IdP Lepida SpA - Relazione trattamento dati personali

Sommario

1 Introduzione

La presente relazione mira a descrivere i trattamenti di dati personali effettuati da IDP SPID LepidaSpA riportandone le informazioni essenziali e le misure messe in atto per conformare tali trattamenti alla normativa sulla protezione dei dati personali.

1.2 Storia del documento

Versione	Data	Cambiamenti apportati
1.0	**28/11/2017**	**Prima stesura**
1.1	**16/02/2018**	**Seconda stesura**
1.2	**15/05/2018**	**Versione Aggiornata** • Modificato paragrafo 3.1 "Richiesta identità digitale": distinzione esplicita tra attributi obbligatori e opzionali • Modificato il paragrafo 4 "Informativa agli utenti": modificato "Periodo di conservazione dei dati" • Modificato paragrafo 3.4 Gestione dei documenti e dei log con aggiunta del dettaglio in merito alle modalità di conservazione dei log
1.3	**15/06/2018**	**Versione Aggiornata** • Modificato paragrafo 3.1 "Richiesta identità digitale"

2 Privacy e trattamento dei dati personali

Preliminarmente, deve essere rappresentato che la scelta di accreditamento di LepidaSpA come IDP SPID nasce dalla volontà della Regione Emilia-Romagna e la comunità degli Enti pubblici, cosiddetta Community Network dell'Emilia-Romagna CNER, prevista dalla Legge Regionale 11/2004 "Sviluppo regionale della Società dell'informazione", di valorizzare l'esperienza pluriennale e le identità pregressa del sistema di autenticazione denominato FedERa (Federazione degli Enti dell'Emilia-Romagna per l'Autenticazione). Tale sistema è stato realizzato da Regione Emilia-Romagna, attraverso LepidaSpA, nell'ambito della CNER, al fine di permettere ai cittadini di acquisire identità digitali (credenziali) con le quali poter richiedere l'accesso ai servizi online erogati dai diversi soggetti aderenti al sistema (Regione, Enti Locali, altre PP.AA. e soggetti di natura pubblica o privata), mediante un sistema di autenticazione federata.
Nell'ottica del riutilizzo delle identità pregresse di FedERa e le funzioni di Identity provider SPID svolte da LepidaSpA su mandato dei soci, pone la stessa società in condizioni di contitolarità dei trattamenti di dati personali afferenti a tale servizio, ai sensi e per gli effetti di cui all'art. 26 del Regolamento UE n. 679/2016. Rinviando l'esauriente delibazione dell'argomento al documento "Modello organizzativo SPID e utilizzo dei dati", in tale sede si rappresenta che gli Enti soci e LepidaSpA formalizzano l'accordo di riparto, in cui disciplinano il corretto inquadramento teorico dei rispettivi ruoli. L'accordo di contitolarità costituisce, quindi, la sede agile, flessibile e funzionale

in cui disciplinare anche gli aspetti più critici dei trattamenti di dati personali che discendono dall'esercizio di IdP. A titolo esemplificativo, l'accordo prevedrebbe la responsabilità di LepidaSpA in caso di data breach, sia con riferimento alla notifica all'Autorità Garante sia con l'esaudimento delle comunicazioni di cui all'art. 34 del Regolamento.
Per quel che concerne invece l'assolvimento dell'onere informativo nei confronti degli utenti FedERA, i due soggetti contitolari effettuano un trattamento di dati personali per finalità diverse da quelle per le quali i dati sono stati inizialmente raccolti. Tale facoltà è consentita dal nuovo regolamento europeo solo se il nuovo trattamento risulti essere compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. Vien da sè che il servizio che gli Enti soci e LepidaSpA, agendo come IdP di SPID, forniscono, è evidentemente sovrapponibile a quello originario per cui i dati furono raccolti (FedERa).

