ACCORDO SUL TRATTAMENTO DEI DATI TRA TITOLARE E RESPONSABILE

Tra

Il Cliente, intendendosi con Cliente il soggetto che ha richiesto il servizio gestionale DANZAGEST (anche a mezzo di delegato) di seguito titolare del trattamento o semplicemente TITOLARE, da una parte

e

Alessandro Monti con sede in Corciano (PG), p.iva 03360700540 di seguito responsabile del trattamento, o semplicemente RESPONSABILE dall'altra

PREMESSO CHE

- Le parti si sono accordate mediante adesione alle condizioni (DISCLAIMER E REGOLAMENTO) presenti sul sito web di DANZAGEST relativamente alla gestione e manutenzione dei servizi informatici adottati dal Titolare e forniti dal responsabile, con particolare riferimento al servizio gestionale DANZAGEST;

- il titolare, a seguito di esame documentale, ha ritenuto che il soggetto indicato responsabile del trattamento, presente garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

I. OGGETTO

Le presenti pattuizioni hanno ad oggetto la disciplina delle condizioni alle quali il RESPONSABILE, per conto del Titolare, si impegna ad effettuare le operazioni di trattamento dei dati e delle informazioni personali come definiti di seguito.
Nell'ambito dei loro rapporti contrattuali, le parti si obbligano a rispettare la normativa vigente e applicabile al trattamento dei dati personali, e in particolare il REGOLAMENTO UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, applicabile dal 25 maggio 2018, di seguito anche semplicemente Regolamento

II. DESCRIZIONE DEI TRATTAMENTI DELEGATI AL RESPONSABILE

Il Responsabile è autorizzato a trattare per conto del Titolare i dati personali necessari a prestare i servizi forniti.
La natura delle operazioni di trattamento è relativa alla fornitura di servizi di assistenza e manutenzione dei programmi software e gestionali forniti come servizio dal Responsabile al Titolare del trattamento dei dati.

FINALITA': tali dati vengono trattati per il corretto funzionamento del sistema gestionale in cloud che è stato adottato dal Titolare e viene fornito dal responsabile del trattamento dei dati come meglio sopra descritto. I dati personali sono forniti dal titolare e sono acquisiti da sistemi informatici e procedure software nel corso del loro normale esercizio.
Tali dati vengono trattati al solo fine di mantenere aggiornati e sicuri i sistemi software forniti, fornire manutenzione e assistenza e risolvere eventuali problematiche degli stessi nonché al fine di gestire le criticità che tali sistemi software potrebbero dare.

La categoria di dati che formano oggetto del trattamento sono:

Tipologie di dati trattati

- Dati comuni relativi a clienti/utenti
- Dati comuni relativi a fornitori
- Dati comuni relativi al personale, o candidati
- Dati comuni relativi ad altri soggetti
- Dati relativi allo svolgimento di attività economica o commerciale
- Dati relativi alla trasmissione su rete una rete telefonica o telematica

Categorie di dati personali

- Dati identificativi (nome e cognome)
- Dati anagrafici (data di nascita, luogo di nascita indirizzo, residenza)
- Dati di contatto (numero di tel. fisso o cell., email, indirizzo per posta cartacea)
- Informazioni demografiche (genere, età)
- Dati di connessione (log o ip)
- Dati personali relativi a minori

III. DURATA DELL'ACCORDO

Il presente accordo avrà durata pari a quella del servizio sostanziale offerto dal Responsabile aderito dal Titolare che giustifica il trattamento da parte del Responsabile

IV. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO NEI CONFRONTI DEL RESPONSABILE

Il titolare del trattamento si obbliga a:

- fornire al responsabile del trattamento dei dati personali di cui al n. II del presente accordo.
- documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del responsabile
- assicurare, sin d'ora e per tutta la durata del trattamento, il rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del responsabile
- supervisionare il trattamento, compresa la realizzazione degli audit e le ispezioni col contributo del responsabile

V. OBBLIGHI DEL RESPONSABILE

Il Responsabile si impegna innanzi al Titolare a:

1. Trattare i dati personali per le sole finalità oggetto del trattamento.

2. Trattare i dati personali in conformità alle istruzioni scritte del titolare, allegate al presente accordo; se il responsabile ritiene che un'istruzione ricevuta dal titolare rappresenti una violazione del Regolamento generale sulla protezione dei dati, o del diritto dell'Unione europea o del diritto di uno Stato membro, egli informa tempestivamente il titolare del trattamento.
   Inoltre, se il responsabile è tenuto a procedere a un trasferimento di dati verso un paese terzo o un'organizzazione internazionale in virtù del diritto dell'Unione o del diritto di uno Stato membro al quale è sottoposto, egli deve informare il titolare del trattamento di tale obbligo giuridico prima del trattamento a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

3. garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto.
4. assicurare che le persone autorizzate a trattare i dati a carattere personale in virtù del presente contratto:

   - si impegnino a rispettare la riservatezza o siano sottoposte a un idoneo obbligo legale di riservatezza
   - ricevano le istruzioni necessarie a mantenere la protezione dei dati a carattere personale.

5. Tengano conto, per quanto riguarda strumenti, prodotti, applicazioni o servizi, dei principi della privacy sin dalla progettazione (privacy by design) e della privacy per impostazione predefinita (privacy by default)

6. Subresponsabili - Autorizzazione generale

   Il Responsabile può ricorrere a un altro responsabile del trattamento (d'ora innanzi sub-responsabile) per l'esecuzione di specifiche attività di trattamento. In questo caso egli informa preventivamente e per iscritto il titolare di tutte le modifiche riguardanti l'aggiunta o la sostituzione dei sub-responsabili. Tali informazioni devono indicare chiaramente le attività di trattamento effettuate dal sub-responsabile, l'identità e i recapiti del sub responsabile, e la data del contratto relativo al sub-trattamento. Il titolare del trattamento dispone di un periodo di 15 giorni a far data dal ricevimento delle informazioni per presentare le proprie obiezioni. Il sub trattamento non può avere inizio sino a che il termine indicato non sia spirato senza che il titolare abbia presentato obiezioni.

   Il sub responsabile è tenuto a rispettare gli obblighi del presente contratto per conto e secondo le istruzioni del titolare del trattamento. È compito del Responsabile assicurare che il sub-responsabile presenti le medesime garanzie sufficienti in ordine alla messa in atto delle misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento generale sulla protezione dei dati.
   Se il sub-responsabile del trattamento omette di adempiere i suoi obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del titolare la piena responsabilità per l'adempimento degli obblighi del sub-responsabile.

7. Diritto degli interessati all'informativa

   È compito del titolare del trattamento fornire l'informativa agli interessati del trattamento al momento in cui i dati sono raccolti.

8. Esercizio dei diritti da parte degli interessati

   Nella misura del possibile il responsabile del trattamento deve aiutare il titolare del trattamento ad adempiere ai propri obblighi di fornire riscontro alle richieste degli interessati in ordine al diritto d'accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, diritto alla portabilità dei dati, o qualora applicabile diritto a opporsi a una decisione individuale automatizzata (compresa la profilazione):
   Quando gli interessati si rivolgano al responsabile per l'esercizio dei loro diritti, il responsabile deve inviare queste richieste, non appena vengono ricevute, per posta elettronica all'indirizzo di posta elettronica indicato in calce al presente accordo (allegato B).
   Ove il Titolare non provveda a tale incombente il Responsabile è libero da ogni obbligo.

9. Notifica delle violazioni dei dati personali

   Il Responsabile comunica al Titolare del trattamento tutte le violazioni di dati a carattere personale nel **termine massimo di 48 ore** dal momento in cui è venuto a conoscenza della violazione, con le seguenti modalità: comunicazione all'indirizzo di posta elettronica indicato nell'allegato B al presente contratto.
   Tale comunicazione è accompagnata dalla notizia della messa a disposizione (ove possibile) di tutta la documentazione utile (la cui modalità di trasmissione verrà concordata tra le parti) al fine di permettere al titolare del trattamento, di provvedere, se necessario, alla notifica di tale violazione all'Autorità di Controllo competente nei termini di legge.

