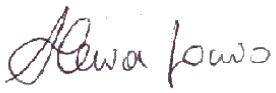
Firmato digitalmente da:SOCCIO ALESSIA
Data:05/03/2021 09:48:52

ENTAKSISOLUTIONS
AZIENDA CON SISTEMA INTEGRATO DI GESTIONE QUALITA', SICUREZZA DELLE INFORMAZIONI, SERVIZI
ISO 9001 | ISO 20000-1 | ISO 22301
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
CONSERVATORE ACCREDITATO AGID

Alessia Soccio
Responsabile SIG



ENTAKSISOLUTIONS

AZIENDA CON SISTEMA INTEGRATO DI GESTIONE
QUALITA', SICUREZZA DELLE INFORMAZIONI, SERVIZI
ISO 9001 | ISO 20000-1 | ISO 22301
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
CONSERVATORE ACCREDITATO AGID

Manuale

AR SIG 20210302 DPIA

Entaksi Solutions Srl

Indice

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Analisi Rischi
Nome documento	AR SIG 20210302 DPIA
Versione	1.0.0
Data creazione	02/03/2021
Ultima revisione	04/02/2021
Autore	Alessia Soccio
Stato	Rilasciato
Classificazione	Pubblico

Riproduzioni cartacee di questo documento sono da considerarsi copie di lavoro non censite dal SIG.

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
02/03/2021	0.0.1	Alessia Soccio	DPO	Creazione bozza.	Pubblico
04/02/2021	1.0.0	Stefano Travelli	RSiGSI	Revisione e rilascio.	Pubblico

Approvazione del documento

Data	Addetto	Mansione	Firma
04/02/2021	Alessia Soccio	Responsabile del SIG	*Firmato digitalmente*

1. Introduzione

1.1. Obiettivo del documento

Il presente documento costituisce la periodica Valutazione di Impatto sulla Protezione dei Dati (DPIA, Data Protection Impact Assessment) realizzata da Entaksi Solutions Srl nell'ambito dell'implementazione del Regolamento Generale sulla Protezione dei Dati (GDPR, General Data Protection Regulation), ovvero il Regolamento UE 2016/679 approvato dalla Commissione Europea e vigente a partire dal 25 maggio 2018 in tutti i paesi dell'Unione.

La valutazione si applica alle attività condotte da Entaksi all'interno del suo Sistema di Gestione della Sicurezza delle Informazioni.

I dati raccolti da Entaksi nell'ambito delle sue funzioni riguardano interessati legati all'azienda da un contratto (clienti, fornitori, dipendenti) o dati inviati o raccolti per finalità aziendali (es.: curriculum vitae).

Nonostante la valutazione di impatto non sia necessaria, in quanto i trattamenti effettuati non rientrano nei casi definiti dall'art. 35 paragrafo 3 del GDPR, in considerazione dell'importanza della protezione dei dati conservati nel sistema di conservazione Entaksi decide di condurre, parallelamente all'analisi dei rischi sul proprio Sistema Integrato di Gestione, una valutazione di impatto specifica per i dati personali.

Il DPIA è costituito da:

- un'analisi dei flussi di dati gestiti da Entaksi Solutions Srl: la panoramica del trattamento, un elenco dei dati trattati, i processi e le risorse utilizzate;
- la descrizione dei principi sui quali si basa il trattamento, e le misure a tutela dei diritti degli interessati;
- un'analisi dei rischi specifica sugli asset che contengono dati personali;
- una verifica dei controlli effettuati e delle contromisure implementate per mitigare questi rischi;
- una valutazione di impatto complessiva che misura il livello di adeguatezza dei sistemi e delle procedure adottati da Entaksi nei confronti del Regolamento.

Il Sistema Integrato di Gestione di Entaksi è conforme alle seguenti norme riferite ai relativi sottosistemi:

- **UNI ISO 9001:2015 – Sistema di Gestione della Qualità (SGQ)**
- **ISO/IEC 20000-1:2018 – Sistema di Gestione per l'Erogazione di Servizi Informatici (SGS)**
- **ISO/IEC 27001:2013 – Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27017:2015 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27018:2019 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 27035:2016 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)**
- **ISO/IEC 22301:2019 - Sistema di gestione della continuità operativa aziendale (BCMS)**
- **Sistema di conservazione documenti digitali accreditato AgID - Sistema di conservazione digitale a norma art. 24 Regolamento UE n° 910/2014 - EIDAS**

I controlli relativi alla sicurezza delle informazioni sono derivanti dall'applicazione di tali norme (e in particolare ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019 eISO/IEC 27035:2016), e sono impiegati nella valutazione del rischio, che Entaksi esegue con un proprio software "Piattaforma Gestione CMDB - Analisi Rischi Entaksi".

La metodologia sulla quase si basa il software e l'analisi che ne deriva è descritta nel capitolo Metodologia analisi rischi.

