

Oggetto: Atto di identificazione del Responsabile del trattamento

Ai sensi degli artt. 28 e seguenti del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, il "**GDPR**") DISCOVERY SRL, con sede legale in Udine, Via della Vigna n.17 int. 2, in qualità di Titolare del Trattamento, (di seguito anche "**DISCOVERY**" o "**Titolare**"),

Premesso che:

- per "Normativa privacy" si intende il GDPR, il d.lgs. 196/03, il d.lgs. 101/18, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile al trattamento dei dati personali, già in vigore o che entrerà in vigore nel periodo di efficacia dell'Atto di identificazione, ivi compresi i provvedimenti, le linee guida e le opinioni del Garante per la Protezione dei dati personali, del Gruppo di Lavoro di cui all'Art. 29 della Direttiva 95/46/EC, del Comitato Europeo per la Protezione dei Dati di cui all'articolo 63 e seguenti del GDPR e di ogni altra autorità competente;
- l'art. 28 paragrafo 1 del GDPR riconosce al titolare del trattamento la facoltà di avvalersi unicamente di uno o più responsabili del trattamento dei dati, che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;
- l'art. 29 del GDPR stabilisce che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*";
- per "trattamento", ai sensi dell'art. 4 paragrafo 2 del GDPR, si intende "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti 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, anche se non registrati in una banca di dati*";
- per "dati personali", ai sensi dell'art. 4 paragrafo 1 del GDPR, si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); altresì si considera identificabile «la persona fisica 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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*";
- per "Misure di Sicurezza" si intendono le misure di sicurezza e ogni altro obbligo previsti della Normativa Privacy al fine di garantire la sicurezza e la riservatezza dei dati personali, ivi comprese le attività da compiere in caso di Violazione dei dati personali anche al fine di evitare o ridurre gli effetti negativi di tale violazione sugli Interessati;
- per "Responsabile della Protezione dei Dati" prevista dagli articoli 37 e seguenti del GDPR si intende la figura designata in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del GDPR;
- per "Incaricato" si intende la persona fisica autorizzata dal Responsabile di eseguire delle attività che comportano il trattamento dei dati personali ai sensi dell'articolo 29 del GDPR. Questo soggetto (a titolo esemplificativo: un lavoratore dipendente del Responsabile), opera sotto la diretta autorità del Responsabile, eseguendo compiti che implicano l'accesso e la gestione dei dati personali;
- per "Sub-responsabile" si intende la persona giuridica, l'ente, l'impresa individuale o il libero professionista incaricato dal Responsabile di eseguire in outsourcing delle attività che comportano il trattamento dei dati personali ai sensi dell'articolo 28, paragrafo 4 del GDPR;
- per "Violazione dei Dati personali" si intende ogni 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;
- per "categorie particolari di dati personali", ai sensi dell'art. 9 del GDPR, si intende "*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*";
- ai fini del rispetto della Normativa Privacy, ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie attività.

Considerato che:

- a) DISCOVERY e il CONSULENTE TURISTICO hanno stipulato un contratto (di seguito, il "Contratto"), di cui il presente Atto di identificazione costituisce parte integrante e sostanziale.
- b) DISCOVERY ha verificato che il CONSULENTE TURISTICO presenta garanzie sufficienti, in particolare in termini di esperienza, professionalità, risorse, capacità e affidabilità, per mettere in atto le misure tecniche e organizzative necessarie affinché il trattamento dei dati personali nell'esecuzione del Contratto avvenga in conformità con la Normativa Privacy;
- c) con il presente atto, relativamente a tutte le attività di trattamento dei dati necessarie e/o opportune per dare esecuzione agli obblighi concordati tra le Parti, DISCOVERY vincola il CONSULENTE TURISTICO a trattare i dati personali nel rispetto delle istruzioni di seguito fornite.

Tutto ciò premesso, con il presente atto DISCOVERY, nella qualità di Titolare del trattamento,

IDENTIFICA

il CONSULENTE TURISTICO quale **Responsabile del trattamento** (di seguito anche il "**Responsabile**") ai sensi dell'art. 28 del GDPR in relazione al trattamento dei dati personali da effettuarsi in conseguenza ovvero in occasione del Contratto, secondo le modalità e nei limiti di seguito specificati.

