

# Modello di contratto per il trattamento dei dati secondo LPD

tra

## **Titolare del trattamento**

Azienda

Via

Luogo

di seguito **mandante**

e

## **Responsabile del trattamento**

Azienda

Via

Luogo

di seguito **mandatario**

## **Nota**

*Il seguente modello di contratto, basato sul modello di contratto per il trattamento dei dati ai sensi dell'art. 28 GDPR della GDD (Gesellschaft für Datenschutz und Datensicherheit), è stato adattato alle disposizioni del progetto di legge federale sulla protezione dei dati (P-LPD), nonché aggiornato in base alla versione adottata in occasione della votazione finale del Parlamento il 25 settembre 2020 (nDSG). Spuntare la casella corrispondente e compilare i dati richiesti.*

## **1. Oggetto e durata del trattamento dei dati**

### **1. Oggetto**

- L'oggetto del trattamento è definito nel contratto ..... del....., al quale si fa riferimento nel presente documento (di seguito accordo di prestazione).

oppure

- L'oggetto del trattamento dei dati definisce i seguenti compiti che il mandatario deve eseguire: ..... (definizione dei compiti)

### **2. Durata**

- La durata del presente accordo per il trattamento dei dati (di seguito DPA) corrisponde al periodo di esecuzione dell'accordo di prestazione.

oppure

- Il trattamento è conferito per la singola esecuzione.

oppure

- La durata del presente trattamento (periodo di esecuzione) è determinata fino al .....

oppure

- Il trattamento è conferito a tempo indeterminato e può essere disdetto da entrambe le parti con un preavviso di ..... al ..... . Resta ferma la possibilità di disdetta immediata.

## **2. Concretizzazione del contenuto dell'accordo**

### **1. Natura e finalità del trattamento dei dati previsto**

- I particolari delle attività di trattamento, segnatamente la natura e la finalità del trattamento dei dati personali, sono descritti in dettaglio nell'accordo di prestazione del .....

oppure

- Definizione più particolareggiata dell'oggetto dell'accordo in relazione alla natura e alla finalità dei compiti spettanti al mandatario: .....

## 2. Luogo del trattamento dei dati

L'esecuzione del trattamento dei dati concordato contrattualmente ha luogo

in Svizzera

e / o

in uno Stato membro dell'Unione Europea (UE) o dello Spazio economico europeo (SEE) oppure in un Paese che dispone di un'adeguata protezione dei dati ai sensi della vigente LPD. Il Paese è il seguente: .....

e / o

in un Paese che non dispone di un'adeguata protezione dei dati. Il Paese è il seguente: ..... La trasmissione dei dati avviene solo previo adempimento dei requisiti speciali della LPD. L'adeguatezza della protezione dei dati è garantita come segue:

da un contratto/accordo internazionale;

da clausole di protezione dei dati previste dal contratto tra il titolare del trattamento o il responsabile del trattamento e la sua/il suo partner contrattuale, preventivamente notificate all'IFPDT;

da specifiche garanzie che l'organo federale competente ha definito e preventivamente comunicato all'IFPDT;

da clausole di protezione standard che l'IFPDT ha preventivamente approvato, rilasciato o riconosciuto; oppure

da disposizioni aziendali vincolanti riguardo il trattamento dei dati, preventivamente approvate dall'IFPDT o dall'autorità di uno Stato competente in materia di protezione dei dati e in grado di garantirne l'adeguatezza del trattamento.

Si rende necessario adottare delle misure aggiuntive idonee a garantire l'adeguatezza del trattamento dei dati, come da allegato 1.

## 3. Natura dei dati

La natura dei dati personali trattati è specificata nell'accordo di prestazione al punto: .....

oppure

Oggetto del trattamento sono le seguenti tipologie/categorie di dati:

dati anagrafici di base

dati di comunicazione (ad es. telefono, e-mail)

dati contrattuali di base (rapporto contrattuale, interesse per il prodotto e/o per il contratto)

storico del cliente

dati relativi alla fatturazione contrattuale e al pagamento

dati di pianificazione e gestione

indicazioni di informazione (da terzi, ad es. agenzie di informazioni o registri pubblici)

...

