PREMESSA al Registro delle Attività di Trattamento dei Dati Personali

Il Regolamento Europeo 2016/679 prevede, all'articolo 30, un importante strumento di compliance aziendale, in materia di dati personali: il registro delle attività di trattamento dei dati personali.

Tenuto anche in formato elettronico dal Titolare del trattamento dei dati, tale registro dovrà essere messo a disposizione dell'Autorità Garante qualora lo richieda, così come è previsto dal par. 4 dell'art. 30.

COSA DEVE CONTENERE IL REGISTRO DEL TRATTAMENTO DATI

- Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- Le finalità del trattamento;
- La descrizione delle categorie di interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- Se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.
- Questo registro rappresenta dunque una delle novità e, al tempo stesso, uno degli adempimenti più importanti concernenti le attività di trattamento.

CHI DEVE DOTARSI DI QUESTO STRUMENTO

L'obbligo di redazione e adozione del registro non è generale: infatti il par. 5 dell'art. 30 specifica che esso non compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'art. 10."

Però non bisogna ritenere che l'adozione del registro sia un mero obbligo, infatti la sua redazione potrebbe avere anche scopi ulteriori:

- Diffondere informazione, consapevolezza e condivisione interna;
- Costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati;

REGISTRO TRATTAMENTO DATI PERSONALI di connessionEtica

ConnessionEtica di Zanolli Andrea, in seguito "**connessionEtica**" pur non avendo un numero di dipendenti superiore a 250, ha deciso di avvalersi del presente REGISTRO allo scopo di avere a disposizione un documento di pianificazione e controllo della politica di sicurezza dei dati e delle banche di dati.

ConnessionEtica non effettua trattamenti di dati che possono presentare un rischio per i diritti e le libertà degli interessati, né stabilmente, né occasionalmente. Pertanto non viene effettuato nessun trattamento che includa categorie particolari di dati di cui all'articolo 9, paragrafo 1 (dati sensibili, con l'aggiunta dei dati genetici e biometrici), nè di dati personali relativi a condanne penali e a reati di cui all'articolo 10.

TITOLARE DEL TRATTAMENTO:

Andrea Zanolli

residente in Via Canestrini, 4 - 38061 Ala (TN)

P.IVA 02448890224 -

C.F. ZNLNDR74P26H612Q

contattabile all'indirizzo email: **commerciale@connessionetica.info**

Non sono presenti in azienda le figure di contitolare del trattamento, rappresentante del titolare del trattamento e responsabile della protezione dei dati, in quanto tutta la gestione del trattamento dati fa capo al "Titolare del Trattamento dei dati" sopra indicato.

FINALITA' DEL TRATTAMENTO DEI DATI PERSONALI:

A) FINALITA' DI SERVIZIO:

rientra in questo punto il trattamento dei dati di cui agli art. 24 lett. a), b), c) Codice Privacy e art. 6 lett. b), e) Regolamento UE – GDPR, effettuato SENZA il consenso espresso dell'interessato, effettuato con le seguenti finalità:

- ✓ inviare via e-mail, e/o posta, e/o sms, e/o contatti telefonici, e/o newsletter, comunicazioni in merito ai prodotti poposti e alle attività organizzate dal Titolare
- ✓ concludere i contratti per i servizi del Titolare
- ✓ adempiere agli obblighi precontrattuali, contrattuali e fiscali derivanti da rapporti in essere con l'interessato
- ✓ adempiere agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria o da un ordine dell'Autorità (come ad esempio in materia di antiriciclaggio)
- ✓ esercitare i diritti del Titolare, ad esempio il diritto di difesa in giudizio

B) FINALITA' DI MARKETING:

rientra in questo punto il trattamento dei dati di cui agli artt. 23 e 130 Codice Privacy e art. 7 Regolamento UE – GDPR, SOLO PREVIO il consenso espresso dell'interessato, effettuato con le seguenti finalità:

- ✓ inviare via e-mail, e/o posta, e/o sms, e/o contatti telefonici, e/o newsletter, comunicazioni commerciali e/o materiale pubblicitario su prodotti o servizi ritenuti dal Titolare meritevoli di interesse da parte dell'interessato
- ✓ rilevazione del grado di soddisfazione sulla qualità dei servizi, effettuato mediante e-mail, e/o posta, e/o sms, e/o contatti telefonici, e/o newsletter
- ✓ inviare via e-mail, e/o posta, e/o sms, e/o contatti telefonici, e/o newsletter, comunicazioni commerciali e/o promozionali di soggetti terzi (ad esempio organismi istituzionali, compagnie assicuratrici, altre affiliate a Connessionetica)
- ✓ inviare via e-mail, e/o posta, e/o sms, e/o contatti telefonici, e/o newsletter, comunicazioni commerciali relative a servizi e prodotti ritenuti dal Titolare meritevoli di interesse da parte dell'interessato, se questi è già cliente di connessionEtica, analoghi a quelli di cui ha già usufruito

TRATTAMENTO DEI DATI PER CONTO TERZI

ConnessionEtica esercita anche attività di RILEVAZIONE DEL GRADO DI SODDISFAZIONE sulla qualità dei servizi per conto dei propri clienti.

Nel dettaglio, i clienti (solitamente appartenenti al settore turismo e ristorazione) forniscono a connessionEtica le credenziali per accedere al portale di gestione delle liste contenenti le email dei propri ospiti (che hanno dato il consenso al ricevimento di email, nel momento in cui hanno richiesto l'accesso al sistema WiFi della struttura di proprietà del cliente). ConnessionEtica si preoccupa di inviare con altrettanta periodicità le email di rilevazione del grado di soddisfazione del servizio fruito.

Le liste contengono solitamente i seguenti dati:

- Nome e cognome del cliente
- Data in cui il cliente si è registrato al sistema WiFi
- Indirizzo Email
- Lingua preferita dal cliente
- Altri campi gestiti dal software del sistema WiFi (es. *Data di nascita, Username, Account Type, Distribution Type, MAC Address, Location Name, Social User, FB Like, ecc.)* che però non vengono considerati nella procedura di importazione sotto riportata.

La procedura seguita da connessionEtica è la seguente:

- connessionEtica si collega al **portale** che gestisce le liste di contatto di ciascun cliente, tramite le credenziali dallo stesso comunicate, ed **esporta** la lista con la periodicità concordata (di solito settimanale): il sistema esporta solo i dati di quei soggetti che hanno dato il **consenso** al ricevimento di email
- connessionEtica salva le liste esportate (si tratta di files generati in formato Excel o CSV) direttamente su una **chiave USB appositamente dedicata**. In questo modo i dati non vengono salvati, nemmeno temporaneamente, sul disco fisso dei pc aziendali. I files vengono aperti e filtrati per controllare che i dati contenuti siano corretti e non vi siano duplicati
- connessionEtica **carica** le liste direttamente dalla chiave USB di cui al punto precedente sulla piattaforma Sendinblue, senza importarvi i campi diversi da *Nome, Email, Lingua*, e **cancella immediatamente** i files corrispondenti dalla chiave USB. Da questo momento in poi il trattamento, la conservazione e la protezione dei dati è di competenza della **piattaforma Sendinblue**, scelta da connessionEtica specificatamente per le caratteristiche di sicurezza e di protezione dei dati, di cui di seguito forniamo le specifiche

Nelle successive 7 pagine, viene descritto il sistema di CONFORMITA' DI SENDINBLUE AL GDPR.

Le iniziative di conformità al GDPR di Sendinblue si concentrano su cinque aree chiave di seguito definite nei dettagli:

1 - Funzionalità chiave

2 - Sicurezza

3 - Gestione di partner e responsabili

4 - Documentazione legale

5 - Organizzazione

1 – L'adattamento delle funzionalità chiave

Sendinblue ha identificato gli obiettivi chiave da raggiungere stabiliti dal GDPR collaborando con un campione di utenti, responsabili del portafoglio clienti, team di prodotto, team tecnico e consulenti legali.