3 Informazioni trattate

Nel rispetto delle linee guida AgID viene effettuata, in caso di creazione di nuova identità digitale, una chiara distinzione tra i dati anagrafici richiesti all'utente strettamente necessari per l'ottenimento dell'identità digitale e le informazioni aggiuntive non obbligatorie raccolte a discrezione del gestore a fini commerciali.
LepidaSpA si limita come IDP SPID a richiedere e a trattare esclusivamente i dati strettamente necessari per l'ottenimento dell'identità digitale e non richiede informazioni aggiuntive nè utilizza i dati raccolti per finalità ulteriori .
Tali informazioni possono essere trattati soltanto da soggetti all'uopo designati incaricati per il trattamento dei dati personali effettuato a mezzo del sistema informativo IdM (Identity Management) realizzato e gestito da LepidaSpA.
Tutte le operazioni vengono svolte in conformità al principio di necessità, di pertinenza e di non eccedenza nel pieno rispetto delle normative e delle Linee Guida AgID relative a SPID.

3.1 Richiesta identità digitale

Vengono richiesti e trattati i dati essenziali per l'erogazione del servizio che comprendono i dati di seguito riportati e una memorizzazione di una scannerizzazione fronte/retro di un documento di identità e della tessera sanitaria.

3.1.1 Persone fisiche

Vengono richiesti e trattati i seguenti dati:

Attributi Identificativi

- nome;
- cognome;
- luogo di nascita;
- data di nascita;
- sesso;
- codice fiscale;
- nazione di nascita;
- provincia di nascita;
- estremi del documento di identità;

- Indirizzo di posta elettronica

Attributi secondari

- telefono mobile;
- pec (opzionale).

3.2 Identificazione dell'utente

A seguito dell'invio della richiesta di emissione di una nuova identità digitale, l'utente richiedente deve seguire un processo di identificazione che viene svolto da un operatore che svolge funzioni di Registration Authority con l'utilizzo di opportune funzionalità web a disposizione dal sistema informativo di LepidaSpA.

L'identificazione avviene secondo una delle seguenti modalità. All'avvio del servizio, disponibile per tutti i cittadini italiani sono disponibili le seguenti modalità di base:

- Identificazione informatica tramite documenti digitali di identità di cui all'art.64 del Dlgs. n.82/2005, tra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi. In caso di richiesta da parte dell'utente di identificazione tramite CNS il sistema prevede apposita procedura di verifica della carte. Terminata la procedura di verifica gli estremi della sessione di log della verifica verranno salvati a sistema come dimostrazione dell'avvenuta identificazione.
- Identificazione informatica tramite firma elettronica qualificata o firma digitale con l'acquisizione del modulo di richiesta di adesione in formato digitale compilato e sottoscritto con firma elettronica qualificata o con firma digitale. La verifica viene fatta automaticamente dal sistema che, dopo aver verificato la validità della firma (anche come data di scadenza) apposta sul documento provvede a confrontare il codice fiscale associato con quello dell'utente soggetto ad identificazione. Il documento firmato digitalmente viene salvato nel sistema come attestazione dell'avvenuta identificazione.

In una fase successiva, verranno messe a disposizione le seguenti ulteriori modalità:

- Identificazione a vista del soggetto richiedente in occasione della quale viene effettuata una scannerizzazione fronte/retro del documento di identità e della tessera sanitaria che vengono caricati nel sistema qualora non fosse già stato fatto dall'utente durante la fase di registrazione.
- Identificazione a vista da remoto tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196. L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile e firma autografa del richiedente stesso e verifica il codice fiscale tramite la tessera sanitaria in corso di validità. La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale con modalità crittografiche atte a garantirne l'accesso esclusivamente dietro richiesta dell'autorità giudiziaria, dell'Agenzia nel corso delle attività di vigilanza, dell'utente e dell'autorità giudiziaria in caso di disconoscimento della stessa. A dimostrazione dell'avvenuta identificazione da remoto l'operatore provvede a caricare a sistema l'intera registrazione della sessione audio/video.

La gestione utenti, include la possibilità per gli operatori di effettuare gli interventi che si possono rendere necessari, come ad esempio il caricamento di documenti che dovessero essere stati nel

frattempo ricevuti su altri canali di comunicazione, l'invio di comunicazioni secondo uno dei canali validati dall'utente (mail e/o SMS). Inoltre, e ai soli operatori, è delegata anche la gestione delle omocodie. In tali casistiche infatti il sistema non è in grado di validare il codice fiscale immesso dall'utente sulla base delle rimanenti informazioni anagrafiche causando l'impossibilità di effettuare la registrazione. All'arrivo di segnalazioni di questa natura l'operatore dovrà accedere ad un'area specifica dalla quale potrà identificare l'utente con il problema e associargli il codice fiscale corretto.

