Accordo sul trattamento dei dati

Osservazioni generali

Il presente accordo (contratto) sul trattamento dei dati specifica gli obblighi del cliente e del responsabile del trattamento (insieme le parti) in relazione alle disposizioni della Legge svizzera sulla protezione dei dati (LPD) e del Regolamento generale sulla protezione dei dati dell'UE (GDPR). Ciò può comportare un unico contratto o più contratti tra il responsabile del trattamento e il cliente (contratto).

L'accordo si applica nella misura in cui sono soddisfatte le seguenti condizioni:

(a) Il cliente agisce in qualità di responsabile o di responsabile del trattamento nell'ambito di applicazione del DPA e/o del GDPR UE e

(b) il Cliente incarica DAUF SA nell'ambito del contratto come incaricato o subresponsabile del trattamento di dati personali o di dati personali che rientrano nell'ambito di applicazione della FADP e/o del GDPR UE **(dati personali).**

1. Oggetto, tipo, finalità e durata del trattamento dei dati

L'oggetto del trattamento dei dati, la sua natura, lo scopo e la durata sono stabiliti nel contratto. Le categorie di dati personali trattati, le categorie di persone interessate dal trattamento dei dati e le misure tecniche e organizzative (TOM) da adottare sono descritte nel contratto e/o negli allegati 1 e 2 del presente accordo.

Qualora il responsabile del trattamento si occupi di ulteriori servizi per il cliente nel corso di un'ulteriore cooperazione, il presente accordo si applica anche a tali servizi.

2. Istruzioni

(a) Conformità alle istruzioni: Il responsabile del trattamento è tenuto a trattare i dati personali esclusivamente in conformità alle disposizioni del contratto e del presente accordo e a seguire le istruzioni del cliente per il loro trattamento. Sono fatti salvi eventuali obblighi diversi previsti dalla legge applicabile (ad esempio, obblighi di legge o ordini vincolanti emessi dalle autorità competenti).

(b) Legalità del trattamento dei dati: il cliente è responsabile della legalità del trattamento dei dati stesso, compresa l'ammissibilità dell'elaborazione di ordini/sottordini.

(c) Istruzioni di emissione: Le istruzioni del cliente sono documentate nel contratto e nel presente accordo. Il cliente può impartire al responsabile trattamento ulteriori istruzioni per iscritto in qualsiasi momento. Tali istruzioni individuali richiedono il consenso preventivo del responsabile del trattamento e devono essere documentate. Il responsabile del trattamento accetta tali istruzioni nella misura in cui possono essere attuate e sono ragionevoli nell'ambito dei servizi concordati nel contratto. Se tali istruzioni comportano costi aggiuntivi per il trasformatore o una modifica dell'ambito dei servizi, si applica la procedura di modifica prevista dal contratto.,

(d) Ammissibilità delle istruzioni: Il responsabile del trattamento informerà immediatamente il cliente se ritiene che un'istruzione violi la FADP o il GDPR dell'UE. In tal caso, il responsabile del trattamento può sospendere l'esecuzione dell'istruzione fino alla sua conferma o modifica da parte del cliente. Le parti convengono che la responsabilità del trattamento dei dati personali in conformità alle istruzioni spetta esclusivamente al cliente. Il responsabile del trattamento può presumere in ogni momento che le istruzioni del cliente relative alle autorizzazioni di accesso ai dati personali o alla loro divulgazione al cliente siano conformi alla legge.

3. Ulteriori obblighi del responsabile del trattamento

(a) Limitazione dello scopo: Il responsabile del trattamento tratterà i dati personali esclusivamente ai fini dell'adempimento del contratto e in conformità alle disposizioni concordate nel contratto e nel presente accordo. Il responsabile del trattamento si riserva il diritto di anonimizzare o aggregare i dati personali in modo che non sia più possibile identificare i singoli interessati e di utilizzarli in questa forma ai fini della progettazione, dell'ulteriore sviluppo e dell'ottimizzazione in base alle esigenze, nonché della fornitura del servizio concordato in conformità al contratto.

