Uffici di prossimità - Note sul trattamento dei dati

DATI DI CONTROLLO DEL DOCUMENTO

Storia del documento				
versione	data	capitolo/paragrafo	modifica apportata	motivo modifica
bozza	20.01.2021 – 23.11.2021	---	nessuna	---

Riferimenti a documenti aziendali:

- Nessuno.

Riferimenti esterni:

- CNIL.”Privacy impact assessment knowledge bases”

Si tratta di una nota informale dove sono raccolte considerazioni relative al trattamento dei dati per il software gestionale degli Uffici di Prossimità. In alcune parti si configura come un promemoria da completare.

Infine in allegato si propone un modello di delega unico per i cittadini che richiedono servizi agli Uffici di Prossimità elaborato integrando quello presente nel toolkit di Regione Piemonte e proponendo una integrazione della sezione finale secondo il modello utilizzato dal Ministero della Giustizia.

INDICE

1. CONTESTO

1.1. Panoramica del trattamento

1.1.1. Il trattamento preso in considerazione

Gli Uffici di Prossimità sono rivolti al territorio per facilitare l'accesso ai servizi giudiziari e sono in grado di effettuare trasmissioni telematiche affidabili e autorizzate in ambito giudiziario tra cittadini e Tribunali. Per fare questo in GProx (software per la Giustizia di Prossimità) si trattano dati di due tipologie:

- dati nativi GProx ovvero quelli raccolti dall'Ufficio di Prossimità attraverso l'interazione con i cittadini-utenti
- dati nativi (del sistema) Giustizia, che sono restituiti/prelevati dal sistema informatico del Ministero della Giustizia.

Da ora in avanti, ove non diversamente esplicitato, si descriveranno in modo distinto i trattamenti dei dati delle due tipologie.

Dati nativi GProx

In GProx vengono trattati dati personali (anagrafici e recapiti) degli utenti che chiedono servizi giudiziari, segnalazioni al sistema socio sanitario o appuntamenti agli Uffici di Prossimità presenti sul territorio regionale. In particolare al momento si trattano i dati dei seguenti soggetti: ricorrente, beneficiario e amministratore di sostegno nominato dal Tribunale. Vengono trattate anche delle copie di lavoro della documentazione che i cittadini, che richiedono servizi giudiziari, debbono presentare al Tribunale. Le copie sono depositate su file system regionale, in modo da essere reperite in tempi diversi da operatori differenti durante il processo di preparazione al deposito presso la cancelleria del Tribunale.

Non vengono trattati i dati dei cittadini che richiedono informazioni e orientamento: si effettua solo una registrazione del numero di accessi anonimi a fini statistici e di monitoraggio del servizio.

Dati nativi Giustizia

In GProx vengono anche trattati dati restituiti al cittadino-utente tramite gli Uffici di Prossimità dal sistema informatico del Ministero della Giustizia sotto forma di comunicazioni (tra cui il numero del fascicolo aperto sul sistema Giustizia), notifiche e provvedimenti (di alcuni dei quali l'Ufficio di Prossimità può rilasciare copia conforme) comunicati dal Tribunale o consultati direttamente sul sistema ministeriale dagli Uffici di Prossimità che sono Punto di accesso (nel seguito PdA).

1.1.2. Le responsabilità e le modalità del trattamento

Ruoli Privacy	Titolare/i del Trattamento Comuni, Comunità Montane, Unioni di Comuni ASL, Ospedali per funzionari in proprio. Regione Liguria e, per essa, l'Azienda Ligure Sanitaria della Regione Liguria (A.Li.Sa.), ai sensi della L.R. n. 17/2016 relativamente alle attività di monitoraggio e controllo dell'efficacia del servizio.	Responsabili del Trattamento Regione, aziende informatiche di riferimento (es. Liguria Digitale) Liguria digitale è fornitore del software e responsabile informatico del trattamento dati per Regione Liguria
La/e finalità/è del trattamento dei dati .personali:	Erogare ai cittadini informativa e servizi in ambito giudiziario e socio sanitario sui temi della Volontaria Giurisdizione in generale e della Amministrazione di Sostegno in particolare.	
Il trattamento comprende le seguenti tipologie di dati personali:	X Dati anagrafici X Dati di contatto X Dati di navigazione, log e IP ☐ Dati idonei a rivelare origine razziale ed etnica ☐ Dati idonei a rivelare convinzioni religiose filosofiche e/o d'altro genere ☐ Dati idonei a rivelare opinioni politiche ☐ Dati idonei a rivelare l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso filosofico, politico o sindacale * Dati relativi allo stato di salute attuale * Dati relativi allo stato di salute pregresso ☐ Dati relativi alla vita sessuale X Dati giudiziari ☐ Dati da sottoporre a maggior tutela (es. HIV, etc.) ☐ Altro (*specificare di seguito*) *Nota: i dati relativi allo stato di salute sono contenuti nei soli file allegati criptati che il sistema non tratta ma semplicemente trasmette.	

Il trattamento comprende le seguenti categorie di interessati:	X Cittadini X Personale addetto agli Uffici di Prossimità (es. dipendenti comunali) ☐ Minori ☐ Soggetti vulnerabili X Altro (specificare di seguito) FUNZIONARI IN PROPRIO (ASSISTENTI SOCIALI, OPERATORI OSPEDALIERI) TENUTI DALLA NORMATIVA A PRESENTARE RICORSO PER AMMINISTRAZIONE DI SOSTEGNO A FAVORE DI LORO ASSISTITI
Informativa al trattamento dei dati personali	L'informativa redatta dal Titolare deve essere: X Consegnata a mano all'interessato X Pubblicata online sul sito degli Uffici di Prossimità ☐ Altro (specificare nello spazio sottostante) ☐ Non applicabile
Gestione consenso	Il trattamento prevede la raccolta e registrazione del consenso tramite: X Informativa e modulo raccolta consenso cartaceo redatto, reso e raccolto a cura del Titolare X Raccolta e registrazione del consenso tramite sistema Gprox ☐ Altro ☐ Non applicabile
Periodo di conservazione	Fino a due anni dopo la chiusura amministrativa della pratica di servizio giudiziario svolto dall'Ufficio di Prossimità
Comunicazione a terzi	Non prevista

1.1.3. Standard applicabili al trattamento

Per tutti i dati trattati gli standard tecnici adottati/adottabili sono i seguenti: anonimizzazione, pseudonimizzazione e criptazione.
Il codice di condotta generale è quello di richiedere al cittadino su apposito modulo il consenso al trattamento dei dati personali siano essi dati nativi GProx quali dati anagrafici, recapiti, documenti o dati nativi Giustizia quali comunicazioni, documenti e provvedimenti. Il consenso esplicito viene richiesto sia nel caso di trasmissione del contatto al sistema sociosanitario regionale (segnalazione al sistema socio sanitario) sia nel caso di delega all'Ufficio di Prossimità per comunicazioni e visibilità nei confronti del Tribunale di riferimento in relazione ad un servizio giudiziario.