La DPIA viene condotta internamente con cadenza periodica e prende in considerazione specifiche minacce riguardanti la sicurezza dei dati personali individuate in base al Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati e alla certificazione ISO/IEC 27018:2019 per la privacy dei servizi in cloud, oltre a più generiche minacce relative la sicurezza delle informazioni.
In questo documento vengono riportate le analisi particolari condotte sulla protezione dei dati personali e i risultati del trattamento.

Il documento viene infine convalidato rispettando i principi definiti per la conduzione della DPIA dalla normativa e la metodologia di trattamento dei rischi e allegato alla periodica analisi dei rischi generale.

1.2. Campo di applicazione

La presente disposizione si applica al Sistema Integrato di Gestione (SIG) di Entaksi Solutions Srl.

1.3. Definizioni e documentazione di riferimento

Per le definizioni ed abbreviazioni si rimanda allo specifico documento "MAN SIG 20200502 Definizioni".

Per i riferimenti alla documentazione, interna o esterna, si rimanda allo specifico documento "MAN SIG 20200511 Documentazione di riferimento".

In particolare per i riferimenti al Regolamento dell'Unione Europea n° 2016/679 sulla protezione dei dati si rimanda al testo pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016.

2. Contesto del trattamento

In questo capitolo viene illustrato il contesto di trattamento dei dati personali operato da Entaksi Solutions Srl.

La società Entaksi Solutions Srl è stata costituita nel marzo del 2007, ed ha iniziato la sua attività rilevando da Gruppo Formula spa (società di provenienza dei tre soci fondatori di Entaksi) il ramo di azienda relativo al prodotto maintenACT, che ha rappresentato l'iniziale core-business della startup.

La mission della società è la progettazione, realizzazione, commercializzazione e supporto di applicazioni con architettura Web, con una attenzione particolare all'utilizzo di ambienti e strumenti Open Source, e l'erogazione in modalità SaaS di sistemi di gestione documentale e conservazione digitale dei documenti a valenza fiscale.

Il Data Protection Impact Assessment condotto da Entaksi si applica a tutto il Sistema Integrato di Gestione (SIG) di Entaksi. Esso riguarda tutti i *data asset* (asset informativi) che contengono, anche potenzialmente, dati personali.

Il Regolamento definisce il "dato personale" come qualsiasi informazione concernente una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. (art. 4 Regolamento).

In ragione di alcuni *data asset* (analizzati nel paragrafo seguente) considerati critici e potenzialmente contenenti dati personali, in particolare in riferimento ai dati contenuti nel Sistema di Conservazione di Entaksi accreditato presso l'Agenzia per l'Italia Digitale e quindi operante anche per la Pubblica Amministrazione, l'azienda ha considerato necessario dotarsi del presente DPIA, e di tutte le misure previste dal Regolamento per la protezione dei dati personali.

2.1. Ruoli e responsabilità

I ruoli e le responsabilità sono definiti e assegnati nel capitolo Matrice delle responsabilità.

2.2. Codici di condotta e certificazioni

Al momento non sono presenti codici di condotta di categoria approvati.

Il Sistema Integrato di Gestione (SIG) di Entaksi Solutions Srl è conforme agli standard dichiarati nel capitolo Introduzione.

3. Conformità del trattamento

Il capitolo illustra le finalità dei trattamenti operati da Entaksi, la loro base giuridica, la proporzionalità e la necessità, i diritti delle persone interessate e gli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

3.1. Ciclo di vita dei dati

I dati personali raccolti da Entaksi sono trattati in base all'esecuzione di contratti e agli obblighi legali derivanti da tale esecuzione.

In generale il ciclo di trattamento è organizzato come segue:

1. **Acquisizione dei dati alla stipula del contratto**: i dati personali necessari per l'esecuzione del contratto vengono acquisiti da Entaksi, e gestiti secondo i requisiti del trattamento. Alla stipula del contratto viene fornita all'interessato un'informativa contenente i termini del trattamento dei dati.
2. **Gestione dei dati**: i dati sono gestiti all'interno del Sistema Integrato di Gestione (SIG), secondo le norme di sicurezza delle informazioni definite dalla ISO/IEC 27001:2013.
3. **Accesso, portabilità, rettifica, opposizione**: in qualsiasi momento del trattamento l'interessato può esercitare i propri diritti in materia di protezione dei dati personali, secondo i canali prestabiliti.
   Tali diritti sono descritti in Esercizio di diritti in materia di protezione dei dati personali.
4. **Distruzione dei dati al termine del contratto**: al termine legale definito dal contratto di servizio i dati, fatto salvo intervenuti obblighi di legge quali contenziosi o ispezioni, vengono cancellati.

3.2. Finalità del trattamento

Il trattamento è considerato necessario e proporzionale in relazione alle finalità e alle misure di sicurezza adottate.

