

# Accordo sul trattamento dei dati personali ai sensi di incarico

<b>I. Preambolo.....</b>	<b>2</b>
1. Definizioni dei Termini.....	2
2. Ruoli Privacy.....	4
3. Obblighi di swizzonic .....	5
4. Obblighi del Cliente .....	5
5. Consenso Subappalto .....	6
6. Trasferimento di Dati Personali .....	6
7. Cooperatione e Respsibilità .....	7
8. Diritti degli Interessati .....	7
9. Restituzione e cancellazione Dati.....	7
10. Trasferimenti.....	7
11. Violazione della Privacy .....	8
12. Recupero in emergenza e garanzia della continuità aziendale.....	8
13. Incari .....	8
<b>ALLEGATO 1.....</b>	<b>8</b>
<b>ALLEGATO 2.....</b>	<b>9</b>
<b>ALLEGATO 3.....</b>	<b>13</b>

# Accordo sul trattamento dei dati personali ai sensi di incarico

## I. PREAMBOLO

Considerato che:

A. Le leggi applicabili sulla protezione dei dati consentono a ogni titolare del trattamento dei dati personali, persona fisica o giuridica, ente pubblico o altra istituzione o associazione, di nominare una persona fisica o giuridica che agisca in qualità di responsabile del trattamento per l'elaborazione dei dati personali per conto del titolare, a condizione che tale soggetto garantisca, sulla base della propria esperienza, competenza e affidabilità, il rispetto delle leggi applicabili sulla protezione dei dati, anche per quanto riguarda gli aspetti di sicurezza.

B. Il responsabile del trattamento nominato deve fornire garanzie sufficienti per attuare misure tecniche e organizzative adeguate volte a proteggere i dati personali e i diritti degli interessati.

C. Il presente accordo di trattamento dei dati, unitamente ai suoi allegati (congiuntamente denominati "DPA" - Data Processing Agreement), è stipulato tra il Cliente (di seguito "Cliente"), ossia la persona fisica o giuridica che ha acquistato il/i Servizio/i come di seguito definito/i e le cui informazioni sono indicate di seguito, e Swizzonic AG ("Swizzonic"); il Cliente e Swizzonic sono congiuntamente indicati come "Parti" e individualmente come "Parte" e con il presente DPA intendono documentare l'accordo delle Parti relativo al trattamento dei dati personali del Cliente ai sensi dei requisiti delle leggi applicabili sulla protezione dei dati.

D. Swizzonic mette a disposizione del Cliente il/i Servizio/i attivato/i dal Cliente ("Servizio/i"), in conformità alle condizioni contrattuali indicate nell'ordine/i di servizio e nei termini e condizioni generali, disponibili congiuntamente al seguente link <https://www.swizzonic.ch/company/legal/condizioni-general/?lang=it> ("TCG"), e può, al fine di fornire tali servizi nell'ambito del presente DPA, trattare dati personali per conto del Cliente.

E. Più precisamente, lo scopo/i scopi del trattamento dei dati personali del Cliente in relazione al Servizio è/sono descritti nell'Allegato 1.

F. Il Cliente riconosce che l'uso del Servizio può essere soggetto alle leggi sulla protezione dei dati di giurisdizioni applicabili che prevedono requisiti specifici in relazione al trattamento dei dati personali.

G. Le Parti hanno stipulato il presente DPA per garantire il rispetto delle leggi applicabili sulla protezione dei dati e per stabilire misure di protezione e procedure per il trattamento lecito dei dati personali. Il Cliente conferma che le disposizioni contenute nel presente DPA riflettono gli obblighi che Swizzonic deve rispettare ai sensi delle leggi applicabili sulla protezione dei dati in relazione al trattamento dei dati personali del Cliente per la fornitura del Servizio. Di conseguenza, Swizzonic si impegna a rispettare le disposizioni contenute nel presente DPA.

Il presente preambolo fa parte integrante del DPA.

## 1. DEFINIZIONI DEI TERMINI

Salvo diversa definizione nella presente DPA, tutti i termini in maiuscolo utilizzati nel presente documento hanno il significato loro attribuito nei Termini e Condizioni Generali (TCG). In caso di conflitto o discrepanza

tra le disposizioni sulla protezione dei dati contenute nella presente DPA e quelle del contratto principale di fornitura del servizio, prevale la presente DPA.

“Decisione di adeguatezza” indica una decisione giuridicamente vincolante della Commissione Europea e/o del Consiglio Federale Svizzero che autorizza il trasferimento di dati personali dall’Area Economica Europea e/o dalla Svizzera verso un paese terzo riconosciuto come adeguato in relazione alla normativa sulla protezione dei dati applicabile.