3.3 Amministrazione del sistema

Gli operatori di una o più sedi del gestore di identità hanno funzioni di amministrazione delle identità digitali di tutti gli utenti SPID rilasciate da LepidaSpA, indipendentemente dalla sede di cui operano. Gli amministratori hanno funzioni di amministrazione del sistema quindi gli viene garantito l'accesso alle funzioni necessarie per la configurazione e gestione del sistema. A questi ultimi è consentito l'accesso anche all'area amministrativa suddivisa nelle seguenti sezioni: 1) Sedi: area per la configurazione delle sedi di afferenza degli operatori. Ad ogni sede deve obbligatoriamente essere associato un ufficio 2) Amministratori: area per l'assegnazione del ruolo di amministrazione ad utenti già registrati nel sistema 3) Variabili: area per la configurazione delle variabili di funzionamento del sistema (ad esempio giorni validità password,etc) 4) Scheduler: componente software adibito all'esecuzione di generici task a specifiche cadenze temporali 5) SP: area per la gestione degli SP abilitati a richiedere l'autenticazione sul sistema mediante l'IdP.
Tutti i soggetti che ricoprono le funzioni di amministratore di sistema, ai sensi e per gli effetti del Provvedimento del 27.11.2008 e ss.mm.ii. del Garante per la protezione dei dati personali, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. Ciascuno di tali soggetti è nominativamente designato, con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. LepidaSpA detiene l'elenco degli amministratori designati sempre aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

3.4 Gestione dei documenti e dei log

La documentazione da conservare include le informazioni e i documenti che sono stati raccolti nel corso dell'attività di registrazione. Al fine di poter documentare la corretta esecuzione dei processi relativi all'attività di rilascio di una identità occorre conservare i riscontri relativi ai processi di identificazione e verifica. Tutta la documentazione inerente alla creazione e al rilascio di una identità digitale viene conservata ai sensi dell'articolo 7, commi 8 e 9, del DPCM.

Viene mantenuta traccia per ogni evento di sistema al fine di consentire una precisa ricostruzione delle attività in caso di necessità. Verranno tracciate le seguenti tipologie di eventi:

- Autenticazioni
- Variazione dati utente
- Variazione stato
- Eventi scheduler

Per tutte le tipologie di eventi verranno indicati i riferimenti temporali e, in aggiunta:

- per gli eventi di autenticazione verranno inoltre indicati il SP e il livello SPID utilizzato;

- per gli eventi di variazione dati verrà indicato se effettuati da operatore o dall'utente stesso. Qualora la modifica sia stata effettuata da un operatore, oltre all'identificativo dell'operatore stesso verrà inserito il link all'eventuale documentazione giustificativa dell'intervento eventualmente caricata;
- per quanto riguarda le variazioni di stato (sospensione, revoca, ecc.) verrà indicato l'eventuale operatore autore della transizione e il link all'eventuale documentazione giustificativa;
- per gli eventi di validazione verrà indicato il riferimento a tipologia e valore del contatto validato;
- per gli eventi generati dallo scheduler verrà indicata la tipologia di evento verificatosi e l'eventuale azione intrapresa (es: evento di scadenza documento con azione di segnalazione all'utente tramite mail).