Entaksi utilizza i **dati personali dei propri clienti** (identificativi, amministrativi, contabili e fiscali, commerciali, informatici e, nell'evenienza, giudiziari direttamente riferiti al cliente o, per i dati essenzialmente identificativi ed informatici, agli altri interessati quali collaboratori, dipendenti, referenti, etc.) comunicati in esecuzione e nello svolgimento dei rapporti con il Titolare e in osservanza e nel rispetto delle disposizioni in materia di trattamento e protezione dei dati personali, per il perseguimento di finalità strumentali e/o complementari alle attività statutariamente espresse e funzionali allo svolgimento del rapporto contrattuale/precontrattuale in essere con il cliente interessato e ciò relativamente ai servizi/prestazioni dallo stesso richieste.

Qualora acconsentito, i dati verranno altresì trattati per l'invio di messaggi informativi e comunicazioni commerciali e promozionali relativi all'attività e ai servizi propri del Titolare, attraverso mezzi automatici, come e-mail ed SMS, nonché mezzi tradizionali, come il contatto telefonico con operatore, nel completo rispetto dei principi di liceità e correttezza e delle disposizioni di legge.

In misura simile Entaksi utilizza i **dati personali dei propri dipendenti** (identificativi, contabili, reddituali, sensibili qualora riferiti nel caso allo stato di salute; all'adesione ad un sindacato e/o ad un partito idonei, altresì, a rivelare convinzioni politiche e religiose ovvero concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali e giudiziari eventuali riferiti all'interessato o presso questo raccolti e riferiti nel caso ai familiari e ai conviventi e giudiziari) per le attività derivanti dagli obblighi contrattuali, quali:

- la corretta quantificazione della retribuzione, nonché per la corresponsione di assegni (anche familiari), premi, altri emolumenti, liberalità e benefici accessori;
- assolvere gli obblighi di legge e di contratto, inclusi quelli derivanti dal contratto collettivo;
- adempiere ed esigere l'adempimento di specifici obblighi o eseguire specifici compiti derivanti da leggi, regolamenti o contratti collettivi anche aziendali, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché del riconoscimento di agevolazioni e dell'applicazione della normativa in materia sindacale e di tutela della salute;
- assolvere gli obblighi nei confronti degli istituti di previdenza ed assistenza, sia obbligatorie che integrative;
- adempiere agli obblighi fiscali nei confronti dell'amministrazione finanziaria, ivi compresa l'eventuale assistenza fiscale;
- adempiere agli obblighi derivanti dalle norme in materia di igiene e di sicurezza sul lavoro;
- compiere tutte le attività a queste strumentali e accessorie e comunque necessarie al perseguimento delle finalità dette (la registrazione, l'archiviazione dei dati, la consultazione etc.).

Le finalità sono pertanto determinate, esplicite e legittime, e contenute nell'informativa privacy allegata al contratto di servizio o al contratto di lavoro e nella disciplinare privacy.

L'impiego dei dati è pertinente a quanto descritto nel contratto di servizio, e la loro conservazione limitata all'arco di tempo definito dallo stesso.
Vengono raccolti da Entaksi solo i dati necessari alla conduzione dei contratti in essere, e conservati per il tempo definito dai contratti.

Il consenso è informato, ed è dato in modo effettivo ed inequivocabile nella suddetta informativa.

Gli ordini di grandezza relativi ai dati personali conservati sono proporzionali al numero di clienti e le procedure di gestione sono progettate per evolvere di pari passo con le procedure di protezione dei dati.

3.3. Esercizio di diritti in materia di protezione dei dati personali

Per quanto riguarda l'esercizio di diritti in materia di protezione dei dati personali Entaksi mette a disposizione dei clienti la casella privacy@entaksi.eu, alla quale l'utente può fare riferimento per le diverse categorie di esercizio. Anche questa categoria di richiesta viene gestita tramite il servizio Redmine: le email inviate all'indirizzo privacy@entaksi.eu aprono automaticamente un ticket nel sistema, che viene gestito dagli operatori in base a delle categorie scelte.

Anche la casella dpo@entaksi.eu è disponibile per l'esercizio di tali richiesta, ma in questo caso è responsabilità diretta del Data Protection Officer (DPO) inserire il ticket nel sistema.

La descrizione dei vari step operativi che compongono il workflow è la seguente:

1. Il richiedente (cliente) invia una mail contenente la richiesta di esercizio dei dei diritti in merito alla protezione dei dati personali a privacy@entaksi.eu, oppure utilizza un altro canale (email, cartaceo o telefonico), e il ticket viene inserito dal tecnico che riceve la segnalazione.
2. La richiesta viene verificata dal Responsabile del Servizio.
3. Se la Richieste di Servizio (RdS) si dimostra attendibile, viene qualificata: accesso ai dati personali, richiesta di intervento sui dati, portabilità dei dati, opposizione al trattamento, o richiesta generica. Il ticket passa in stato "in elaborazione".
4. La RdS viene evasa entro un mese, in accordo a quanto previsto dalla legislazione. Nel caso non sia possibile evadere la richiesta è comunque necessario, ai sensi dell'art.12, par. 4 del GDPR fornire al richiedente i motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste, e in particolare di eventuali condizioni che impediscono al titolare di identificarlo come interessato, (art.11, par.2).
5. Al termine della corretta evasione delle RdS, il ticket viene chiuso a cura del Responsabile del Servizio.