“Leggi applicabili sulla protezione dei dati” indica, negli Stati membri dell’UE, il Regolamento nonché le leggi complementari sulla protezione dei dati negli Stati membri dell’UE, inclusi tutti i linee guida e/o codici di condotta emessi dall’autorità di controllo competente all’interno dell’UE; e/o nei Paesi non appartenenti all’UE, qualsiasi legge sulla protezione dei dati applicabile relativa alla tutela e al trattamento lecito dei dati personali.

“Cliente” indica la persona che ha acquistato il Servizio.

“Dati personali del Cliente” indica i dati personali relativi agli interessati e trattati in relazione al Servizio fornito da Swizzonic al Cliente.

“Titolare del trattamento” indica generalmente la persona fisica o giuridica, l’autorità, l’istituzione o altro organismo che, da solo o congiuntamente ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

“Esportatore dei dati” ha il significato stabilito nelle Clausole Contrattuali Standard.

“Importatore dei dati” ha il significato stabilito nelle Clausole Contrattuali Standard.

“Responsabile del trattamento” indica generalmente una persona fisica o giuridica, un’autorità, un’istituzione o altro organismo che tratta dati personali per conto del titolare del trattamento.

“Interessato” ha il significato attribuito dalle leggi applicabili sulla protezione dei dati.

“Diritti dell’interessato” indica i diritti spettanti all’interessato ai sensi delle leggi applicabili sulla protezione dei dati. I “Diritti dell’interessato” comprendono, ad esempio, il diritto di ottenere dal titolare del trattamento l’accesso ai dati personali, la rettifica o la cancellazione, la limitazione del trattamento, l’opposizione al trattamento e il diritto alla portabilità dei dati.

“DPA” indica il presente accordo globale di trattamento dati unitamente agli allegati 1, 2 e 3.

“SEE” indica lo Spazio Economico Europeo.

“UE” indica l’Unione Europea.

“Elenco dei sub-responsabili” indica l’elenco disponibile su richiesta scritta all’indirizzo [legal@swizzonic.com](mailto:legal@swizzonic.com).

“Sub-responsabili extra-SEE/Svizzera” indica qualsiasi soggetto che agisce in qualità di responsabile del trattamento (o sub-responsabile) e che tratta dati personali del Cliente per la fornitura del Servizio in un paese al di fuori del SEE e della Svizzera.

“Titolari extra-SEE/Svizzera” indica qualsiasi soggetto che agisce in qualità di titolare del trattamento, a cui Swizzonic fornisce servizi e che è stabilito in un paese al di fuori del SEE e della Svizzera.

“Dati personali” indica tutte le informazioni relative a una persona fisica identificata o identificabile; si considera identificabile una persona fisica che può essere identificata, direttamente o indirettamente, in particolare mediante l’assegnazione a un identificativo come nome, numero di identificazione, dati di localizzazione, identificatore online o a uno o più elementi specifici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Per evitare dubbi, “dati personali” ha il significato attribuito dal Regolamento e dalle leggi applicabili sulla protezione dei dati.

“Trattamento” o “trattare” indica qualsiasi operazione o insieme di operazioni effettuate con o senza l’ausilio di processi automatizzati relative a dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione.

“Regolamento” indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

“Violazione della protezione dei dati personali” indica una violazione della sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati.

“Servizio/i” ha il significato indicato alla lettera D. del preambolo.

“Servizi con sub-responsabili extra-SEE/Svizzera” indica i servizi “Micro Site, Simply Site e Simply Shop”, il cui ordine di servizio è disponibile al seguente link: <https://www.swizzonic.ch/company/legal/prodotti-sitoweb/?lang=it>.

“Categorie particolari di dati personali” indica i dati personali da cui emergono l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l’appartenenza sindacale, nonché il trattamento di 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 di una persona fisica, inclusi dati relativi a condanne penali e reati o misure di sicurezza, procedimenti amministrativi e sanzioni nonché misure di sicurezza sociale.

“Clausole contrattuali standard” indica le clausole contrattuali standard per il trasferimento di dati personali verso paesi terzi ai sensi del Regolamento, approvate dalla Commissione Europea con la decisione di esecuzione (UE) 2021/914 e riconosciute dall’EDPB, fatto salvo quanto eventualmente richiesto dall’EDPB in integrazione.

“Sub-responsabile” indica un soggetto incaricato da Swizzonic che assiste Swizzonic nel trattamento dei dati personali del Cliente ai fini dell’adempimento degli obblighi previsti dal presente DPA (o che effettua il trattamento stesso), come indicato nell’elenco dei sub-responsabili approvato dal Cliente ai sensi dell’art. 5 della presente DPA.