(b) Misure tecniche e organizzative (TOM): Il responsabile del trattamento adotterà le appropriate, ma in ogni caso almeno le TOM descritte nell'allegato 2 per la protezione dei dati personali. Durante il periodo di validità del contratto, il responsabile del trattamento è autorizzato ad adattare le misure tecniche e organizzative, a condizione che il livello di sicurezza non venga ridotto. In caso di contraddizione, i TOM più specifici regolati nell'accordo avranno la precedenza su quelli dell'allegato 2

(c) Registro del trattamento dei dati: Il responsabile del trattamento deve tenere un registro del trattamento dei dati personali in conformità ai requisiti dell'art. 12, comma 1, della FADP e dell'art. 30, comma 2, del GDPR. Su richiesta, il responsabile del trattamento consentirà al cliente di accedere alle parti del registro del trattamento che riguardano il trattamento dei dati personali rilevanti per i servizi forniti al responsabile del trattamento.

(d) Riservatezza e non divulgazione: Il responsabile del trattamento deve garantire che alle persone coinvolte nel trattamento dei dati personali sia vietato trattarli per scopi diversi da quelli concordati e in deroga al presente accordo. Dovrà inoltre garantire che tutte le persone che hanno accesso ai dati personali siano soggette a un obbligo di riservatezza/confidenzialità legale o contrattuale. Nel caso in cui i dati personali elaborati siano soggetti al segreto professionale, il responsabile del trattamento agirà come persona ausiliaria e adempirà agli obblighi di legge applicabili.

(e) Notifica di violazioni della sicurezza: In caso di violazioni della sicurezza concretamente sospettate e rilevate presso il Responsabile del trattamento o un sub-incaricato che comportino la distruzione, la perdita, l'alterazione o la divulgazione di dati personali, siano esse illecite, contrarie al contratto o alle istruzioni o non intenzionali, il Responsabile del trattamento dovrà informare quanto prima il Cliente in modo appropriato circa la natura e l'entità della violazione e le possibili misure correttive. In tal caso, le parti adotteranno le misure necessarie per garantire la protezione dei dati personali e ridurre al minimo le possibili conseguenze negative per gli interessati e le parti e si consulteranno immediatamente.

(f) Obblighi di sostegno:

(i) Se una persona interessata si rivolge al responsabile del trattamento in relazione a reclami ai sensi della legge sulla protezione dei dati (ad esempio, con una richiesta di rettifica, informazione o cancellazione), il responsabile del trattamento inoltrerà senza indugio la relativa richiesta al cliente. Il responsabile del trattamento fornirà al cliente un'assistenza adeguata all'elaborazione di tali richieste. L'incaricato dell'elaborazione degli ordini può richiedere un compenso separato da concordare in anticipo per quantità di lavoro maggiori.

(ii) Il responsabile del trattamento dovrà assistere il cliente nell'esecuzione di una valutazione d'impatto sulla protezione dei dati, nelle consultazioni con l'autorità di vigilanza, nelle notifiche a quest'ultima e simili con i dati e le informazioni necessarie. Il responsabile del trattamento può richiedere un compenso separato, da concordare in anticipo, per le spese di maggiore entità.

(g) Obbligo di restituzione e cancellazione:

(i) I dati personali saranno restituiti o cancellati al termine del contratto in conformità alle disposizioni contrattuali o alle istruzioni del cliente, a meno che il responsabile del trattamento non sia obbligato per legge a continuare a conservare i dati personali. Il responsabile del trattamento utilizzerà le procedure standard del settore per la cancellazione dei dati personali.

4. Doveri e obblighi del cliente

(a) Obblighi normativi: Il Cliente dovrà adempiere a tutti gli obblighi normativi applicabili al suo ruolo di responsabile trattamento dei dati personali. È l'unico responsabile della liceità del trattamento dei dati personali e della salvaguardia dei diritti degli interessati nel rapporto tra le parti. Qualora terzi dovessero avanzare pretese nei confronti del responsabile trattamento sulla base dell'elaborazione dei dati personali in conformità al presente contratto, il cliente dovrà tenere indenne il responsabile del trattamento da tutte queste pretese.

(b) Misure tecniche e organizzative (TOM): il cliente stesso adotterà misure tecniche e organizzative adeguate per proteggere i dati personali nella sua area di responsabilità (ad esempio i suoi sistemi e i suoi edifici).

(c) Obblighi di informazione:

(i) Il Cliente dovrà informare immediatamente il Responsabile del trattamento qualora riscontri una violazione della protezione dei dati nella fornitura di servizi da parte del Responsabile del trattamento.

(ii) Se il responsabile del trattamento è obbligato nei confronti di un ente governativo o di una persona a fornire informazioni sul trattamento dei dati personali o a collaborare con tali enti in qualsiasi altro modo, il cliente è tenuto a sostenere il responsabile del trattamento nell'adempimento di tali obblighi.