Le varie categorie di richieste per l'esercizio dei diritti in materia di protezione dei dati personali sono descritte nei paragrafi successivi.

3.3.1. Accesso ai dati personali

Descritta nell'art. 15 del GDPR, avviene secondo il seguente schema:

1. Il cliente richiede conferma che sia in meno in corso un trattamento dei dati personali che lo riguardano.
2. Entaksi apre un ticket specifico, per rispondere al quesito, consultando il proprio database.
3. In caso di esito positivo il cliente può richiedere l'accesso ai propri dati personali, una copia degli stessi, e informazioni in merito a:
   - finalità del trattamento;
   - categorie di dati trattati;
   - destinatari o categorie di destinatari a cui i dati sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
   - periodo di conservazione previsto;
   - origine dei dati;
   - esistenza o meno di un processo decisionale automatizzato, compresa profilazione, e logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
4. Entaksi fornisce tali informazioni, entro un mese dalla data di ricevimento della richiesta, consultando il proprio registro del trattamento.

Nel caso non sia possibile evadere la richiesta è comunque necessario, ai sensi dell'art.12, par. 4 del GDPR, fornire al richiedente i motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste, e in particolare di eventuali condizioni che impediscono al titolare di identificarlo come interessato, (art.11, par.2).

3.3.2. Portabilità dei dati personali

Descritta nell'art. 20 del GDPR, avviene secondo il seguente schema:

1. Il cliente richiede di ricevere i propri dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico, o di trasmetterli direttamente a diverso titolare.
2. Entaksi apre un ticket specifico, e se non sono già state specificate nella richiesta richiede a quale nuovo titolare debba trasferire i dati, e se tutti i dati o un sottoinsieme di dati, e nello specifico quali categorie.
3. Entaksi risponde alla richiesta entro un mese dalla data di ricevimento della stessa, inviando i dati in suo possesso in formato CSV.
   Nel caso non sia possibile evadere la richiesta è comunque necessario, ai sensi dell'art.12, par. 4 del GDPR fornire al richiedente i motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste, e in particolare di eventuali condizioni che impediscono al titolare di identificarlo come interessato, (art.11, par.2).

3.3.3. Richiesta di intervento sui dati personali

Descritta negli artt. 16-18 del GDPR, avviene secondo il seguente schema:

1. Il cliente richiede la rettifica o l'aggiornamento dei propri dati personali (art. 16), o la cancellazione (art. 17), link, copie o riproduzione dei suoi dati, o la limitazione del trattamento (art.18).
2. Entaksi apre un ticket specifico, e se non sono già state specificate nella richiesta richiede a quali specifici dati personali, o categorie, il cliente fa riferimento.
3. Se non precedentemente indicato richiede, per quanto riguarda la limitazione del trattamento, per quali motivi viene effettuata la richiesta.
4. Entaksi risponde alla richiesta entro un mese dalla data di ricevimento della stessa, aggiornando il proprio registro del trattamento e dandone comunicazione al cliente.

Nel caso non sia possibile evadere la richiesta è comunque necessario, ai sensi dell'art.12, par. 4 del GDPR fornire al richiedente i motivi che impediscono al titolare di fornire le informazioni o svolgere mile operazioni richieste, e in particolare di eventuali condizioni che impediscono al titolare di identificarlo come interessato, (art.11, par.2).

3.3.4. Opposizione al trattamento dei dati personali

Descritta nell'art. 21 del GDPR, avviene secondo il seguente schema:

1. Il cliente tramite richiesta si oppone al trattamento dei propri dati personali, in generale o specificamente per attività di marketing.
2. Entaksi apre un ticket specifico, e se non sono già state specificate nella richiesta richiede a quali dati si riferisca il cliente, se a tutti i dati o un sottoinsieme di dati, e nello specifico quali categorie.
3. Entaksi risponde alla richiesta entro un mese dalla data di ricevimento della stessa, inviando i dati.

Nel caso non sia possibile evadere la richiesta è comunque necessario, ai sensi dell'art.12, par. 4 del GDPR, fornire al richiedente i motivi che impediscono al titolare di fornire le informazioni o svolgere mile operazioni richieste, e in particolare di eventuali condizioni che impediscono al titolare di identificarlo come interessato, (art.11, par.2).

3.4. Ricognizione dei trattamenti

Tutti i *data asset* sono conservati da Entaksi all'interno del perimetro sottoposto alle certificazioni definite nel capitolo Introduzione.