## 4. Categorie di persone interessate

- Le categorie di persone interessate dal trattamento dei dati sono specificate nell'accordo di prestazione al punto:.....

oppure

- Le categorie di persone interessate dal trattamento dei dati sono:

- clienti
- parti interessate
- abbonati
- dipendenti
- fornitori
- rappresentanti di commercio
- referenti
- ...

### **3. Misure tecnico-organizzative**

Prima di iniziare con il trattamento dei dati, il mandatario documenta l'attuazione delle necessarie misure tecniche e organizzative stabilite alla stipula dell'accordo, segnatamente per quel che concerne la sua specifica esecuzione, e provvede a inoltrarle al mandante per l'apposita verifica. Una volta accettate dal mandante, le misure documentate costituiscono la base dell'accordo di prestazione. Se invece la verifica/l'audit del mandante esige un adeguamento, quest'ultimo dovrà essere attuato di comune accordo.

Il mandatario deve garantire la sicurezza dei dati ai sensi della LPD.

Le misure tecniche e organizzative sono soggette al progresso tecnologico e all'ulteriore sviluppo. In tal senso, il mandatario è autorizzato ad attuare delle misure alternative appropriate, fermo restando che non è possibile scendere oltre il livello di sicurezza risultante dalle misure prestabilite. Eventuali sostanziali modifiche devono essere documentate.

Il mandatario è tenuto a definire le misure di sicurezza dei dati. In generale, le misure da adottare sono idonee a garantire la sicurezza dei dati e un livello di protezione adeguato al rischio per quanto concerne la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, tenuto conto dello stato dell'arte, della natura, della entità, nonché delle finalità del trattamento [i dettagli nell'allegato 1].

### **4. Rettifica, limitazione e cancellazione dei dati**

Il mandatario deve eseguire le istruzioni documentate del mandante e non può quindi di sua iniziativa rettificare o cancellare i dati né limitarne il trattamento. Se a tal riguardo la persona interessata si rivolge direttamente al mandatario, quest'ultimo provvederà senza indugio a inoltrare la richiesta al mandante.

Per quanto compresi nelle prestazioni, il concetto di cancellazione, il diritto all'oblio, la rettifica e l'accesso ai dati sono garantiti direttamente dal mandatario conformemente alle istruzioni documentate del mandante.

### **5. Garanzia della qualità e ulteriori obblighi del mandatario**

Il mandatario garantisce in particolare l'ottemperanza alle seguenti prescrizioni:

- a)  Ha designato per iscritto un responsabile della protezione dei dati.
- i.  I dati di contatto del responsabile saranno comunicati al mandante ai fini di un contatto diretto. Il mandante sarà debitamente informato in merito a un'eventuale sostituzione del responsabile della protezione dei dati.
  - ii.  Il responsabile della protezione dei dati designato dal mandatario è la signora/il signor [inserire: nome, cognome, unità organizzativa, telefono, e-mail]. Il mandate sarà debitamente informato in merito a un'eventuale sostituzione del responsabile della protezione dei dati.
  - iii.  I dati di contatto aggiornati del responsabile sono facilmente accessibili sulla homepage del mandatario.
- iv. oppure
- Qualora il mandatario non abbia designato alcun responsabile della protezione dei dati, la seguente persona sarà designata referente della protezione dei dati o del presente contratto: [nome, cognome, unità organizzativa, telefono, e-mail]
- b) Il mandatario si impegna a mantenere il segreto su tutte le informazioni e tutti i documenti riservati, ecc. che gli sono forniti o di cui viene a conoscenza durante la stipula e l'esecuzione dell'accordo di prestazione, nonché a bloccarne l'accesso diretto e indiretto a terzi. Tale obbligo, essendo illimitato nel tempo, permane anche dopo lo scioglimento dell'accordo di prestazione.
  - c) Nell'adempiere i suoi compiti, il mandatario si avvale esclusivamente di dipendenti che ottemperano all'obbligo di riservatezza e che sono stati precedentemente istruiti circa le disposizioni rilevanti in materia di protezione dei dati. Il mandatario e tutte le persone a lui sottoposte con accesso ai dati personali dovranno trattare questi ultimi esclusivamente in conformità alle istruzioni fornite dal mandante, compresi i poteri conferiti dal presente accordo contrattuale, salvo che essi non siano legalmente obbligati al trattamento.
  - d) L'attuazione e il rispetto di tutte le misure tecniche e organizzative che il trattamento impone ai sensi della LPD [i dettagli nell'allegato 1].
  - e) Nell'esercizio delle loro funzioni, il mandante e il mandatario collaborano su richiesta con l'IFPDT.
  - f) Il mandatario è tenuto a informare senza indugio il mandante nel caso di ispezioni di controllo e provvedimenti da parte dell'IFPDT, nella misura in cui si riferiscono al presente trattamento dei dati. Altrettanto vale se un'autorità competente effettua degli accertamenti nell'ambito di una procedura giudiziaria riguardante i dati personali che il mandatario sta trattando.
  - g) Laddove il controllo dell'IFPDT, la procedura giudiziaria, la responsabilità della persona interessata o di terzi o qualsiasi altra pretesa legata al trattamento dei dati dovessero chiamare in causa il mandante, il mandatario è tenuto a sostenerlo al meglio delle sue capacità.
  - h) Il mandatario sottopone periodicamente a verifica i processi interni e le misure tecniche e organizzative, affinché il trattamento di sua competenza possa aderire ai requisiti imposti dall'attuale legge sulla protezione dei dati, nonché garantire la protezione dei diritti della persona interessata.
  - i) Nel quadro dei poteri di controllo conferitigli al punto 7 del presente accordo, il mandatario provvede ad assicurare al mandante la verificabilità delle misure tecniche e organizzative predisposte.