5. Contatti

(a) Cliente: Persona di contatto indicata nel contratto tra il cliente e DAUF SA

(b) Responsabile del trattamento: DAUF SA, Via Figino 6, 6917 Barbengo, dataprotection@dauf.ch

6. Sub- responsabili del trattamento

(a) Diritto di coinvolgimento: a meno che il contratto non contenga disposizioni restrittive sul coinvolgimento di terzi, il Responsabile del trattamento è autorizzato a coinvolgere subincaricati. Ciò vale a condizione che l'Incaricato stipuli un accordo con il subincaricato per garantire il rispetto degli obblighi previsti dal presente Contratto.

(b) Autorizzazione: Il Responsabile del trattamento deve informare il cliente prima del subappalto o di qualsiasi modifica prevista. Entro un mese dalla notifica da parte del responsabile del trattamento, il cliente può presentare un'obiezione se vi sono importanti motivi di protezione dei dati contro il coinvolgimento del subincaricato in questione. L'obiezione del cliente deve essere formulata per iscritto e deve contenere i motivi dell'obiezione. Se sussiste un motivo importante ai sensi della legge sulla protezione dei dati e non è possibile una soluzione amichevole tra le parti, al cliente sarà concesso il diritto di recesso in relazione al servizio interessato dal cambio di subincaricato.

7. Luogo di trattamento dei dati

La divulgazione di dati personali da parte del responsabile del trattamento all'estero o a un'organizzazione internazionale è consentita solo se il responsabile del trattamento rispetta le disposizioni degli artt. 16 e segg. FADP o del capitolo V del GDPR dell'UE. Tuttavia, se tale divulgazione di dati personali è richiesta dal cliente o viene effettuata per suo conto, il rispetto delle disposizioni in materia è di esclusiva responsabilità del cliente.

8. Diritti di verifica

(a) Diritto di ispezione: Il responsabile del trattamento è tenuto a fornire al cliente, su richiesta, le informazioni necessarie a documentare il rispetto degli obblighi concordati. Il Cliente ha il diritto di verificare l'osservanza da parte del responsabile del trattamento degli obblighi previsti dal presente Contratto. Il Responsabile del trattamento è tenuto a collaborare adeguatamente a ogni ispezione. Nella pianificazione e nell'esecuzione della verifica, il Cliente terrà conto delle esigenze e dei requisiti di sicurezza del Responsabile del trattamento e rispetterà gli obblighi di riservatezza del Responsabile del trattamento. Se non diversamente stabilito nel contratto, il cliente dovrà sostenere tutti i costi di tali audit (compresi i costi interni comprovati sostenuti dal responsabile del trattamento per partecipare all'audit).

(b) Misure correttive: Se durante il controllo sono state individuate e provate violazioni del presente accordo, il trasformatore deve adottare immediatamente le misure correttive appropriate.

9. Disposizioni finali

(a) Ambito di applicazione: nel contratto le parti regolano esclusivamente il rapporto di elaborazione degli ordini ai sensi della legge sulla protezione dei dati. Non intendono estendere o limitare il catalogo dei servizi concordati nell'accordo di servizio.

(b) Responsabilità: la responsabilità derivante da violazioni del presente Contratto sarà disciplinata dalle disposizioni in materia di responsabilità concordate per i Servizi o applicabili per legge. Il Cliente si impegna inoltre a risarcire il Responsabile del trattamento da eventuali multe inflitte al Responsabile del trattamento nella misura in cui il Cliente è responsabile del reato sanzionato dalla multa.

(c) Durata: la durata del presente Contratto si baserà sulla durata di tutti i contratti tra il Responsabile del trattamento e il Cliente in base ai quali il Responsabile del trattamento tratta i Dati personali per il Cliente, a meno che dal presente Contratto non derivino obblighi ulteriori.

(d) Notifiche: Le notifiche previste dal presente contratto devono essere effettuate espressamente e in forma testuale (ad esempio, via e-mail o per posta), se non diversamente concordato.

(e) Modifiche e integrazioni: In deroga a qualsiasi requisito di forma scritta previsto dal contratto, il presente accordo può essere concordato o modificato anche per via elettronica tra le parti.

(f) Risoluzione delle controversie: la legge applicabile e il foro competente sono stabiliti dal contratto. Tuttavia, il cliente conserva il diritto di richiedere misure cautelari presso qualsiasi tribunale competente e di far valere i propri diritti nei confronti del responsabile del trattamento in caso di reclamo da parte di terzi presso il tribunale dell'azione principale.