Sulla lista dei log saranno possibili filtri per tipologia evento e data nonché l'esportazione dei dati in formato CSV o PDF.
I record di log verranno salvati su database e dovranno risultare consultabili per almeno 24 mesi secondo le modalità descritte nell'art.29 delle modalità attuative SPID. Al crescere del numero di record e al fine di salvaguardare il funzionamento del database risulta possibile prevedere procedure automatiche di svuotamento parziale della tabella di log con contestuale salvataggio su file system. Una apposita procedura dello scheduler si occuperà di eliminare selettivamente i log non più necessari basandosi sull'identificativo utente.
Considerato l'elevato numero di eventi tracciati la gestione dello storage su database avverrà mediante sistema di code di messaggi asincrono. Sia IdP che IdM potranno aggiungere messaggi alla coda che verranno poi elaborati dal sistema in modo asincrono evitando di introdurre colli di bottiglia nella procedure di runtime.
I sistemi attraverso i quali LepidaSpA eroga il servizio IdP SPID possiedono livelli di protezione logica e fisica estremamente elevati.
I sistemi sono fisicamente allocati presso il Datacenter di LepidaSpA di Ravenna, il quale è fornito di accorgimenti tecnici e procedurali che impediscono compromissioni fisiche, accessi non autorizzati e danneggiamenti dovuti ad eventi accidentali.
L'accesso ai server per qualsiasi iterazione con il sistema IdP avviene mediante sistema di autenticazione e attraverso una utenza personale ed univoca esclusivamente relativa al personale incaricato.
Le tracciature previste dalla normative SPID e gli eventi registrati su ogni server che compone l'architettura del servizio IdP LepidaSpA vengono registrati con un riferimento temporale recuperato attraverso l'abilitazione del servizio NTP (Network Time Protocol).
L'NTP rappresenta un protocollo TCP/IP che permette di sincronizzare l'ora di sistema delle macchine all'interno di una rete e, conseguentemente di impostare il proprio orologio. Tutti gli eventi perciò vengono rilevati e memorizzati con l'orario sincronizzato e sempre corretto.
Per garantire l'integrità e la non repudiabilità del registro delle transazioni, ad ogni tracciatura viene apposta una marca temporale e una firma elettronica da parte del servizio di gestione dei log.
Inoltre le tracciature vengono replicate in maniera sincrona su sistema SIEM (Security Information and Event Management) collegato, il quale a sua volta fornisce garantisce integrità dei file tramite calcolo di hash.

3.5 Sicurezza

Il sistema informatico è realizzato in piena compatibilità con le linee guida regionali in termini di IT governance in materia di sicurezza garantendo confidenzialità, integrità delle risorse. Vengono inoltre rispettate le linee guida di sicurezza emanate dal progetto OWASP e riportate nell'Avviso 1 di SPID Gestione Della Sicurezza Del Canale Di Trasmissione. Il sistema garantisce la sicura identificazione dell'utente che accede alle risorse nonché la limitazione degli accessi sulla base del ruolo assegnato. Tutte le comunicazioni garantiscono un livello di sicurezza tale da non risultare alterabili da utenti esterni e al tempo stesso non permettere a terzi l'intercettazione di dati considerati sensibili. Al fine di garantire tale livello di sicurezza ad ogni canale di comunicazione verrà attribuito un grado di pericolosità. I livelli utilizzati sono: alto, medio e basso. Per ogni livello sono state definite specifiche politiche di sicurezza da implementare sul canale soggetto a tale rischiosità.

La memorizzazione delle credenziali associate alle identità digitali vengono memorizzate nella banca dati del sistema con utilizzo di algoritmo di hashing robusto (SHA-256, SHA-512) e vengono offuscate le password nei file di configurazione delle connessioni al database.

4 Informativa agli utenti

Informativa sul trattamento dei dati personali resa ai sensi dell'art.13 del D.lgs. 196/2003 e art. 13 del Regolamento europeo n. 679/2016

Lepida SpA e gli Enti della CNER (.. inserire link ad elenco..) forniscono le seguenti informazioni riguardanti il trattamento dei dati personali dell'utente ai fini dell'attribuzione dell'identità digitale e di fruizione dei servizi erogati online dai "Fornitori di servizi" tramite il Sistema Pubblico per la gestione dell'Identità Digitale.

Fonte dei dati
I dati personali sono da Lei forniti agli operatori del servizio di registrazione ed anche attraverso le tecniche di comunicazione a distanza di cui Lepida e gli Enti della CNER si avvale al momento della richiesta dell'utenza SPID.