“Autorità di controllo” indica qualsiasi autorità competente a vigilare e far rispettare l’applicazione delle leggi applicabili sulla protezione dei dati in relazione al trattamento dei dati personali del Cliente nell’ambito della fornitura del Servizio.

## 2. RUOLI PRIVACY

### 2.1. Le Parti concordano che:

- a) Il Cliente è il Titolare del trattamento dei Dati personali del Cliente, salvo che e quando il Cliente agisca come Responsabile del trattamento dei Dati personali del Cliente per conto di un terzo che agisca esso stesso come Titolare o Responsabile del trattamento. Il Cliente, o il Titolare del trattamento pertinente, determina le finalità della raccolta e del trattamento dei Dati personali del Cliente;
- b) Swizzonic agisce, in ogni caso, come Responsabile del trattamento dei Dati personali del Cliente per la fornitura del Servizio; e
- c) la presente DPA disciplina il rapporto tra le Parti in termini di rispettivi doveri e obblighi

concernenti il trattamento dei Dati personali del Cliente da parte di Swizzonic, in qualità di Responsabile del trattamento, nell'ambito della fornitura del Servizio.

### 3. OBBLIGHI DI SWIZZONIC

3.1. Il Cliente o il rispettivo Titolare del trattamento determina le finalità del trattamento dei dati personali del Cliente nell'ambito della fornitura del Servizio.

3.2. In relazione alla fornitura del Servizio, Swizzonic si impegna a rispettare i seguenti obblighi, inclusi quelli definiti negli Allegati 1 e 2 della presente DPA:

- a) Swizzonic tratta i dati personali del Cliente solo nella misura necessaria per la fornitura del Servizio e esclusivamente in conformità alle istruzioni scritte del Cliente contenute nella presente DPA;
- b) Swizzonic informa il Cliente qualora ritenga che una istruzione scritta del Cliente violi le leggi sulla protezione dei dati applicabili. Tuttavia, Swizzonic non è in alcun caso obbligata a effettuare una verifica legale esaustiva in merito a una istruzione scritta del Cliente;
- c) Swizzonic, in qualità di Responsabile del trattamento, informa tempestivamente il Cliente di qualsiasi contatto o comunicazione ricevuta da un'autorità di controllo relativa al trattamento dei dati personali del Cliente. Le Parti riconoscono e concordano che la responsabilità per la risposta a tali richieste spetta al Cliente e non a Swizzonic;
- d) Swizzonic ha implementato misure operative, tecniche e organizzative - incluse quelle descritte nell'Allegato 2 della presente DPA - finalizzate a proteggere i dati personali del Cliente. Le Parti riconoscono e concordano che Swizzonic è espressamente autorizzata ad adottare misure alternative ragionevoli o a utilizzare sedi alternative, a condizione che il livello di sicurezza delle misure o delle sedi sia mantenuto o migliorato rispetto a quanto indicato;
- e) Qualora Swizzonic divulghi dati personali del Cliente al proprio personale incaricato direttamente ed esclusivamente della fornitura del Servizio, Swizzonic garantisce che tale personale: i) sia vincolato alla riservatezza o soggetto ad un obbligo legale equivalente di segretezza; e ii) tratti i dati personali del Cliente in conformità alle istruzioni di Swizzonic e agli obblighi previsti dalla presente DPA.

### 4. OBBLIGHI DEL CLIENTE

4.1. Il Cliente riconosce e accetta che, per la fornitura del Servizio da parte di Swizzonic, è necessaria la trasmissione dei dati personali del Cliente a Swizzonic. Il Cliente si impegna a verificare se le misure di sicurezza elencate nell'Allegato 2 del presente contratto siano compatibili con le tipologie di dati personali che intende affidare a Swizzonic.

4.2. Il Cliente garantisce e assicura che:

- a) dispone di una base giuridica adeguata (ad esempio, consenso dell'interessato, interesse legittimo, autorizzazione dell'autorità di controllo competente, ecc.) per trattare e trasmettere a Swizzonic i dati personali del Cliente nell'ambito della fornitura del Servizio; e
- b) le disposizioni stabilite nella presente DPA riflettono gli obblighi che le leggi applicabili impongono a Swizzonic in relazione al trattamento dei dati personali del Cliente nell'ambito della prestazione del Servizio.

## 5. CONSENSO SUBAPPALTO

5.1. Il Cliente riconosce, accetta e acconsente che, esclusivamente per la finalità della fornitura del Servizio e nel rispetto delle disposizioni della presente DPA, i dati personali del Cliente possano essere trattati da Swizzonic o dai suoi sub-processor, come indicato nell'elenco dei sub-processor.

