CONSIGLIO NAZIONALE FORENSE
PRESSO IL MINISTERO DELLA GIUSTIZIA

SPECIFICHE TECNICHE DEL SISTEMA INFORMATICO CENTRALE ADOTTATO AI SENSI E PER GLI EFFETTI DEL DECRETO DEL MINISTERO DELLA GIUSTIZIA 16 AGOSTO 2016, N. 178

1. Architettura di funzionamento del sistema e flussi informativi.

Il SIC consiste in una *web-application* per la gestione dei dati degli iscritti ad albi o elenchi tenuti dai Consigli dell'ordine degli avvocati (COA) territoriali, che abbia caratteristiche idonee a garantire un *repository in cloud* di tali dati. Inoltre, lo stesso è in grado di esporre un'interfaccia di consultazione web (ricerca avvocato) ed è dotato di una funzionalità per l'export dei dati al fine di rendere disponibile in tempo reale al Ministero della Giustizia gli indirizzi di posta elettronica certificata degli avvocati, ai sensi dell'art. 14 del DM 178/2016.

In particolare, il SIC consiste in una soluzione applicativa web, compatibile con tutti i browser ed i sistemi più comuni, utilizzabile su diversi *device*, in grado di realizzare un database relazionale che contiene i dati di tutti gli iscritti ai vari ordini ed al contempo in un'applicazione in grado di consultare e rappresentare opportunamente i dati archiviati.

I dati personali oggetto di trattamento nell'ambito del SIC consistono nell'insieme dei dati anagrafici degli iscritti agli albi territoriali, corredati dall'indirizzo di Posta Elettronica Certificata. Il SIC è infatti abilitato a contenere (e potrà mettere a disposizione del pubblico) le informazioni relative agli iscritti previste dagli artt. 2, 3, 4 e 5 del DM 22 settembre 2016, n. 178.

Il SIC è altresì abilitato a conservare lo storico delle modifiche conformemente all'art. 5, co. 1, penultimo ed ultimo periodo del DM 178/2016, per cui «*Il sistema informatico centrale e quelli di cui si avvalgono i consigli dell'ordine a norma del terzo periodo del presente comma procedono al tracciamento delle operazioni di inserimento di dati e documenti informatici effettuate. I documenti informatici contenenti la registrazione cronologica delle operazioni informatiche di cui al periodo precedente sono conservati per almeno tre anni*».

Oltre a disporre delle funzionalità di consultazione dei dati, l'applicazione è progettata per mettere a disposizione del CNF una serie di funzioni di export necessarie per il trasferimento degli stessi verso sistemi applicativi esterni, allorquando sussista un'idonea base giuridica per effettuare una comunicazione di dati personali[1].

I tracciati record utilizzati per lo scambio di dati in entrata (dai COA verso il CNF), comprese le informazioni pubblicate per legge (quali ad es. i gli estremi delle polizze assicurative ex art. 5, co. 1 del DM Giustizia del 22 settembre 2016[2]) e i dati integrativi pertinenti e non eccedenti in relazione all'attività professionale di cui all'art. 61, co. 3 del d.lgs. 196/2003, fermo restando quanto previsto

[1] «Il sistema informatico centrale esegue, con modalità telematiche ed automatizzate, le comunicazioni dei dati contenuti nell'albo, nei registri e negli elenchi previste dalla legge».

[2] «1. Fatta salva l'informazione da rendere al cliente ai sensi dell'art. 12, comma 1, della legge 31 dicembre 2012, n. 247, gli estremi delle polizze assicurative attuative dell'obbligo sono resi disponibili ai terzi senza alcuna formalità presso l'Ordine al quale l'avvocato è iscritto e presso il Consiglio nazionale forense, e sono pubblicati sui rispettivi siti internet».

dall'art. 2, co. 3, del D.M. 16/08/2016, n. 178[3] sono allegati alle presenti specifiche tecniche e ne formano parte integrante (all. 1 "TipiBaseCNF.xsd"; all. 2 "AlboTelematicoCNF.xsd"; all. 3 "TipoCarriera.xlsx").

2. Modalità di accesso al sistema informatico centrale per l'inserimento dei dati, modalità di interconnessione e interazione del sistema centrale con i sistemi dei consigli dell'ordine.

2.1. Interconnessione e accesso attraverso l'utilizzo di sistema gestionale dotato di cooperazione applicativa.

Al fine di un corretto assolvimento di tutti gli obblighi di legge, il SIC è realizzato affinché possa esporre delle API per garantire la cooperazione applicativa utile all'aggiornamento dei dati di un iscritto.