10. Ausilio del responsabile per il rispetto, da parte del Titolare, degli obblighi gravanti sul Titolare stesso:

    - Il responsabile aiuta il titolare del trattamento nell'effettuazione della valutazione di impatto sulla protezione dei dati personali.
    - Il responsabile del trattamento aiuta il titolare del trattamento nell'effettuazione della consultazione preventiva rivolta all'Autorità di controllo

11. Misure di sicurezza

    Il responsabile si obbliga, ai sensi dell'articolo 32, a mettere in atto le misure di sicurezza descritte nell'allegato "security policy Danzagest" che il Titolare dichiara adeguate e conformi alle istruzioni da impartire.
    Il Titolare delega al responsabile l'adozione di misure diverse rispetto a quelle descritte nell'allegato ""security policy Danzagest"" a condizione che il responsabile rispetti i parametri definiti dall'articolo 32 del Regolamento. Il responsabile, valutato il rischio e qualora lo ritenga necessario anche in considerazione dei costi e dello stato dell'arte si obbliga a mettere in atto le misure di sicurezza seguenti, se applicabili e congrue:

    - la pseudonimizzazione e la cifratura dei dati personali;
    - misure che abbiano la capacità di assicurare su base permanente la riservatezza,
    - l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    - misure che abbiano la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

    Inoltre, ove occorrer possa e per quanto concerna i trattamenti effettuati per fornire il Servizio dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Responsabile è tenuto altresì al rispetto delle previsioni pro tempore applicabili relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009. Il Responsabile, in particolare, si impegna ad attribuire le funzioni di amministratore di sistema solo previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
    Si impegna altresì a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.
    Si impegna, infine, ad adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell´evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

12. Sorte dei dati

    Al termine della prestazione del servizio relativo al trattamento dei dati il responsabile si obbliga a restituire tutti i dati personali al titolare del trattamento, salvo che questi gli ordini di distruggerli.
    La restituzione si accompagna alla distruzione delle anagrafiche esistenti nel sistema informatico del responsabile.

13. Responsabile per la protezione dei dati (data protection officer, DPO o RPD)

    Il responsabile del trattamento non effettua trattamenti su larga scala per i quali è obbligatoria la nomina del Responsabile per la protezione dei dati.
    Qualora venisse nominato un Responsabile per la protezione dei dati su base volontaria o per altre ragioni la nomina si rendesse necessaria (ad esempio: modifica dell'attività principale, acquisizioni di rami d'azienda, incorporazioni, fusioni o acquisizioni da parte di imprese che svolgono attività per cui la nomina è obbligatoria) il Responsabile del trattamento si impegna a darne pronta comunicazione al Titolare, unitamente ai dati di contatto.

14. Registro delle attività di trattamento

    Il Responsabile dichiara di tenere per iscritto un registro di tutte le attività di trattamento effettuate per conto del titolare comprendente tutti gli elementi elencati a tal fine dall'articolo 30 del Regolamento.

15. Documentazione

    Il responsabile mette a disposizione del titolare del trattamento la documentazione necessaria a dimostrare il rispetto di tutti i suoi obblighi, e per consentire gli audit, comprese le ispezioni, al titolare del trattamento o altro soggetto da questi a tal fine incaricato, e contribuire agli audit.

VI. Obblighi del titolare del trattamento nei confronti del responsabile del trattamento

Il Titolare del trattamento si obbliga a:

- fornire al responsabile del trattamento dei dati personali di cui al n. II del presente accordo.
- documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del responsabile
- assicurare, sin d'ora e per tutta la durata del trattamento, il rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del responsabile
- supervisionare il trattamento, compresa la realizzazione degli audit e le ispezioni col contributo del responsabile

VII. Clausole finali

Le premesse e gli allegati fanno parte integrante del presente accordo.