Tutti i datacenter utilizzati da Entaksi si trovano all'interno dell'Unione Europea, in particolare i datacenter utilizzati per i dati relativi alle Pubbliche Amministrazioni italiane si trovano in territorio italiano, come richiesto dalla normativa.

Le categorie di interessati per i trattamenti sono:

- Clienti.
- Fornitori.
- Dipendenti.
- Aspiranti collaboratori.
- Esterni.

Per ciascun trattamento vengono qui definite:

- la natura, la finalità e il contesto del trattamento (fonti presso cui i dati vengono raccolti, estensione del trattamento, se sono o meno coinvolte terze parti all'esterno o all'interno del territorio europeo, etc);
- categorie di dati oggetto del trattamento, e i soggetti interessati a cui si riferiscono;
- durata del trattamento;
- flussi informativi (possibile cessione o trasferimento dei dati, soggetti destinatari, se i dati vengono o meno comunicati a soggetti terzi);
- descrizione funzionale delle operazioni di trattamento;
- modalità di trattamento (quali tecnologie vengono impiegate);
- soggetti che hanno accesso ai dati (e per quale finalità).

Per quanto riguarda la **distruzione dei dati** presenti sui supporti di memorizzazione di massa viene utilizzato, a seconda dei casi, il software DBAN per la distruzione dei dati di un PC o latptop, o il software badblocks.

Le ubicazioni dei dati sugli asset Entaksi sono registrate nella Piattaforma Gestione CMDB - Analisi Rischi Entaksi e costituiscono un dato confidenziale.

Trattamento dei contratti con i clienti	
Dati interessati	Database erogazione servizi Database di autenticazione Database log Console servizi Sistema di gestione dei contratti ToS Server di posta elettronica
Tipo di dati	Credenziali degli utenti che accedono ai servizi Credenziali dei dipendenti che accedono al sistema informativo Log degli accessi sul sistema Single Sign On Documenti archiviati dai clienti del sistema di conservazione Documenti registrati nel sistema documentale Fatture elettroniche trasmesse, ricevute e conservate per conto dei clienti del servizio eCON FE Ordini di acquisto elettronici trasmessi, ricevuti e conservati per conto dei clienti del servizio eNSO (eDoc API) Anagrafica del TOS che contiene l'anagrafica dei clienti Messaggi di posta elettronica inviati e ricevuti.
Cessione a terze parti	No
Flussi informativi verso altri soggetti	No

Durata del trattamento	Definita dal contratto di servizio, con scarto obbligatorio nei termini previsti dalla legge.
Interessati	Clienti servizi / prodotti.
Accesso	Responsabili definiti nel funzionigramma, sviluppatori incaricati (previa sottoscrizione di accordo di riservatezza).
Finalità	Esecuzione dei contratti per servizi e prodotti Entaksi.
Modalità di raccolta	Imputazione dei dati da parte dell'utente.
Modalità di trattamento	Il trattamento è inserito nel Sistema Integrato di Gestione (SIG) Entaksi, certificato per la sicurezza delle informazioni (ISO/IEC 27001:2013).

Trattamento dei contratti con i fornitori	
Asset	Sistema di Gestione Amministrativo
Tipo di dati	Anagrafica fornitori
Cessione a terze parti	No
Flussi informativi verso altri soggetti	No
Durata del trattamento	Definita dal contratto di servizio, con scarto obbligatorio nei termini previsti dalla legge.
Interessati	Fornitori Entaksi.
Accesso	Responsabili definiti nel funzionigramma, sviluppatori incaricati (previa sottoscrizione di accordo di riservatezza).
Finalità	Esecuzione dei contratti di fornitura.
Modalità di raccolta	Imputazione dei dati da parte dell'utente.
Modalità di trattamento	Il trattamento è inserito nel Sistema Integrato di Gestione (SIG) Entaksi, certificato per la sicurezza delle informazioni (ISO/IEC 27001:2013).

Trattamento dei contratti con i dipendenti	
Asset	Sistema di Gestione Amministrativo
Tipo di dati	Cedolini, CU e altra documentazione amministrativa dei dipendenti Entaksi Certificati di malattia e stati di famiglia dei dipendenti Entaksi
Cessione a terze parti	No
Flussi informativi verso altri soggetti	No
Durata del trattamento	Definita dal contratto di lavoro con Entaksi, con scarto obbligatorio nei termini previsti dalla legge, o definita dai termini di legge per i dati personali (curriculum 6 Mesi).
Interessati	Dipendenti Entaksi.
Accesso	Direzione e responsabili definiti dalla Direzione.

Finalità	Accesso ai dati finalizzato alla gestione amministrativa di Entaksi al fine della conduzione delle proprie attività nei termini di legge.
Modalità di raccolta	Imputazione dei dati da parte dell'utente.
Modalità di trattamento	Il trattamento è inserito nel Sistema Integrato di Gestione (SIG) Entaksi, certificato per la sicurezza delle informazioni (ISO/IEC 27001:2013).

