ACCORDO di ELABORAZIONE DATI

Data protection agreement (art. 28 GDPR)

Il presente **Accordo di Elaborazione Dati** è parte integrante del **Contratto** stipulato tra **DM di Masserini Davide - via Locatelli, 14 Fiorano al Serio (BG) - P.I. 03558220160** ed il **Cliente**, e che definisce i termini e le condizioni applicabili ai servizi offerti. In caso di conflitto tra l'Accordo e le disposizioni del Contratto, il presente Accordo prevale sul Contratto. Scopo dell'Accordo è definire le condizioni in base alle quali DM, quale **Responsabile del trattamento** (di seguito **Responsabile**) in base agli artt. 4 e 28 del Regolamento europeo 679/2016 (GDPR), e come parte dei Servizi definiti nel Contratto, tratta, nel rispetto delle istruzioni del Cliente, i dati personali per contro del Cliente, questi in qualità di Titolare del trattamento. Il presente Accordo annulla e sostituisce ogni altra precedente intesa eventualmente intervenuta tra le parti nella medesima materia.

Per tutto ciò che non è regolamentato dal presente accordo si deve fare riferimento alle norme europee e nazionali in materia di protezione dei dati personali, che le parti si impegnano a conoscere e rispettare.

Indice

Oggetto del trattamento

Il Responsabile del trattamento è autorizzato esclusivamente al trattamento dei dati personali di cui il Cliente è Titolare/Responsabile per l'esecuzione e la fornitura dei servizi oggetto del Contratto, nei limiti necessari e relativi all'esecuzione delle prestazioni.
Per i dettagli si fa riferimento alle **Condizioni Generali e alle Condizioni Speciali** pubblicate sul sito web alla pagina https://a.ware.ly/termini-e-condizioni-di-utilizzo, che qui si intendono riportate per esteso.

Natura e scopo del trattamento

La raccolta dei dati per conto del Cliente avviene per le seguenti finalità:
- fornitura del servizio richiesto dal Cliente in base al contratto;
- verifica del funzionamento corretto del servizio;
- verifica della sicurezza del servizio e dei dati stessi.

Categorie di dati

Oggetto del trattamento sono le seguenti categorie di dati:
- dati e parametri del dispositivo di connessione al servizio;
- dati e parametri del tipo di browser utilizzato per la connessione;
- dati dell'internet service provider (ISP);
- data, orario e durata della visita;
- pagina web di provenienza (referral) e di uscita;
- nazione di provenienza;
- eventualmente il numero di click;
- dati demografici;
- dati geografici;
- comportamento sul sito web (frequenza e regency);
- nomi a dominio;
- indirizzi mail;
- e comunque ogni altro dato fornito dal Cliente tramite i servizi attivati e specificato nel Contratto.

Durata del trattamento

Il trattamento sarà effettuato fino alla scadenza del contratto col Cliente, così come previsto dalle Condizioni Generali di Contratto e/o dai listini online, o comunque fino al verificarsi di condizioni che rendono impossibile continuare l'esecuzione del contratto (es. mancato pagamento e conseguente risoluzione). Alla scadenza i dati forniti saranno restituiti o cancellati a scelta del Cliente, a meno che non sia previsto un obbligo legale di conservazione dei dati (es. garanzia, motivi fiscali). Le copie di sicurezza dei dati saranno cancellate.

Luogo del trattamento

I dati sono trattati presso la sede del Responsabile e presso i datacenter del fornitore Siteground, localizzati sia in Europa che al di fuori di essa. Il trasferimento di dati al di fuori del SEE (Spazio Economico Europeo), qualora sia richiesto dal Cliente anche tramite le impostazioni del servizio (es. utilizzo di servizi di analytics), è ammesso a condizione che il paese di destinazione garantisca un livello di protezione adeguato oppure esistano specifiche decisione di adeguatezza emanate dalla Commissione europea o clausole contrattuali utilizzate dal Cliente.

Qualora un servizio selezionato dal Cliente implichi un trasferimento di dati al di fuori del SEE, e ciò comporti la sottoscrizione di apposita clausola o DPA con il servizio in questione, tale sottoscrizione dovrà essere operata dal Cliente, comunicandone espressamente al Responsabile l'adozione.

Aggiornamento e certificazioni

Il Responsabile si obbliga a curare l'aggiornamento delle proprie competenze specifiche e a tenersi aggiornato in merito a codici di condotta e alle certificazioni approvate dalle autorità di controllo e verificate dagli istituti di certificazione.

Limitazione dell'autorità del Responsabile

Il Responsabile elabora i dati personali solo su istruzioni del Cliente e alle condizioni stabilite nel presente accordo.
Il Responsabile si impegna ad informare il Cliente se, a suo parere, un'istruzione viola il GDPR o altre disposizioni applicabili in materia di protezione dei dati.