Questo consenso-delega diventa un passo fondamentale e necessario del flusso di lavoro e si traduce nell'acquisizione della scansione del modulo di consenso-delega datato e firmato dal cittadino sotto forma di copia di lavoro nel sistema. Senza aver eseguito questa attività non è possibile proseguire nell'iter di qualunque pratica dell'Ufficio di Prossimità.
Per il deposito telematico di atti di cancelleria ci si riferisce a standard di interoperabilità del Ministero della Giustizia.

1.2. Dati, processi e risorse di supporto

1.2.1. I dati trattati

Dati nativi GProx
I dati raccolti e trattati da GProx sono i dati anagrafici dei soggetti:

- codice fiscale
- cognome
- nome
- data nascita
- luogo nascita
- sesso

e dati relativi ai recapiti del soggetto

- indirizzo residenza
- cap residenza
- comune residenza
- telefono
- cellulare
- e-mail.

Questi dati vengono raccolti per i richiedenti/ricorrenti, per i beneficiari e per gli amministratori di sostegno che richiedono servizi giudiziari all'Ufficio di Prossimità se e solo se costoro danno la delega per comunicazione e visibilità all'Ufficio di Prossimità.
Inoltre un sottoinsieme di questi dati è raccolto nel caso di richiesta di segnalazione al sistema socio sanitario regionale e limitatamente ad alcuni dei recapiti anche per i cittadini che richiedono un appuntamento presso un Ufficio di Prossimità.
Altri dati raccolti e trattati da GProx sono le copie di lavoro dei documenti presentati dal cittadino-utente e da trasmettere al Tribunale.

Dati nativi Giustizia
I dati mutuati dal sistema informatico del Ministero della Giustizia sono dati inerenti fascicoli aperti sul sistema Giustizia coinvolgenti i cittadini-utenti che si rivolgono all'Ufficio di Prossimità. Si tratta di dati identificativi quali:

- estremi del fascicolo di Giustizia

- estremi di un provvedimento del Tribunale

e di documenti visionabili compresi nel fascicolo.

Coloro che raccolgono e accedono ai dati sono

- gli operatori degli Uffici di Prossimità, che trattano tutte le tipologie di dati descritti sopra
- i funzionari in proprio (personale di ASL, AO e altri servizi sociali o sanitari) che debbono presentare ricorso presso il Tribunale per beneficiari loro assistiti, quindi trattano solo i dati relativi al deposito di un ricorso per amministrazione di sostegno.

I dati non sono acceduti da nessun altro utente del sistema GProx e sono destinati alla trasmissione al Tribunale, dove deve essere depositato l'atto giudiziario. La trasmissione di dati e documenti del ricorrente e del beneficiario avviene secondo le regole del Ministero della Giustizia tramite PEC e dentro una busta strutturata.
Anche gli estremi dei fascicoli di Giustizia e quelli dei provvedimenti del Tribunale sono mantenuti nella base dati come attributi della pratica GProx e non vengono acceduti da nessun altro utente del sistema GProx diverso dagli operatori degli Uffici di Prossimità.
I documenti del cittadino-utente raccolti, in quanto copie di lavoro, sono cancellati già al termine del flusso di lavoro della pratica dell'Ufficio di Prossimità, ovvero dopo che la trasmissione al Tribunale ha dato un esito.
I documenti visionati sul sistema Giustizia e/o sulle comunicazioni del Tribunale, tra cui anche quelli trasmessi come copia conforme al cittadino-utente, sono cancellati al termine del flusso di lavoro della pratica dell'Ufficio di Prossimità sia essa una mera consultazione tramite PdA oppure un deposito di atti.
I dati personali sono conservati per 2 anni. Trascorso questo tempo, anche i dati personali vengono cancellati in modo che la pratica venga mantenuta sul sistema di gestione dell'Ufficio di Prossimità in forma anonima (ai fini statistici). Contestualmente alla cancellazione dei dati personali vengono cancellati anche gli estremi del fascicolo di Giustizia collegato e dei provvedimenti di cui sono state rilasciate copie conformi.
Ovviamente qualora un utente revochi la delega all'Ufficio di Prossimità, la pratica viene terminata (portata anticipatamente a fine iter), le copie di lavoro di tutti i documenti sono cancellate, i dati personali anonimizzati e la pratica è mantenuta sul sistema in forma anonima allo stesso modo delle pratiche giunte a fine conservazione.
Inoltre si prevede di implementare un trattamento che l'operatore dell'Ufficio di Prossimità potrà avviare manualmente per le pratiche 'interrotte' (quelle che sono state abbandonate per lungo tempo dopo aver raccolto delega e dati) tale da terminare queste pratiche. In questo modo anche le pratiche 'interrotte' verranno anonimizzate insieme alle altre, una volta giunte a fine conservazione.

1.2.2. Ciclo di vita del trattamento dei dati

I dati oggetto di trattamento hanno natura differente e di conseguenza sono memorizzati su supporti diversi:

- dati personali (ovvero dati anagrafici, recapiti di richiedenti, beneficiari e amministratori di sostegno e estremi di pratiche e provvedimenti che li coinvolgono) custoditi su tavole di base dati
- copie di lavoro di documenti (ovvero scansione dei documenti del cittadino da depositare in Tribunale e documenti scaricati da Giustizia per trasmetterli al cittadino-utente) appoggiati come copie di lavoro su file system.