Trattamento di documenti provenienti dall'esterno che possono contenere dati personali	
Asset	Sistema di Gestione Amministrativo
Tipo di dati	Documenti provenienti dall'esterno che possono contenere dati personali (es. CV, richieste, proposte commerciali)
Cessione a terze parti	No
Flussi informativi verso altri soggetti	No
Durata del trattamento	Definita dai termini di legge per i dati personali (curriculum 6 Mesi).
Interessati	Chiunque decida di inviare dati sensibili a Entaksi.
Accesso	Direzione e responsabili definiti dalla Direzione.
Finalità	Accesso ai dati finalizzato alla gestione amministrativa di Entaksi al fine della conduzione delle proprie attività nei termini di legge.
Modalità di raccolta	Imputazione dei dati da parte dell'utente.
Modalità di trattamento	Il trattamento è inserito nel Sistema Integrato di Gestione (SIG) Entaksi, certificato per la sicurezza delle informazioni (ISO/IEC 27001:2013).

Dati inviati tramite email	
Asset	Server di posta elettronica
Tipo di dati	Contenuto delle email
Cessione a terze parti	No
Flussi informativi verso altri soggetti	No
Durata del trattamento	Definita dal contratto di assunzione, con scarto obbligatorio nei termini previsti dalla Legge.
Interessati	Chiunque decida di inviare dati sensibili a Entaksi.
Accesso	Responsabili definiti nel funzionigramma del servizio eCON, sviluppatori incaricati (previa sottoscrizione di accordo di riservatezza), responsabili per prodotti e servizi.
Finalità	Accesso ai dati finalizzato alla gestione dei servizi Entaksi alla comunicazione con i clienti e qualunque altro utente.
Modalità di raccolta	Email.

Modalità di trattamento	Il trattamento è inserito nel Sistema Integrato di Gestione (SIG) Entaksi, certificato per la sicurezza delle informazioni (ISO/IEC 27001:2013).

Dati inviati ad assistenza@entaksi.eu (Help Desk)	
Asset	Sistema di Tracking Assistenza
Tipo di dati	Contenuto dei ticket di assistenza
Cessione a terze parti	No
Flussi informativi verso altri soggetti	No
Durata del trattamento	Definita dal contratto di assunzione, con scarto obbligatorio nei termini previsti dalla Legge.
Interessati	Chiunque decida di inviare dati sensibili a Entaksi.
Accesso	Responsabili definiti nel funzionigramma del servizio eCON, sviluppatori incaricati (previa sottoscrizione di accordo di riservatezza), responsabili per prodotti e servizi.
Finalità	Accesso ai dati finalizzato alla gestione dei servizi Entaksi e allo svolgimento delle attività di manutenzione, oltre che alla comunicazione con i clienti stessi.
Modalità di raccolta	Email.
Modalità di trattamento	Il trattamento è inserito nel Sistema Integrato di Gestione (SIG) Entaksi, certificato per la sicurezza delle informazioni (ISO/IEC 27001:2013).

4. Misure per la protezione dei dati personali

Le misure poste in essere da Entaksi Solutions Srl per garantire la protezione dei dati personali trattati sono descritte nel documento "MAN SIG 20200511 Politica per la sicurezza delle informazioni". Il documento è pubblico, ed è disponibile nel sito Entaksi.

4.1. Formazione

Al fine di rendere operativo il DPIA e mitigare il rischio legato a errori umani, Entaksi provvede alla formazione dei propri dipendenti sulle tematiche di sicurezza emerse dal rapporto di valutazione.

5. Metodologia analisi rischi

L'analisi dei rischi svolta da Entaksi si articola nelle seguenti fasi:

- **Identificazione della Designated Community**, dove per la conduzione della DPIA si intende gli interessati al trattamento.
- **Identificazione degli asset / CI** ossia, per la DPIA, tutti quegli asset nel CMDB Entaksi che contengano dati personali.
- **Identificazione delle minacce** definite come eventi o fenomeni potenzialmente dannosi cui possono essere esposti gli asset durante l'operatività dell'azienda.
- **Definizione del rischio accettabile** ossia il calcolo della "soglia di rischio accettabile", individuata arbitrariamente dall'organizzazione come limite della tollerabilità, dopo una attenta valutazione dei costi/benefici indotti dalla adozione di eventuali contromisure di mitigazione.
- **Stima della probabilità di accadimento delle minacce** calcolata sulla verosimiglianza che il fenomeno si verifichi entro un determinato periodo di tempo, convenzionalmente stabilito in tre anni.
- **Stima degli impatti**, il danno derivante dagli eventi avversi che si potrebbero produrre sugli asset critici a fronte delle minacce identificate, calcolato sul danno economico che ne deriverebbe all'azienda (anche in relazione all'art. 83 GDPR).
- **Calcolo della vulnerabilità**, ossia la 'propensione' di un asset ad essere danneggiato da una particolare minaccia.
- **Analisi dei rischi** ingresso dei valori di probabilità, impatto e vulnerabilità di ciascuna minaccia su asset contenenti dati personali, calcolati sui valori dell'analisi precedente e su misure effettuate sui sistemi.
- **Contromisure adottate** applicazione esecuzione di attività o adozione di comportamenti che possono portare al contenimento, alla riduzione, al trasferimento o all'eliminazione del rischio.
- **Gestione del Rischio Residuo** il ricalcolo del rischio dopo l'applicazione delle contromisure, e la sua gestione.
- **Redazione del Rapporto di valutazione dei rischi e del Piano di trattamento dei rischi**.