## 6. Rapporti di subappalto

Ai sensi del presente regolamento, per rapporti di subappalto si intendono le prestazioni di servizio direttamente correlate alla erogazione della prestazione principale. Anche nel caso di prestazioni accessorie esternalizzate, il mandatario è tenuto a stipulare degli accordi contrattuali adeguati e conformi

alla legge, nonché ad adottare delle apposite misure di controllo che assicurino la protezione e la sicurezza dei dati del mandante.

Esternalizzare i dati a un subappaltatore è:

- vietato**;
- consentito**, a condizione che venga stipulato un accordo contrattuale ai sensi della LPD e che anche il subappaltatore sia soggetto a tutte le disposizioni della catena contrattuale; l'esternalizzazione a un subappaltatore avviene:
  - in Svizzera;
  - in uno Stato membro dell'Unione Europea (UE) o dello Spazio economico europeo (SEE);
  - LPD: in un Paese che in base all'elenco degli Stati dell'IFPDT<sup>1</sup> dispone di una protezione dei dati adeguata;
  - in un Paese che non dispone di una protezione dei dati adeguata, nella misura in cui sono soddisfatti i requisiti speciali della LPD.

Il mandante accetta di conferire il trattamento dei dati ai seguenti appaltatori:

Appaltatore	Prestazione	Contatto/Paese	Garanzia

- Sostituire un appaltatore già esistente o avvalersi di un nuovo appaltatore è consentito, ammesso che:
  - il mandatario notifichi al mandante l'esternalizzazione all'appaltatore in ragionevole anticipo per iscritto o sotto forma di testo,
  - che, sino alla consegna dei dati, il mandante non si opponga al mandatario, per iscritto o sotto forma di testo, relativamente alla prevista esternalizzazione dei dati,
  - che alla base vi sia un accordo contrattuale ai sensi della LPD (il cosiddetto accordo per il trattamento dei dati) e
  - che in caso di trasmissione in un Paese che non dispone di protezione dei dati adeguata, siano altresì soddisfatte le garanzie speciali ai sensi della LPD (capitolo 2.2).

La trasmissione di dati personali all'appaltatore, nonché il suo primo intervento in quanto tale sono consentiti solo previa sussistenza di tutti i requisiti elencati in questo capitolo.

L'ulteriore esternalizzazione da parte dell'appaltatore

- è consentita;
- non è consentita;
- necessita del consenso esplicito del mandante principale;
- necessita del consenso esplicito del mandatario principale;

Tutte le disposizioni della catena contrattuale si applicano anche all'appaltatore successivo.

## 7. Diritti di controllo del mandante

Il mandatario mette il mandante in condizione di persuadersi della sua ottemperanza agli obblighi ai sensi della LPD. Il mandatario si impegna inoltre a fornire al mandante le informazioni richieste e, in particolare, a documentargli l'attuazione delle misure tecniche e organizzative.