5.2. Ai sensi dell'art. 5.1, Swizzonic dispone di un'autorizzazione generale a incaricare sub-processor, a condizione che Swizzonic:

- a) fornisca preventivamente al Cliente informazioni sull'identità dei sub-processor secondo l'elenco dei sub-processor e informi il Cliente di eventuali modifiche, affinché questi possa opporsi all'incarico;
- b) stipuli con i sub-processor accordi contenenti gli stessi obblighi relativi al trattamento dei dati personali del Cliente come stabilito nella presente DPA;
- c) eserciti una dovuta diligenza nella selezione dei sub-processor e rimanga responsabile del rispetto degli obblighi previsti dalla presente DPA da parte di questi ultimi;
- d) fornisca al Cliente, su richiesta, informazioni adeguate sulle misure e precauzioni adottate da Swizzonic e dai suoi sub-processor per assicurare il rispetto pratico della presente DPA.

## 6. TRASFERIMENTO DI DATI PERSONALI

6.1. Qualora il Cliente acquisti uno o più Servizi che prevedano l'impiego di sub-processor non appartenenti allo Spazio Economico Europeo (SEE) o alla Svizzera, Swizzonic potrà, ai sensi degli artt. 5.1 e 5.2, trasferire dati personali del Cliente a uno o più di tali sub-processor. Questi ultimi saranno considerati, ai sensi delle Clausole Contrattuali Standard, come Importatori di dati. Nel caso in cui per il relativo sub-processor non appartenente al SEE o alla Svizzera non sia stato adottato un decisione di adeguatezza, Swizzonic garantisce che sono state concluse Clausole Contrattuali Standard con il sub-processor interessato, applicando esclusivamente le disposizioni del MODULO TRE: trasferimento da processore a processore (esclusi gli altri moduli). Qualora previsto dal diritto applicabile sulla protezione dei dati, Swizzonic si impegna inoltre a concludere Clausole Contrattuali Standard anche per il trasferimento di dati personali del Cliente dalla Svizzera a sub-processor nel SEE.

6.2. Nessuna disposizione della presente DPA potrà essere interpretata come prevalente rispetto a una clausola contraddittoria delle Clausole Contrattuali Standard.

6.3. Su richiesta, il Cliente potrà prendere visione delle Clausole Contrattuali Standard. Nella misura necessaria a proteggere segreti commerciali o altre informazioni confidenziali, inclusi dati personali, Swizzonic avrà il diritto di oscurare parti delle Clausole Contrattuali Standard prima della loro comunicazione.

6.4. Il Cliente riconosce che è sua responsabilità adempiere a tutte le ulteriori disposizioni legali applicabili affinché il trasferimento dei dati personali a Swizzonic e ai sub-processor non appartenenti al SEE o alla Svizzera avvenga in conformità con la normativa vigente sulla protezione dei dati.

6.5. Qualora il Cliente sia un Titolare del trattamento non appartenente al SEE o alla Svizzera, Swizzonic e il Cliente convengono che le Clausole Contrattuali Standard sono incorporate mediante rinvio nella presente DPA, relativamente a ciascun trasferimento di dati personali dal Titolare del trattamento non appartenente al SEE o alla Svizzera a Swizzonic nell'ambito della fornitura del Servizio. In tal caso si applicano le seguenti disposizioni delle Clausole Contrattuali Standard:

- (i) si applica la Clausola 7 delle Clausole Contrattuali Standard;
- (ii) si applicano esclusivamente le clausole del MODULO QUATTRO: trasferimento da processore a titolare (esclusi tutti gli altri moduli);
- (iii) le Clausole 14 e 15 non si applicano, poiché i Servizi non comportano la combinazione dei dati personali ricevuti dal Titolare non appartenente al SEE o alla Svizzera con altri dati raccolti da Swizzonic nell'UE o in Svizzera;

- (iv) ai sensi della Clausola 17 delle Clausole Contrattuali Standard si applica la legge italiana;
- (v) ai sensi della Clausola 18 delle Clausole Contrattuali Standard, i tribunali competenti sono quelli di Firenze (Italia);
- (vi) si applica esclusivamente l'Allegato 1 della presente DPA, che si intende altresì come Allegato I delle Clausole Contrattuali Standard.

## 7. COOPERATIONE E RESPONSABILITÀ

7.1. Le Parti collaborano in buona fede per garantire il rispetto delle disposizioni della presente DPA, inclusi, ma non limitati a, l'esercizio corretto e tempestivo dei diritti degli interessati nonché la gestione degli incidenti relativi a violazioni della sicurezza o della protezione dei dati, al fine di minimizzare eventuali impatti negativi.