Raccolta

Se e solo se il servizio giudiziario richiesto prevede un deposito presso il Tribunale e il cittadino ha firmato la delega all'Ufficio di Prossimità, vengono raccolti i dati personali dagli operatori dell'Ufficio. Per prima cosa gli operatori dell'Ufficio di Prossimità effettuano il riconoscimento del cittadino richiedente tramite i documenti attestanti l'identità e il suo codice fiscale. Con i dati anagrafici (cognome, nome e codice fiscale) vengono ricercati sull'anagrafe di riferimento regionale sia il richiedente che il beneficiario in modo da importare i dati personali nei contatti di GProx. Mentre il richiedente potrebbe essere non presente nell'anagrafe regionale, per il beneficiario deve esserci un riscontro. I dati mancanti (non reperiti da anagrafe regionale di riferimento) possono essere inseriti direttamente a mano dall'operatore dell'Ufficio di Prossimità sui contatti di GProx (tipicamente i dati di recapito cellulare ed e-mail saranno quasi sempre inseriti a mano).
Nel corso della pratica di deposito il cittadino richiedente dovrà produrre i documenti (moduli compilati, certificati e altro) da inviare al Tribunale, di questi saranno scansionate delle copie di lavoro.

Trattamento

Per tutta la durata di una pratica di deposito dell'Ufficio di Prossimità, il cui iter prevede la preparazione, il controllo dei documenti richiesti dal Tribunale, l'invio al Tribunale e l'attesa dell'esito del deposito, le copie di lavoro dei documenti del richiedente per il deposito sono trattate da GProx. Il trattamento consiste nell'accesso e nell'eventuale sostituzione o aggiunta di copie di lavoro di documenti e infine nell'invio via PEC alla cancelleria del Tribunale di riferimento della documentazione raccolta dopo averla imbustata secondo le specifiche del Ministero della Giustizia.
Per lo stesso periodo i dati personali sono mantenuti e acceduti da GProx al fine di gestire la pratica dell'Ufficio di Prossimità. In questo periodo tali dati possono essere aggiornati, soprattutto quelli relativi ai recapiti.
Durante una pratica di deposito sono trattati anche dati nativi Giustizia, quali estremi del fascicolo di Giustizia e nomine provvisorie/definitive di amministratore

di sostegno. Inoltre nelle pratiche di consultazione tramite PdA vengono sicuramente visionati documenti nativi Giustizia, ma la pratica di consultazione è una pratica di durata estremamente limitata nel tempo.

Archiviazione
Non è prevista archiviazione per le copie di lavoro di tutti i documenti trattati (vedi nella sezione *Distruzione*).
I dati personali di richiedente, beneficiario o amministratore di sostegno, al termine delle pratiche che li coinvolgono, vengono mantenuti in GProx senza poter essere modificati (solo in lettura) fino a che lo stesso contatto non avvii una nuova pratica di deposito tramite l'Ufficio di Prossimità o fino alla scadenza dei termini per la conservazione.

Conservazione
Per un periodo di 2 anni i dati personali presenti su GProx e collegati esclusivamente a pratiche chiuse sono conservati in sola lettura.
Per i dati di recapito (indirizzo e-mail e/o telefono) degli utenti che prenotano un appuntamento il periodo di conservazione potrebbe essere ridotto ad 1 anno dopo la data dell'appuntamento.

Distruzione
Una volta che una pratica di deposito è arrivata a fine iter (è stato registrato l'esito definitivo della pratica di Giustizia) le copie di lavoro dei documenti del richiedente vengono cancellate da GProx.
I dati personali su GProx collegati a pratiche dell'Ufficio di Prossimità chiuse da 2 anni sono anonimizzati: la pratica arrivata a fine conservazione viene collegata a dati anonimi con le sole caratteristiche statistiche (ad esempio sesso, fascia di età, zona di provenienza) e, qualora non esistano altre pratiche collegate, il contatto viene cancellato; contestualmente sono cancellati gli estremi di fascicoli e provvedimenti di Giustizia. Per i recapiti degli utenti che hanno prenotato appuntamenti passato un anno dalla data dell'ultimo appuntamento prenotato vengono cancellati i recapiti forniti.

1.2.3. Risorse di supporto ai dati

Le copie di lavoro dei documenti sono dei file pdf custoditi su un file system criptato. Alcuni dati generali relativi a questi file (tipo di copia di lavoro, pratica a cui la copia è collegata) sono custoditi sulla base dati PostgreSQL nello schema dati per la gestione del flusso di lavoro.
I dati personali dei contatti sono memorizzati sulla base dati PostgreSQL nello schema dati per la anagrafica. I dati nativi Giustizia sono memorizzati sempre sulla base dati PostgreSQL nello schema dati per le pratiche GProx.

I dati di tracciamento degli accessi ai contatti sono sulla base dati PostgreSQL nelle schema dati dedicato all'audit.
Nel caso di servizi giudiziari di deposito per la creazione della busta telematica di deposito atto vengono appoggiati sul PostgreSQL i dati anagrafici richiesti dal file xml relativo al deposito scelto. Inoltre relativamente allo scambio di messaggi PEC tra Ufficio di Prossimità mittente del deposito e Ufficio Giudiziario destinatario del deposito sempre su PostgreSQL sono memorizzati gli identificativi univoci dei messaggi scambiati, ma non i contenuti dei messaggi.

2. PRINCIPI FONDAMENTALI

2.1. Proporzionalità e necessità

2.1.1. Scopi del trattamento specifici, espliciti e legittimi

Lo scopo del trattamento sia dei dati personali che delle copie di lavoro dei documenti è quello di fornire i servizi giudiziari per le materie di volontaria giurisdizione presidiate dagli Uffici di Prossimità.
Pertanto mentre per i cittadini che si recano presso l'Ufficio solo per informazioni e orientamento non viene eseguito alcun trattamento dei dati (è tutto anonimo), per coloro che chiedono

- di depositare atti
- di consultare fascicoli presso Giustizia
- di essere segnalati ai servizi socio sanitari

è necessario trattare dati personali (anagrafici e di recapito) e copie di lavoro di documenti del cittadino, come sicuramente le copie della delega-consenso. Nel caso dei depositi tra le copie di lavoro saranno presenti copie di moduli di richiesta, certificati ed altra documentazione prodotta dal cittadino ricorrente (colui che intende ricorrere presso un Tribunale) e copie di provvedimenti quali nomine provvisorie e definitive di amministratore di sostegno. Nel caso di consultazioni potranno essere trattate copie di atti presenti sui fascicoli consultati.
Anche dei cittadini che prenotano un appuntamento presso l'Ufficio di Prossimità (con gli operatori dell'Ufficio, con gli Avvocati volontari o con altre figure disponibili) è necessario avere un recapito per eventuali informazioni sull'appuntamento stesso. In questo caso non vengono raccolti dati anagrafici nel rispetto del principio di minimizzazione.