Obbligo di fornire informazioni relative alla responsabilità: sul sito web (https://help.sendinblue.com) sono disponibili molte fonti informative relative ai diritti di chi fa email marketing nel quadro del GDPR e le migliori pratiche da attuare per ottemperare alla legge. Queste risorse sono disponibili sulla piattaforma per aiutare gli utenti a essere conformi nelle fasi chiave di utilizzo della piattaforma:

Importazione di contatti:

- Creazione di moduli di sottoscrizione di email per acquisire il consenso dei contatti
- Creazione di campagne email da inviare agli abbonati

Nel Centro assistenza è stata aggiunta una sezione ad hoc per il GDPR e continueranno inoltre a organizzare regolarmente webinar informativi sul tema.

Diritto di rettifica, portabilità e oblio: i diritti di rettifica, portabilità e oblio sono ormai assodati da anni e, come indicato precedentemente, sono stati nel tempo forniti maggiori dettagli sulle modalità di esercizio di tali diritti.

Moduli di sottoscrizione di email: è stata dedicata particolare attenzione ai moduli di sottoscrizione di email durante il processo di messa in conformità perché è un elemento

essenziale per la conformità degli utenti. Ora è possibile gestire le preferenze dell'abbonato all'email aggiungendole a liste specifiche in base alle scelte fatte al momento dell'iscrizione. Inoltre è consentito agli utenti di aggiungere una nota standard in calce ai moduli di sottoscrizione per l'accesso all'informativa sulla privacy del marchio.

Prova del consenso: una volta raccolti i dati di un contatto, la prova del consenso sarà disponibile nel profilo del contatto. Ogni profilo di contatto includerà il momento esatto della sottoscrizione, l'ID del modulo usato per la sottoscrizione e il relativo indirizzo IP. Questi dati potranno essere esportati per consentire agli utenti Sendinblue di fornire facilmente una prova del consenso qualora necessario.

2 – Verifica di sicurezza avanzata

Consci che la sicurezza dei dati è un argomento delicato per molti, Sendinblue l'ha sempre considerata una priorità. Il GDPR consente di fare un ulteriore passo avanti, assicurando un trasferimento e una conservazione dei dati ineccepibili e migliorando il monitoraggio e il controllo dei dati per un accesso più facile e sicuro per gli utenti.

Installazione di sistemi di archiviazione e tracciabilità di dati: per prevenire la violazione di dati, è necessario avere uno stretto controllo del trattamento dei dati che avviene sulla nostra piattaforma. Usando la tracciabilità dei dati e l'identificazione dei log, Sendinblue ha attivato un sistema di tracciabilità dei dati per tutte le procedure di trattamento dati sulla piattaforma. Sendinblue cerca inoltre di massimizzare la sicurezza dei dati archiviati degli utenti: questi dati ora sono conservati in database separati e i dati personali sono stati criptati.

Questi archivi sono conservati a fini puramente legali. Una volta terminato il periodo di conservazione vengono eliminati dal database.

Test di penetrazione della rete: Sendinblue ha iniziato a lavorare con una ditta di consulenza specializzata in cybersicurezza e ha ricevuto un feedback molto positivo in relazione alla difficoltà di penetrare nel nostro sistema.

Consci di poter fare sempre di più per garantire la sicurezza dei dati, Sendinblue si è rivolta a Bounty Factory. Questa piattaforma inglese consente di fare crowdsourcing per una ricerca più approfondita sulla sicurezza della rete e dei dati ad opera di una vasta community di "white hat" o hacker etici e ricercatori sul tema della sicurezza. Questo programma, noto come bug bounty, incoraggia caldamente la ricerca di vulnerabilità del sistema, premiando l'individuazione di ogni vulnerabilità (o "bug") con una ricompensa finanziaria.

Il sistema di compensazione crea un forte incentivo per i ricercatori a scoprire tutte le possibili vulnerabilità nel sistema Sendinblue, riducendo al minimo il rischio di possibili attacchi maligni.

3 – La gestione dei partner e responsabili di Sendinblue

Uno dei principi chiave introdotti dal GDPR è la responsabilità condivisa. Ciò significa essenzialmente che tutti gli attori, siano essi il titolare (la parte che determina i fini e i mezzi dell'elaborazione dei dati) o uno dei responsabili dei dati più in basso nella catena, hanno una parte di responsabilità legale in quanto oggetto del trattamento sono i dati personali.

Svolgendo il doppio ruolo di titolare e responsabile, Sendinblue ha il compito di affrontare il principio della responsabilità da entrambe le parti.