La sincronizzazione avviene automaticamente, previa autorizzazione rilasciata dal Presidente dell'Ordine o suo Delegato, in caso di possibilità di accesso diretto ai server dell'Ordine, oppure attraverso specifiche credenziali di autenticazione informatica rilasciate dal CNF (codice di autorizzazione e identificativo univoco dell'Ordine che serviranno a costruire la chiamata XML per l'invio dei dati). Dette interfacce sono documentate e messe a disposizione di qualunque produttore di soluzioni software gestionali per Ordini Forensi e sono necessarie per completare le funzionalità di inserimento/modifica/cancellazione dei dati di un qualunque iscritto al COA.

L'interconnessione può avvenire tramite cooperazione applicativa anche tra il SIC e i sistemi gestionali telematici di albo, eventualmente già forniti ai COA da un prestatore di servizi alla data di entrata in vigore del D.M. 178/2016, conformemente a quanto stabilito dall'art. 5, co. 1 del D.M. 178/2016[4] (c.d. SIL).

Ove vi sia coincidenza tra il fornitore del SIC e quello del SIL, l'interconnessione tra i predetti sistemi può, altresì, avvenire con modalità tali da garantire la replica in tempo reale dei dati del SIL sul SIC, al fine di consentire il suo immediato aggiornamento. Il fornitore adotta specifiche misure tecniche e organizzative adeguate al livello di rischio derivante da tale modalità di interconnessione,

[3] «Con decreto dirigenziale del Ministero della giustizia, sentito il Garante per la protezione dei dati personali e il Consiglio nazionale forense, può essere previsto che gli albi, i registri e gli elenchi contengano informazioni accessorie che siano pertinenti ai dati previsti dal presente regolamento e non eccedenti in relazione all'attività professionale, in conformità a quanto previsto dall'art. 61, commi 3 e 4, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 20 giugno 2003, n. 196».

[4] «1. Gli albi, il registro e gli elenchi sono tenuti esclusivamente con modalità informatiche. Per la tenuta degli albi, dei registri e degli elenchi i consigli dell'ordine utilizzano il sistema informatico centrale. I consigli dell'ordine che alla data di entrata in vigore del presente decreto dispongono di sistemi informatici per la tenuta degli albi, dei registri e degli elenchi possono continuare ad avvalersene, a condizione che, alla data di pubblicazione dell'avviso di cui all'art. 14, comma 2, tali sistemi siano dotati di tutte le funzionalità prescritte dal presente regolamento con riguardo al sistema informatico centrale e che abbiano basi di dati interconnesse con la base di dati del predetto sistema informatico centrale.(…)».

Sede Amministrativa
Roma – via del Governo Vecchio, 3 – tel. 06.977488 – fax 06.97748829

garantendo, in ogni caso, un'adeguata separazione fisica o logica dei dati oggetto di trattamento per conto di ciascun titolare.

2.2. Interconnessione e accesso attraverso l'utilizzo di sistema gestionale non dotato di cooperazione applicativa.

Agli Ordini territoriali che si avvalgono di un sistema gestionale di tenuta dell'albo non dotato di cooperazione applicativa sono assegnate utenze nominali per l'accesso al SIC, a cui sono attribuiti specifici profili di autorizzazione per l'inserimento, l'aggiornamento e la cancellazione dei pertinenti dati presenti nel SIC.

L'accesso al SIC da parte dell'Operatore dell'Ordine territoriale avviene previo superamento di una procedura di autenticazione informatica a due fattori, che prevede l'utilizzo di credenziali di autenticazione rilasciate dal CNF (username/password) e di un codice OTP che è inviato, ad ogni login, alla e-mail istituzionale di ciascun soggetto autorizzato previamente comunicata dall'Ordine territoriale al CNF.

La menzionata utenza garantisce al COA di accedere al SIC per effettuare l'upload del file XML di aggiornamento. Detto file XML può essere altresì inviato via PEC dal COA, previo accreditamento degli indirizzi PEC del mittente, conformemente alle modalità definite nella Circolare CNF 5 marzo 2010, n. 9-C/2010, ai sensi dell'art. 4, co. 3 del D.L. 29 dicembre 2009, n. 193 (convertito con modificazioni dalla l. n. 24/2010).

3. Misure di sicurezza per la riservatezza e l'integrità dei dati personali

3.1. Misure di natura tecnica

3.1.1. Sicurezza dei siti web e dei canali informatici

I portali web che ospitano i servizi del SIC sono mantenuti in sicurezza utilizzando metodi e strumenti per ridurre il rischio che le caratteristiche di un sito web siano sfruttate al fine di pregiudicare dati personali.