7.2. Le Parti collaborano in buona fede per fornire reciprocamente e alle Autorità di controllo le informazioni necessarie a dimostrare la conformità alle leggi sulla protezione dei dati applicabili.

## 8. DIRITTI DEGLI INTERESSATI

8.1. Tenendo conto della natura del trattamento, Swizzonic supporta il Cliente mediante misure tecniche e organizzative adeguate nell'adempimento del proprio obbligo di rispondere alle richieste di esercizio dei diritti degli interessati.

8.2. Swizzonic garantisce al Cliente una collaborazione e un supporto ragionevoli, fornendo le informazioni necessarie entro limiti ragionevoli per rispondere alle richieste degli interessati o per consentire al Cliente di adempiere ai propri obblighi ai sensi delle leggi applicabili in materia di protezione dei dati relativi ai diritti degli interessati. Il Cliente riconosce e accetta che, in caso di un significativo dispendio di risorse da parte di Swizzonic per tale supporto, potrà essere applicato un compenso, previa comunicazione e consenso anticipati del Cliente.

## 9. RESTITUZIONE E CANCELLAZIONE DATI

9.1. Su richiesta del Cliente e alla scadenza o risoluzione anticipata del presente DPA, Swizzonic restituirà o cancellerà i dati personali del Cliente senza addebito, previa richiesta scritta del Cliente con un preavviso ragionevole, salvo che leggi applicabili imperative (inclusi, a titolo esemplificativo ma non esaustivo, leggi sulla protezione dei dati o ordini delle autorità di polizia o di vigilanza) ne vietino la restituzione o la cancellazione da parte di Swizzonic.

9.2. Le richieste specifiche del Cliente riguardanti la restituzione dei dati personali saranno soddisfatte entro limiti tecnici e organizzativi ragionevoli, tenendo conto dell'estensione, della categorizzazione e della quantità dei dati personali trattati.

9.3. La restituzione dei dati personali del Cliente effettuata secondo le procedure standard interne di Swizzonic è gratuita per il Cliente. In tutti gli altri casi, la restituzione potrà comportare costi ragionevoli a carico del Cliente.

9.4. Qualora il Cliente scelga la cancellazione dei dati personali - fatto salvo l'articolo 9.5 - Swizzonic rilascerà una conferma dell'avvenuta cancellazione.

9.5. Swizzonic potrà conservare i dati personali del Cliente memorizzati nell'ambito di backup regolari, in conformità con i protocolli interni di disaster recovery e continuità operativa (vedi art. 12), a condizione che Swizzonic (e i suoi sub-responsabili) non trattino attivamente o intenzionalmente tali dati per scopi diversi dalla fornitura del Servizio.

## 10. TRASFERIMENTI

10.1. I dati personali trasmessi da Swizzonic tramite Internet in relazione al Servizio saranno criptati in modo adeguato. Tuttavia, le Parti riconoscono che la sicurezza delle trasmissioni via Internet non può essere garantita. Swizzonic non è responsabile per l'accesso a Internet del Cliente, per l'intercettazione o

l'interruzione della comunicazione Internet, né per modifiche o perdite di dati personali durante la trasmissione su Internet.

10.2. In caso di sospetta violazione della protezione dei dati, Swizzonic può sospendere immediatamente l'utilizzo del Servizio via Internet da parte del Cliente fino al completamento di un'indagine, a condizione che Swizzonic informi il Cliente della sospensione appena ragionevolmente possibile e adotti tutte le misure ragionevoli per ristabilire l'uso del Servizio via Internet il prima possibile, collaborando con il Cliente per continuare la fornitura del Servizio tramite canali di comunicazione alternativi.

10.3. Il Cliente si impegna a prendere tutte le misure ragionevoli per mantenere la riservatezza dei nomi utente e delle password del proprio personale per l'utilizzo dei Servizi. Il Cliente è responsabile delle conseguenze derivanti da qualsiasi uso improprio del Servizio da parte del proprio personale.

## 11. VIOLAZIONE DELLA PRIVACY

11.1 Il Cliente riconosce e accetta che Swizzonic non è responsabile per violazioni della protezione dei dati personali che non derivano da negligenza di Swizzonic.

11.2 Nel caso in cui Swizzonic venga a conoscenza di una violazione della protezione dei dati personali, Swizzonic si impegna a:

a) adottare misure appropriate per contenere e mitigare l'incidente e informare immediatamente il Cliente, in modo che quest'ultimo possa avviare le misure di risposta. Swizzonic si riserva il diritto di adottare autonomamente le misure necessarie per conformarsi alle leggi sulla protezione dei dati o per tutelare i propri interessi;

b) collaborare con il Cliente per indagare sull'incidente - in particolare riguardo alla natura, alla portata, alle categorie di dati coinvolti e alle possibili conseguenze;

c) ove richiesto dalla legge, seguire le istruzioni del Cliente nel caso in cui questi sia obbligato a notificare le autorità di controllo o le persone interessate. Il Cliente ha la piena responsabilità di decidere:

- i. se e a chi effettuare le notifiche (ad esempio autorità, persone interessate);
- ii. il contenuto della notifica e le eventuali misure correttive offerte.

