Privacy Governance in ePersonam

Informazioni per i soggetti interessati

ing. U. Brighetti
07/07/2021 v2.0

Legenda

Azienda (o di seguito 'Advenias'): Advenias s.r.l.
Direzione: F. Bovard (CEO), ing. U. Brighetti (DTO), ing. P. Semprini (DCO)
Collaboratori/personale: dipendenti, o collaboratori esterni
LTA: licenza temporanea annuale di utilizzo di ePersonam
Cliente: il Cliente di Advenias s.r.l. che ha una LTA di ePersonam
GDPR: Reg. UE n. 679/2016 in materia di protezione dei dati personali
CERTIFICAZIONI: ADVENIAS s.r.l. ha ottenuto le certificazioni di QUALITA' ISO9001:2015 e di SICUREZZA ISO27001:2013 e le specializzazioni, Sistema GDPR certificato UNI/PDR43, GAMP5 (per prescrizione e somministrazione farmaci)

- ISO/IEC 27017:2015 (vedi certificato)
- ISO/IEC 27018:2014 (vedi certificato)
- ISO 13485:2016 cat. I
- GDPR Certificato UNI/PDR 43.2:2018 (vedi certificato)
- GAMP5

Sistema di Gestione Certificato ISO 9001:2015 AQS/Q/34502018
Sistema di Gestione Certificato ISO/IEC 27001:2013 AQS/SI/36242018
Sistema di Gestione Certificato ISO 13485:2016 AQS/DM/54812020
Certificato **UNI/PDR 43.2:2018**

Disposizioni generali

ePersonam è un software di gestione ERP dei pazienti e degli operatori di una struttura sociosanitaria. In particolare, il software permette di organizzare e gestire le attività di assistenza del paziente e di ottimizzare lo svolgimento del lavoro degli operatori. Mediante il suo regolare funzionamento il software comporta per sua stessa natura il trattamento di alcuni dati personali e categorie particolari di dati personali riferiti a tali soggetti. Pertanto, con il presente documento, da ritenersi parte integrante del contratto di fornitura di ePersonam sottoscritto tra il Cliente e l'Azienda, vengono forniti i dettagli e le linee guida seguite da ePersonam per garantire la protezione dei dati personali e assicurare idonee garanzie circa la sicurezza fisica, logica e organizzativa delle attività di trattamento degli stessi.

Le attività di trattamento svolte dal software sono realizzate sempre per conto del Cliente, che ha concluso con l'Azienda regolare contratto avente ad oggetto la LTA di ePersonam: pertanto l'Azienda, in ragione delle sue attività di assistenza e formazione al Cliente (Titolare del trattamento), nonché quelle di predisposizione e manutenzione del software, riveste il ruolo di Responsabile del trattamento con funzioni di Amministratore di Sistema, ai sensi dell'art. 28 GDPR e del Provvedimento del 23 novembre 2008 in materia di Amministratori di Sistema pronunciato dall'Autorità Garante per la protezione dei dati personali. In osservanza della normativa di cui sopra, l'Azienda (Responsabile del trattamento) viene istruita dal Cliente (Titolare del trattamento) al momento dell'affidamento dell'incarico, mediante la conclusione di un apposito addendum contrattuale o altro atto idoneo ai sensi dell'art. 28 GDPR, definito sulla base delle intese intercorse tra l'Azienda e il Cliente stesso
I dati personali e le categorie particolari di dati personali dei clienti (d'ora in avanti anche solo 'dati') sono conservati su database PostgreSql deployato su Heroku che, essendo host provider del servizio di database e dell'applicazione, risulta essere sub responsabile del trattamento. Per questa ragione, in fase di conclusione dell'addendum di cui al punto sopra, il cliente accetta e individua quale sub-responsabile Salesforce, di cui Heroku è un prodotto, e Amazon AWS come sub-responsabili del trattamento dei dati personali. Per quanto riguarda le garanzie a dei dati personali trattati da parte di Saleforce/Heroku e Amazon AWS (per la conservazione dei documenti allegati) consultare i seguenti link (e collegati):

https://www.heroku.com/policy/security
https://devcenter.heroku.com/articles/logging
https://devcenter.heroku.com/articles/heroku-postgres-settings
https://devcenter.heroku.com/articles/audit-trail
https://devcenter.heroku.com/articles/regions#data-residency
https://www.salesforce.com/company/privacy/
https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf
https://aws.amazon.com/it/compliance/data-privacy-faq/