Categorie soggetti del trattamento

Il Responsabile si impegna a trattare i dati solo tramite **autorizzati al trattamento** appositamente designati che operano in base alle istruzioni fornite, verificando che applichino le prescrizioni di sicurezza e riservatezza dei dati, assicurandosi che siano a conoscenza delle norme a tutela dei dati personali, provvedendo alla loro formazione e al loro aggiornamento, prescrivendo che abbiano accesso ai soli dati strettamente necessari per adempiere ai compiti loro assegnati.

Il Responsabile utilizza anche soggetti esterni per la fornitura di servizi specializzati:
- Siteground Spain, fornitore di servizi hosting e mail;
- Let's Encrypt, fornitore di certificati di sicurezza SSL.

Ulteriori soggetti ai quali possono essere comunicati i dati sono:
- fornitori eventuali;
- consulenti fiscali e commercialisti;
- consulenti legali.

Registro delle attività di trattamento

Il Responsabile dichiara di tenere per iscritto un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare del trattamento e che comprendono:
- nome e dati del Cliente e, se applicabili, del Responsabile della protezione dei dati (DPO);
- categorie di trattamenti effettuati per conto del Cliente;
- se applicabili, i trasferimenti di dati a carattere personale verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'articolo 49, paragrafo 1, secondo comma del GDPR, i documenti che attestano l'esistenza di opportune garanzie;
- per quanto possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative, ivi compresi, fra gli altri, secondo le necessità: la pseudonimizzazione e la numerazione dei dati a carattere personale;
- i mezzi che permettono di garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;

- i mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
- la procedura che mira a testare, ad analizzare ed a valutare regolarmente l'efficacia delle misure tecniche ed organizzative per assicurare la sicurezza del trattamento.

Obbligo di riservatezza

Il Responsabile è vincolato dall'obbligo di riservatezza con riferimento a tutti i dati trattati per conto del Cliente, come anche il personale autorizzato ed incaricato del trattamento, che viene istruito in merito agli obblighi particolari relativi alla protezione dei dati derivanti dal presente mandato, nonché al vincolo sussistente alle disposizioni e alla finalità. Il Responsabile vigila sull'osservanza delle istruzioni e degli obblighi imposti.
Tale obbligo di riservatezza non si applica nel caso in cui il Cliente abbia autorizzato la fornitura di tali informazioni a terzi, laddove la fornitura delle informazioni a terzi sia ragionevolmente necessaria in considerazione della natura delle istruzioni e dell'attuazione di queste Accordo per l'elaborazione dei dati, o se vi è l'obbligo legale di rendere l'informazione disponibile a terzi.

Misure tecnico-organizzative e di sicurezza

Il Responsabile propone Servizi con misure organizzative e di sicurezza specificatamente studiate per il trattamento anche di dati a trattamento speciale ex art. 9 GDPR (sensibili, giudiziari, ecc...).
Il Responsabile adotta tutte le preventive misure previste dalle norme e dalle prassi internazionali o comunque ritenute idonee al fine di ridurre al minimo i rischi di distruzione, perdita anche accidentale, accesso non autorizzato o comunque trattamento non consentito dei dati, tenendo conto dello stato dell'arte della tecnologia, dell'importanza dei dati trattati e dei costi relativi. Non può, però, garantire che tali misure siano efficaci in ogni circostanza.

Le misure tecniche e organizzative sono soggette al progresso tecnico e all'ulteriore sviluppo. Il Responsabile, in attuazione del principio della protezione dei dati fin dalla progettazione del sistema e del principio di protezione per impostazione predefinita (**privacy by design e by default**, ai sensi dell'art. 25 GDPR) verifica periodicamente l'adeguatezza delle misure di sicurezza adottate, valutando eventuali modifiche delle stesse in base alle mutate tecnologie, che saranno opportunamente documentate sul sito web, a meno che non si tratti di informazioni riservate o commercialmente sensibili.

Il Responsabile comunica al Cliente casi di **accesso ai dati non autorizzato** o non consentito o non conforme alle istruzioni ricevute (*data breach*) senza ritardo, indicando la causa (sospetta), la sequenza della violazione, la soluzione adottata o proposta, le misure prese.

La **sicurezza del trattamento** dati è garantita dalle seguenti misure:
- accesso alle strutture e/ locali ristretto alle sole persone autorizzate e misure di controllo fisiche dei locali;
- monitoraggio costante di temperatura, umidità e rilevazione fumo o incendi dei locali dove sono custoditi i dati;
- accesso al sistema informatico alle sole persone autorizzate, con controllo degli accessi e delle operazioni;
- profili di autorizzazione per limitare gli accessi ai dati;
- credenziali di accesso e autorizzazione modificate periodicamente;
- backup e duplicazione dati;

- procedure di *disaster recovery* per garantire la continuità operativa e la sicurezza dei dati;
- tempestivo ripristino dei dati in caso di incidente fisico o tecnico;
- cifratura dei dati e dei supporti di backup e custodia degli stessi;
- protezione dei dati e degli applicativi software;
- separazione fisica e/o logica dei dati per servizi e per clienti;
- formazione e aggiornamento del personale autorizzato al trattamento dei dati;
- accordi di riservatezza e non divulgazione dei dati;
- limitazione della creazione di materiale cartaceo e smaltimento sicuro degli stessi;
- divieto di utilizzo di supporti e dispositivi di memorizzazione portatili non crittografati a meno di eccezioni.