Finalità di trattamento
I suoi dati personali sono trattati al solo fine dell'attribuzione dell'identità digitale e di fruizione dei servizi erogati online dai "Fornitori di servizi" tramite il Sistema Pubblico per la gestione dell'Identità Digitale.

Modalità di trattamento
I trattamenti sui dati personali sono eseguiti con modalità cartacea, informatica e telematica con logiche strettamente correlate alle finalità sopra indicate e, in ogni caso, con modalità tali da garantire la riservatezza degli stessi.

I Contitolari
LepidaSpA e gli Enti della CNER (di seguito anche solo "Contitolari") sono contitolari del trattamento di dati personali relativo al funzionamento e alla gestione delle utenze del Sistema Pubblico per la gestione dell'Identità Digitale-SPID. L'elenco dei responsabili del trattamento è reperibile presso la sede di LepidaSpA.

Soggetti che possono trattare i tuoi dati personali

I tuoi dati personali sono trattati da personale interno previamente designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, *modus operandi,* tutti volti alla concreta tutela dei tuoi dati personali.
I Contitolari possono avvalersi di soggetti terzi per l'espletamento di attività e relativi trattamenti di dati personali mantengono, in tutti i casi, la titolarità. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati. Sono formalizzate istruzioni, compiti ed oneri in capo a tali soggetti terzi con la designazione degli stessi a "Responsabili del trattamento". Tali soggetti sono sottoposti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.
Inoltre, i Contitolari comunicheranno al Prestatore di servizi erogati online di cui l'utente intende usufruire gli attributi identificativi e secondari dell'interessato afferenti alla sua utenza SPID.

Obbligatorietà o facoltatività del consenso
Il conferimento dei dati è necessario. In assenza di conferimento non sarà possibile fornire l'utenza SPID nè i servizi ad essa correlati.

Trasferimento dei dati all'estero
I suoi dati personali non sono diffusi nè trasferiti all'estero verso Paesi, diversi da quelli appartenenti all'Unione Europea, che non assicurino livelli di protezione dei dati personali in linea con la normativa, anche di natura secondaria.

Periodo di conservazione dei dati
I tuoi dati personali sono trattati e conservati ai sensi dell'articolo 7, commi 8 e 9, del DPCM 24 ottobre 2014.
I dati delle tracciature degli accessi sono conservati presso il Datacenter di LepidaSpA di Ravenna per 24 mesi, mentre la documentazione e i dati inerenti al processo di adesione (identificazione e verifica della identità) sono conservati, presso il medesimo Datacenter, per un periodo pari a vent'anni decorrenti dalla scadenza o dalle revoca dell'identità digitale o, se ricevuta in momento precedente, sino alla ricezione della revoca del tuo consenso.

I tuoi diritti
In relazione ai trattamenti dei tuoi dati personali effettuati da LepidaSpA, puoi esercitare i diritti a te riconosciuti dall'art. 7 del D.lgs. 196/2003, di cui si riporta, al termine del presente paragrafo, integralmente il testo.
In particolare, hai sempre il diritto di ottenere dai Contitolari la conferma del trattamento o meno di dati personali che ti riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. Inoltre, ti segnaliamo che hai, comunque, il diritto di opporti in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che ti riguardano, ancorché pertinenti allo scopo della raccolta e, in qualsiasi momento e per qualsiasi motivo, al trattamento di dati personali che ti riguardano a fini di invio di materiale pubblicitario o di marketing diretto o di comunicazione commerciale. Ti segnaliamo che hai diritto di opporti al trattamento effettuato per finalità di marketing sia attraverso modalità automatizzate di contatto, sia a mezzo di posta cartacea e di chiamate tramite operatore. Resta salva la possibilità di esercitare tale tuo diritto in parte, ai sensi dell'art. 7, comma 4, lett. b), del Codice, ossia, in tal caso, opponendosi, ad esempio, al solo invio di comunicazioni promozionali effettuato tramite strumenti automatizzati.