(g) Risoluzione dei conflitti: a meno che il contratto o le disposizioni di legge speciali non contengano disposizioni più severe o di maggiore portata, il presente accordo prevale sul contratto in caso di contraddizioni. Per il resto, le disposizioni del contratto, comprese le ulteriori disposizioni in materia di protezione dei dati e di sicurezza, restano invariate.

Allegato 1: Concretizzazione dell'elaborazione dei dati dell'ordine

1. Tipi di dati personali

Il trattamento dei dati dell'ordine può comprendere in particolare le seguenti categorie di dati personali:

a. *Dati anagrafici* (dati che si riferiscono direttamente alla persona e alle sue caratteristiche; ad esempio, nome, cognome, data di nascita, età, sesso, nazionalità, numero AVS, stato civile, dettagli sul profilo professionale e sull'occupazione, storia della clientela, ecc.)
b. *Dati sulla salute* (dati relativi allo stato di salute di una persona; ad esempio, diagnosi, ecc.
c. *Dati contrattuali* (dati derivanti dalla conclusione o dall'elaborazione del contratto; ad esempio, rapporto contrattuale, prodotto o interesse contrattuale, dati di fatturazione e pagamento, ecc.)
d. *Dati di* comunicazione (ad es. indirizzo e-mail, numero di telefono, indirizzo, contenuto della corrispondenza, dati marginali, ecc.)
e. *Dati tecnici e informazioni sull'utente* (dati generati in relazione all'utilizzo del sito web o dell'applicazione, ad esempio indirizzo IP, dati di login, numero di cliente, numero di personale, ecc.)
f. *Dati comportamentali* (ad esempio, dati sull'utilizzo di siti web, informazioni sull'utilizzo di comunicazioni elettroniche)
g. *Dati sulle preferenze* (dati che forniscono informazioni su esigenze, interessi, preferenze, caratteristiche o comportamenti previsti).
h. *Altri dati* (ad esempio, dati in relazione a procedimenti ufficiali o giudiziari, nel contesto di concetti di protezione, foto, video e registrazioni sonore, dati di registrazione).

2. Dati personali particolarmente sensibili

Si tratta di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici e biometrici intesi a identificare in modo univoco una persona fisica, dati sanitari e dati relativi alla vita privata

3. Dati riservati

Questi dati possono, ad esempio, essere soggetti al segreto professionale o all'obbligo di riservatezza ai sensi della legge sulla sicurezza sociale.

4. Persone interessate

Il trattamento dei dati degli ordini può interessare in particolare le seguenti categorie di persone:

a. Clienti finali attuali, precedenti e potenziali, farmacie, drogherie, case anzini e varie.
b. Dipendenti attuali, precedenti e potenziali e altre persone ausiliarie del cliente
c. Partner commerciali, venditori, fornitori, consulenti, rappresentanti del cliente che siano persone fisiche e loro dipendenti.

Allegato 2: Misure tecniche e organizzative

Il presente allegato descrive le misure tecniche e organizzative adottate dal Responsabile del trattamento per garantire un livello di protezione adeguato al rischio. Le misure devono essere intese in modo generico e vengono applicate in ogni caso se il contratto non prevede nulla di diverso. Se il trattamento dei dati viene effettuato da subresponsabile incaricati del trattamento, l'Incaricato dovrà garantire, mediante opportuni accordi contrattuali, che i subresponsabile rispettino misure analoghe.

La valutazione dell'adeguatezza delle misure tecniche e organizzative descritte di seguito per proteggere i dati affidati al responsabile del trattamento (in particolare nel caso di dati personali particolarmente sensibili o di dati riservati) è di esclusiva responsabilità del cliente.