## 12. RECUPERO IN EMERGENZA E GARANZIA DELLA CONTINUITÀ AZIENDALE

12.1 Swizzonic mantiene adeguati protocolli di ripristino di emergenza e di continuità aziendale, che variano a seconda del servizio. Il Cliente può richiedere un riepilogo di tali protocolli. Swizzonic può modificare tali piani in qualsiasi momento, purché non riduca la capacità di ripristino al di sotto del livello vigente al momento dell'inizio del contratto.

## 13. INCARI

13.1 Con la firma della presente DPA, inclusi gli Allegati 1, 2 e 3, il Cliente autorizza espressamente Swizzonic a svolgere le attività menzionate all'Art. 5 per conto del Cliente.

13.2 Con la firma della presente DPA, Swizzonic accetta il mandato, che viene eseguito gratuitamente in relazione al servizio, e conferma legalmente di aver letto e compreso le istruzioni ricevute.

# ALLEGATO 1

## **1. SOGGETTI INTERESSATI**

I dati personali trattati possono riguardare, a seconda del servizio attivato, le seguenti categorie di soggetti interessati, che non possono essere determinate in anticipo:

- Cliente e/o dipendenti del cliente;
- Fornitori del cliente;
- Utenti del cliente;
- Clienti del cliente;
- Persone interessate i cui dati personali sono trattati dal cliente utilizzando i servizi forniti da Swizzonic.

## **2. CATEGORIE DI DATI PERSONALI TRATTATI PER OGNI SERVIZIO**

I dati personali trattati per ciascun servizio che possono essere messi a disposizione del Cliente e che non sono determinabili in anticipo si riferiscono esclusivamente a dati personali ai sensi delle leggi applicabili sulla protezione dei dati, con esclusione espressa di dati personali relativi a condanne penali e reati, nonché altre categorie particolari di dati personali.

In particolare, le seguenti categorie di dati personali vengono trasmesse/trattate:

- Dati di contatto (nome e cognome, indirizzo e-mail, indirizzo postale, numero di telefono);
- Data di nascita;
- Età;
- Sesso;
- Altre categorie di dati personali che il cliente tratta utilizzando i servizi forniti da Swizzonic.

## **3. CATEGORIE PARTICOLARI DI DATI**

I dati personali trattati non riguardano dati personali relativi a condanne penali e reati, né altre categorie particolari di dati personali.

## **4. FINALITÀ DEL TRATTAMENTO**

I dati personali possono essere trattati solo per la prestazione del servizio descritto nei Termini e Condizioni Generali (TCG).

## **5. TIPO DI LAVORAZIONE**

La natura delle operazioni di trattamento varia a seconda del servizio specifico attivato tramite i Termini e Condizioni Generali (TCG).

## **6. FREQUENZA DI ELABORAZIONE**

La frequenza delle operazioni di trattamento varia a seconda del servizio specifico attivato tramite i Termini e Condizioni Generali (TCG).

## **7. DURATA DEL TRATTAMENTO**

I dati personali del cliente vengono conservati per tutto il tempo in cui il servizio è attivo.

# **ALLEGATO 2**

## **Descrizione delle misure tecniche e organizzative di sicurezza**

Swizzonic e i sub-responsabili del trattamento si impegnano a rispettare almeno le misure tecniche e organizzative descritte di seguito.

### **Informazioni sulle misure di sicurezza**

#### **Procedure di sicurezza delle informazioni**

##### **Organizzazione interna**

Sono stati definiti e assegnati ruoli e responsabilità separati per la sicurezza delle informazioni alle persone dell'azienda responsabili delle attività di trattamento (di seguito anche "Utenti"), al fine di evitare conflitti di interesse e prevenire attività inappropriate.

##### **Sicurezza nel personale**

##### **Dispositivi mobili e lavoro da remoto**

Esiste una politica di sicurezza per l'utilizzo di tutti i dispositivi aziendali, in particolare dispositivi mobili, ed è stato implementato un controllo adeguato.

##### **Cessazione o modifica del rapporto di lavoro**

Al termine del rapporto di lavoro di un utente o in caso di cambiamento sostanziale del ruolo ricoperto, i diritti di accesso vengono aggiornati immediatamente, mentre gli strumenti aziendali vengono restituiti e ripristinati sia fisicamente sia a livello di sistema.