2.1.2. Basi legali che rendono lecito il trattamento

La basi legali del trattamento sono insite nella promozione e costituzione degli Uffici di Prossimità stessi da parte del Ministero della Giustizia con lo scopo di avvicinare la Giustizia (nel caso della volontaria giurisdizione) ai cittadini tramite sportelli sul territorio.
Qui vanno citati in dettaglio i riferimenti normativi che istituiscono e disciplinano gli Uffici di Prossimità.

2.1.3. Minimizzazione dei dati

I dati raccolti sono minimizzati (ovvero adeguati, pertinenti e limitati a quanto necessario) rispetto ai diversi servizi da erogare ai cittadini.

I dati personali sono necessari per l'invio a Giustizia e il supporto del cittadino nella compilazione, trasmissione e ricezione di informative ed esiti del Tribunale di riferimento. I dati personali contemplano solo quelli anagrafici, i recapiti e gli estremi delle pratiche di Giustizia collegate, perché l'Ufficio possa contattare e supportare il cittadino che l'Ufficio di Prossimità "rappresenta/della cui identità e intenzione si fa garante" presso il Tribunale.
Le copie di lavoro dei documenti che il cittadino deposita presso il Tribunale di riferimento sono necessarie per creare la busta di invio al Tribunale, nella quale vengono incluse e firmate digitalmente dall'operatore incaricato dell'Ufficio di Prossimità. Le copie di lavoro di documenti nativi Giustizia sono necessarie per rilasciate copie conformi di quei documenti, ove possibile.
Qualora i dati anagrafici non sono indispensabili, come nel caso della prenotazione di appuntamenti, non vengono raccolti e ci si limita a raccogliere i recapiti indispensabili per erogare il servizio.

2.1.4. Esattezza e aggiornamento dei dati

Dati nativi GProx

I dati personali vengono reperiti in parte dai documenti di identità e dal codice fiscale, che debbono venire presentati all'operatore incaricato dell'Ufficio di Prossimità dal cittadino che richiede servizi giudiziari, e in parte dalla anagrafica regionale di riferimento. Gli altri (i recapiti personali) sono forniti dallo stesso cittadino all'operatore.
Le copie di lavoro dei documenti sono create dall'operatore incaricato dell'Ufficio di Prossimità sulla base degli originali forniti dal cittadino. Tali originali sono controllati e 'verificati' formalmente dall'operatore dell'Ufficio di Prossimità (che ricordiamo è un funzionario pubblico).
Tra l'acquisizione di dati e documenti e il vero e proprio deposito con invio della busta via PEC al Tribunale non si presume che intercorra un tempo troppo lungo. Tuttavia prima della composizione busta e invio via PEC il software presenta dati e documenti raccolti in visualizzazione e ne richiede una esplicita conferma di validità. Prima della composizione della busta sia dati che copie di lavoro dei documenti possono essere aggiornati e sostituiti dall'operatore dell'Ufficio di Prossimità.

Dati nativi Giustizia

I dati nativi Giustizia sono direttamente trasmessi dal Tribunale oppure reperiti sul sistema Giustizia tramite PdA, quindi frutto di un accesso ufficiale e controllato. Il loro trattamento non dura a lungo prima della chiusura della pratica GProx della quale sono attributi, sia sotto forma di dati che di eventuali copie di lavoro di documenti.

2.1.5. Periodo di conservazione dei dati

Dati nativi GProx

Le copie di lavoro dei documenti sono mantenute in GProx esclusivamente per la trasmissione al Tribunale, pertanto non appena la pratica di deposito dell'Ufficio di Prossimità viene chiusa con la registrazione di un esito da parte del Tribunale la conservazione delle copie di lavoro può cessare.

I dati personali invece vengono conservati per un periodo più lungo tra i contatti dell'Ufficio di Prossimità: per 2 anni a partire dalla chiusura della pratica per cui erano stati raccolti ovvero dell'ultima pratica chiusa per cui erano stati raccolti, nel caso in cui un cittadino abbia più di una pratica attiva con l'Ufficio di Prossimità. Il periodo di 2 anni individuato si motiva con la necessità di seguire al meglio un cittadino; ad esempio in una pratica di amministrazione di sostegno la presentazione dei rendiconti ha spesso cadenza annuale e con questo periodo di conservazione il deposito dei rendiconti annuali è agevolato.

Nel caso dei dati di recapito privi di dati anagrafici collegati raccolti per la gestione degli appuntamenti il periodo di conservazione decorre dalla data dell'appuntamento e può essere anche più breve di 2 anni. Si ipotizza un periodo di 1 anno.

Dati nativi Giustizia

Le copie di lavoro dei documenti nativi di Giustizia sono mantenute in GProx esclusivamente per la trasmissione al cittadino-utente che le richiede/cui sono destinate. Quindi non appena la pratica di consultazione o deposito dell'Ufficio di Prossimità, cui sono riferite, viene chiusa la conservazione delle copie di lavoro può cessare.

I dati personali nativi Giustizia conservati tra gli attributi della pratica GProx vengono conservati per lo stesso periodo per il quale sono conservati i dati personali nativi GProx: 2 anni dalla chiusura della pratica di cui sono attributi.

2.2. Misure a tutela degli interessati

2.2.1. Informazione del trattamento per gli interessati

I cittadini, che chiedono servizi giudiziari o segnalazioni ai servizi socio sanitari, sono informati sul trattamento dei dati da loro forniti e richiesti per i servizi di cui intendono fruire dai moduli che debbono necessariamente sottoscrivere all'inizio di ogni pratica, che fornisca i servizi giudiziari o socio sanitari, aperta con l'Ufficio di Prossimità.

I modelli per il trattamento dei dati sono moduli di progetto standardizzati, quindi al di là di differenze stilistiche il loro contenuto è uguale per tutti gli Uffici di Prossimità sul territorio nazionale.

2.2.2. Consenso degli interessati

Vanno dettagliate le modalità operative e in particolare deve essere definito un

- codice di comportamento per il personale degli Uffici di Prossimità.