1. OGGETTO DELL'ATTO DI IDENTIFICAZIONE

1.1. L'ambito di trattamento consentito ai fini del presente atto da parte del Responsabile è quello strettamente connesso all'esecuzione del Contratto, come descritto nell'**Allegato**

1.

- 1.2. Il trattamento di dati personali effettuato dal Responsabile, sia direttamente sia tramite i suoi Incaricati, che non si riferisce direttamente alle attività previste dal Contratto, non è incluso nel presente Atto di identificazione. Questo include, per esempio ma non in modo limitativo, la raccolta autonoma di dati personali da parte del CONSULENTE TURISTICO relativi ai suoi clienti o potenziali clienti per finalità proprie, che non sono correlate all'adempimento del Contratto. Quindi in tali casi il CONSULENTE TURISTICO non agirà in relazione ai dati personali come Responsabile del trattamento, bensì quale autonomo Titolare del trattamento; parimenti il CONSULENTE TURISTICO che violi le istruzioni di DISCOVERY sarà considerato autonomo Titolare del trattamento (a titolo esemplificativo e non esaustivo: l'utilizzo della casella email aziendale assegnatagli in uso da DISCOVERY per attività o finalità che esulino dal Contratto).

2. DURATA

- 2.1 Il presente Atto di identificazione produce i suoi effetti a partire dalla data della sua sottoscrizione e rimarrà in vigore fino alla data di cessazione del Contratto cui si riferisce.
- 2.2 All'atto di scadenza del Contratto o in caso di cessazione, a qualunque titolo e per qualunque ragione, dell'efficacia del Contratto e conseguentemente del presente Atto di identificazione, il Responsabile provvederà a cessare immediatamente qualsiasi trattamento dei dati personali (a eccezione della eventuale conservazione dei dati trattati in attesa della restituzione al Titolare), procedendo su richiesta esplicita del Titolare alla cancellazione o alla restituzione di tutti i dati personali in un formato interoperabile entro 30 (trenta) giorni dalla richiesta.
- 2.3 Il Responsabile si impegna ad assicurarsi che anche i propri Incaricati si conformino agli obblighi di cui al precedente punto, secondo le modalità e la tempistica ivi indicata.
- 2.4 Il Responsabile riconosce e accetta che nel caso in cui lui e/o uno dei propri Incaricati fosse tenuto per legge o per l'esercizio/difesa in giudizio dei propri interessi a tenere copia, in tutto o in parte, dei dati personali successivamente alla cessazione del Contratto, dovrà essere considerato un autonomo Titolare del trattamento.

3. NATURA, FINALITÀ E MODALITÀ DEL TRATTAMENTO

- 3.1 Il Responsabile riconosce e accetta la natura obbligatoria delle attività oggetto del presente Atto di identificazione.
- 3.2 Il Responsabile del trattamento si impegna a:
- trattare i dati personali al fine di dare esecuzione al Contratto e nei limiti e secondo le modalità di quanto disposto dallo stesso, dal presente Atto di identificazione e dalla Normativa Privacy, attenendosi strettamente alle istruzioni impartite da DISCOVERY e informando immediatamente per iscritto quest'ultimo qualora ritenga che un'istruzione o uno più profili del trattamento sia in violazione della Normativa Privacy o in generale della legge applicabile;
 - trattare solamente i dati personali che sono necessari per dare corretta e piena esecuzione al Contratto o per adempiere a obblighi di legge;
 - trattare i dati personali in modo lecito, secondo correttezza e in piena osservanza dei principi applicabili al trattamento, del presente Atto di identificazione e dei requisiti previsti dalla Normativa Privacy;
 - assistere e collaborare con DISCOVERY in caso di richieste da parte delle autorità competenti, degli Interessati e al fine di conformarsi agli obblighi di cui alla Normativa Privacy, anche con riferimento all'esecuzione delle attività di cui alla Sezione 3 del Capo IV del GDPR e mettendo a disposizione di DISCOVERY tutte le informazioni necessarie per dimostrare il rispetto da parte del Titolare degli obblighi di cui alla Normativa Privacy;
 - consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate da DISCOVERY o da un altro soggetto da questi incaricato, anche ai sensi del successivo articolo 11.