I dati trattati mediante la piattaforma di ePersonam sono di 2 tipologie:

- dati imputati all'interno del DB PostgreSQL
- dati presenti all'interno degli allegati in AWS S3

il DB ePersonam è un Premium 4, dotato di meccanismi di cifratura avanzati, in High Availability e residente in Region EU (più precisamente: le farm di Heroku in Germania/Irlanda)
La comunicazione client/server avviene via protocollo RSA 2048 bits (SHA256withRSA)

Politiche di trattamento dei dati personali da parte dell'Azienda

I dati dei clienti trattati dall'Azienda e dal suo personale (dipendenti/collaboratori), seguono la seguente policy:

- tutti i dipendenti/collaboratori sono autorizzati specificamente dall'Azienda, obbligati alla riservatezza e formati sui principi da osservare in materia di protezione dei dati personali
- è fatto divieto di tenere copia dei dati personali trattati nel contesto dell'attività svolta per conto del Cliente su pc o altri supporti informatici, personali e/o aziendali

- periodicamente (almeno 1 volta l'anno in modo non programmato) viene effettuato un controllo di sicurezza sui pc dei dipendenti/collaboratori, per verificare che il criterio sopra riportato venga rispettato
- qualunque dato sensibile e/o riferimento a persone/dati reali non possono essere portati al di fuori di Advenias in qualunque formato (supporto informatico, cartaceo, ecc.)
- è fatto divieto di divulgare all'esterno di Advenias qualunque dato personali di cui si sia venuti a conoscenza nello svolgimento delle proprie mansioni
- è fatto divieto di utilizzare i dati per qualunque finalità differente da quella prevista nei trattamenti autorizzati riportati di seguito
- ogni accesso ai dati effettuato tramite applicazione o direttamente al DB viene effettuato con credenziali personali non cedibili a terzi dal solo personale autorizzato
- i pc utilizzati (personali o aziendali) dai collaboratori Advenias possiedono sistemi di cifratura volti ad abbattere il rischio di violazione dei dati personali
- le password devono essere modificate almeno ogni 3 mesi oppure, in alternativa, deve essere attivata l'autenticazione a due fattori 2FA su tutti i servizi che ospitano sistemi di accesso al dato personale, ossia:

    - AWS (MFA)
    - Heroku (sotto le impostazioni di account)
    - Bitbucket (sotto le impostazioni di account)
    - GMail aziendale

- i dati in ePersonam non sono mai modificati se non dietro specifica richiesta scritta del Cliente e comunque, in tal caso, solo da personale autorizzato a svolgere adeguatamente tale attività

Responsabilità del Cliente

Il Cliente è responsabile, in qualità di Titolare del trattamento, di tutti i dati inseriti in ePersonam e della adeguata qualità degli stessi al momento del conferimento.
E' responsabilità del Cliente il corretto controllo e la gestione dei profili autorizzativi da Lui assegnati all'interno di ePersonam: quando viene creata una nuova struttura in ePersonam, vengono creati anche dei profili autorizzativi standard che il cliente è tenuto a verificare e, se lo ritiene opportuno, modificare in totale autonomia. Nel caso in cui il cliente abbia dubbi sul significato dell'autorizzazione da modificare può chiedere ad Advenias di farlo per suo conto ma solo ed esclusivamente per iscritto. Advenias non modifica profili autorizzativi se non per specifiche ragioni di urgenza e sempre solo su richiesta scritta del cliente. Parimenti, Advenias accetta le richieste di modifica solo da personale autorizzato dal cliente alla modifica dei profili stessi.
Il Cliente è inoltre responsabile dell'identificazione univoca degli utenti e degli operatori in ePersonam tramite cognome, nome e codici fiscali reali e corretti.
Il Cliente è responsabile del corretto utilizzo delle funzionalità di ePersonam e della formazione dei propri operatori al fine del corretto utilizzo del programma.
Quando un operatore cessa di lavorare per il Cliente, quest'ultimo è tenuto a disabilitare immediatamente l'account dell'operatore, cessando il rapporto con l'apposita funzionalità di ePersonam
Non va indicato cognome e nome dell'utente o qualunque altra informazione testuale ad esso riferibile in qualunque campo di testo del software che non siano cognome e nome in anagrafica.