In qualità di responsabile, ha stabilito mezzi per garantire la conformità al GDPR lungo tutta la catena del trattamento dei dati con tutti i partner fornitori di software.

In qualità di titolare, deve garantire inoltre la conformità dei responsabili dei dati alla nuova regolamentazione. Di conseguenza, hanno contattato i responsabili dei dati ponendo domande specifiche sui loro metodi di trattamento dei dati: ciò ha permesso di garantire che le loro procedure relative al trattamento dei dati siano in linea con il GDPR e con gli impegni che Sendinblue ha preso verso i suoi clienti. E' stata messa fine alla collaborazione con tutti i responsabili dei dati che non erano in grado di fornire risposte soddisfacenti alle nostre domande.

Una volta ricevute risposte soddisfacenti dagli altri responsabili dei dati, Sendinblue ha definito contrattualmente i suoi requisiti in accordi per il trattamento dei dati (DPA). Il DPA è un documento che specifica il tipo e i metodi di trattamento dei dati utilizzati dal responsabile a nome di Sendinblue, cosa che permette di garantire un quadro legale e la tracciabilità dei dati.

Per i responsabili dei dati che si trovano negli Stati Uniti Sendinblue ha inoltre verificato la loro certificazione relativa alla certificazione Scudo per la privacy, condizione necessaria per il trattamento di dati di cittadini europei.

4 – Documentazione legale

Alla luce dei nuovi requisiti forniti dal GDPR, Sendinblue ha aggiornato la propria documentazione legale di conseguenza. In particolare, sono state modificate le Condizioni generali e la informativa sulla privacy, entrambe disponibili sul sito web.

È stata redatta e aggiunta alle Condizioni generali una clausola sul responsabile dei dati per definire nei dettagli il ruolo e le responsabilità di Sendinblue nei confronti dei suoi utenti come fornitore di servizi terzo.

5 – Implicazioni interne del GDPR sull'organizzazione Sendinblue

Il GDPR ha imposto inoltre a Sendinblue di ottimizzare l'organizzazione interna e di elaborare le migliori pratiche e procedure a sostegno dei principi chiave indicati dal regolamento.

Consapevolezza dei dipendenti: presso Sendinblue alcune persone hanno un ruolo che richiede un accesso privilegiato ai dati personali. I responsabili del portafoglio clienti, per esempio, possono aver bisogno di accedere ad alcuni elementi dell'account di un utente per poter rispondere a una domanda di assistenza. Si è iniziato estendendo la clausola di riservatezza nei contratti dei dipendenti stipendiati e promuovendo sessioni di formazione.

La formazione include una panoramica generale dei requisiti del GDPR e sessioni specializzate ideate per sviluppare la formazione iniziale per determinati team che trattano regolarmente dati sensibili. Ciò fornisce a tutto il personale una visione chiara degli obblighi relativi al nuovo regolamento.

Procedure e controlli interni: per garantire un'attuazione delle misure di messa in conformità, Sendinblue ha riesaminato tutte le procedure interne che riguardano la gestione dell'accesso del personale ai dati personali, la gestione delle richieste di persone che vogliono esercitare i loro diritti relativi ai loro dati personali e il trattamento che concerne la conservazione e l'eliminazione dei dati. È stato realizzato un piano di controllo per verificare regolarmente l'applicazione corretta di queste procedure e l'aggiornamento della documentazione corrispondente.

Nomina di persone con l'incarico di mantenere una conformità adeguata: l'attuazione delle misure di messa in conformità poste in essere da Sendinblue è gestita dal Direttore operativo interno. Parallelamente, è stato nominato come DPO (Responsabile della protezione dei dati) **Jule Jeanroy**, che ha la responsabilità di garantire la conformità continua di Sendinblue al GDPR nel corso del tempo. Il DPO ha inoltre la responsabilità di monitorare l'applicazione di diversi aspetti del regolamento e garantire che vengano rispettati i principi chiave del GDPR, in particolare il principio della "Privacy by Design," che si riferisce alla conformità di una procedura di trattamento dei dati prima che sia realmente attuata. In Sendinblue il DPO è assistito da una SecOps per aspetti specificamente

correlati alla sicurezza e alla tracciabilità dei dati. In caso di necessità, è possibile contattare il DPO direttamente per email all'indirizzo **dpo@sendinblue.com**.