4 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

- 4.1 In conformità con l'articolo 30, paragrafo 2, del GDPR, il Responsabile si impegna, ove rientri tra i soggetti obbligati, a tenere un registro separato continuamente aggiornato di tutte le categorie di attività relative al trattamento dei dati personali svolte per conto di DISCOVERY.
- 4.2 Ove rientri tra i soggetti obbligati, il Responsabile si impegna a fornire prontamente copia del registro di cui all'articolo 4.1 a richiesta di DISCOVERY nei limiti dei trattamenti che il Responsabile svolge per conto del Titolare e/o su richiesta delle autorità competenti nei limiti di quanto indicato dalle stesse.
- 4.3 Il Responsabile si impegna a fornire a DISCOVERY tutte le informazioni relative al trattamento dei dati personali necessarie alla stessa al fine di poter predisporre il registro delle attività di trattamento di cui all'articolo 30 del GDPR.

5 OBBLIGHI DEL RESPONSABILE

- 5.1 Il Responsabile si impegna:
- a fare in modo che i propri Incaricati abbiano accesso e trattino esclusivamente quei dati personali che sono strettamente necessari per dare corretta e piena esecuzione al Contratto o per adempiere a obblighi di legge in ogni caso nei limiti e in conformità con i termini del presente Atto di identificazione, del Contratto e della Normativa Privacy;
 - a consentire il trattamento dei dati personali unicamente a persone autorizzate per iscritto al trattamento che operino sotto la sua direzione e/o autorità che:
 - per esperienza, capacità e formazione risultano idonei ad assicurare il rispetto della Normativa Privacy e che debbano accedervi al fine di poter dare esecuzione al Contratto;
 - siano al corrente degli obblighi previsti dalla Normativa Privacy;
 - abbiano ricevuto dettagliate istruzioni operative circa gli obblighi a cui sono tenuti nel trattamento dei dati personali e in particolare circa le precauzioni da adottarsi per garantire il trattamento dei dati personali in conformità con l'Atto di identificazione e la Normativa Privacy;
 - siano stati istruiti circa le procedure da rispettare in caso di Violazione dei dati personali;
 - ricevano periodica formazione in relazione ai principi previsti dalla Normativa e agli obblighi richiamati dalla stessa;
 - siano vincolati a garantire la riservatezza in merito a tutte le informazioni conosciute in relazione all'esecuzione del Contratto;
 - ad approntare misure fisiche, tecniche e organizzative che garantiscano che:
 - ciascun Incaricato abbia accesso esclusivamente ai dati personali che può trattare in base al suo profilo di autorizzazione, tenendo conto dell'attività che deve compiere nell'esecuzione del Contratto;
 - eventuali trattamenti dei dati personali in violazione del Contratto e/o della Normativa Privacy siano prontamente identificati e notificati a DISCOVERY, anche in conformità alla procedura e alla tempistica di cui all'articolo 8 in caso di Violazione dei dati personali;
 - alla cessazione del rapporto tra Responsabile e l'Incaricato (ivi compresi i casi di cessazione del rapporto lavorativo o di collaborazione), quest'ultimo cessi immediatamente il trattamento dei dati personali e non conservi nella propria disponibilità, a qualunque titolo e in qualunque formato, copia dei dati;