2.2.3. Diritti di accesso e portabilità dei dati

Vanno dettagliate le modalità operative e in particolare ci si deve focalizzare su

- accesso e portabilità.

Sebbene qui non sembrino troppo rilevanti, occorrerà una procedura non informatica per consentire agli utenti di esercitare tali diritti.

2.2.4. Diritti di rettifica e cancellazione (diritto all'oblio)

Vanno dettagliate le modalità operative per esercitare i diritti di

- rettifica come sopra, salvo il fatto che durante la vita della pratica (dato il contatto di persona con l'operatore dell'Ufficio di Prossimità) la rettifica è costante
- oblio come sopra, ma sicuramente così come la delega-consenso viene registrata in base dati, anche la revoca della stessa deve venire memorizzata in base dati con la data di revoca; inoltre l'oblio scatena la fine anticipata della pratica cui si riferisce, qualora la pratica non sia già terminata e sempre l'anonimizzazione della pratica in oggetto nella data della revoca o la prima data utile immediatamente successiva, dichiarando esplicitamente quale possa essere il tempo di latenza massimo.

2.2.5. Diritti di limitazione e opposizione

Vanno dettagliate le modalità operative affinché gli utenti esercitino i loro diritti di

- limitazione e opposizione.

Deve essere individuata una procedura non informatica per consentire agli utenti di esercitare tali diritti.

2.2.6. Obblighi dei responsabili del trattamento

Vanno dettagliati per ogni responsabile del trattamento

- ambito
- contratti, codici di condotta, certificazioni degli obblighi.

Non si prevede il trasferimento dei dati trattati da GProx in paesi extra-Ue.

3. PEC PER COMUNICAZIONI TRA UFFICI DI PROSSIMITÀ E UFFICI GIUDIZIARI

3.1. Utilizzo della Posta Elettronica Certificata per il progetto GProx

Le modalità di colloquio con il Ministero della Giustizia sono codificate dal Ministero stesso e per quanto riguarda i depositi di atti presso gli Uffici Giudiziari è necessario che:

- gli Uffici di Prossimità siano registrati sul ReGIndE (Registro Generale degli Indirizzi Elettronici) del Ministero come strutture e con i nominativi dei funzionari abilitati ai depositi
- i funzionari abilitati ai depositi abbiano a disposizione come strumento di lavoro la stessa mail PEC che compare sul ReGIndE
- i funzionari abilitati ai depositi abbiano a disposizione come strumento di lavoro una loro firma digitale
- il sistema informatico sia in grado di preparare utilizzando la chiave pubblica dell'Ufficio Giudiziario destinatario la busta telematica da allegare al messaggio di deposito inviato da PEC di Ufficio di Prossimità a PEC di Ufficio Giudiziario.

Gli Uffici di Prossimità svolgendo questo servizio giudiziario di deposito debbono quindi avere almeno una PEC per ciascun Ufficio da cui depositare gli atti che i cittadini affidano loro.

3.2. Modello organizzativo di riferimento per gli Uffici di Prossimità

Dal punto di vista del ReGIndE ogni funzionario potrebbe avere associato un differente indirizzo PEC. Tuttavia un solo indirizzo PEC per ogni Ufficio di Prossimità è non solo sufficiente, ma addirittura conveniente, in quanto permette la condivisione della casella e dei relativi messaggi.

Gli Uffici di Prossimità dipendono dai Comuni o dalle Comunità Montane o dalle Unioni di Comuni che hanno manifestato l'interesse per la loro apertura alla propria Regione. Dal momento che la regia della loro apertura, compreso l'allestimento, è regionale si ipotizza che la PEC sia fornita dalla Regione. In questo modo si auspica che il dominio di queste caselle sia lo stesso a livello regionale e riporti il comune di riferimento ad esempio per la Liguria l'ufficio di Chiavari qualcosa del tipo "chiavari@udppec.liguria.it".

3.3. Trattamento di dati e documenti veicolati via PEC dagli Uffici di Prossimità

Gli Uffici di Prossimità per i servizi giudiziari di deposito hanno la funzione di "postini qualificati". La documentazione cartacea prodotta dal cittadino viene controllata dal funzionario dell'Ufficio di Prossimità, il quale ha prima riconosciuto il cittadino attraverso

i suoi documenti di identità e ha raccolto la delega del cittadino all'Ufficio per operare il deposito.

Del controllo della documentazione fa parte la scansione dei documenti ricevuti e l'apposizione della firma digitale del funzionario che deposita ad attestare che quanto trasmesso all'Ufficio Giudiziario sia effettivamente quello consegnato dal cittadino.

La trasmissione avviene da PEC a PEC con i documenti imbustati e non leggibili se non dall'Ufficio Giudiziario destinatario che applica la sua chiave privata per decodificare il contenuto della busta.

Pertanto l'ufficio di prossimità svolge il ruolo di vettore tra il cittadino e il tribunale di destinazione. Per questo motivo e dal momento che la busta contenente i documenti del cittadino non risulta leggibile e gli originali cartacei restano di proprietà del cittadino non si prevede né protocollazione né conservazione.

In questo contesto la protocollazione configurerebbe la comunicazione via PEC come soggetto attivo della comunicazione e non come semplice vettore.

Gli Uffici di Prossimità producono solo un modulo di delega/autorizzazione da firmare. Anche in questo caso si tratta di un documento cartaceo con le firme autografe del cittadino delegante e del funzionario che raccoglie la delega per conto dell'Ufficio di Prossimità.

Analogamente alla delega, qualora il cittadino intendesse revocare la delega concessa all'Ufficio di Prossimità, potrebbe esistere un modello di revoca della delega, se previsto dal toolkit di Regione Piemonte. In ogni caso a seguito di una richiesta di revoca, il sistema Gprox deve attivare l'apposita funzionalità di anonimizzazione e distruzione dei documenti.

I documenti fisici della delega e della revoca debbono essere conservati dagli Uffici di Prossimità, in quanto sono la base del loro operare sui servizi giudiziari.

Le copie di lavoro (scansione delle deleghe e delle revoche firmate e controfirmate) di questi documenti sono custodite sul sistema su file system criptato, al pari dell'altra documentazione.