Stato attuale e fasi successive: la conformità al GDPR in Sendiinblue non finisce mai. È un processo continuo che richiede un monitoraggio costante e la conferma che i principi della legge sono difesi internamente grazie al trattamento dei dati attuale e alla valutazione continua che utilizza il criterio della Privacy by Design per ogni nuova procedura che comprenda il trattamento di dati personali.

Sendinblue è fiera di avere completato la prima parte di questa sfida. Continuerà a mantenere il suo impegno alla conformità per continuare a essere un partner terzo fidato nella fornitura di software per i suoi utenti. Lo svolgimento di questa enorme operazione di messa in conformità ha fornito a Sendinblue numerosi vantaggi, tra cui:

- L'avere radunato l'intera azienda attorno a un obiettivo comune e la collaborazione tra team differenti per raggiungere tale obiettivo
- L'attuazione di procedure ancora più rigorose relative alla gestione e al trattamento dei dati per continuare a migliorare la propria sicurezza
- Il rapido ottenimento della conformità con l'aiuto di partner esterni
- L'esecuzione di una valutazione innovativa della sicurezza della prorpia rete e l'attuazione delle misure correttive necessarie
- Il rafforzamento del legame tra Sendinblue e i suoi utenti fornendo gli strumenti necessari per la conformità al GDPR sulla sua piattaforma

Sendinblue è un'organizzazione che comprende quasi 150 persone: tutti si dichiarano impegnati a garantire la sicurezza e la riservatezza dei dati personali che sono stati loro affidati. Sendinblue prende sul serio questa responsabilità come parte della propria missione principale per fornire una piattaforma completa di marketing digitale per piccole e medie imprese in crescita e di successo.

Sendinblue ha istituito un canale diretto per rispondere a eventuali domande o per discutere eventuali dubbi su Sendinblue e il GDPR in qualsiasi momento. Basta scrivere via email in qualsiasi momento all'indirizzo **contact@sendinblue.com**.

SICUREZZA E CONSERVAZIONE DEI DATI OPERATA DA SENDINBLUE

LUOGHI DI CONSERVAZIONE DEI DATI

I server di hosting su cui SendinBlue elabora e conserva i database si trovano esclusivamente all'interno dell'Unione Europea, su server proprietari, su Google Cloud o su AWS. Sendinblue affitta rack in centri dati che si trovano in Francia (centri dati DC2 e DC3 d'Online, che si trovano a Vitry-sur-Seine, nell'Ile-de-France), le attrezzature sono di SendinBlue. I dati archiviati su cloud sono su Google Cloud in Belgio o su AWS in Irlanda.

Tutti i dati sono copiati tre volte in almeno due luoghi diversi. Nell'ipotesi di uno scenario catastrofico, SendinBlue effettua inoltre dei backup regolari dei tuoi dati. Essi sono criptati prima di essere archiviati in un Cloud Storage (AWS o Google Cloud). L'intervallo di backup dei dati dipende dal loro utilizzo, con una frequenza minima di una volta a settimana.

SICUREZZA DEI LUOGHI DI CONSERVAZIONE DEI DATI

Tutti i centri dati di Sendinblue sono dotati di un modello di sicurezza multi-livello che include tra le altre cose i seguenti dispositivi: carte di accesso elettroniche nominative, allarmi, barriere per controllare l'accesso dei veicoli, chiusure di sicurezza, metal detector e tecnologie biometriche. Ogni centro dati è inoltre dotato di un sistema di rilevamento delle intrusioni.

I centri dati di Sendinblue sono sorvegliati 24h/24, 7/7 tramite videocamere interne ed esterne. In caso di incidente sono analizzati i registri di accesso, i registri delle attività e le registrazioni delle videocamere. I centri dati sono sorvegliati da agenti di sicurezza di grande esperienza, sottoposti a una formazione avanzata e a una verifica rigorosa.