Luogo
Perugia

Allegato A

Nominativo del DPO del Titolare (se applicabile)	Dati di contatto

Allegato B - Recapiti

Recapiti del Titolare per le comunicazioni previste nel presente accordo

Evento	Dati di contatto
Data Breach	
istanze di accesso	
Autorità Garante o Altra Autorità	

Recapiti del Responsabile per le comunicazioni previste nel presente accordo

Evento	Dati di contatto
Data Breach	danzagest@pec.it
istanze di accesso	danzagest@pec.it
Autorità Garante o Altra Autorità	danzagest@pec.it

Allegato C

"Sub-responsabili"

Il Responsabile è autorizzato a sub-appaltare parte delle operazioni di trattamento ai seguenti sub-responsabili (siano essi o meno appartenenti al Gruppo del Responsabile).

La seguente tabella mappa i sub-responsabili ingaggiati dal Responsabile:

Paese in cui è stabilito il Titolare	Responsabile	Sub-responsabili
Italia	Italia	Italia

Subresponsabile	dati di contatto	DPO
Aruba S.p.A.,	privacy@staff.aruba.it	dpo@staff.aruba.it
Agile Telecom S.p.A.,	agiletelecom@pec.it	

Restano esclusi i servizi non forniti dal Responsabile e soggetti a separati accordi tra il Sub-responsabile e il Titolare.

La tabella dei sub-responsabili verrà aggiornata di volta in volta e il Titolare verrà notificato di con-seguenza in modo che possa opporsi all'impiego di nuovi sub-responsabili.

Allegato D

MODELLO PER LA COMUNICAZIONE DELLA VIOLAZIONE DEI DATI DAL RESPONSABILE AL TITOLARE (AI FINI DEL C.D. "DATA BREACH")

Occorre prestare la massima attenzione nel compilare il report della violazione.
Il report deve essere compilato e inviato senza ritardo a:

Nominativo e ruolo
_____

indirizzo di posta elettronica
_____

Parte 1: avviso di violazione	Da compilare a cura di chi ha scoperto la violazione
data della scoperta della violazione:	
Data della violazione	
Dove si è verificata la violazione? Denominazione e descrizione della banca dati o dello strumento (computer rete, pc portatile, tablet, chiavetta usb altra memoria rimovibile, disco esterno, file o parte di un file, strumento di backup, documento cartaceo o altro -specificare)	
Ubicazione dello strumento o banca dati	
Nome della persona che ha scoperto la violazione	
contatti della persona che ha scoperto la violazione	
Breve descrizione della violazione: • lettura (presumibilmente i dati non sono stati copiati) • Copia (i dati sono ancora presenti sui sistemi del titolare) • Alterazione (i dati sono presenti sui sistemi ma sono stati alterati) • Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione) • Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione) • Altro (specificare)	
Numero di interessati coinvolti (prima stima approssimativa; se è possibile determinarlo, nel caso coinvolga tutti gli interessati, specificarlo; specificare altresì se non è possibile determinare il numero e se il numero presumibilmente resterà ignoto):	
La violazione costituisce un rischio per gli interessati? (descrivere brevemente se si ritiene che comporti un rischio)	
Breve descrizione delle azioni già intraprese per mitigare il rischio	
Da compilare a cura del ricevente	
Ricevuto da	
Data	
Prossime azioni (notifica comunicazione)	
Entro il	