4. RISCHI

4.1. Misure esistenti o pianificate

4.1.1. Crittografia

Attualmente i dati personali sono memorizzati in archivi separati da quelli gestionali.
Il codice identificativo interno dell'archivio anagrafico è conservato sotto forma di impronta criptografica (hash SHA512 - AES).
Il ricongiungimento con i dati gestionali è effettuato mediante una funzione di correlazione tra i due codici identificativi.
Per lo scambio dati con il Ministero di Giustizia sono adottati gli standard specificati in "*Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante regolamento concernente le regole tecniche per l'adozione, nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2 del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24*"
Gli utenti che accedono via internet utilizzano il protocollo https.

4.1.2. Anonimizzazione

Sono stati implementati meccanismi di anonimizzazione da applicare subito in caso di revoca o trascorso il periodo di conservazione dal completamento della pratica.

4.1.3. Partizionamento

Il partizionamento è effettuato a livello di base informativa mediante la pseudonimizzazione sui codici identificativi come descritto al paragrafo 4.1.1.

4.1.4. Controllo degli accessi logici

L'accesso all'applicazione viene effettuato mediante SPID di livello 2/CIE. Il sistema di autenticazione è quello regionale con infrastruttura NAM.

L'accesso diretto alla base informativa è effettuato con le seguenti utenze:

- Utenze d'amministrazione
- Utenze proprietarie (modello dati e procedure) separate da quelle di servizio
- Utenze applicative di servizio (ovvero le utenze utilizzate dalle applicazioni).

4.1.5. Tracciabilità

- Accessi amministrativi di sistema operativo ("syslog" Linux)
- Accessi amministrativi DBMS
- Accessi altre utenze DBMS
- Accessi via sistema di autenticazione

Per gli accessi degli "amministratori di sistema" vengono applicate le disposizioni di cui al provvedimento del garante del 2008 e della circolare AGID per le misure di sicurezza della 18/04/2017
Registrazione di utente e data dell'ultimo aggiornamento per ciascuna occorrenza delle tavole gestionali.

4.1.6. Archiviazione

I dati personali sono conservati e gestiti principalmente mediante DBMS; i datafile sono protetti dai meccanismi di sistema operativo del database server.
Sono svolti giornalmente i salvataggi.
I dati in archivi su file-system sono protetti all'accesso dai meccanismi di sistema operativo.
In Regione Liguria è prevista una cifratura dell'intera macchina virtuale sia per applicazione sia per DBMS.
Al momento i dati non sono storicizzati.

4.1.7. Minimizzazione dei dati

Si rimanda a quanto specificato nel precedente paragrafo 2.1.3 "minimizzazione dei dati".
A livello di applicazione:

- Componente di profilazione degli utenti

In base ai ruoli di base dati assegnati esistono diversi livelli di visibiltà/gestione.
Esiste un sistema applicativo di configurazione con cui l'amministratore può abilitare e profilare gli operatori di sportello.

4.1.8. Integrare la protezione della privacy nei progetti

Come descritto nelle misure precedenti e successive la protezione dei dati avviene sin dalla progettazione (*by design*) e per impostazione predefinita (*by default*).

4.1.9. Sicurezza dei canali informatici

Il dialogo con gli utenti avviene su protocollo https.
L'autenticazione avviene tramite SPID.
Il dialogo con gli uffici giudiziari avviene tramite PEC secondo le specifiche del Ministero di Giustizia, indicate al §4.1.1 "Crittografazione".

4.1.10. Altre misure

Per le seguenti misure previste dalla valutazione di impatto si rimanda alle misure infrastrutturali e organizzative previste da Regione Liguria

- Vulnerabilità
- Lotta contro il malware
- Gestione postazioni
- Sicurezza dei siti web
- Backup
- Manutenzione
- Contratto con il responsabile del trattamento
- Controllo degli accessi fisici
- Sicurezza fisica e ambientale Sicurezza dell'hardware
- Prevenzione delle fonti di rischio
- Protezione contro fonti di rischio non umane
- Sicurezza dei documenti cartacei
- Politica di tutela della privacy
- Gestione delle politiche di tutela della privacy
- Gestione dei rischi
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Gestione del personale
- Gestione dei terzi che accedono ai dati
- Vigilanza sulla protezione dei dati

4.2. Accesso illegittimo ai dati

4.2.1. I principali impatti sugli interessati se il rischio si dovesse concretizzare

- Disturbi psicologici minori ma oggettivi (diffamazione, reputazione)
- Problemi di relazione con conoscenze personali o professionali (ad esempio immagine, reputazione offuscata, perdita di riconoscimento)
- Pubblicità mirata su un aspetto di vita riservato
- Sensazione di violazione della privacy con danni irreversibili
- Intimidazione sui social network
- Mancata promozione della carriera
- Ricezione di invii mirati non richiesti che potrebbero danneggiare la reputazione degli interessati

4.2.2. Le principali minacce che potrebbero concretizzare il rischio

- Accesso diretto interattivo alla base informativa
- Violazione dell'applicazione
- Furto o perdita dei supporti di salvataggio

- Consegna di documentazione personale a destinatario errato, non autorizzata
- Errore umano che può destinare dati a persone errate
- Errore del software che può destinare dati a persone errate

Riconducibili alle classificazioni del CNIL §1.7 del documento "*Privacy impact assessment knowledge bases*".

4.2.3. Le fonti di rischio

Persona esterna malintenzionata. Persona interna al titolare/responsabile malintenzionata o incompetente.

4.2.4. Misure che contribuiscono a mitigare il rischio

Crittografia, Partizionamento, Controllo degli accessi logici, Minimizzazione dei dati, Sicurezza dei canali informatici, Archiviazione.
(misure applicative)

Sicurezza dei documenti cartacei, Gestione dei terzi che accedono ai dati, Gestione delle postazioni, Lotta contro il malware, Vulnerabilità (misure infrastrutturali)

4.2.5. Stima di gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate

Limitata. Pur trattandosi di dati socio-sanitari ed economici, le misure adottate riducono significativamente il rischio.

4.2.6. Stima di probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Limitata. Le misure adottate dovrebbero ridurre significativamente il rischio in questione.