- d) informare tempestivamente DISCOVERY di ogni questione rilevante ai fini del rispetto della normativa in materia di protezione dei dati personali;
- e) comunicare prontamente a DISCOVERY qualsiasi situazione di cui sia venuta a conoscenza che possa compromettere il corretto trattamento dei dati personali;
- f) ove applicabile, in relazione al Provvedimento Generale del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema", come modificato dal Provvedimento del 25 giugno 2009), a:
 - i) garantire che il sistema informatico utilizzato in relazione al rapporto di cui al Contratto venga gestito e amministrato esclusivamente da parte di personale specificamente nominato come Amministratore di Sistema e che sia in possesso dei requisiti di esperienza, capacità e affidabilità richiesti dai Provvedimenti sopra richiamati;
 - ii) mantenere a disposizione di DISCOVERY un aggiornato elenco dei soggetti designati quali Amministratori di Sistema;
 - iii) con cadenza annuale, verificare l'operato degli Amministratori di Sistema, in modo da controllare la rispondenza alle istruzioni fornite.
- g) comunicare al Titolare ogni informazione che possa incidere sulla sussistenza delle garanzie prescritte a norma dell'art. 28 paragrafo 1 del Regolamento (a titolo esemplificativo: modifiche societarie; variazioni patrimoniali; perdita di certificazioni; notizie di procedimenti e/o sanzioni in materia di trattamento di dati personali; ecc.).

6 SUB-RESPONSABILE

6.1 DISCOVERY non autorizza il Responsabile a ricorrere a uno o più Sub-responsabili per l'adempimento delle attività di trattamento connesse all'esecuzione del Contratto.

7 MISURE DI SICUREZZA

- 7.1 Il Responsabile si impegna ad adottare correttamente tutte le Misure di Sicurezza in conformità con i termini di cui alla Normativa Privacy e al presente Atto.
- 7.2 In particolare, il Responsabile, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati personali, nonché del rischio che il trattamento presenta per i diritti e le libertà delle persone fisiche e della probabilità e gravità dello stesso, si impegna a mettere in atto le misure tecniche e organizzative indicate nell'[Allegato 3](#).

8 VIOLAZIONE DEI DATI PERSONALI

- 8.1 Nell'ipotesi in cui si verifichi una Violazione dei dati personali, il Responsabile dovrà:
 - a) informare senza ingiustificato ritardo e, comunque, entro 48 ore dalla conoscenza, DISCOVERY, inviando una comunicazione via email all'indirizzo indicato all'articolo 16, redatta sulla base del modulo allegato al presente Atto di identificazione ([Allegato 2](#));
 - b) di concerto con DISCOVERY, adottare ogni necessaria misura di sicurezza fisiche e/o logiche e/o organizzative per minimizzare i rischi di qualsivoglia natura per i dati personali derivanti dalla Violazione dei dati personali e porre in essere ogni eventuale operazione necessaria per porre rimedio alla Violazione dei dati personali, per attenuarne i possibili effetti negativi e per investigarne le cause.

9 DIRITTI DEGLI INTERESSATI

- 9.1 Il Responsabile dovrà garantire l'effettivo esercizio dei diritti riconosciuti agli Interessati dalla Normativa Privacy, impegnandosi a notificare per iscritto a DISCOVERY entro un termine di sette giorni qualsivoglia richiesta di esercizio di tali diritti eventualmente formulata da parte degli Interessati e relativa alle attività di cui al Contratto.
- 9.2 Il Responsabile si obbliga a collaborare con DISCOVERY per garantire che le richieste di esercizio dei diritti degli Interessati previsti dagli artt. 12 e ss. del GDPR, incluse le richieste di opposizione al trattamento e le richieste di portabilità dei dati personali, siano soddisfatte entro i tempi e secondo le modalità di legge e, più in generale, per assicurare il pieno rispetto della Normativa Privacy. A tal fine, il Responsabile dichiara e garantisce di avere misure tecniche e organizzative adeguate per consentire l'esercizio dei diritti degli Interessati ai sensi della Normativa Privacy.

10 COMUNICAZIONE E TRASFERIMENTO DEI DATI PERSONALI

- 10.1 Il Responsabile si impegna a:
 - c) non agire quale Titolare autonomo del trattamento in relazione ai dati personali trattati per conto di DISCOVERY, astenendosi dal diffondere o comunicare i predetti dati a terzi (ivi compresi eventuali Sub-responsabili) a meno che ciò non sia espressamente previsto dal Contratto e fatto salvo quanto previsto ai paragrafi 1.2 e 2.4 del presente Atto di identificazione;
 - d) trasferire i dati personali al di fuori dello Spazio Economico Europeo (SEE) solo previa autorizzazione scritta di DISCOVERY e, in assenza di decisione di adeguatezza che interessi il Paese terzo di destinazione ai sensi dell'art. 45 del GDPR, previa verifica dell'adeguatezza delle condizioni applicate per il trasferimento dei dati personali tra quelle indicate all'art. 46 del GDPR, salvo che non si possa applicare una delle deroghe di cui all'art. 49 del GDPR.