Obblighi a carico del Cliente

Il Cliente si impegna ad **informare gli interessati** (cioè i suoi clienti o utenti) correttamente e compiutamente con riferimento ai dati trattati, alle modalità e le finalità del trattamento e ai diritti attribuiti dalla legge, nonché sulle conseguenze del consenso, tramite apposita informativa redatta ai sensi delle leggi vigenti, e a **raccogliere il relativo consenso** qualora previsto dalle norme, o a stabilire una base legale del trattamento. Si impegna altresì a tenere indenne l'azienda DM da eventuali richieste legali relative alla non conformità dell'informativa agli utenti/interessati del trattamento e/o della raccolta del consenso.
Il Cliente si impegna a fornire per iscritto tutte le istruzioni necessarie per il trattamento dei dati, e qualunque informazione necessaria per la creazione dei registri del Responsabile sulle attività di trattamento dei dati. Il Cliente resta l'unico responsabile per le informazioni trattate e le istruzioni comunicate.

Spetta al Cliente valutare la sussistenza di un obbligo di comunicazione agli interessati o alle Autorità di controllo (Garante) di una **violazione dei dati** (*data breach*) e la relativa comunicazione.
Spetta al Cliente valutare se il suo trattamento comporta un elevato rischio per i diritti o la libertà di persone fisiche, se si tratta di decisione automatizzate con conseguenze legali sugli interessati, monitoraggio sistematico, trattamento di dati a trattamento speciale (ex art. 9 GDPR), e quindi se si rende necessaria una **valutazione di impatto del trattamento** (DPIA). L'eventuale DPIA dovrà essere portata a conoscenza del Responsabile.
Spetta al Cliente valutare se il suo trattamento comporta la nomina di un **Data Protection Officer** (DPO). L'eventuale nomina dovrà essere portata a conoscenza del Responsabile.

Esenzione

I dati verranno trattati dal Responsabile con mezzi automatizzati e comunque secondo modalità che non comportano la conoscenza effettiva di attività o di informazioni o fatti o circostanze descritti nelle informazioni trattate. Si applicano, quindi, le esenzioni di cui alla direttiva 2000/31/CE e al D.Lgs 70/2003. Il Cliente/Titolare si impegna comunque a tenere indenne il Responsabile da eventuali azioni legali conseguenti alla commissione di illeciti da parte di clienti/utenti del Cliente/Titolare.

Subappalto (sub-responsabili)

Il Responsabile è autorizzato a far ricorso a subappaltatori (ulteriori Responsabili del trattamento) senza necessità di approvazione preventiva del Cliente, qualora nell'ambito del trattamento o dell'utilizzo di dati personali si debba far ricorso a fornitori di servizi esterni.

Elenco dei sub-responsabili → https://a.ware.ly/terzi

Questi saranno comunque vincolati alle istruzioni di cui al presente accordo. Il Responsabile risponde comunque nei confronti del Cliente per le prestazione dell'ulteriore Responsabile designato.
Non si devono intendere quali rapporti di subappalto i servizi cui il Responsabile ricorre presso terzi quale prestazione accessoria per supportare la fornitura del servizio, quali ad esempio servizi di telecomunicazione, manutenzione e assistenza utente, addetti alle pulizie. Tuttavia, ai fini della garanzia della protezione e della sicurezza dei dati del Committente, il Responsabile è tenuto, anche in caso di prestazioni accessorie demandate a terzi, a stipulare accordi contrattuali adeguati e conformi alla legge e ad adottare le opportune misure di controllo. Se l'ulteriore Responsabile del trattamento non adempisse alle proprie obbligazioni in materia di protezione dei dati, il Responsabile del trattamento iniziale è interamente responsabile nei confronti del Cliente del trattamento dell'esecuzione da parte dell'altro Responsabile del trattamento dei suoi obblighi.