4.3. Modifiche indesiderati dei dati

4.3.1. I principali impatti sugli interessati se il rischio si dovesse concretizzare

- Negazione dell'accesso a servizi amministrativi (ad esempio perdita di riconoscimento del bisogno)
- Trattamento di dati errati che creano malfunzionamenti
- Spese impreviste
- Cancellazione o modifica non concordata di appuntamenti
- Dati non aggiornati
- Manomissione dell'iter della pratica

- Disturbi psicologici minori ma oggettivi (diffamazione, reputazione)
- Sensazione di violazione della privacy senza danni irreversibili

4.3.2. Le principali minacce che potrebbero concretizzare il rischio

- Accesso diretto interattivo alla base informativa
- Violazione dell'applicazione
- Consegna di documentazione personale a destinatario errato, non autorizzata
- Errore umano che può portare a gestione errata della pratica
- Errore del software che può portare a gestione errata della pratica

Riconducibili alle classificazioni del CNIL §1.8 del documento "*Privacy impact assessment knowledge bases*".

4.3.3. Le fonti di rischio

Persona esterna malintenzionata. Persona interna al titolare/responsabile malintenzionata o incompetente

4.3.4. Misure che contribuiscono a mitigare il rischio

Crittografia, Partizionamento, Controllo degli accessi logici, Minimizzazione dei dati, Sicurezza dei canali informatici, Archiviazione, Tracciabilità (misure applicative)

Sicurezza dei documenti cartacei, Gestione dei terzi che accedono ai dati, Gestione delle postazioni, Lotta contro il malware, Vulnerabilità, Backup, Gestione del personale (misure infrastrutturali)

4.3.5. Stima di gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate

Limitata. Pur trattandosi di dati socio-sanitari ed economici, le misure adottate riducono significativamente il rischio.

4.3.6. Stima di probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Limitata. Le misure adottate dovrebbero ridurre significativamente il rischio in questione.

4.4. Perdite di dati

4.4.1. I principali impatti sugli interessati se il rischio si dovesse concretizzare

- Ritardo nella presa in carico nel processo istruttorio della pratica

- Negazione dell'accesso a servizi amministrativi
- Spese impreviste
- Cancellazione senza preavviso di appuntamenti
- Dati non aggiornati
- Disturbi psicologici minori ma oggettivi
- Sensazione di violazione della privacy senza danni irreversibili

4.4.2. Le principali minacce che potrebbero concretizzare il rischio

- Spionaggio, sovraccarico, alterazione, danni e perdita dell'hardware
- Uso anomalo, Sovraccarico, Alterazione e Perdita totale del software, Cancellazione totale o parziale di un programma software
- Indisponibilità dell'infrastruttura di comunicazione
- Disagio del personale nello svolgimento dell'attività lavorativa
- Calamità naturali

Riconducibili alle classificazioni del CNIL §1.9 del documento "*Privacy impact assessment knowledge bases*".

4.4.3. Le fonti di rischio

Persona esterna malintenzionata. Persona interna al titolare/responsabile malintenzionata o incompetente. Non umane

4.4.4. Misure che contribuiscono a mitigare il rischio

Crittografia, Partizionamento, Controllo degli accessi logici, Minimizzazione dei dati, Sicurezza dei canali informatici, Archiviazione, Tracciabilità (misure applicative)

Sicurezza dei documenti cartacei, Gestione dei terzi che accedono ai dati, Gestione delle postazioni, Lotta contro il malware, Vulnerabilità, Backup, Gestione del personale, Sicurezza dell'hardware, Manutenzione, Prevenzione delle fonti di rischio, Protezione contro fonti di rischio non umane, Controllo degli accessi fisici (misure infrastrutturali)

4.4.5. Stima di gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate

Limitata, Pur trattandosi di dati socio-sanitari ed economici, le misure adottate riducono significativamente il rischio.

4.4.6. Stima di probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Limitata. Le misure adottate dovrebbero ridurre significativamente il rischio in questione.

5. ALLEGATI

5.1. Modello unico Uffici di Prossimità per la raccolta delega-consenso

Si propone di utilizzare un unico modello per la raccolta sia delle deleghe per visibilità e/o comunicazione sia delle autorizzazioni alla segnalazione al sistema socio sanitario.
Quindi nella pagina seguente si riporta una proposta di modello unico per la raccolta del consenso al trattamento dei dati o della delega per servizi giudiziari, che modifica solo nella parte iniziale quello proposto nel toolkit di Regione Piemonte.

MODELLO DI DELEGA E AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Il/La sottoscritto/a COGNOME NOME
nato/a a CITTA' DI NASCITA il gg /mm/aaaa
identificato a mezzo documento identificativo tipologia n° numero
rilasciato da ENTE RILASCIO in data gg /mm/aaaa
residente in CITTA' DI RESIDENZA
indirizzo INDIRIZZO
C.F. CODICE FISCALE RICHIEDENTE in qualità di richiedente per
COGNOME NOME C.F. CODICE FISCALE BENEFICIARIO

in data gg/mm/aaaa

- ○ DELEGA PER VISIBILITA'
- ○ DELEGA PER COMUNICAZIONE (DA ABILITARE IN CASO DI DEPOSITO)
- ○ AUTORIZZA ALLA SEGNALAZIONE AL SISTEMA SOCIO SANITARIO

l'Ufficio di Prossimità di UFFICIO DI PROSSIMITA' alle seguenti attività

- ○ Deposito di atto presso la Cancelleria del Giudice Tutelare del TRIBUNALE
- ○ Consultazione di fascicolo presso Giustizia
- ○ Segnalazione dati personali del beneficiario al sistema socio Sanitario Regionale.