Le parti possono concordare delle ulteriori prove documentate, che il mandante è autorizzato a fornire dietro remunerazione separata:

- l'ottemperanza alle regole comportamentali approvate ai sensi della LPD;
- la certificazione ai sensi della LPD;
- attestati, rapporti o loro estratti aggiornati forniti da organismi indipendenti (ad es. esperti contabili, organi di revisione, consulenti della protezione dei dati, reparti di sicurezza IT, auditor della protezione dei dati e della qualità);
- una certificazione adeguata ottenuta tramite audit sulla sicurezza IT o sulla protezione dei dati (ad es. la protezione di base secondo BSI o ISO 27001).

Opzione: la prova documentata di tali misure è solitamente fornita dal mandatario che invia al mandante una copia dell'attestato aggiornato unitamente a un estratto del corrispondente rapporto di audit.

Il mandante e, laddove previsto dalla legge, l'autorità di controllo della protezione dei dati del mandante hanno, in accordo con il mandatario, il diritto di effettuare dei controlli supplementari oppure di farli effettuare designando, nel singolo caso, degli appositi auditor. Il mandante ha il diritto di accertarsi che il mandatario rispetti l'accordo nell'esercizio della sua attività e, a tal fine, può disporre dei controlli a campione che in genere è tenuto a notificare per tempo. Il mandatario può far valere il diritto alla remunerazione per aver acconsentito ai controlli disposti dal mandante.

## 8. Notifica nel caso di violazioni da parte del mandatario

Il mandatario supporta il mandante nell'ottemperanza ai suoi obblighi per quanto concerne la sicurezza dei dati personali, la notifica nel caso di violazioni dei dati, la valutazione d'impatto sulla protezione dei dati e le consultazioni preventive. Questi includono, tra l'altro,

- la garanzia di un livello adeguato di protezione attraverso l'adozione di misure tecniche e organizzative che tengano conto delle circostanze e delle finalità del trattamento, nonché, preventivamente, del rischio e della serietà di possibili violazioni del diritto dovute a falle nella sicurezza e, ancora, che consentano di individuare tempestivamente i casi rilevanti di violazione;
- il dovere di notificare senza indugio al mandante tutte le violazioni dei dati personali (eventuali incidenti nel contesto della sicurezza dei dati e delle informazioni);
- il dovere di sostenere il mandante riguardo all'obbligo di informazione nei confronti della persona interessata e delle autorità competenti, nonché di fornirgli al riguardo tempestivamente tutte le informazioni rilevanti;
- il dovere di sostenere il mandante nell'esecuzione di una valutazione d'impatto sulla protezione dei dati, nella misura in cui si riferisce all'oggetto dell'accordo di prestazione;
- il dovere di sostenere il mandante nel contesto delle consultazioni preventive con l'IFPDT o con l'Ufficio cantonale per la protezione dei dati.

Il mandatario può far valere il diritto alla remunerazione per le prestazioni di supporto non comprese nell'accordo di prestazione o nel presente DPA, a condizione che non siano imputabili alla negligenza dello stesso.

## **9. Potere direttivo del mandante**

Il mandante è tenuto a confermare senza indugio le istruzioni verbali impartite (quantomeno sotto forma di testo, ad esempio tramite e-mail).

Se il mandatario ritiene che un'istruzione violi le disposizioni sulla protezione dei dati deve comunicarlo tempestivamente al mandante. Il mandatario ha il diritto di sospendere l'esecuzione della relativa istruzione fintanto che non sarà riconfermata o riformulata dal mandante.

## **10. Cancellazione e restituzione dei dati personali**

La produzione di copie o duplicati dei dati all'insaputa del mandante è vietata, fatta eccezione per le copie di sicurezza, se necessarie a garantire il regolare trattamento dei dati, nonché per i dati volti a ottemperare agli obblighi di conservazione previsti dalla legge.