11 AUDIT

- 11.1 Il Responsabile riconosce e accetta che DISCOVERY potrà valutare periodicamente il rispetto da parte del Responsabile degli obblighi normativamente e/o contrattualmente imposti in materia di trattamento dei dati personali trattati in esecuzione del Contratto. A tal fine, DISCOVERY avrà il diritto di accedere direttamente o tramite propri incaricati, con un preavviso minimo di sette giorni lavorativi, ai locali e alle componenti del sistema informativo utilizzati dal Responsabile, laddove ciò sia ritenuto necessario per verificare che il Responsabile agisca in conformità alla Normativa Privacy o per accertare eventuali Violazioni dei Dati.
- 11.2 L'accesso a detti luoghi sarà consentito dal Responsabile solo ai loro Incaricati e ai rappresentanti o incaricati di DISCOVERY che abbiano ragionevolmente provato la loro identità e abbiano provato di essere stati debitamente autorizzati in conformità con il presente Atto di identificazione.

12 CORRISPETTIVO

- 12.1 Il Responsabile riconosce e accetta che il corrispettivo per l'attività propria di Responsabile del trattamento ai sensi del presente Atto di identificazione è da intendersi ricompreso nel corrispettivo previsto dal Contratto. Nessun corrispettivo ulteriore sarà dovuto a IL CONSULENTE TURISTICO in relazione alle attività oggetto del presente Atto di identificazione.

13 COLLABORAZIONE DEL RESPONSABILE IN EVENTUALI PROCEDIMENTI RELATIVI AI DATI PERSONALI TRATTATI

13.1 Il Responsabile si impegna a collaborare attivamente con DISCOVERY riguardo a ogni eventuale procedimento relativo a dati personali trattati dal Responsabile, sia esso giudiziale o amministrativo, ivi compresi procedimenti davanti al Garante per la protezione dei dati personali o altre autorità competenti. Rimane inteso che tutti i costi derivanti da eventuali accertamenti giudiziari o amministrativi di responsabilità saranno a carico del soggetto che abbia compiuto la violazione oggetto dell'accertamento.

14 MANLEVA E RISARCIMENTO DANNI

14.1 Il Responsabile si obbliga a manlevare, tenere indenne e/o risarcire il Titolare per ogni danno patrimoniale e non patrimoniale, costo, onere e spesa, incluse eventuali spese legali e danni reputazionali, derivanti da eventuali:

- a) violazioni della Normativa Privacy o del presente Atto di Identificazione o delle istruzioni impartite dal Titolare;
- b) sanzioni comminate dalle autorità competenti, ivi compreso il Garante per la protezione dei dati personali, dovute alla condotta del Responsabile;
- c) azioni giudiziali da parte degli Interessati o terzi per violazioni della Normativa Privacy e/o del Contratto e/o del presente Atto di Identificazione dovute alla condotta del Responsabile.

15 RISOLUZIONE

15.1 Impregiudicato ogni ulteriore diritto di DISCOVERY, qualora il CONSULENTE TURISTICO risulti inadempiente rispetto alle disposizioni del presente Atto di Identificazione e/o alle istruzioni impartite dal Titolare, il Contratto si risolverà a norma dell'art. 1456 c.c.

16 DISPOSIZIONI CONCLUSIVE

16.1 Ogni comunicazione tra DISCOVERY e il Responsabile relativa al trattamento di dati personali dovrà avvenire tramite email o posta elettronica certificata ai seguenti indirizzi:

Per DISCOVERY:

All'attenzione dell'Amministratore Unico

E-mail: info@travelangels.it

PEC: discoveryzahresrl@pec.it

Per il Responsabile

All'attenzione di _____

E-mail _____

PEC _____

16.2 Il presente Atto di identificazione è regolato dalla legge italiana. Ogni controversia derivante dal presente Atto sarà rimessa alla competenza esclusiva del foro indicato nel Contratto.