Parte 2 - valutazione del rischio	Da compilare a cura del soggetto competente a effettuare la valutazione
Descrizione dei sistemi IT, degli strumenti, dei device degli archivi coinvolti nella violazione:	
Misure tecniche e organizzative applicate ai dati	
Descrizione dell'evento : • Perdita • Indisponibilità • lettura (presumibilmente i dati non sono stati copiati) • Copia (i dati sono ancora presenti sui sistemi del titolare) • Alterazione (i dati sono presenti sui sistemi ma sono stati alterati) • Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione) • Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione) • Accesso esterno non autorizzato • Accesso interno non autorizzato • errore • Fenomeno naturale (incendio, inondazione ecc.) • Altro	
Qual è la natura delle informazioni interessate dalla violazione (copia informatica di documenti cartacei, documenti informatici, documenti cartacei)?	
Quanti dati sono interessati? In caso di perdita o furto di laptop o altro device: Quando era stato fatto l'ultimo backup disponibile?	
Si tratta di informazioni uniche? Questa violazione può comportare conseguenze finanziarie legali danni all'immagine o reputazioni al Titolare o al responsabile o agli interessati o ad altre terze parti se resa nota?	
Quanti interessati coinvolge la violazione?	
Sono coinvolte particolari categorie di dati o altri dati ad alto rischio? (indicare le categorie coinvolte)cfr categorie indicate di seguito	
Dati anagrafici/codice fiscale Dati di accesso e di identificazione (user name, password, customer ID, altro) **Dati ad alto rischio:** dati che rivelano: • l'origine razziale o etnica • le opinioni politiche • le convinzioni religiose o filosofiche • l'appartenenza sindacale • oppure • dati relativi allo stato di salute • dati relativi alla vita sessuale o all'orientamento sessuale • dati genetici • biometrici • dati relativi a reati o condanne penale	
Tipologia di interessati • Candidati • Dipendenti • Dipendenti dei partner commerciali (e.g. dealer, fornitori, etc..) • Clienti (inclusi i prospects)	

attenzione in particolare a: a) informazioni personali relative a categorie particolarmente vulnerabili o relative a minori; b) informazioni particolari relative ai lavoratori, come ad esempio test attitudinari, buste paga ecc. c) whistleblower	
Conseguenze ipotizzabili a) provocare danni fisici, materiali o immateriali alle persone fisiche (ad esempio informazioni che possono compromettere la sicurezza degli interessati se rese note); b) furti di identità o usurpazioni (informazioni che possono essere utilizzate per competere furti di identità o altri reati come ad esempio account bancari o altre informazioni finanziare e identificative come ad esempio copie di carte di identità e passaporti o altri documenti di riconoscimento); c) perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti; d) discriminazione (esempio dati sulla etnia, razza religione convinzioni filosofiche orientamento sessuale, talvolta appartenenza sindacale) e) perdite finanziarie, f) decifratura non autorizzata della pseudonimizzazione (es. whistleblowing) g) pregiudizio alla reputazione, h) perdita di riservatezza dei dati personali protetti da segreto professionale i) qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. j) grave disagio e stress se le informazioni vengono rese note o divulgate; informazioni relative all'identità di individui che si sono avvalsi di procedure di whistleblowing e causare ritorsioni	
la violazione è localizzata o generalizzata all'intero sistema?	
E' possibile superare l'incidente che ha provocato la violazione con le normali operazioni di ripristino?	
In alternativa; è necessario l'intervento di soggetti esterni?	
La violazione è solo temporanea o è permanente?	

Parte 3: Azioni intraprese	Da compilarsi a cura del soggetto competente
Data	
Annotazione nel registro /n. violazione	
Quante registrazioni di dati personali sono state colpite dalla violazione dei dati personali? **Indicare numero approssimativo:** • da 1 a 100 • da 100 a 1000 • da 1000 a 10.000 • da 10.000 a 100.000 • da 100.000 a 500.000 • da 500.000 a 1.000.000 • oltre 1.000.000	
Azioni intraprese - Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?	
Quali misure tecnologiche e organizzative sono state adottate (o ci si propone di adottare) per attenuare i possibili effetti negativi della violazione?	
Follow up	
Occorre procedere alla notifica all'Autorità territoriale competente	sì/no
Occorre dare comunicazione agli interessati	sì/no (dettagli)
La violazione potrebbe riguardare: a) informazioni che possono compromettere la sicurezza degli interessati se rese note; b) informazioni che possono comportare discriminazione se rese note c) informative relative a minori o soggetti deboli d) informazioni che se diffuse arrecano pregiudizio alla reputazione informazioni che possono causare grave disagio o stress se rese note	

Allegato E

Istruzioni generali impartite dal Titolare al Responsabile del Trattamento

Il Responsabile, sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate, oltre agli ulteriori obblighi previsti nel suesteso accordo, e dunque dovrà:

- effettuare la ricognizione delle banche dati, degli archivi (cartacei e non) relativi ai trattamenti effettuati in esecuzione delle obbligazioni che scaturiscono dal rapporto sostanziale e giustificano il trattamento operato dal responsabile per conto del Titolare (di seguito semplicemente "servizio")
- tenere un registro, come previsto dall'art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Società, contenente:

    - il nome e i dati di contatto del Responsabile e del Titolare e, laddove applicabile, del Responsabile della protezione dei dati;
    - le categorie dei trattamenti effettuati per conto del Titolare;
    - ove applicabile, i trasferimenti di dati personali verso un paese non appartenente all'Unione Europea, compresa l'identificazione di tale paese e, per i trasferimenti di cui al secondo comma dell'art. 49 del GDPR, la documentazione delle garanzie adeguate;
    - ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate;

- organizzare le strutture, gli uffici e le competenze necessarie e idonee a garantire la corretta esecuzione del servizio;
- astenersi dal contattare per finalità diverse dall'incarico i nominativi trattati attraverso il servizio;
- non diffondere o comunicare a terzi le informazioni, ivi inclusi i dati personali trattati per rendere il Servizio;
- provvedere ad individuare per iscritto i soggetti autorizzati al trattamento ai sensi della Normativa applicabile e impartire a questi ultimi specifiche e dettagliate istruzioni dirette ad assicurare il pieno rispetto delle disposizioni di cui alla Normativa applicabile;
- **avvisare il Titolare del trattamento, di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria eventualmente ricevuta inviando copia delle istanze all'indirizzo e-mail indicato dal Titolare per concordare congiuntamente il riscontro;**
- predisporre idonee procedure interne finalizzate alla verifica periodica della corretta applicazione e della congruità degli adempimenti posti in essere ai sensi della Normativa applicabile, attuate in accordo con il Titolare anche in applicazione delle misure tecniche e organizzative di sicurezza;
- mantenere un costante aggiornamento sulle prescrizioni di legge in materia di trattamento dei dati personali, nonché sull'evoluzione tecnologica di strumenti e dispositivi di sicurezza, modalità di utilizzo e relativi criteri organizzativi adottabili;garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali non coerente con gli specifici trattamenti svolti in adempimento dell'incarico medesimo;

Allegato F

Security Policy Danzagest

COME DANZAGEST PROTEGGE I TUOI DATI

Versione: 1
Ultimo aggiornamento: 16 Settembre 2018

Introduzione

Al fine di proteggere i tuoi dati Danzagest ha affrontato le seguenti criticità:

1. **Protezione fisica del dato:**
   Custodire i tuoi dati in un datacenter sicuro e non accessibile a personale non autorizzato.

2. **Sicurezza del nostro software:**
   Prevenire possibili data breach che sfruttino vulnerabilità sul software e/o sugli apparati da noi utilizzati per erogare servizi ai nostri clienti.

3. **Come opera Danzagest in qualità di responsabile del trattamento:**
   Come Danzagest rispetta gli obblighi imposti al Responsabile del trattamento dal Regolamento UE 2016/679.

   - Sicurezza dei dati
   - Avvisare, assistere e consigliare il titolare
   - Privacy by designs e by default
   - Siamo obbligati a nominare un responsabile per la protezione dei dati (rpd o dpo)?
   - Siamo disponibili a sottoscrivere accordi sul trattamento
   - Siamo dotati di un registro delle attività di trattamento
   - Obblighi del responsabile che nomini un sub-responsabile
   - Violazione dei dati
   - Ruolo del responsabile nella valutazione di impatto

1. PROTEZIONE FISICA DEL DATO

Il nostro fornitore di servizi informatici sono dotati di mezzi e/o strumenti ritenuti idonei a tutelare nella maniera più efficace la sicurezza delle informazioni (fisica, logica, informatica ed organizzativa) e certificato ISO 27001:2013.

In particolare i data center dove viene ospitato Danzagest e i dati dei suoi clienti rispettano i massimi standard di resilienza previsti dal livello Rating 4* (former Tier 4) ANSI/TIA 942-A.