Ad esempio: non deve ritenersi consentito inserire in anamnesi medica del sig. Rossi un testo del tipo “Il sig. Rossi è affetto da….”. In questo modo l’unico riferimento identificativo all'utente è l’id anagrafico che potrà poi, come da accordi tra Azienda e Cliente, essere anonimizzato.
Poichè Advenias compie i suddetti trattamenti per conto dei clienti (titolari del trattamento), riveste il ruolo di responsabile del trattamento EX ART. 28 REG. UE nr 679/2016
Il cliente, in qualità di Titolare del trattamento, deve assicurarsi di svolgere le attività di trattamento di dati personali in conformità ai principi di cui all’art. 5 GDPR ed alle basi giuridiche previste dagli art. 6 e 9 GDPR. Al riguardo deve assicurarsi di raccogliere anche i consensi eventualmente richiesti quali basi giuridiche dei trattamenti svolti mediante il software, in modo adeguato rispetto alla normativa e conservarli coerentemente con le finalità con cui sono stati resi. A titolo di supporto per la realizzazione di tale attività – e previe intese specifiche tra l’Azienda ed il Cliente - Advenias può fornire dei template da completare a cura del titolare:

- MODELLO 1) l’informativa utenti qualora i dati siano resi dall'utente stesso; i relativi consensi (trattamento dati e marketing) possono essere liberamente resi dall’interessato;
- MODELLO 2) l’informativa utenti qualora i dati dell'utente siano stati resi da un suo parente; i relativi consensi (trattamento dati e marketing) possono essere liberamente resi dall’interessato
- MODELLO 3) l’informativa parenti qualora i dati dei parenti siano stati resi dall'utente; l’informativa gli andrà fornita al primo momento utile da parte delil Titolare dei dati; in quell’occasione potrà prestare i consensi contestuali all'informativa
- MODELLO 4) l’informativa parenti qualora i dati dei parenti siano stati resi direttamente dal parente stesso; in questo caso entrambi i consensi potranno essere acquisiti direttamente al momento della resa dell’informativa
- MODELLO 5) l’informativa utenti che il parente/tutore potrà firmare in ottemperanza all’Autorizzazione 2/2016 sempre il parente/tutore potrà validamente prestare il primo consenso (trattamento dati) a nome dell'utente ma non potrà essere possibile che egli presti il secondo consenso (marketing) a nome dell'utente

solo successivamente alla raccolta di tali consensi essi potranno essere registrati a programma. In caso contrario, si ricorda che il Titolare si espone a sanzioni penali, civili e amministrative/pecuniarie secondo quanto previsto dalla normativa di settore
Pertanto, in via di sintesi, si ricorda che il Cliente dovrà:

1. fornire tutte le opportune informazioni di cui agli artt. 13 e 14 REG. UE nr. 679/2016
2. raccogliere il/i consenso/i o assicurarsi della regolare presenza di idonea base giuridica per garantire la liceità del trattamento
3. registrare il/i consenso/i acquisito/i a sistema (in ePersonam)
4. garantire il rispetto dei principi di cui all’art. 5 del GDPR

Anche e soprattutto con riferimento a quest’ultimo punto, il Titolare è tenuto a definire il criterio e la durata di conservazione dei dati, impostando i parametri previsti da ePersonam sulla conservazione dei dati in chiaro e anonimizzati

Restituzione dei dati personali trattati mediante ePersonam

La restituzione dei dati personali trattati tramite ePersonam è regolata dal paragrafo 5.3 del contratto tra Advenias e il Titolare.

Trattamenti autorizzati

Gli unici trattamenti al momento oggetto di autorizzazione da parte di Advenias nei confronti dei propri collaboratori sono:

- Gestione credenziali di autorizzazione e autenticazione per l'accesso ai sistemi
- Manutenzione dei siti, dei domini, dei software e strumenti
- Gestione/manutenzione dei database conferiti all'Azienda in outsourcing (*)
- Gestione di flussi di dati
- Gestione strumenti e apparati di sicurezza
- Gestione sistemi software legati ai prodotti della Società
- Salvataggio periodico dei dati (backup/recovery)
- Cancellazione sicura dei dati registrati
- Gestioni aggiornamento dei sistemi/software (patch)
- Gestione e tracciamento dei log di accesso

(*) Gestione database: permessi su la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati
Le tipologie di azioni dirette sui dati trattati mediante ePersonam ed effettuabili dai collaboratori di Advenias autorizzate sono 4:

1. accesso e utilizzo delle funzionalità dell'applicazione ePersonam
2. l'accesso diretto al Database
3. inserimento/modifica/cancellazione del dato attraverso l'applicazione ePersonam
4. inserimento/modifica/cancellazione del dato attraverso l'accesso diretto al Database

all'interno di queste tipologie di azione, svolta sempre e solo su istruzione del Cliente, vengono identificate, 3 finalità:

1. T: finalità tecniche, ovvero di sviluppo del prodotto ePersonam e/o assistenza ai clienti
2. C: finalità commerciali (per demo, e verifica correttezza e qualità dei dati del cliente, numero operatori e numero posti letto)
3. A: finalità amministrative (per verifica dati cliente, numero operatori e numero posti letto)

Ogni accesso ai dati effettuato tramite applicazione o direttamente al DB viene effettuato con credenziali personali non cedibili a terzi.
Ogni accesso/modifica ai dati attraverso l'applicazione viene tracciato dal versioning dell'applicazione.
Ogni accesso/modifica ai dati direttamente su DB viene tracciato dal sistema di gestione degli access log di Heroku/PostgreSQL.

Collaboratori autorizzati al trattamento e profili di autorizzazione

Legenda:

1. T: finalità tecniche, ovvero di sviluppo del prodotto ePersonam
2. S: support/assistenza ai clienti
3. C: finalità commerciali (per demo, e verifica correttezza e qualità dei dati del cliente, numero operatori e numero posti letto)
4. A: finalità amministrative (per verifica dati cliente, numero operatori e numero posti letto)

Collaboratore	finalità del trattamento	1. consultazione tramite ePersonam	2. consultazione diretta sul DB	3. modifica da ePersonam	4. modifica diretta sul DB
U. Brighetti	TCA	✓	✓	✓	✓
P. Semprini	CA	✓			
F. Gasparroni	TS	✓			
S. Malaguti	A	✓			
E. Curumi	A	✓			
S. Granata	TS	✓	✓	✓	✓
A. Salicetti	TS	✓	✓	✓	✓
A. Saxena	T	✓	✓	✓	✓
F. Negretti	TS	✓	✓	✓	✓
R. Gamberini	TS	✓		✓	
M.R. Tufano	S	✓		✓	
S. Gabellini	TS	✓	✓	✓	✓
S. Simoni	C	✓			
R. Putignano	CS	✓			
A. Giampaolo	C	✓			
F. Ferro	C	✓			
U. Frazzetto	TS	✓	✓		
A. Sonis	TS	✓	✓	✓	✓
A. Straface	TS	✓	✓	✓	✓
A. Quintavalla	CS	✓			

M. Bertipaglia	CS	✓	✓	✓	
P. Biasi	C	✓			
C. Vitiello	S	✓		✓	
E. Bologna	S	✓		✓	
M. Tufano	S	✓		✓	

Nomina del DPO

In osservanza degli artt. 37 e ss. GDPR, Advenias ha nominato come proprio DPO l'Avv. Stefano Orlandi , nato a Forlì il 17/09/1968, residente a Bologna, in via Mazzini 82/5, 40138 con Studio Legale in Bologna, via Corsica 10 C.F. RLNSFN68P17D704A/PIVA 01865271207
Si è deciso di designare un DPO esterno sia per garantire l'imparzialità e la terzietà rispetto alla Direzione Aziendale, sia per garantire la massima professionalità e qualità del servizio offerto

Tipi di dati personali

Dati personali trattati:

- dati personali operatori
- dati personali ospiti/utenti/assistiti
- dati personali parenti/riferimenti

Operatori

Tipologie di dati trattati:

- Dati personali: tutti i dati anagrafici come cognome, nome, cf, data nascita, luogo di nascita, luogo di residenza/domicilio, nome coniuge, telefoni e-mail.

Ospiti / Utenti / Assistiti

Tipologie di dati trattati:

- personali: tutti i dati anagrafici come cognome, nome, cf, data nascita, luogo di nascita, luogo di residenza/domi nome coniuge, telefoni e-mail
- Categorie di dati personali quali:
    - religione, gruppo sanguigno
    - patologie, problemi, icf, esenzioni, invalidità, accompagnamento, handicap, pensione

- scale di valutazione multidimensionali
- anamnesi remota, recente, famigliare
- valutazione psicologica, sanitaria, comportamentale, sociale
- parametri vitali e misurazioni
- esami e visite, refertazioni
- terapie somministrate
- misure di contenzione
- ausili e incontinenza
- cadute ed altri eventi negativi
- documenti allegati di tipo sanitario e non

Parenti / riferimenti

Tipologie di dati trattati:

- Dati personali: tutti i dati anagrafici come cognome, nome, cf, data nascita, luogo di nascita, luogo di residenza/domicilio, nome coniuge, telefoni e mail