16.3 Ogni modifica dell'Atto di identificazione sarà valida solo se effettuata per iscritto. Le parti si impegnano reciprocamente a modificare il presente Atto in conseguenza di una modifica della Normativa Privacy, ivi compresi provvedimenti, linee guida od opinioni da parte delle autorità competente.

16.4 In caso di contrasto tra l'Atto di identificazione e la parte rimanente del Contratto, il presente Atto prevarrà in merito a questioni relative al trattamento dei dati personali.

16.5 L'eventuale inefficacia e/o invalidità, totale o parziale, di una o più clausole del presente Atto di Identificazione non comporterà l'invalidità delle altre, le quali dovranno ritenersi pienamente valide ed efficaci.

Per DISCOVERY

Per il **Responsabile**

Data: 7 giugno 2024

Data: 7 giugno 2024

Ruolo: Amministratore Unico

Ruolo: Consulente turistico

Nome e cognome: Deborah Rainis

Nome e cognome: _____

Firma:



Firma: _____

Ai sensi e per gli effetti degli articoli 1341 e 1342 del codice civile, il Responsabile dichiara di aver compreso e di accettare espressamente i seguenti articoli del presente Atto di Identificazione: 10 (Comunicazione e trasferimento dei dati personali), 13 (Collaborazione del Responsabile in eventuali procedimenti relativi ai dati personali trattati), 14 (Manleva e Risarcimento Danni), 15 (Risoluzione) e 16.2.(Disposizioni conclusive).

Firma: _____

ALLEGATO 1
DESCRIZIONE DEL TRATTAMENTO

Categoria di interessati	Natura dei dati personali	Tipologia di dati
Clienti (anche potenziali) e familiari	<input checked="" type="checkbox"/> Dati personali e identificativi <input type="checkbox"/> Dati particolari <input type="checkbox"/> Dati relativi a reati/condanne penali	Dati identificativi e di contatto. Dati economici e contabili.
Clienti (anche potenziali) e familiari	<input type="checkbox"/> Dati personali e identificativi <input checked="" type="checkbox"/> Dati particolari <input checked="" type="checkbox"/> Dati relativi a reati/condanne penali	Dati relativi allo stato di salute. Dati giudiziari per ESTA e visti.
Fornitori	<input checked="" type="checkbox"/> Dati personali e identificativi <input type="checkbox"/> Dati particolari <input type="checkbox"/> Dati relativi a reati/condanne penali	Dati identificativi e di contatto. Dati economici e contabili.

Finalità per le quali i dati personali sono trattati per conto del Titolare del trattamento:

Il trattamento dei dati personali è effettuato per l'adempimento del contratto, ossia fornire ai diretti interessati la consulenza tecnica necessaria in ambito turistico per soddisfare le loro necessità attraverso le idonee soluzioni ed i servizi e prodotti turistici dell'Agenzia.

ALLEGATO 2
MODULO PER NOTIFICA DI VIOLAZIONI DI DATI

1. Soggetto che compila il modulo relativo alla Violazione dei dati personali e nome della società (ivi compresi eventuali Sub-responsabili) che sono stati oggetto della Violazione dei dati personali
2. Data e orario in cui la Violazione dei Dati si è verificata o in cui il Responsabile o l'eventuale Sub-Responsabile ne sono venuti a conoscenza
3. Natura della Violazione dei dati personali che si è verificata
4. Categorie e numero approssimativo di Interessati i cui dati personali sono stato oggetto della Violazione dei dati personali
5. Categorie e il numero approssimativo di registrazioni dei dati personali oggetto della Violazione dei dati personali
6. Nome e i dati di contatto del Responsabile della Protezione dei Dati del Responsabile, se previsto
7. Probabili conseguenze della Violazione dei dati personali

ALLEGATO 3 ISTRUZIONI E MISURE DI SICUREZZA

CAPITOLO 1: INTRODUZIONE

1.1 **Scopo dell'Allegato**: Questo allegato è progettato per fornire ai consulenti turistici istruzioni chiare e dettagliate sull'uso sicuro e responsabile delle risorse informatiche. Il suo scopo è garantire che tutte le attività informatiche siano condotte in modo sicuro, proteggendo i dati aziendali e quelli dei clienti e promuovendo una cultura della sicurezza informatica all'interno dell'organizzazione.