5.1. Risorse di supporto ai dati

Le risorse di supporto ai dati, comprensive di asset fisici, software, professionali e di processo sono elencate nel CMDB della Piattaforma Gestione CMDB - Analisi Rischi Entaksi di Entaksi.
L'elenco viene revisionato con cadenza almeno semestrale (o in base ai cambiamenti occorsi).

5.2. Controlli applicati

I controlli applicati sono censiti nella Piattaforma Gestione CMDB - Analisi Rischi Entaksi di Entaksi.

La scelta e l'attuazione dei controlli da effettuare discende da una metodica pianificazione, attenta anche al particolare. Nella pianificazione dei controlli non è trascurato il coinvolgimento di tutte le parti interessate, cioè oltre agli operatori della Sicurezza delle Informazioni, anche utenti, fornitori, clienti ed esperti di organizzazioni esterne.

I controlli applicati soddisfano tutti i requisiti per la protezione dei dati personali.

Il presente DPIA viene definito dal titolare del trattamento e approvato dalla direzione, pubblicato e trasmesso a tutti i dipendenti per conoscenza, e aggiornato in occasione delle periodiche analisi dei rischi sul sistema.

5.3. Valutazione minacce e analisi rischi

La valutazione delle minacce relative al trattamento dei dati ricalca quella già attuata da Entaksi relativa alla propria analisi rischi, riassunta nel capitolo Metodologia analisi rischi e trattata puntualmente nel documento interno "MAN SIG 20200503 Metodologia analisi rischi".

L'analisi dei rischi viene effettuata dal Responsabile del Sistema Integrato di Gestione (SIG) almeno annualmente o, come nel caso dell'introduzione del GDPR, ogni qualvolta venga attuato un intervento sui siti oggetto di applicazione tale da modificare l'assetto tecnologico, infrastrutturale o organizzativo, eventualmente rivalutando e/o riclassificando le grandezza coinvolte, o al verificarsi di un'incidente.

Per quanto riguarda le minacce specifiche per la sicurezza delle informazioni si fa riferimento all'esecuzione dei controlli dell'Annex A della norma ISO/IEC 27001:2013 come riportato in tabella, e alla totalità dei controlli derivati dalle estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

Minaccia	Controlli di sicurezza SiSGI	ID Minacce GDPR

Minacce materiali		
Furto	A.6.2.1, A.6.2.2, A.11.1.3, A 11.2.6	16, 32
Guasto	A.11.2.4	28, 30
Uso improprio	A.8.1.3, A.8.1.4, A.8.3.2, A.11.2.5, A.11.2.6	33, 35
Danneggiamento	A.11.1.3, A.6.1.3	13, 14
Invecchiamento	A.12.3.1, A.14.2.4	86
Minacce logiche		
Mancanza policy sicurezza e procedure	A.5.1.1 A.8.2.3 A.12.1.1	37, 38, 39, 87
Alterazione	A.12.2.1	52
Assenza o mancata esplicitazione	A.13.1.1	57
Danno immateriale	A.6.1.3 A.12.1.2,	43, 45
Mancata manutenzione	A.14.2.2, A.14.2.3	82, 84
Errore umano		
Sottrazione di credenziali di autenticazione	A.9.2.1, A.9.2.6, A.9.3.1, A.11.1.1	9, 11, 70
Carenza di consapevolezza, disattenzione, incuria	A.6.1.1, A.6.1.2, A.6.1.4, A.7.2.2	1, 2, 5
Comportamenti sleali o fraudolenti	A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.9.2.6, A.11.1.1	2, 7
Minacce materiali	A.6.1.2, A.7.2.2, A.8.3.1, A.8.3.2	3, 60, 61, 62, 63
Minacce strumentali		
Virus informatico, programmi atti al furto di informazioni	A.12.2.1	54
Accessi esterni non autorizzati	A.6.1.2 A.9.1.1, A.9.1.2, A.9.2.1	47, 68
Mancato monitoraggio	A.12.5.1	65
Intercettazioni	A.9.2.1, A.13.1.1	57
Accessi fisici non autorizzati	A.11.1.4, A.11.2.1	22, 23
Errori di contesto		
Eventi naturali distruttivi	A.11.1.4	17, 18, 19, 20, 21