Conservazione dei dati e anonimizzazione

Estrazione periodica delle cartelle e Restituzione dei dati

In costanza di contratto, il Cliente può sempre autonomamente estrarre le singole cartelle degli utenti o degli operatori a Lui riferiti, attraverso l'accesso alla sezione report e analisi, imputando nella voce "utenti" il comando di stampa della cartella utente e selezionando tutti i valori: Advenias resta a disposizione del Cliente per supportarlo nel contesto di tali procedimenti unicamente con azioni di formazione sulla procedura da eseguire.
Con riferimento all'operazione di restituzione dei dati personali trattati da Advenias in qualità di Responsabile del trattamento, si rappresenta che in caso di scioglimento e/o cessazione dell'efficacia del Contratto per qualsiasi causa intervenuta, i dati in oggetto resteranno – per un periodo non superiore a 15 giorni dalla data di cessazione - nella disponibilità del Cliente per l'estrazione in formato CSV. Sarà onere del Cliente stesso compiere tale attività mediante le funzionalità messe a disposizione dal software: Advenias resta a disposizione del Cliente per supportarlo nel contesto di tali procedimenti unicamente con azioni di formazione sulla procedura da eseguire. Advenias potrà comunque, su richiesta del Cliente, effettuare tali attività concordandone previamente costi e modalità con quest'ultimo.
Resta inteso che Il Cliente non potrà richiedere l'export dei dati secondo altre modalità o in altro formato da quelli indicati nel predetto documento. se non concordandone previamente modalità ed eventuali costi con Advenias.
In ogni caso, dalla data di scioglimento e/o cessazione dell'efficacia del contratto Advenias non avrà più alcuna responsabilità in merito alla conservazione dei dati del Cliente.

Anonimizzazione dei dati

Al termine del periodo di conservazione di cui al punto precedente, i dati personali ed eventuali copie in possesso di Advenias, saranno sottoposti a meccanismi di anonimizzazione irreversibili, tali da garantire la successiva

irrintracciabilità della persona fisica cui si riferivano originariamente. Tali dati anonimi saranno utilizzati per finalità statistiche, di ricerca e di sviluppo tecnico del software.

I dati anonimizzati sono trattati fuori dall'ambito di applicazione materiale del GDPR per lo sviluppo del programma e contribuire alla ricerca scientifica e statistica.
Nessun dato personale trattato mediante il software sarà utilizzato per tali finalità.

Data retention

Rif. AGID	Tipo retention	Significato	Durata
SLI10	Retention period of backup data	Il periodo di tempo in cui vengono mantenuti i backup	6 mesi
SLI14	Data retention period	Il periodo di tempo in cui i dati del cliente vengono mantenuti dopo la notifica di cessazione del servizio.	15 gg per l'estrazione dati da parte del cliente prima dell'anonimizzazione. *Vedi anche condizioni contrattuali ai punti 5.3 e 5.4*
SLI15	Log retention period	Il periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.	24 mesi

Esercizio dei diritti e tempistiche di riscontro

Diritto di accesso

ePersonam, fornisce profili autorizzativi standard (MOSTRA ELENCO, VISUALIZZA, STAMPA) che il cliente è tenuto a verificare e, se lo ritiene opportuno, modificare in totale autonomia.
Nel caso in cui il cliente abbia dubbi sul significato dell'autorizzazione da modificare può chiedere ad Advenias di farlo per suo conto ma solo ed esclusivamente per iscritto. Advenias non modifica profili autorizzativi se non su richiesta scritta del cliente e accetta richieste di modifica solo da personale autorizzato dal cliente alla modifica dei profili stessi.
I log di accesso ad ePersonam possono essere richiesti per iscritto dal cliente e verranno forniti in forma intellegibile entro 5 gg lavorativi.
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.

Diritto di rettifica

Come per il diritto di accesso ePersonam, fornisce profili autorizzativi standard (CREAZIONE, MODIFICA) che il cliente è tenuto a verificare e, se lo ritiene opportuno, modificare in totale autonomia.
Nel caso in cui il cliente abbia dubbi sul significato dell'autorizzazione da modificare può chiedere ad Advenias di farlo per suo conto ma solo ed esclusivamente per iscritto. Advenias non modifica profili autorizzativi se non su

richiesta scritta del cliente e accetta richieste di modifica solo da personale autorizzato dal cliente alla modifica dei profili stessi.
I log di rettifica ad ePersonam possono essere richiesti per iscritto dal cliente e verranno forniti in forma intelleggibile entro 5 gg lavorativi.
Il cliente, nel caso non possa farlo autonomamente, può richiedere per iscritto ad Advenias la rettifica dei dati.
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.

