ (8 per MILLE)
2. importo senza IVA del nuovo contratto esecutivo (ovvero contratto di fornitura) > € 1.000.000,00 - contributo dovuto a Consip 5‰ (5 per MILLE)
3. importo proroga contratto esecutivo senza IVA contributo dovuto a Consip 3‰ (3 per MILLE).

Ai fini del pagamento si specifica che i contributi di cui all'art.18, comma 3 del D.LGS.1 dic.2009 n .177 sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972 e pertanto non sussistono obblighi di fatturazione per Consip.

[2] Il pro rata di detrazione dell'IVA per l'Ente è indicato in base al dato definitivo per l'Ente del 2018. La percentuale potrebbe variare negli anni seguenti

Dimensionamento ed analisi dei costi

Sulla base dell'analisi effettuata in merito ai servizi disponibili nell'ambito del Contratto Quadro SPC Cloud – Lotto 2, è emerso che per soddisfare il fabbisogno risultano occorrenti i servizi di seguito riportati.

Catalogo delle misure di sicurezza (SP1)

Descrizione servizi professionali richiesti	Quantità
Capo Progetto	60
Specialista di tecnologia/prodotto Senior	0
Specialista di tecnologia/prodotto	0
Security Architect	250

Assessment applicativo (SP2)

Descrizione servizi professionali richiesti	Quantità
Capo Progetto	40
Specialista di tecnologia/prodotto Senior	0
Specialista di tecnologia/prodotto	0
Security Architect	185

Di seguito il fabbisogno complessivo riferito al servizio L2.S3.9

SERVIZI DI SICUREZZA (L2.S3)										
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Profilo	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno	Q.tà V Anno
L2.S3.9	SERVIZI PROFESSIONALI	On premise	A corpo (gg/uu)	Figura Professionale	Capo progetto	100	0	0	0	0
					Security architect	435	0	0	0	0
					Specialista di tecnologia/prodotto Senior	0	0	0	0	0
					Specialista di tecnologia/prodotto	0	0	0	0	0

Spesa per Servizio Catalogo delle misure di sicurezza (SP1)

Servizio L2.S3.9 – CATALOGO DELLE MISURE DI SICUREZZA							2020		
ID	ID SPC	Descrizione	Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Totale
SP.1	L2.S3.9	Servizi professionali	giorno/ uomo	H8	Capo progetto	€ 300,00	60	€ 18.000,00	€ 18.000,00
					Security Architect	€ 372,90	250	€ 93.225,00	€ 93.225,00
					Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00	€ 0,00
					Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00	€ 0,00
			giorno/ uomo	H24	Specialista di tecnologia/prodotto Senior (H24)	€ 1.180,00	0	€ 0,00	€ 0,00
					Specialista di tecnologia/prodotto (H24)	€ 930,00	0	€ 0,00	€ 0,00
Totale Servizio SP.1								€ 111.225,00	€ 111.225,00

Spesa per Servizio Assessment applicativo (SP2)

Servizio L2.S3.9 - ASSESSMENT APPLICATIVO							2020		
ID	ID SPC	Descrizione	Metrica	Servizio	Figura professionale	Prezzo unitario	Nun.tà	Prezzo	Totale
SP.2	L2.S3.9	Servizi professionali	giorno/ uomo	H8	Capo progetto	€ 300,00	40	€ 12.000,00	€ 12.000,00
					Security Architect	€ 372,90	185	€ 68.986,50	€ 68.986,50
					Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00	€ 0,00
					Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00	€ 0,00
			giorno/ uomo	H24	Specialista di tecnologia/prodotto Senior (H24)	€ 1.180,00	0	€ 0,00	€ 0,00
					Specialista di tecnologia/prodotto (H24)	€ 930,00	0	€ 0,00	€ 0,00
Totale Servizio SP.2								**€ 80.986,50**	**€ 80.986,50**

TOTALE COMPLESSIVO DEI SERVIZI	**€ 192.211,50**	**€ 192.211,50**

Spesa complessiva per i Servizi SP1 ed SP2

gg/uu x Figura professionale		2020	
Capo progetto	€ 300,00	100	€ 30.000,00
Security Architect	€ 372,90	435	€ 162.211,50
Specialista di tecnologia/prodotto Senior	€ 295,00	0	€ 0,00
Specialista di tecnologia/prodotto	€ 235,00	0	€ 0,00
TOTALE			**€ 192.211,50**

La spesa da sostenere, al netto del contributo da corrispondere a Consip SpA descritto nel successivo paragrafo, risulta pertanto pari a € 192.211,50, oltre IVA.

Conclusioni

Sulla base delle considerazioni svolte, si rende necessario acquisire i servizi descritti per un impegno massimo di spesa pari a € 192.211,50 + € 3.652,02*, comprensivo del contributo da corrispondere a Consip SpA e del 5% di IVA indetraibile, mediante stipula di un nuovo contratto esecutivo con il RTI Leonardo SPA, secondo le modalità previste nel Contratto Quadro SPC Cloud – Lotto 2.

L'impegno di spesa indicato nel presente Progetto è coerente con il bilancio preventivo deliberato dal CdG di AdeR per il triennio 2020-2022 e in corso di approvazione per la Direzione Relazioni esterne e Governance.

Il Responsabile del Procedimento

Fabio Esposito

(Firmato digitalmente)
FABIO ESPOSITO
31.03.2020 09:06:24 UTC