Conformemente all'art. 13 del regolamento europeo n. 679/2016, ti segnaliamo che hai il diritto di:

- richiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che ti riguardano o di opporti al loro trattamento, oltre al diritto alla portabilità dei dati;
- revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca
- proporre reclamo all'Autorità Garante per il trattamento dei dati personali

Puoi liberamente e in qualsiasi momento esercitare i tuoi diritti, con richiesta rivolta a LepidaSpA all'indirizzo mail privacy@lepida.it, in modalità cartacea inviando la tua richiesta a Lepida S.p.A. in Via della Liberazione, 15, 40128 Bologna BO. Per esigenze di sintesi, di seguito sono riportati i tuoi diritti come riconosciuti dal Codice in materia di protezione dei dati personali, all'art. 7:

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. 2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati. 3. L'interessato ha diritto di ottenere:a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato. 4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Al seguente link http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679 puoi consultare gli artt. da 15 a 23 del Regolamento europeo n. 679/2016 ove sono disciplinati i tuoi diritti.

Cookie policy

Cosa sono e per quali finalità sono raccolti

Un "cookie" è un piccolo file di testo creato da alcuni siti web per immagazzinare informazioni sul computer dell'utente al momento in cui questo accede al sito. I cookie sono inviati da un server web al browser dell'utente e memorizzati sul computer di quest'ultimo; vengono, quindi, re-inviati al sito web al momento delle visite successive.

Tipologie di cookies utilizzati

Cookies tecnici

Sono i cookie necessari a permettere la navigazione di questo sito e per utilizzare diverse funzioni e servizi richiesti dagli utenti.

L'utilizzo di tali cookie permette ai gestori del sito, ad esempio, di accrescere la sicurezza del servizio richiesto dall'utente bloccando l'accesso a seguito di ripetuti login falliti da un'area riservata, oppure a ricordare la preferenza, ad esempio la lingua, in merito alle pagine web visitate.
A norma dell'art. 122 del Codice per la protezione dei dati personali e del provvedimento del Garante per la protezione dei dati personali relativo all'"Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie" dell'8 maggio 2014, pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014, questo sito può installare nel browser degli utenti i cookie tecnici essenziali per il corretto funzionamento di un sito web senza il preventivo consenso degli stessi.

Cookies di profilazione
Questo sito non utilizza cookie di profilazione: nessun dato personale raccolto da questo sito durante la navigazione degli utenti viene utilizzato per inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente durante la navigazione in rete

Cookie di terze parti
Non sono utilizzati cookie di "terze parti".

***

Come disabilitare i cookies
E' possibile disabilitare l'utilizzo dei cookie modificando le impostazioni del proprio browser, per esempio:

- Firefox
- Internet Explorer
- Chrome
- Safari
- Safari IOS

Alcuni browser, grazie ad apposite funzioni, permettono di bloccare specificatamente i cookie di terze parti,
Se il browser utilizzato non è tra quelli proposti, selezionare la funzione "Aiuto" sul proprio browser per trovare le informazioni su come procedere.
Attiva la modalità di "navigazione anonima"
Mediante questa funzione disponibile ormai in tutti i browser, è possibile navigare in Internet senza salvare alcuna informazione sui siti e sulle pagine visitate.
Tuttavia, i dati di navigazione, pur attivata tale funzionalità, sono registrati e conservati dai gestori dei siti web e dai provider di connettività.

Elimina direttamente i cookie
Attualmente quasi tutti i browser consentono di eliminare tutti i cookie installati.
Per maggiori istruzioni, consultare la guida del proprio browser o visitare uno dei seguenti link:

- Internet explorer
  http://windows.microsoft.com/it-IT/internet-explorer/delete-manage-cookie#ie=ie-9
- Mozilla Firefox https://support.mozilla.org/it/kb/Eliminare%20i%20cookie
- Google Chrome
  https://support.google.com/chrome/answer/95647?hl=it&ref_topic=3421433
- Safari (IOS) http://support.apple.com/kb/HT1677

Tuttavia, ad ogni nuova navigazione saranno installati nuovamente i cookie; in ragione di ciò si invita ad eseguire tale operazione periodicamente o utilizzare funzioni automatizzate per la cancellazione periodica dei cookie.

Link a siti esterni

Questo sito internet non contiene collegamenti ipertestuali detti “link” (ossia strumenti che consentono il collegamento ad una pagina web di un altro sito).