Diritto di cancellazione (diritto all'oblio)

Come per il diritto di accesso ePersonam, fornisce profili autorizzativi standard di CANCELLAZIONE che il cliente è tenuto a verificare e, se lo ritiene opportuno, modificare in totale autonomia.
Nel caso in cui il cliente abbia dubbi sul significato dell'autorizzazione da modificare può chiedere ad Advenias di farlo per suo conto ma solo ed esclusivamente per iscritto. Advenias non modifica profili autorizzativi se non su richiesta scritta del cliente e accetta richieste di modifica solo da personale autorizzato dal cliente alla modifica dei profili stessi.
I log di cancellazione ad ePersonam possono essere richiesti per iscritto dal cliente e verranno forniti in forma intellegibile entro 5 gg lavorativi.
I dati vengono gestiti dall'applicazione con "soft deletion", ovvero posti in uno "stato cancellato": i dati in stato cancellato vengono fisicamente eliminati automaticamente dopo 1 anno.
Il cliente, nel caso non possa farlo autonomamente, può richiedere per iscritto ad Advenias la cancellazione definitiva dei dati. I dati oggetto di oblio vengono anonimizzati.

Diritto alla limitazione al trattamento

Il cliente, nel caso non possa farlo autonomamente, può richiedere per iscritto ad Advenias la limitazione del trattamento per i dati, specificando:

- a quali dati applicare la limitazione
- che tipo di limitazione applicare
- eventualmente il tempo di validità della limitazione

Advenias risponderà alla richiesta entro 5 gg lavorativi, esplicitando l'eventuale tempo di espletamento dell'operazione.
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.

Diritto alla portabilità dei dati

Il cliente, nel caso non possa farlo autonomamente, può richiedere per iscritto ad Advenias l'estrazione dei dati in forma intellegibile, specificando:

- quali dati estrarre
- per quale lasso temporale
- l'eventuale formato richiesto (diverso da quelli previsti da Advenias: pdf, csv)

Advenias risponderà alla richiesta entro 5 gg lavorativi, esplicitando se fattibile e l'eventuale tempo di espletamento dell'operazione.
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.

Diritto di opposizione

Il cliente, nel caso non possa farlo autonomamente, può richiedere per iscritto ad Advenias di bloccare il trattamento dei dati di un assistito / parente / operatore.
Advenias risponderà alla richiesta entro 5 gg lavorativi, esplicitando se fattibile e l'eventuale tempo di espletamento dell'operazione.
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.

Utilizzo dei dati GPS

Per lo svolgimento di alcune attività di assistenza, è possibile che il Cliente richieda l'utilizzo di una specifica feature di ePersonam che si avvale dell'utilizzo di un sistema GPS. In questo caso dati GPS possono essere memorizzati solo dall'APP di ePersonam (in genere utilizzata per la registrazione delle attività domiciliari o su commesse specifiche).
All'apertura dell'APP viene chiesto all'operatore se acconsente all'accesso alla posizione attuale tramite GPS.
Se l'operatore risponde no, la registrazione dati di localizzazione non avviene
Se risponde si l'APP memorizza la posizione in 2 circostanze (e non continuativamente):

- al momento in cui l'operatore preme START (localizzazione GPS di inizio dell'attività)
- al momento in cui l'operatore preme STOP (localizzazione GPS di fine dell'attività)
- se la modalità di utilizzo non è START/STOP ma solo FATTO viene memorizzata 1 volta la localizzazione e salvata sia in GPS_START che in GPS_STOP

Advenias non utilizza i dati di localizzazione se non su specifica richiesta scritta del cliente (Titolare)
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.
Resta inteso che le attività di conformità normativa in materia di protezione dei dati personali e gli eventuali oneri informativi nei confronti di pazienti e operatori restano a carico del Cliente, che in qualità di Titolare del trattamento deve fornire le adeguate garanzie richieste per l'utilizzo di tali sistemi sia dal GPDR e dalla normativa gius-lavoristica (segnatamente art. 4 l. 300/1970) sia dai Provvedimenti di rilievo emanati dall'Autorità Garante per la protezione dei dati personali.