ACCESSO AI DATI

Sendinblue controlla inoltre l'accesso ai locali di produzione dei tecnici incaricati delle applicazioni di produzione. Utilizzia un sistema centralizzato di gestione dei ruoli e dei gruppi per definire e controllare l'accesso dei tecnici ai servizi di produzione. Nel quadro del protocollo di sicurezza, i tecnici effettuano l'autenticazione usando certificati con chiave pubblica personale di breve durata. L'emissione di questi certificati è a sua volta protetta attraverso un'autenticazione a due fattori.

RELAY SMTP

Per garantire una latenza minima, Sendinblue dispone di relay SMTP in diversi luoghi. Quando si utilizza smtp-relay.sendinblue.com si viene automaticamente collegati al relay SMTP disponibile che fornirà la migliore prestazione possibile. Se i propri server che contattano il relay SMTP di Sendinblue si trovano in Europa, i server SMTP usati saranno solitamente quelli situati in Europa. I

dati non sono archiviati dai relay SMTP, si limitano a transitarvi per essere indirizzati verso i centri dati Sendinblue in Europa.

PASSWORD DEGLI ACCOUNT

È tecnicamente impossibile indovinare una catena di caratteri casuali sufficientemente lunga. Con i mezzi attuali e disponendo di un numero di tentativi illimitati ci vorrebbero centinaia d'anni. Inoltre è stato dimostrato che maggiori sono i vincoli imposti all'utente, maggiori sono, oltre al fastidio, le possibilità che usi una password debole o che la annoti per ricordarla. Ecco perché l'unico vincolo per creare una password su SendinBlue è che sia costituita da almeno 8 caratteri. All'utente viene lasciato il compito di definire una password che non possa essere indovinata ovvero che non corrisponda alle password abituali ("lamiapassword", "1234567890", "qwerty1234", ecc.) o a una combinazione di caratteri palese (data di nascita, nome dei figli, ecc.). Sendinblue raccomanda per esempio di utilizzare una catena di caratteri casuale la cui pronuncia possa servirte da mezzo mnemonico o, meglio ancora, di usare un software di gestione di password (Dashlane, Lastpass, ecc.), che permetterà anche di usare una password diversa per ogni servizio. SendinBlue effettua l'hash di tutte le password prima di archiviarle, pertanto è impossibile che qualcuno, compresi i componenti del team Sendinblue, abbia accesso ai dati o possa recuperarli.

In conclusione, al seguente indirizzo si accede alla "Politica sulla Privacy Protezione dei Dati Pesonali" di Sendinblue: **https://it.sendinblue.com/legal/privacypolicy/**

CATEGORIE DI INTERESSATI

FINALITA' DI TRATTAMENTO	TIPO DI TRATTAMENTO	CATEGORIE DI INTERESSATI
FINALITA' DI SERVIZIO	Comunicazioni in merito ai prodotti poposti e alle attività organizzate dal Titolare	Possibili clienti e Clienti
	Concludere i contratti per i servizi del Titolare	Clienti e Fornitori
	Adempiere agli obblighi precontrattuali, contrattuali e fiscali derivanti da rapporti in essere con l'interessato	Clienti e Fornitori
	Adempiere agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria	Clienti, Fornitori, Collaboratori
	Esercitare i diritti del Titolare	Clienti, Fornitori, Collaboratori
FINALITA' DI MARKETING	Comunicazioni commerciali e/o materiale pubblicitario su prodotti o servizi ritenuti meritevoli di interesse da parte dell'interessato	Possibili clienti e Clienti
	Rilevazione del grado di soddisfazione sulla qualità dei servizi	Clienti
	Comunicazioni commerciali e/o promozionali di soggetti terzi	Possibili clienti e Clienti
	Comunicazioni commerciali relative a servizi e prodotti, se questi è già cliente di connessionEtica, analoghi a quelli di cui ha già usufruito	Clienti

CATEGORIE DI DATI TRACCIATI:

LEGENDA DEI CODICI CATEGORIA DEI DATI TRACCIATI		
[A] dati che rivelano l'origine razziale o etnica (art. 9)	[E] dati genetici (artt. 4, par. 1, n. 13 e 9)	[K] dati relativi a condanne penali e reati (art. 10)
[B] dati che rivelano le opinioni politiche (art. 9)	[F] dati biometrici (artt. 4, par . 1, n. 14 e 9)	[W] puri e semplici dati anagrafici e indirizzi email
[C] dati che rivelano le convinzioni religiose o filosofiche (art. 9)	[G] dati relativi alla salute (artt. 4, par. 1, n. 15 e 9)	
[D] dati che rivelano l'appartenenza sindacale (art. 9)	[H] dati relativi alla vita/orientamento sessuale (art. 9)	

FINALITA' DI TRATTAMENTO	TIPO DI TRATTAMENTO	CODICE CATEGORIA DEI DATI TRACCIATI
FINALITA' DI SERVIZIO	Comunicazioni in merito ai prodotti poposti e alle attività organizzate dal Titolare	[W]
	Concludere i contratti per i servizi del Titolare	[W]
	Adempiere agli obblighi precontrattuali, contrattuali e fiscali derivanti da rapporti in essere con l'interessato	[W]
	Adempiere agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria	[W]
	Esercitare i diritti del Titolare	[W]
FINALITA' DI MARKETING	Comunicazioni commerciali e/o materiale pubblicitario su prodotti o servizi ritenuti meritevoli di interesse da parte dell'interessato	[W]
	Rilevazione del grado di soddisfazione sulla qualità dei servizi	[W]
	Comunicazioni commerciali e/o promozionali di soggetti terzi	[W]
	Comunicazioni commerciali relative a servizi e prodotti, se questi è già cliente di connessionEtica, analoghi a quelli di cui ha già usufruito	[W]

COMUNICAZIONE DEI DATI PERSONALI TRATTATI

ConnessionEtica non trasmette all'esterno i dati personali soggetti a trattamento, né a soggetti residenti in Italia, né a destinatari di Paesi terzi, né a organizzazioni internazionali.

DURATA DELLA CONSERVAZIONE / GESTIONE DEI DATI PERSONALI

ConnessionEtica tratterà i dati personali per il tempo necessario ad adempiere alle finalità indicate nel documento INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI (a cui si può accedere direttamente dal link "Privacy Policy" presente sul sito web www.connessionetica.com) e comunque osserverà le seguenti limitazioni:

- il trattamento non supererà i 10 anni dalla cessazione del rapporto per le FINALITA' DI SERVIZIO sopra indicate
- il trattamento non supererà i 2 anni dalla raccolta dei dati per le FINALITA' DI MARKETING sopra indicate

Trascorso il periodo limite di cui sopra, i dati saranno cancellati in modo definitivo dal server dove sono memorizzati, mediante le funzioni messe a disposizione dal sistema informatico.

ConnessionEtica non archivia dati personali su supporto cartaceo. In caso di utilizzo temporaneo di documenti cartacei per la registrazione di tali dati, registrazione effettuata solo per inserire i dati nel sistema informatico, gli stessi documenti che li contengono saranno distrutti tramite distruggi-documenti non appena la registrazione sarà eseguita (al massimo entro la giornata lavorativa).

SICUREZZA DEL TRATTAMENTO

Come richiesto dall'articolo 32 del Regolamento UE (GDPR), connessionEtica ha predisposto alcune misure di sicurezza, in misura proporzionale al tipo di importanza dei dati trattati.

ConnessionEtica ha installato il proprio sito web su un dominio protetto da un protocollo di comunicazione sicura HTTPS, il quale fornisce una cifratura bidirezionale delle comunicazioni tra il client e il server, fornendo una garanzia del fatto che si sta comunicando esattamente con il sito web voluto, oltre a garantire che i contenuti delle comunicazioni tra l'utente e il sito web non possano essere intercettate o alterate da terzi. Sul dominio è infatti presente il Certificato **SSL DV** (Domain Validated) fornito dal provider Aruba, il quale verifica che il dominio sia assegnato al richiedente o che sia sotto il controllo del richiedente. Tale certificato consente la cifratura della sessione con chiavi da 128 bit o superiore per cui i visitatori del sito possono trasmettere informazioni ed effettuare transazioni online in modo sicuro e protetto, ed è supportato dai principali web browser sui dispositivi pc, tablet e smartphone.