In particolare, i portali operano all'interno di una connessione protetta tramite crittografia asimmetrica garantendo:

- autenticazione del sito web visitato, mediante l'utilizzo di un certificato digitale emesso da una *certification authority* che fornisca adeguate garanzie di affidabilità;

Sede Amministrativa
Roma – via del Governo Vecchio, 3 – tel. 06.977488 – fax 06.97748829

- integrità e riservatezza dei dati scambiati tra le parti comunicanti, mediante l'utilizzo esclusivo di protocolli di rete e di *cipher suite* (ossia l'insieme di algoritmi utilizzati per lo scambio delle chiavi crittografiche, la crittografia e la verifica dell'integrità e dell'autenticità dei messaggi scambiati) che assicurino un adeguato livello di sicurezza, tenendo conto anche delle raccomandazioni in merito allo standard *Transport Layer Security* (TLS) adottate dall'Agenzia per l'Italia Digitale.

3.1.2. Sicurezza perimetrale dei siti web

Un'ulteriore componente della sicurezza dei servizi è garantita da firewall, ovvero elementi di sicurezza perimetrale dell'infrastruttura su cui operano i sistemi. Si tratta di apparati di rete per la gestione della sicurezza informatica, posti sul confine della rete, che hanno lo scopo di controllare gli accessi alle risorse del sistema filtrando tutto il traffico che tale sistema scambia con l'esterno. Il firewall filtra il traffico sulla base di un insieme di policy che si attengono al criterio di *default-deny*, vale a dire che viene permesso solo ciò che viene dichiarato esplicitamente, il resto viene vietato.

3.1.3. *Security Assessment*

Sono eseguite, almeno con cadenza annuale, attività di *Vulnerability Assessment* e *Penetration Test* (VA/PT).

Per VA si intende un processo atto a individuare eventuali vulnerabilità del sistema e misurare il relativo grado di gravità. Per PT si intende invece un esercizio che simula un attacco reale, come ad esempio l'elusione delle difese o lo sfruttamento delle vulnerabilità tramite l'utilizzo di cosiddetti exploit.

Entrambe le attività producono report di riscontro fornendo indicazioni in merito alle eventuali attività da pianificare in seno all'area IT per il rientro delle condizioni ottimali di sicurezza.

3.1.4. Gestione delle Vulnerabilità

Inoltre, il fornitore di servizi garantisce l'attivazione di politiche volte a limitare la probabilità e la gravità dei rischi per le risorse informatiche utilizzate durante la loro operatività.

3.1.5. Accesso amministrativo ai sistemi di produzione

Tutte le comunicazioni tra client e server avvengono tramite canale cifrato, utilizzando anche una specifica console IPMI (*Intelligent Platform Management Interface*).

3.1.6. Controllo degli accessi logici

Gli accessi ai dati oggetto del trattamento sono resi disponibili a seguito di precise procedure di autenticazione degli utenti a tal uopo autorizzati. Alle utenze sono attribuiti profili di autorizzazione che garantiscono l'accesso ai soli dati di pertinenza impedendo qualunque altro accesso verso dati non di pertinenza dell'utenza stessa, prevedendo l'impiego di credenziali di autenticazione informatica costituite da username e password scelte direttamente dall'utente e rilasciate seguendo regole di sicurezza prestabilite. In caso di password dimenticata, l'utente potrà avviare la procedura di reset password sicura senza l'intervento di alcun operatore.

Sede Amministrativa
Roma – via del Governo Vecchio, 3 – tel. 06.977488 – fax 06.97748829

3.1.7. Crittografia

La crittografia è applicata alla chiave di autenticazione per l'accesso ai sistemi. Le password utilizzate per l'autenticazione informatici degli utenti sono salvate in base dati mediante l'utilizzo di idonee tecniche crittografiche secondo lo stato dell'arte.

3.1.8. Gestione workstation aziendali

Sono adottate idonee misure di sicurezza al fine di ridurre la possibilità che le postazioni di lavoro delle risorse possano essere sfruttate per danneggiare i dati personali, quali la limitazione dei diritti delle utenze l'installazione di antivirus attivi e aggiornati, la *governance* centralizzata degli aggiornamenti ai sistemi operativi, la connessione delle postazioni alla rete locale per il raggiungimento delle sole risorse necessarie al normale svolgimento della propria funzione.

3.1.9. Backup

Sono adottate politiche di salvataggio dei dati ed azioni di backup con regolarità giornaliera (incrementale) e periodica (integrale), tali da assicurare la disponibilità e l'integrità dei dati personali, tutelandone la riservatezza.

3.1.10. Ridondanza e Alta Affidabilità dei sistemi

I sistemi di produzione che ospitano i servizi sono ospitati in server dedicati, adottando politiche di ridondanza, alta affidabilità delle risorse utilizzate e protezione da attacchi alla disponibilità (DoS, DDos, ecc.)

3.1.11. Implementazione di *Disaster Recovery* e di Continuità operativa

In caso di blocco del server principale sono previste procedure che a seconda della natura del blocco (malfunzionamento software, guasto hardware, indisponibilità della linea, ecc.), permettano nel minor tempo possibile di ripristinare operatività del software su un secondo server, già preconfigurato a questo scopo e che rimane sempre attivo e a disposizione per ogni evenienza.