##### **Gestione delle risorse aziendali**

##### **Responsabilità per risorse e beni aziendali**

Tutti gli strumenti e beni aziendali sono accuratamente inventariati e la loro assegnazione ai rispettivi utenti, responsabili della loro sicurezza, viene monitorata. Inoltre, è stata definita una politica per il loro corretto utilizzo.

##### **Classificazione delle informazioni**

Tutte le informazioni sono classificate e catalogate dagli utenti responsabili secondo i requisiti di sicurezza e trattate di conseguenza.

##### **Gestione dei supporti**

Le informazioni memorizzate sui supporti vengono gestite, controllate, modificate e utilizzate in modo da non comprometterne il contenuto e vengono eliminate in modo appropriato.

##### **Controllo degli accessi**

##### **Requisiti organizzativi per il controllo degli accessi**

I requisiti organizzativi aziendali per il monitoraggio dell'accesso alle risorse informative sono documentati in una policy e attuati praticamente tramite una procedura di controllo degli accessi; ciò significa che l'accesso alla rete e alle connessioni è limitato.

##### **Gestione degli accessi degli utenti**

L'assegnazione dei diritti di accesso agli utenti viene controllata dal momento della loro registrazione fino alla revoca dei diritti di accesso, quando non più necessari, comprese restrizioni speciali per i privilegi di accesso e la gestione delle "informazioni di autenticazione segrete". Sono previsti controlli regolari e aggiornamenti dei diritti di accesso ove necessario. Nella gestione degli accessi viene applicato il principio dei privilegi minimi, secondo cui gli utenti possono accedere solo ai dati necessari per le loro funzioni lavorative e attività aziendali. I diritti di accesso aggiuntivi richiedono un'autorizzazione speciale.

##### **Responsabilità dell'utente**

Gli utenti sono consapevoli delle proprie responsabilità anche nel mantenimento di un controllo degli accessi efficace, ad esempio scegliendo una password complessa, la cui complessità viene verificata dal sistema, e mantenendola segreta.

##### **Sistemi e applicazioni per il controllo degli accessi**

L'accesso alle informazioni è soggetto a restrizioni in conformità con la policy di controllo degli accessi, tramite un sistema di accesso sicuro, gestione delle password, controllo degli strumenti privilegiati e accesso limitato a tutti i codici sorgente.

### **Crittografia**

#### **Controllo crittografico**

Esiste una policy sull'uso della crittografia per i supporti e i dati utente. Le autenticazioni sono crittografate.

### **Sicurezza fisica e ambientale**

Sono state implementate misure di sicurezza fisica e ambientale per impedire accessi non autorizzati o accidentali, perdite o diffusione di dati.

### **Aree sicure: data center**

I servizi aziendali sono erogati e ospitati in diversi data center nel mondo, di cui quello che memorizza i dati personali dei clienti è uno dei pochi data center certificati Tier IV in Italia, offrendo la massima garanzia che un data center può offrire. Tutti i data center nella catena di fornitura offrono piena ridondanza di tutti i circuiti elettrici, di raffreddamento e di rete. Sono dotati di illuminazione perimetrale e sistema di rilevamento presenze con telecamere CCTV; le uscite di emergenza sono dotate di allarmi. Tutti gli allarmi sono centralizzati in sale di controllo.

L'accesso fisico è regolato e controllato da processi di autorizzazione, identificazione e registrazione, ed è limitato alle aree per cui è stata concessa l'autorizzazione grazie al sistema di controllo accessi.

### **Attrezzature**

Esiste una policy per lo smaltimento delle apparecchiature obsolete, volta a garantire la distruzione sicura di tutte le informazioni in esse contenute.

### **Sicurezza delle operazioni**

#### **Procedure e responsabilità operative**

Le responsabilità operative in ambito IT sono documentate e le modifiche a impianti e sistemi IT sono controllate. I sistemi di sviluppo, verifica e produzione sono separati. Sono presenti utenti responsabili del corretto funzionamento delle procedure. La gestione della sicurezza logica dei sistemi operativi e delle applicazioni installate dal cliente ricade invece sotto la responsabilità del cliente dei singoli servizi forniti dall'azienda (di seguito anche "Cliente").

### **Protezione da malware**

La protezione antivirus e contro il malware è attiva sui dispositivi aziendali ed è diffusa la consapevolezza tra gli utenti.

Per quanto riguarda i servizi di Virtual Server o Dedicated Server, il cliente è responsabile dell'installazione di software antivirus e antimalware e - qualora il relativo servizio non sia stato acquistato - di un firewall. Per il servizio di hosting è attiva una protezione in tempo reale sui dispositivi front-end.