1.2 **Importanza della Sicurezza Informatica**: La sicurezza informatica è fondamentale per proteggere l'integrità e la riservatezza delle informazioni aziendali e personali. In un mondo sempre più digitale, è essenziale che i consulenti siano consapevoli delle minacce alla sicurezza, come il phishing, i malware e le violazioni dei dati, e sappiano come prevenirle. Questo allegato serve come guida per navigare in modo sicuro nell'ambiente informatico, riducendo i rischi e aumentando la consapevolezza sulla sicurezza.

CAPITOLO 2: ACCESSO AI SISTEMI

2.1 **Procedure di Accesso ai Sistemi Informatici**: In questo capitolo vengono delineate le procedure specifiche per l'accesso ai vari sistemi informatici utilizzati dall'agenzia di viaggi:

- webmail: accesso tramite <https://webmail.aruba.it/> e proprie credenziali. Il cambio password può essere fatto all'interno della webmail dalle impostazioni.

- Aves: accesso al server tramite software desktop remoto con le credenziali fornite da Datagest, non modificabili in quanto utilizzate per accedere da tutta l'organizzazione. Successivo login al software gestionale con username e password personali. Per cambio password è necessario contattare Datagest oppure la Travel Angels.

- Zoho: accesso tramite <https://www.zoho.com/> o app Cliq con proprie credenziali. La password può essere cambiata da <https://accounts.zoho.eu/> dal menu Sicurezza.

Procedure Generali: Tutti i software richiedono autenticazione forte. Le password devono essere cambiate ogni 6 mesi e devono soddisfare criteri di complessità definiti. In caso di sospetto abuso o smarrimento delle credenziali, il consulente deve immediatamente segnalare l'incidente a mezzo e-mail scrivendo a info@travelangels.it.

CAPITOLO 3: SICUREZZA DEI DISPOSITIVI

3.1 **Requisiti di Sicurezza per Dispositivi Personali**: I requisiti di sicurezza includono l'installazione di software antivirus aggiornato, l'attivazione di un firewall personale, il mantenimento degli aggiornamenti per sistema operativo e software applicativi, e la crittografia completa dell'hard disk per proteggere i dati.

3.2 **Procedure di Uso Sicuro**: I consulenti devono seguire queste linee guida per un uso sicuro dei dispositivi: - Evitare reti Wi-Fi pubbliche non protette per accedere a dati aziendali. - Non lasciare dispositivi incustoditi in luoghi pubblici. - Utilizzare password complesse e uniche.

3.3 **Responsabilità dei Consulenti**: È responsabilità dei consulenti garantire la sicurezza dei loro dispositivi personali e avvisare tempestivamente l'agenzia in caso di smarrimento, furto o potenziale compromissione di tali dispositivi.

CAPITOLO 4: CONNESSIONE SICURA

4.1 **Utilizzo di Rete Sicura e VPN** I consulenti devono sempre utilizzare reti Wi-Fi protette, specialmente quando accedono a informazioni sensibili dell'agenzia. È obbligatorio l'impiego di reti VPN (Virtual Private Network) fornite dall'azienda per garantire una connessione sicura durante l'accesso ai sistemi aziendali da remoto.

4.2 **Precauzioni per Connessioni da Luoghi Pubblici** Quando si utilizzano reti pubbliche, i consulenti devono evitare transazioni che richiedono l'inserimento di informazioni sensibili, assicurarsi che la connessione sia crittografata e sicura, e non salvare password o altri dati sensibili su dispositivi utilizzati in luoghi pubblici.

CAPITOLO 5: GESTIONE E UTILIZZO DEGLI ACCOUNT DI POSTA ELETTRONICA ASSEGNATI AI CONSULENTI

5.1 **Assegnazione dell'Account di Posta Elettronica** Ad ogni consulente verrà assegnato un account di posta elettronica unico e personale, che deve essere utilizzato esclusivamente per scopi professionali e inerenti alle attività di cui al Contratto. L'account è da considerarsi uno strumento di lavoro e proprietà del Titolare.