Sicurezza del trattamento

Privacy by design

Nel rispetto del principio di privacy by design, ogni sviluppo dell'applicazione parte dalla valutazione che la nuova funzionalità abbia o meno impatto sulla privacy dell'interessato. Nel caso in cui sia valutato dal team di sviluppo un impatto sia di processo che di funzione sulla privacy ne viene data evidenza in un documento di analisi della funzionalità.
Da qui ne consegue:

- valutazione del rischio
- individuazione di soluzioni specifiche

Se il team di sviluppo ha dubbi in merito deve consultare il DPO e la Direzione, fornendo tutte le specifiche possibili di progetto ai fini di una corretta valutazione del rischio.
ePersonam prevede, in caso di abbandono della postazione, un logout automatico dopo 20 minuti, parametrizzabile dal Titolare che è responsabile della variazione del parametro e della conseguente possibile diminuzione della sicurezza (parametro > => sicurezza <).
Ogni volta che la postazione viene abbandonata è necessario premere ESCI/LOGOUT in modo da tracciare la chiusura della sessione. In caso contrario la sessione viene disconnessa al termine del timeout di sessione.
Il Titolare deve adeguatamente formare gli operatori su questi aspetti.

Privacy by default

Nel rispetto del principio di Privacy by default, le nuove funzionalità introdotte che vengono reputate rilevanti per il trattamento del dato ai fini della privacy possono essere:

- disabilitate by default per tutti (indipendentemente dal profilo utente): dati immodificabili via programma ma solo direttamente sul database (es. data/ora creazione, operatore creatore, data/ora ultima modifica, operatore ultima modifica)
- disabilitate by default sui profili, ma lasciando al cliente la possibilità di abilitarle tramite profilazione.

E' chiaro che se nella modifica di un certo dato entra in gioco il concetto di profilo, essendo la profilazione a carico del Titolare, almeno 1 operatore potrà essere in grado di autorizzare 1 o più profili e di conseguenza tutte le funzionalità per tutti i profili.

Data breach

Eventuali data breach verranno comunicati al cliente tramite Changlog dell'applicazione ePersonam, entro 48 ore dalla rilevazione dell'evento, riportando:

- data di rilevazione dell'evento
- tipologia ed entità del data breach
- soluzione immediata adottata
- soluzione correttiva per evitare il ripetersi nel futuro
- comunicazione al Garante

Password

Le password sono da ritenersi come personale riferite ai singoli operatori. Ciascuna di essere deve essere modificata ogni 3 mesi: ePersonam avvisa ogni utente della scadenza prossima della password. Scaduta la password l'operatore è in grado di inserire nuova password con un meccanismo di recupero su mail personale.
La mail personale per il recupero password è modificabile solo dall'operatore stesso, così come la password.
E' onere del Titolare verificare il corretto utilizzo del programma da parte degli operatori.
Di default la password deve contenere almeno 8 caratteri.
Non è possibile reinserire la password precedente e non può contenere nome, cognome, cf,
non può essere composta da tutto o una parte dello username, non può contenere parte della data di nascita.

La password è criptata e nemmeno il personale di Advenias può visualizzarle.
Al primo accesso l'operatore deve cambiare la password.
E' già possibile implementare, su richiesta del cliente (opzione a pagamento), un sistema di sms OTP (One Time Password), che consenta la 2FA (2 Factor Authentication) alla piattaforma ePersonam.
In questo modo per accedere l'operatore deve:

1. inserire username e password
2. inserire in OTP il codice di accesso che riceve via sms sul proprio cellulare

Antivirus/anti malware

Viene sempre monitorato lo stato di salute generale del software (unicamente sotto il profilo tecnico) tramite New Relic e Status Cake (Add-On che dialogando con Heroku)

Aggiornamento del software

Gli aggiornamenti vengono regolarmente effettuati più volte al giorno, il più delle volte senza che gli operatori ne abbiano evidenza o che sia necessario interromprne il lavoro.

Utilizzo credenziali di gestione tecnica

Come si è detto ogni operatore tecnico autorizzato da Advenias accede con proprie credenziali personali sia al programma ePersonam che al database (ove previsto, vedi trattamenti autorizzati). In questo modo possono essere tracciati gli accessi e le modifiche in modo univoco e nominale.
L'accesso alle piattaforme AWS ed Heroku avviene attraverso 2FA

Formazione

Al personale di Advenias è stata effettuata adeguata formazione in merito al trattamento dei dati personali e sono stati forniti i documenti necessari (vedi file Formazione)

Valutazione del livello di sicurezza

Nel valutare l'adeguatezza del livello di sicurezza si è tenuto conto dei rischi legati alla distruzione, perdita, modifica, divulgazione non autorizzata o accesso in modo accidentale o illegale ai dati personali coinvolti dal trattamento.