Per il servizio email, il traffico viene analizzato in tempo reale sia in entrata che in uscita, per rilevare virus, malware e identificare e filtrare lo spam. L'analisi avviene in modo automatico, basandosi sul contenuto, interrogazioni di banche dati internazionali e reputazione derivante da una serie di parametri.

### **Backup**

Vengono eseguiti backup periodici, con l'eccezione dei servizi per cui il cliente è responsabile del salvataggio e della gestione dei backup (Dedicated Servers e Virtual Servers). Per i servizi di hosting e posta elettronica, vengono effettuati backup periodici ai quali il cliente può accedere in caso di hosting. Backup aggiuntivi, non accessibili ai clienti, sono creati esclusivamente a fini di Disaster Recovery.

### **Autenticazione e monitoraggio**

#### **Autenticazione e sincronizzazione**

Ogni attività ed evento legato alla sicurezza delle informazioni da parte degli utenti di sistema e degli amministratori/operatori avviene previo inserimento delle credenziali di autenticazione o certificati di identità. Gli orologi di tutti i dispositivi sono sincronizzati.

### **Controllo del software dei sistemi operativi**

L'installazione di software nei sistemi operativi è controllata e monitorata.

Per quanto riguarda i Virtual Servers e Dedicated Servers, i sistemi operativi sono forniti con immagini di installazione aggiornate, anche durante l'installazione da parte del cliente. Spetta inoltre al cliente aggiornare il firmware e le applicazioni o software da lui installati.

### **Gestione delle vulnerabilità tecniche**

#### **Patch management**

Ogni vulnerabilità tecnica viene corretta tramite patch adeguate, e sono in atto procedure per tutte le fasi di test e successiva installazione del software e aggiornamenti, che avvengono solo se tutti i test risultano positivi.

### **Considerazioni sui controlli dei sistemi informativi**

Vengono effettuati controlli regolari per garantire che gli impatti negativi sui sistemi di produzione siano ridotti al minimo e che non vi sia accesso non autorizzato ai dati.

### **Sicurezza delle comunicazioni**

#### **Gestione della sicurezza di rete**

Le reti e i servizi online sono protetti anche tramite separazione e segmentazione.

### **Trasferimento di informazioni**

Sono in vigore accordi per il trasferimento delle informazioni da e verso terzi.

### **Sicurezza nei processi di sviluppo e supporto**

Le regole che disciplinano la sicurezza nello sviluppo di software e sistemi sono definite in una policy. Le modifiche ai sistemi (sia per applicazioni sia per sistemi operativi) sono controllate. La sicurezza del sistema viene testata e vengono definiti criteri di approvazione che includono aspetti di sicurezza.

### **Rapporto con i fornitori**

#### **Sicurezza delle informazioni nei rapporti con i fornitori**

Esistono contratti o accordi che regolano la protezione e il trattamento delle informazioni dell'organizzazione e dei clienti, accessibili a terzi nell'ambito IT e ad altri fornitori lungo tutta la catena di fornitura.

### **Gestione dei servizi forniti dal fornitore**

L'erogazione dei servizi forniti dai fornitori è monitorata e verificata rispetto al contratto o all'accordo. Qualsiasi modifica al servizio è soggetta a controllo.

### **Gestione degli incidenti di sicurezza**

#### **Gestione degli incidenti di sicurezza delle informazioni e miglioramenti**

Sono previste responsabilità e procedure specifiche per la gestione coerente ed efficace di tutti gli eventi e incidenti legati alla sicurezza delle informazioni (es. la cosiddetta procedura di Data Breach).

### **Aspetti della sicurezza delle informazioni relativi alla continuità operativa**

#### **Ridondanza**

Tutti i principali impianti IT sono progettati con ridondanza per soddisfare i requisiti di disponibilità. Dove questa ridondanza non è presente, sono implementate misure adeguate per garantire la continuità del servizio o minimizzare la perdita di dati.

### **Conformità**

#### **Conformità ai requisiti legali e contrattuali**

L'azienda identifica e documenta i propri obblighi verso le autorità esterne e altre terze parti in relazione alla sicurezza delle informazioni, incluso la proprietà intellettuale, la documentazione contabile e i dati personali.

### **Verifica della sicurezza delle informazioni**

I progetti dell'organizzazione in ambito sicurezza delle informazioni e le policy di sicurezza vengono verificati e, se necessario, vengono adottate misure correttive.

## ALLEGATO 3

Allegato 3 (Elenco dei sub-responsabili del trattamento) è disponibile su richiesta via e-mail a:

[legal@swizzonic.com](mailto:legal@swizzonic.com).