Allega copia del proprio documento di identità e codice fiscale.
Chiede inoltre, nel caso di deposito, che le comunicazioni relative alla procedura vengano inviate via PEC al suddetto Ufficio di Prossimità, eletto a domicilio, e delegato, altresì al ritiro di copie dei provvedimenti emessi.
Tutte le eventuali attività di notifica (ad esempio la notifica della data di fissazione di udienza di esame nell'amministrazione di sostegno) sono a carico del ricorrente.
Luogo , li / / Firma
Soggetto incaricato al ritiro Firma
Firma dell'incaricato all'invio dell'Ufficio di Prossimità

Informativa ex art. 13 del Regolamento Europeo in materia di protezione dei dati personali n. 2016/679

I dati personali del delegante sono trattati nel rispetto del Regolamento europeo in materia di protezione dei dati personali n. 2016/679, del d. lgs. n. 196/2003 (codice della privacy) come modificato dal d. lgs. n. 101/2018 e della normativa vigente in materia di protezione dei dati personali. I dati personali sono raccolti esclusivamente per le finalità espresse nel presente documento e sono forniti direttamente dagli interessati. Il mancato conferimento dei dati personali comporta l'impossibilità di accettare la delega. I dati saranno trattati in forma cartacea e informatica, per tutti gli adempimenti connessi allo svolgimento dell'attività richiesta. Non è prevista la comunicazione, diffusione, trasmissione dei dati sensibili.
Il titolare dei dati è TITOLARE contitolare è CONTITOLARE
Il Responsabile esterno è RESPONSABILE

Autorizzazione al trattamento dei dati personali

Preso atto dell'informativa di cui all'art. 13 del regolamento europeo 2016/679, il delegante autorizza il trattamento e la comunicazione dei propri dati personali per le finalità connesse allo svolgimento delle attività delegate.
Luogo , li / / Firma

5.2. Integrazione modello “Informazioni sul trattamento dei dati personali”

Nella parte denominata “Informativa ex art. 13 del Regolamento Europeo in materia di protezione dei dati personali n. 2016/679” nel modulo riportato qui sopra potrebbero essere inserite ulteriori informazioni, quali quelle riportate nella sezione finale del modulo per la richiesta del censimento delle PPAA del Ministero della Giustizia.

In particolare la suddivisione in diverse sezioni (come dall’indice seguente) aiuta la lettura delle informazioni:

- Oggetto del trattamento
- Titolare del trattamento
- Responsabile della protezione dei dati
- Finalità del trattamento dei dati
- Base giuridica del trattamento
- Modalità del trattamento
- Conseguenze della mancata comunicazione dei dati personali
- Conservazione dei dati
- Comunicazione dei dati
- Profilazione e diffusione dei dati
- Diritti dell’interessato
- Diritto di reclamo
- Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

Pertanto si riporta qui sotto a titolo di esempio/ispirazione la sezione corrispondente del documento denominato “ModelloRichiestaCensimentoPPAA_New.doc” del Ministero della Giustizia.

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Oggetto del trattamento

I dati oggetto del trattamento sono qualificabili ai sensi dell'art. 4, par. 1, n. 1, del Regolamento.

Titolare del trattamento

Il Ministero della Giustizia, con sede in via Arenula, n. 70, 00186, Roma (centralino tel. +39 - 06 68851; redazione@giustiziacert.it), è titolare del trattamento dei dati conferiti per la sottoscrizione delle convenzioni.

Responsabile della protezione dei dati

dr.ssa Doris Lo Moro (D.M. 7 agosto 2018), via Arenula n. 70 - 00186 Roma;
tel.: + 39 06 6885 2283
PEC: responsabileprotezionedati@giustiziacert.it
PEO: responsabileprotezionedati@giustizia.it

Finalità del trattamento dei dati

Il trattamento dei dati personali è finalizzato a consentire il censimento dell'indirizzo di PEC della amministrazione pubblica o di suoi organi, articolazioni, anche territoriali, e aree organizzative omogenee nell'elenco di cui al comma 12 dell'art. 16 del decreto-legge n. 179 del 2012 conv..to, con modificazioni, dalla legge n. 221 del 2012 e successive modifiche.

Base giuridica del trattamento

I dati personali sono trattati dal Ministero della Giustizia nell'esecuzione dei propri compiti pubblici o comunque connessi all'esercizio dei propri pubblici poteri e per le finalità connesse a questi compiti e derivanti dall'articolo 16 sopra citato.

Modalità del trattamento

I dati personali potranno essere trattati a mezzo sia di archivi cartacei sia informatici e trattati con modalità e per il tempo strettamente necessari a far fronte alle finalità sopra indicate.
Per il trattamento con strumenti automatizzati sono osservate specifiche misure di sicurezza per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Conseguenze della mancata comunicazione dei dati personali

La mancata comunicazione dei dati personali impedisce l'avvio della procedura di censimento dell'indirizzo di PEC dell'amministrazione pubblica nell'elenco di cui al citato art. 16.

Conservazione dei dati

I dati personali, oggetto di trattamento per le finalità sopra esposte, saranno conservati per il periodo di durata del censimento e, successivamente, per il tempo in cui il Ministero sia soggetto a obblighi di conservazione previsti da norme di legge o regolamenti.

Comunicazione dei dati

I dati personali potranno essere comunicati, sempre nel rispetto della normativa sulla protezione dei dati, a:

1. ai soggetti responsabili designati dal titolare o a quelli incaricati del trattamento e che operano sotto la diretta autorità del titolare o del responsabile;
2. all'Autorità Giudiziaria, se richiesto con specifico ordine;
3. all'Avvocatura dello Stato, se necessario per la tutela dei diritti dell'amministrazione per atti o fatti derivanti dalle operazioni di censimento;
4. agli altri soggetti per i quali la legge impone detta comunicazione.

Profilazione e Diffusione dei dati

I dati personali non sono soggetti a diffusione, se non per adempiere ad obblighi di legge espressamente previsti, né ad alcun processo decisionale interamente automatizzato, ivi compresa la profilazione.

Diritti dell'interessato

L'interessato ha il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione, l'aggiornamento e la rettifica oppure di limitarne il trattamento secondo quanto previsto dagli artt. 15, 16, 17, 18 e 21 del Regolamento (UE) 2016/679. In particolare, ai sensi e nei limiti del citato art. 17 e del D.lvo 196/2003, l'interessato ha il diritto di chiedere la cancellazione dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Diritto di reclamo

L'interessato, il quale ritenga che il trattamento dei dati personali al medesimo riferiti sia effettuato in violazione di quanto previsto dal Regolamento UE n. 679 del 2016, ha il diritto di proporre reclamo al Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento cit., o di adire le opportune sedi giudiziarie (art. 79 del Regolamento UE n. 679 del 2016).
Sito del Garante per la protezione dei dati personali: www.garanteprivacy.it

Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali

Qualora sia previsto il trasferimento dei dati extra-UE o a organizzazioni internazionali, il titolare del trattamento si impegna a chiarire all'interessato la sussistenza dei presupposti e delle garanzie necessarie per procedere al trasferimento di cui agli artt. 44 e ss. del Regolamento (UE) 2016/679 attraverso un'adeguata informativa.