Controllo degli accessi:

- Le aree sono suddivise in zone di sicurezza con diversi livelli di sicurezza. Le zone pubbliche sono accessibili a tutti. Per accedere alle zone sicure è necessario un badge, una chiave o simili. I badge utilizzati devono essere sempre personalizzati. Se si utilizzano badge non personalizzati, viene tenuto un registro dei titolari temporanei. Anche il rilascio di chiavi o simili alle persone autorizzate viene registrato. La procedura di rilascio di badge, chiavi o simili è regolata nei documenti corrispondenti. I visitatori devono registrarsi e sono accompagnati dai dipendenti responsabili nelle zone sicure.
- I data centre dispongono delle misure di protezione fisica necessarie per rilevare tempestivamente gli accessi non autorizzati e attivare un allarme corrispondente.
- I data centre dispongono delle altre misure di protezione necessarie per ridurre i rischi derivanti da eventi naturali quali fulmini, pioggia, inondazioni, ecc. in misura tale da non essere più rilevanti per le operazioni dei data centre.
- Se si utilizzano centri dati di terzi per l'archiviazione permanente dei dati per i servizi, si garantisce che i gestori di tali centri dati soddisfino condizioni analoghe e quindi un livello di sicurezza equivalente.
- I centri dati possono essere monitorati con video. Il periodo di conservazione e l'accesso alle registrazioni sono definiti.
- Nel caso in cui il cliente memorizzi i propri dati in loco, DAUF SA può fornire raccomandazioni su come questi locali debbano essere protetti. È responsabilità del Cliente adottare le necessarie misure di protezione.
- Il personale viene selezionato con cura.
- All'inizio del rapporto di lavoro, i nuovi dipendenti vengono informati sulle norme relative alla sicurezza personale e alla sicurezza dei dati.
- I dipendenti esistenti vengono regolarmente formati per un'attenta gestione dei dati e sensibilizzati sui rischi per la sicurezza.
- Quando i dipendenti lasciano DAUF SA, l'identificazione sui sistemi e l'accesso agli edifici sono bloccati.

Controllo degli accessi:

- L'accesso ai sistemi di DAUF SA avviene con identificazioni personalizzate.
- L'accesso ai sistemi è sempre protetto da almeno una password o da una funzione di autenticazione equivalente e dagli ID utente corrispondenti.
- Esistono requisiti minimi per la complessità della password.
- In caso di login errato, l'identificazione viene temporaneamente bloccata dopo diversi tentativi falliti. Esiste una procedura per ripristinare le identificazioni bloccate.

Controllo degli accessi:

- Le autorizzazioni sui sistemi sono strutturate in modo tale da consentire l'accesso solo ai dati necessari per svolgere il compito.
- Se un dipendente ha bisogno di diritti aggiuntivi, può ordinare un ruolo aggiuntivo. Questo ruolo aggiuntivo è autorizzato dal proprietario del ruolo.
- Tutti i ruoli vengono controllati regolarmente per verificare se gli utenti assegnati ne hanno ancora bisogno.
- Il traffico di dati tra la rete del Cliente e DAUF SA è criptato, ove possibile. La crittografia può avvenire in vari modi.
- La rete è protetta da un firewall, da un sistema di rilevamento delle intrusioni (IDS) e dalla segmentazione della rete.
- Gli antivirus sono in uso e vengono aggiornati regolarmente.
- I sistemi server e client sono sottoposti a patch regolari.
- L'accesso ai dati e ai sistemi viene registrato.

Controllo del traffico:

- L'accesso ai dati rilevanti via Internet avviene sempre tramite una connessione criptata.

Controllo della memoria:

- Le strutture di archiviazione permanente nei data center sono dotate di alimentazioni ridondanti e dei sistemi necessari per consentire il funzionamento autonomo per un periodo di tempo definito.
- I data centre sono dotati di sistemi di allarme antifumo e antincendio per proteggere dai danni causati da fumo e incendio.
- In caso di difetto, i supporti dati vengono resi fisicamente inutilizzabili o consegnati a un'azienda di smaltimento certificata, al fine di escludere completamente la possibilità di accesso.
- I supporti dati funzionanti vengono cancellati utilizzando le procedure di cancellazione standard del settore in modo tale che sia praticamente impossibile ricostruire i dati in essi contenuti. Se tale procedura non è possibile, i supporti dati vengono resi fisicamente inutilizzabili o distrutti.

Controllo di Input:

- Vengono registrati gli inserimenti o le modifiche nei sistemi di elaborazione dei dati.

Controllo della disponibilità:

- Vengono eseguiti backup regolari per evitare la perdita di dati in caso di problemi al sistema.
- Per garantire la disponibilità dei dati, i sistemi di archiviazione sono configurati in modo tale che più di un componente possa guastarsi e i dati siano ancora disponibili.

Requisiti di separazione:

- È garantito a livello logico e fisico che i dati dei clienti non possano essere visualizzati da altri.

Revisione, valutazione e verifica:

- Gli audit vengono effettuati periodicamente.

In caso di discrepanze fa fede la versione in tedesco