Al fine di minimizzare gli impatti di possibili perdite di dati, eseguiamo backup periodici relativi ai nostri sistemi.

In caso di sospetta violazione dei nostri sistemi useremo la procedura di data breach ed incident response.

* Il Rating 4 (former Tier 4) è il massimo livello previsto da ANSI/TIA 942-A e classifica un data center quale infrastruttura in grado evitare interruzioni dei servizi anche in presenza di guasti gravi grazie ad elevati livelli di ridondanza degli impianti.

Un data center di Rating 4 (former Tier 4) ha componenti ridondati sempre attivi, oltre a percorsi multipli di alimentazione e raffreddamento degli hardware.

Il data center è attrezzato per sopportare un guasto in un qualsiasi punto dell'impianto senza causare downtime ed è protetto nei confronti degli eventi fisici tra i quali anche le catastrofi naturali (es. incendio, alluvione, terremoto, etc.).

Un data center può essere certificato Rating 4 (former Tier 4) per il design anche in fase di progettazione (Design Validation). Una volta in esercizio, il data center verrà sottoposto a una ispezione da parte di ANSI/TIA che ne verificherà la costruzione di livello Rating 4 (former Tier 4), As Built Validation.

ANSI/TIA 942-A è uno dei principali standard di riferimento al mondo per la valutazione della qualità infrastrutturale e la garanzia di continuità dei servizi di un data center. Il TIA-942 è l'unico standard di riferimento e classificazione adottato dall'AGID (Agenzia per l'Italia Digitale) per la classificazione dei CED della Pubblica Amministrazione italiana.

2. SICUREZZA DEL NOSTRO SOFTWARE

Al fine di proteggere i dati dei nostri clienti prevenendo al massimo la possibilità di data breach utilizziamo le seguenti policy di sicurezza o i seguenti standard:

- utilizzare utenze personali per loggarsi sui sistemi sia remoti che locali e rimuovere gli utenti di default o inibirne la possibilità di autenticazione da remoto
- policy di uso delle password che prevedano una complessità adeguata
- implementare un sistema centralizzato di gestione degli utenti e delle autorizzazioni
- aggiornare periodicamente i software utilizzati su tutti gli apparati e rimanere informati relativamente a vulnerabilità di sicurezza al fine di essere tempestivi nel patching delle vulnerabilità
- usare algoritmi di hashing (MD5) per conservare password delle nostre Utenze
- inibire l'accesso ai nostri sistemi dopo diversi tentativi di login errata per l'indirizzo ip sorgente che ha generato tali tentativi di accesso
- Consentire l'accesso ai nostri servizi ai clienti finali solo tramite canali cifrati

3.COME OPERA DANZAGEST IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO

SICUREZZA DEI DATI

Non solo garantiamo la sicurezza dei dati, adottando tutte le misure di sicurezza adeguate al rischio, come dispone l'articolo 32 del GDPR e che dettagliato ai punti precedenti, ma garantiamo la anche la riservatezza dei trattamenti (vincolando alla riservatezza i nostri collaboratori), e abbiamo adottato politiche sulle violazioni di dati personali per avvisare senza ingiustificato ritardo il titolare del trattamento di tutte le violazioni di dati di cui dovessimo a conoscenza, Infine, secondo le istruzioni ricevute dal titolare gli consentiamo di esportare o cancellare i dati relativi ad anagrafiche e movimenti contabili attraverso i comandi che il titolare stesso potrà utilizzate dal pannello di controllo, una volta terminata la prestazione di servizi e quindi la cancellazione dell'account Danzagest saranno necessari 30 prima che ogni dato venga cancellato dai nostri sistemi.

AVVISARE, ASSISTERE E CONSIGLIARE IL TITOLARE

Collaboriamo col titolare del trattamento dei dati personali avvisandolo, assistendolo e consigliandolo in merito al funzionamento dei nostri sistemi;
Presteremo assistenza al titolare per consentirgli di evadere le richieste inerenti l'esercizio dei diritti degli interessati e, tenendo conto della natura del trattamento e delle informazioni a nostra disposizione, aiuteremo il titolare a garantire la conformità con i requisiti di sicurezza del trattamento, notifica delle violazioni di dati e valutazioni di impatto sulla protezione dei dati.