Ulteriori misure di sicurezza

Crittografia/Cifratura del DB
Non ripetibilità della password (criptazione)
Connessione sicura RSA 2048 bits (SHA256withRSA)
E' già possibile implementare, su richiesta del cliente (opzione a pagamento), un sistema di sms OTP (One Time Password), che consenta la 2FA (2 Factor Authentication) alla piattaforma ePersonam.

In questo modo per accedere l'operatore deve:

1. inserire username e password
2. inserire in OTP il codice di accesso che riceve via sms sul proprio cellulare

Gestione dei profili

Come si è detto gran parte delle funzionalità di ePersonam sono soggette a profili utenti di cui viene data un'impostazione standard per ogni profilo e che il cliente deve verificare e volendo modificare autonomamente. Il cliente però non può aggiungere o eliminare profili.
Advenias non modifica l'impostazione dei profili cliente se non su specifica richiesta scritta da parte del cliente stesso.
Advenias si riserva il diritto di chiedere un corrispettivo per l'attività svolta.

Cloud

Servizi e fornitori

Advenias valuta e seleziona i servizi e i fornitori della piattaforma in base ai seguenti requisiti (non in ordine di importanza):

- innovazione tecnologica delle soluzioni (tendenzialmente presenti nel magic quadrant Gartner)
- livello di qualità del servizio offerto
- livello di affidabilità del servizio
- livello di scalabilità del servizio
- livello di sicurezza del servizio
- livello di parametrizzazione del servizio
- rapporto costi/benefici del servizio

Vedi elenco servizi e fornitori

Aggiornamenti

I provider cloud effettuano aggiornamenti di sicurezza della propria piattaforma ed informano puntualmente i clienti degli aggiornamenti effettuati sui propri siti.
Analogamente Advenias effettua aggiornamenti della propria piattaforma e ne dà comunicazione ai propri clienti attraverso lo strumento di Changelog di ePersonam

Utilizzo dei dati

Per vedere le SLA dei fornitori Cloud della piattaforma ePersonam è possibile visitare i seguenti link e collegati:
https://www.heroku.com/policy/security

https://www.salesforce.com/company/privacy/
https://aws.amazon.com/it/compliance/data-privacy-faq/

Misure di sicurezza adottate dai fornitori

Sono state adottate misure tecniche ed organizzative volte a ridurre al minimo rischi quali distruzione, perdita anche accidentale dei dati, accesso non autorizzato, di trattamento non consentito, di trattamento non conforme alla finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati.
In particolare Heroku fornisce un servizio sui sistemi premium di High Availability che consente in caso di rottura/malfunzionamento del DB, di passare automaticamente ad una copia calda funzionante, senza che l'utente finale ne abbia consapevolezza.
Inoltre è presente un follower (altra copia "calda") per il balancing delle performance (report, API).
Nel caso di cancellazione totale dei dati nel DB, è possibile ripristinare la situazione precedente alla cancellazione ad una precisa data/ora (con una retention di 7 giorni).
Anche i documenti allegati, salvati su AWS S3 sono cifrati e conservati in EU Region.

Trasferimenti all'estero di dati personali

Non sono previsti trasferimenti al di fuori della Region EU nel contesto dei trattamenti realizzati mediante ePersonam per conto del Cliente.

ADVENIAS
YOUR IDEA OF SOFTWARE

Ulteriori Caratteristiche software GDPR compliant

ing. U. Brighetti (CEO Advenias)
01/03/2019 v1.1

Caratteristica	**versione GDPR compliant**
Filesystem cifrato/criptato	✓
Database cifrato/criptato	✓
Gestione informative pazienti/parenti	✓
Gestione consensi	✓
Gestione log visualizzazione dati	✓
Gestione log modifica dati	✓
Gestione log cancellazione dati	✓
Diritto di accesso	✓
Diritto oblio	✓
Diritto di limitazione	✓
Diritto portabilità	✓
Limitazione della conservazione	✓
Automatismi presenti e futuri di visualizzazione log	✓
Connessione protetta SSL (per sw web/cloud)	✓
High Availability (per sw web/cloud)	✓
Disaster Recovery (per sw web/cloud)	✓
Anonimizzazione utenti/assistiti	✓
Anonimizzazione parenti riferimenti	✓
Anonimizzazione operatori	✓
Sicurezza Cloudflare (per sw web/cloud)	✓