Grazie all'impiego del Certificato SSL, si abilitano due servizi di sicurezza:

Secure channel: tutti i dati trasferiti tra il sito web e l'utente finale sono cifrati e possono essere decifrati solamente nel momento della connessione stessa: NON potranno essere intercettati o interpretati da altri che non siano coinvolti nella connessione.

Server authentication: l'utente può verificare l'identità ed autenticità del sito web al quale si è collegato.

In questo modo i dati memorizzati sul database del sito web sono garantiti in materia di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento.

Sia giornalmente che settimanalmente viene eseguito, da parte del provider, un **backup automatico** di tutti i dati presenti sul dominio: questa procedura garantisce che connessionEtica è in grado di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Periodicamente, connessionEtica esegue una verifica sull’effettiva esecuzione delle procedure di backup sopra esposte, al fine di garantire la sicurezza del trattamento.

RISCHI A CUI POSSONO ESSERE SOTTOPOSTI I DATI TRATTATI

TIPO DI DATO	RISCHIO	POSSIBILE DANNO	SOLUZIONE
Dati trattati per conto terzi	Corruzione del supporto (chiave USB) dove i dati vengono scaricati	Nessun danno, in quanto l'esportazione della lista dei contatti può essere rifatta	ConnessionEtica è dotata di chiave USB di riserva
Dati trattati per conto terzi	Corruzione del sistema gestito dalla piattaforma Sendinblue	Perdita dei dati salvati sulla piattaforma Sendinblue	Viste le caratteristiche della gestione dei dati di Sendinblue, elencate alle pagine precedenti, i loro sistemi di ripristino danno la massima garanzia contro la perdita di dati
Dati trattati per conto terzi	Furto di dati dalla piattaforma Sendinblue	Divulgazione dei dati	Viste le caratteristiche della gestione dei dati di Sendinblue, elencate alle pagine precedenti, i loro sistemi di sicurezza danno la massima garanzia contro l'accesso non autorizzato ai dati
Dati direttamente gestiti da connessionEtica	Corruzione del sistema informatico aziendale dove i dati sono memorizzati	Temporanea indisponibilità dei dati	Come precedentemente indicato, sono attivi sia un sistema di backup giornaliero che settimanale dei dati, direttamente sui server di Aruba.
Dati direttamente gestiti da connessionEtica	Furto, incendio o altra calamità all'interno dei locali di connessionEtica	Divulgazione non autorizzata dei dati o distruzione degli stessi	Non sono presenti in azienda dati personali su supporto cartaceo. Inoltre connessionEtica non esegue backup locali sui propri server, né su supporti esterni, dei dati personali trattati

Poichè, come indicato nelle pagine precedenti, i dati trattati appartengono alla categoria dei dati anagrafici, il rischio legato al loro trattamento è di livello basso. Di conseguenza le misure sopra esposte garantiscono un livello di sicurezza più che adeguato al rischio stesso.

Il presente Registro è conservato in formato elettronico sul server di connessionEtica e in formato cartaceo presso la sede della stessa. Il "Titolare del trattamento dei dati" è il responsabile della conservazione del Registro.

Il "Titolare del trattamento dei dati" ha la facoltà di permettere la consultazione a terzi del Registro, ed è suo compito accertarsi che i dipendenti e collaboratori di connessionEtica siano a conoscenza delle direttive in esso riportate.

Il presente Registro sarà revisionato dal "Titolare del trattamento dei dati" con cadenza semestrale o minore nel caso in cui dovessero presentarsi situazioni urgenti che rendano non più attuali le disposizioni ivi contenute.

Ala, 10 maggio 2018

Il Titolare del trattamento dei dati

Andrea Zanolli

Revisioni del presente Registro		
Data	**Motivo della revisione**	**Revisione a cura di**
04/05/2018	*Prima emissione del registro*	*Andrea Zanolli*
19/10/2018	*Verificata l'adeguatezza dei contenuti del registro al modificarsi delle attività aziendali*	*Andrea Zanolli*
19/03/2019	*Modifica dovuta alla chiusura del rapporto con la piattaforma MailUp e contestuale sottoscrizione di un contratto con la piattaforma Sendinblue (rif. documentazione da pag. 5 a pag. 11)*	*Andrea Zanolli*