PRIVACY BY DESIGN E BY DEFAULT

Consapevoli degli obblighi che gravano sul Titolare in ordine ai principi di privacy by design e privacy by default, ai sensi dell'articolo 25 del Regolamento, e della strumentalità che caratterizza il ruolo del responsabile, abbiamo messo in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.
In particolare:

- Sin dalla fase di progettazione dei nostri sistemi, mettiamo in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati come la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (privacy by design).
- mettiamo in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. (privacy by default).

SIAMO OBBLIGATI A NOMINARE UN RESPONSABILE PER LA PROTEZIONE DEI DATI (RPD O DPO)?

Non siamo obbligati a nominare un DPO: La nomina, infatti, è obbligatoria in tre ipotesi:

- il l trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
- l'attività principale, effettuata per conto del titolare, comporta il monitoraggio regolare e sistematico degli interessati su larga scala;
- l'attività principale effettuata per conto del titolare consiste nel trattamento di dati sensibili (categorie particolari di dati personali) o giudiziari (dati relativi a condanne penali e a reati) su larga scala.

Le indicazioni per definire meglio il campo di obbligatorietà della designazione del DPO si traggono dalle Linee – guida sui responsabili della protezione dei dati (RPD o DPO) pubblicate dal Gruppo di Lavoro Articolo 29 che, al paragrafo 2.2, si dedica alla designazione del DPO da parte del responsabile, fornendo anche alcuni esempi.
Poiché la nostra attività principale non è rappresentata da trattamenti su larga scala come quelli sopra descritti, non siamo soggetti all'obbligo di nomina.

SIAMO DISPONIBILI A SOTTOSCRIVERE ACCORDI SUL TRATTAMENTO

Ci rendiamo disponibili a fornire o sottoscrivere accordi che prevedano (per iscritto):

- l'oggetto e la durata della prestazione che il responsabile effettuerà per conto del titolare;
- la natura e la finalità del trattamento;
- il tipo di dati personali trattati per conto del titolare;
- le categorie di interessati,
- gli obblighi e i diritti del titolare del trattamento
- gli obblighi e i diritti del responsabile del trattamento, come previsti dall'articolo 28 del Regolamento.

SIAMO DOTATI DI UN REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Come previsto dal Regolamento, teniamo un registro dei trattamenti che effettuiamo per conto del titolare.
Il registro, teniamo per iscritto, contiene:

- il nome e i dati di contatto di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, e la documentazione delle garanzie adeguate su cui si fondano;
- una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento.

OBBLIGHI DEL RESPONSABILE CHE NOMINI UN SUB-RESPONSABILE

Siamo consapevoli che il responsabile del trattamento può designare un altro responsabile del trattamento solo previa autorizzazione scritta del titolare del trattamento.
Comunichiamo i dati dei nostri subresponsabili al momento della sottoscrizione dell'accordo sul trattamento, che prevederà la delega per la le successive nomine.
Imponiamo al sub-responsabile, mediante un contratto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto stipulato tra il titolare del trattamento e il responsabile del trattamento.

VIOLAZIONE DEI DATI

La violazione dei dati personali è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Ove venissimo a conoscenza di una violazione, ne informeremo il titolare del trattamento senza ingiustificato ritardo.
Abbiamo adottato una politica aziendale che ci permette di assistere il titolare nel garantire la conformità dei trattamenti alle norme che presiedono alla loro sicurezza, comprese quelle inerenti alla violazione dei dati personali.

RUOLO DEL RESPONSABILE NELLA VALUTAZIONE DI IMPATTO

A dover effettuare la valutazione di impatto sulla protezione dei dati a norma dell'articolo 35 RGPD è il titolare, e la relativa responsabilità gli pende in capo e non può essere traslata sul responsabile.
Tuttavia prestiamo assistenza al titolare nella conduzione della DPIA fornendo ogni informazione necessaria, come previsto nell'accordo sul trattamento.