5.2 **Utilizzo Responsabile dell'Account di Posta** È vietato l'utilizzo dell'account di posta per comunicazioni personali non autorizzate, invio o ricezione di materiale offensivo, illegale o inappropriato, e per attività che possano compromettere la sicurezza o la reputazione del Titolare.

5.3 **Sicurezza e Gestione delle Comunicazioni Elettroniche** I consulenti sono responsabili della sicurezza del proprio account di posta elettronica e devono seguire linee guida precise per la gestione delle comunicazioni, inclusa l'archiviazione ordinata e il rispetto delle politiche di conservazione e cancellazione dei dati in conformità con il GDPR.

CAPITOLO 6: USO DEI PORTALI DEI TOUR OPERATOR

6.1 **Procedure di Accesso e Gestione delle Informazioni sui Portali** I consulenti devono accedere ai portali utilizzando solo le credenziali fornite dall'agenzia, evitare la memorizzazione automatica delle password nei browser, e disconnettersi sempre al termine di ogni sessione. È essenziale inserire o aggiornare le informazioni dei clienti seguendo le procedure specifiche di ogni portale.

6.2 **Sicurezza e Riservatezza** Tutte le informazioni reperite sui portali devono essere trattate con la massima riservatezza. I consulenti non devono utilizzare le informazioni dei clienti (e/o potenziali clienti) per scopi non autorizzati e sono tenuti a segnalare immediatamente qualsiasi anomalia o problema di sicurezza riscontrato.

CAPITOLO 7: PROTEZIONE DEI DATI DEI CLIENTI

7.1 **Responsabilità nella Gestione dei Dati** I consulenti hanno il dovere di trattare tutti i dati dei clienti (e/o potenziali clienti) con la massima riservatezza. L'accesso a tali dati è permesso solo per scopi lavorativi legittimi e autorizzati.

7.2 **Conservazione e Utilizzo dei Dati** I dati dei clienti (e/o potenziali clienti) devono essere salvati esclusivamente sui sistemi di archiviazione sicuri forniti dall'agenzia. È proibito l'uso di dispositivi di archiviazione esterni o servizi cloud personali per memorizzare tali dati.

7.3 **Crittografia e Protezione dei Dati** Per garantire ulteriore protezione, l'hard disk del dispositivo utilizzato per il lavoro deve essere completamente criptato.

7.4 **Procedure di Backup e Ripristino** I consulenti devono seguire le procedure stabilite dall'agenzia per il backup regolare dei dati e devono essere a conoscenza delle procedure per il ripristino dei dati in caso di perdita o danneggiamento.

7.5 **Cancellazione Sicura dei Dati** Quando i dati dei clienti non sono più necessari, devono essere cancellati in modo sicuro e conforme alle politiche aziendali e alle normative sulla privacy.

CAPITOLO 8: AGGIORNAMENTI SOFTWARE E MANUTENZIONE

8.1 **Importanza degli Aggiornamenti di Sicurezza** È essenziale eseguire regolarmente gli aggiornamenti software sui dispositivi utilizzati per il lavoro, compresi i sistemi operativi e le applicazioni. Anche i software di sicurezza, come antivirus e firewall, devono essere sempre aggiornati.

8.2 **Procedura di Aggiornamento** I consulenti devono seguire le notifiche di aggiornamento fornite dai sistemi operativi e dalle applicazioni.

8.3 **Manutenzione Regolare dei Dispositivi** Deve essere effettuato un controllo periodico per assicurarsi che i dispositivi funzionino correttamente e in modo sicuro.

CAPITOLO 9: FORMAZIONE E CONSAPEVOLEZZA SULLA SICUREZZA

9.1 **Importanza della Formazione Continua** I consulenti sono tenuti a partecipare a sessioni di formazione periodiche sulla sicurezza informatica e sulla protezione dei dati, organizzate dall'agenzia. È importante mantenere aggiornate le proprie conoscenze sulle minacce alla sicurezza informatica e sulle migliori pratiche per prevenirle.