3.2. Misure organizzative

3.2.1. Consapevolezza e formazione del personale

Sono svolte con regolarità iniziative di *security awareness* per tutto il proprio personale dipendente.

3.2.2. Politica di protezione dei dati personali

È prevista l'adozione di una policy aziendale di protezione dei dati personali per tutto il personale dipendente e che disegni compiti e responsabilità nella corretta protezione dei dati personali.

La policy di protezione dei dati personali, in particolare:

Sede Amministrativa
Roma – via del Governo Vecchio, 3 – tel. 06.977488 – fax 06.97748829

- supporta i processi di ideazione, progettazione e realizzazione di Prodotti/Servizi conformi ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita;
- prescrive i comportamenti che devono essere adottati da ciascun dipendente per reagire e rispondere nel rispetto delle definizioni del Regolamento nel caso di verificassero violazioni sui dati personali trattati;
- definisce ii comportamenti necessari a reagire e rispondere a minacce esterne e interne che possono causare perdita, alterazione, furto o cancellazione dei dati personali conservati dal fornitore definendo altresì la gestione delle comunicazioni obbligatorie, nei confronti dell'Autorità di Controllo e, se del caso, degli interessati, tenendo presenti i requisiti e le tempistiche prescritte dal Regolamento.

3.2.3. Gestione del personale

Le operazioni di trattamento dei dati gestiti sono effettuate solo da soggetti autorizzati/incaricati che operano sotto la diretta autorità del fornitore, attenendosi alle istruzioni impartite.

3.3. Misure di sicurezza fisica

La sicurezza fisica dei locali all'interno dei quali viene svolto il trattamento dei dati e delle informazioni gestite dal sistema è garantita attraverso l'adozione di dispositivi antiintrusione che prevedano l'accesso tramite badge elettronico o chiave di cui il personale dipendente autorizzato è dotato.

Per quanto riguarda i locali che ospitano i server, le misure di sicurezza fisica per l'accesso ai locali sono ricomprese entro il seguente schema:

- adozione di una policy di diritti di accesso;
- pareti divisorie (o dispositivi equivalenti) tra le diverse zone;
- telecamere alle entrate e alle uscite degli edifici, così come negli ambienti che ospitano i server;
- accessi sicuri controllati da lettori di badge;
- sistema di rilevamento dei movimenti;
- meccanismi anti-intrusione alle entrate e alle uscite dei data center;
- meccanismi di rilevamento delle intrusioni (sorveglianza 24 ore su 24 e videosorveglianza);
- un centro di sorveglianza permanente che controlla l'apertura delle porte di entrata e di uscita.

4. Criteri di individuazione degli incaricati del trattamento dei dati

Fatto salvo quanto già esposto *supra*, al SIC possono accedere gli utenti del CNF all'uopo autorizzati. L'accesso avviene tramite username/password e codice OTP inviato ad ogni login sulla e-mail associata ad ogni utente in fase di registrazione.

Gli accessi eseguiti da parte degli Operatori sono memorizzati in appositi log. Sono inoltre registrate tutte le variazioni di dati eseguite dagli stessi Operatori.

I log sono distinti in:

Sede Amministrativa
Roma – via del Governo Vecchio, 3 – tel. 06.977488 – fax 06.97748829

1. Log dell'applicazione:

1.1 Log degli accessi all'applicazione. Il log degli accessi all'applicazione contiene i dati riferiti agli accessi degli Operatori, in particolare vengono registrati: - ID dell'Operatore che ha eseguito l'accesso; - data e ora dell'accesso, identificativo della postazione di lavoro utilizzata per l'accesso.

1.2 Log delle operazioni compiute mediante l'applicazione. Il log delle operazioni compiute mediante l'applicazione contiene le operazioni eseguite dagli Operatori, nel dettaglio: - ID dell'Operatore che ha eseguito la variazione; - Data e ora della variazione; - Dato originale prima della variazione; - Dato modificato a seguito della variazione, identificativo della postazione di lavoro utilizzata per l'accesso;

2. Log di Sistema (ad es.: - Log automatici gestiti dal Server; - Data e ora dell'evento; - Tipo evento (accesso, errore, warning); - IP di provenienza; - Codice (es.: 200, 500, ecc..); - Risorsa chiamata (es.: Get/img/test.html); - Origine (pagina che ha generato la chiamata).

Il log di sistema, il log degli accessi all'applicazione e il log dell'applicazione riguardante le variazioni sono conservati per tre anni, conformemente a quanto disposto dall'art. 5, comma 1, ultimo periodo del D.M. 178/2016.

Sede Amministrativa
Roma – via del Governo Vecchio, 3 – tel. 06.977488 – fax 06.97748829