Assistenza al Cliente in relazione all'esercizio dei diritti delle persone interessate

Il Responsabile si impegna per quanto possibile ad assistere il Cliente nell'adempimento dell'obbligo di questi consistente nell'evadere le richieste di esercizio dei diritti degli interessati. I sistemi software (es. posta, posta certificata) sono progettati per facilitare il compito del Cliente. Il Responsabile rimane a disposizione del Cliente per ulteriori eventuali informazioni. Nel caso il Cliente richiedesse servizi aggiuntivi (es. il trattamento diretto da parte del Responsabile) per l'evasione delle richieste degli interessati, tali forniture dovranno essere oggetto di separato accordo.
Qualora le persone interessate esercitino tale diritto presso il Responsabile del trattamento presentandogli la relativa richiesta, il Responsabile del trattamento inoltrerà tempestivamente tali richieste al Titolare al contatto indicato in sede di stipula del Contratto.

Assistenza al Cliente in relazione ai propri diritti

Il Responsabile si impegna, nei limiti delle sue possibilità, ad assistere il Cliente nel garantire il rispetto dei suoi compiti e delle sue funzioni, quali le misure di sicurezza, la notifica delle violazioni dei dati personali, l'eventuale esecuzione di valutazioni di impatto del trattamento (DPIA). Si impegna a mettere a disposizione del Cliente, tramite pubblicazione sul sito web o a richiesta, tutte le informazioni necessarie a dimostrare la conformità agli obblighi di legge del trattamento dei dati, delle misure di sicurezza e in genere delle procedure. Ulteriori informazioni potranno essere richieste per iscritto a DM. La fornitura di servizi specifici dovrà essere oggetto di separato accordo.
In caso di verifiche da parte dell'Autorità di controllo (Garante Privacy) con riferimento al trattamento dati del Cliente, il Cliente si impegna a tenere indenne il Responsabile da spese o eventuali costi.

I registri e le misurazioni fornite dal Responsabile sono considerati autentici a meno che il Cliente non fornisca prove convincenti del contrario.

Audit

Il Cliente avrà facoltà di svolgere un audit tramite una terza parte indipendente, al fine di confermare la conformità del trattamento del Responsabile al presente Accordo e al GDPR. L'audit può essere intrapreso solo quando vi sono motivi specifici e documentati per sospettare l'uso improprio dei dati personali, e non prima di due settimane dopo che il Cliente ha fornito una comunicazione scritta al Responsabile. L'audit deve essere eseguito senza interferire in modo irragionevole con le attività aziendali del Responsabile. Le conclusioni dell'audit saranno discusse e valutate dalle parti e, se del caso, attuate di conseguenza da una delle parti o congiuntamente. I costi dell'audit sono a carico del Cliente. Sia il Cliente che la terza parte indipendente sono tenuti a osservare la riservatezza in merito allo svolgimento e alle conclusioni dell'audit.

Responsabilità

Il Responsabile del trattamento risponde unicamente del trattamento dei dati personali effettuato ai sensi del presente Accordo e non di ulteriori trattamenti di dati personali, inclusi, a titolo esemplificativo ma non esaustivo, trattamenti per scopi non segnalati dal Titolare ed elaborati da terze parti. Risponde solo dei danni causati a seguito di mancato rispetto degli obblighi di cui al GDPR con riferimento ai Responsabili del trattamento, o della violazione delle legittime istruzioni scritte fornite dal Cliente.
Il Cliente dichiara e garantisce di avere un'idonea base legale per elaborare i dati personali, e che i contenuti non sono illegali e non violano alcun diritto di terzi. Dichiara altresì che i dati da lui trasmessi sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti. Di conseguenza si impegna ad indennizzare il Responsabile con riferimento a tutti i reclami o azioni legali di terzi relativi alla elaborazione di dati personali illecita o illegittima.
Qualora il Responsabile e il Cliente siano coinvolti in una procedura relativa all'esecuzione del presente Accordo, il Cliente si farà carico di indennizzare per la totalità l'interessato e solo in seconda battuta si rivarrà sul Responsabile per la eventuale parte di responsabilità dell'Azienda.

Cliente che opera quale Responsabile del trattamento

Qualora il Cliente operi quale Responsabile del trattamento in nome di titolari terzi (es., Agenzia Web che gestisce siti per conto di terzi), **il Cliente garantisce di aver ricevuto regolare nomina/designazione quale responsabile del trattamento dal titolare terzo e che DM sia stata designata quale sub-responsabile del trattamento.**
Il Cliente dovrà ulteriormente garantire che le istruzioni fornite a DM siano allineate e compatibili con le istruzioni ricevute dal suo titolare del trattamento.
Il Cliente dovrà garantire che le istruzioni saranno fornite solo dal Cliente e non dal titolare, a meno che il Cliente non abbia cessato l'attività.
Il Cliente manterrà indenne DM per qualsiasi inadempienza del titolare del trattamento.

Modifiche all'Accordo

Il presente Accordo può essere modificato e adattato, in particolare in caso di cambiamenti della legislazione in materia di protezione dei dati personali, o di provvedimenti delle Autorità di controllo.
Il Cliente dovrà fornire piena collaborazione alla modifica del presente Accordo.