Guasto a sistemi complementari (elettrico, connessione...)	A.11.2.2	24, 25
Danno ambientale	A.11.2.2 A.11.2.3	26, 27
Errori organizzativi	A.7.2.1, A.12.1.3	89, 91, 93
Danni economici e di reputazione	A.16.1.1, A.18.1.1	104, 108
Minacce specifiche relative alla gestione della privacy		
Non conformità	A.18.1.1, A.13.2.3	109, 110, 111, 107
Accesso improprio o errato dei dati	A.7.2.2, A.12.1.1	95, 96, 97, 98, 99, 100
Raccolta e utilizzo improprio dei dati	A.8.2.3, A.17.2.1	101, 102, 103
Mancata impostazione privacy by design e by default	A.14.2.1	105, 106

5.4. Rapporto di valutazione rischi

Il rapporto di valutazione rischi riassume ed evidenzia le attività eseguite durante l'analisi rischi condotta a fronte dell'adeguamento del Sistema Integrato di Gestione al GDPR, focalizzando l'attenzione sulle minacce/asset che durante la fase di analisi hanno presentato livelli di rischio inaccettabili.

Nel documento vengono riportate:

- le attività condotte;
- la descrizione del perimetro analizzato;
- l'elenco degli asset coinvolti;
- i rischi individuati e le contromisure adottate;
- l'elenco dei provvedimenti da adottare per adeguare il SIG a quanto rilevato;
- le evidenze emerse;
- le proposte per la redazione del piano di trattamento rischi.

Il documento è classificato come confidenziale e destinato al solo uso interno.

Il rapporto di valutazione rischi redatto per questa DPIA riporta, in merito ai controlli individuati per la protezione dei dati personali, che le contromisure adottate riducono il rischio fino al livello accettabile per ciascuna minaccia.

5.5. Piano trattamento rischi

Qualora l'adozione delle contromisure individuate durante la fase di analisi si concretizzi in azioni che per motivi tecnici o economici devono essere pianificate, viene formalizzato un **piano di trattamento dei rischi** che riporta:

- il riferimento all'analisi rischi effettuata;
- l'elenco delle contromisure individuate;
- la data stimata di implementazione;
- il costo stimato di realizzazione;
- lo stato di avanzamento della implementazione al momento della redazione del documento.

Il documento è classificato come confidenziale e destinato al solo uso interno.

6. Matrice delle responsabilità

Il **Titolare del trattamento dei dati**, secondo quanto disposto dall' art. 4. par. 1 del GDPR, è:
Entaksi Solutions Srl

La sede legale è sita in via la Piana 76, fraz. Pontepetri, 51028 San Marcello Piteglio (PT).

Il GDPR sulla protezione dei dati prevede alcune figure alle quali sono attribuiti specifici obblighi e diritti in relazione all'attività di trattamento dei dati personali.

Queste figure si riassumono in:

Titolare del trattamento dei dati

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Il Titolare del trattamento esercita il potere decisionale sulle finalità e sulle modalità del trattamento ivi compreso il profilo della sicurezza; questi è responsabile delle scelte in materia di sicurezza dei dati trattati della cui mancata adozione risponde anche penalmente.

Responsabili del trattamento

Le persone fisiche o giuridiche, l'autorità pubblica, il servizio o altro organismo che trattano dati personali per conto del Titolare del trattamento.
Sono scelti fra le figure aziendali che forniscono idonea garanzia del pieno rispetto delle disposizioni in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza; i responsabili agiscono in base alle istruzioni specifiche ricevute dal titolare e rispondono della loro ingiustificata inosservanza, e hanno obblighi specifici circa la comunicazione di eventuali problematiche la cui risoluzione comporta l'intervento decisionale del titolare.

Amministratori di Sistema

Sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi è affidato spesso anche il compito di vigilare sulla protezione dei sistemi informatici di un'azienda o di una pubblica amministrazione.

Incaricati

Soggetti che, nominati direttamente dal titolare o dal responsabile, operano sotto la loro diretta autorità nel rispetto delle istruzioni da questi ricevute e condivise.

Responsabile della protezione dei dati o **Data Protection Officer**

Un consulente esperto, che affianca il Titolare nella gestione delle problematiche del trattamento dei dati personali, e fornisce consulenza e vigila sull'osservanza del Regolamento.

Il Data Protection Officer nominato da Entaksi Solutions Srl è: Alessia Soccio.

Attività	TdT	RdT	DPO	RSIG
Definizione e manutenzione del documento	R	C	C	I
Identificazione degli asset	R	C	C	I
Identificazione rischi	R	C	C	I
Valutazione dei rischi	R	C	C	I
Definizione del piano controlli	R	C	C	I

Attività	TdT	RdT	DPO	RSIG
Valutazione	R	C	C	I
Approvazione e rilascio	I	I	R	R

R = Responsabile I = Informato C = Collabora

TdT = Titolare del Trattamento RdT = Responsabile del Trattamento DPO = Data Protection Officer RSIG = Responsabile SIG