A conclusione dei lavori concordati contrattualmente o anche prima su richiesta del mandante – ma al più tardi con la risoluzione dell'accordo di prestazione – il mandatario è tenuto a consegnare al mandante tutti i documenti in suo possesso, i risultati in merito al trattamento e utilizzo dei dati assieme ai database relativi al rapporto contrattuale, oppure a distruggerli previo consenso e conformemente al diritto sulla protezione dei dati. Lo stesso vale per il materiale di prova e di scarto. Laddove richiesto, occorre presentare il verbale della cancellazione.

Il mandatario deve conservare tutta la documentazione che dimostri il regolare e corretto trattamento dei dati anche dopo la cessazione dell'accordo, in conformità con i rispettivi termini di conservazione. Per ridurre l'onere, a fine accordo egli può anche decidere di consegnare la stessa documentazione al mandante.

## **11. Firma**

Data; firma del mandante:

Data; firma del mandatario:

## Allegato 1 – Misure tecnico-organizzative

**Nota:** Le presenti misure tecnico-organizzative forniscono degli esempi che devono essere adattati sia al servizio di esternalizzazione che agli specifici rischi ivi connessi.

<b>Controllo degli ingressi</b> ( <i>misure per prevenire gli ingressi non autorizzati agli impianti di trattamento dei dati</i> )	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Sistema automatizzato di controllo degli ingressi <input type="checkbox"/> Sistema di allarme <input type="checkbox"/> Sistema di chiusura biometrico <input type="checkbox"/> Serrature di sicurezza <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Identificazione della persona <input type="checkbox"/> Verbalizzazione degli ingressi <input type="checkbox"/> Regolamento chiavi <input type="checkbox"/> Selezione accurata del personale <input type="checkbox"/> Badge per dipendenti e ospiti <input type="checkbox"/> Impianto di videosorveglianza <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Controllo dell'accessibilità</b> ( <i>misure per prevenire l'accesso non autorizzato agli impianti di trattamento dei dati</i> )	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Autenticazione della persona <input type="checkbox"/> Utilizzo di software antivirus <input type="checkbox"/> Utilizzo di Firewall <input type="checkbox"/> Utilizzo di Mobile Device Management <input type="checkbox"/> Utilizzo di tecnologie VPN <input type="checkbox"/> Blocco chassis	<input type="checkbox"/> Concetto di autorizzazione <input type="checkbox"/> Gestione delle autorizzazioni amministrative all'utente <input type="checkbox"/> Creazione dei profili utente <input type="checkbox"/> Regole per la password <input type="checkbox"/> Verbalizzazione degli accessi <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)

<input type="checkbox"/> Crittografia dei supporti dati <input type="checkbox"/> Crittografia degli smartphone <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	
<b>Controllo degli accessi</b> <i>(le persone autorizzate possono accedere esclusivamente ai dati per cui hanno diritto di accesso).</i>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Verbalizzazione degli accessi <input type="checkbox"/> Cancellazione fisica dei supporti dati <input type="checkbox"/> Distruggidocumenti <input type="checkbox"/> Distruggidocumenti esterno (DIN 32757) <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Numero minimo di amministratori <input type="checkbox"/> Gestione delle autorizzazioni amministrative all'utente <input type="checkbox"/> Mobile Device Policy <input type="checkbox"/> Promemoria Protezione e sicurezza dei dati <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Controllo della separazione dei dati</b> <i>(i dati personali raccolti per finalità differenti devono poter essere trattati separatamente)</i>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Separare i dati pseudonomizzati dai file di associazione <input type="checkbox"/> Separare i dati attivi dai dati di prova <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Spazi di archiviazione separati in maniera coerente (creazione di un caso) <input type="checkbox"/> Concetto di autorizzazione <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Controllo della trasmissione dei dati</b> <i>(misure idonee a garantire che durante il trasporto o la registrazione su database i dati non vengano in alcun modo letti, copiati, modificati o rimossi senza previa autorizzazione)</i>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Creazione di tunnel VPN	<input type="checkbox"/> Documentazione dei destinatari di dati

<input type="checkbox"/> Crittografia di e-mail/utilizzo della firma elettronica <input type="checkbox"/> Contenitori per il trasporto sicuri <input type="checkbox"/> Trasmissione di dati anonimizzati <input type="checkbox"/> Trasmissione di dati pseudonomizzati <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Documentazione della restituzione dei dati <input type="checkbox"/> Documentazione del periodo di conservazione e della cancellazione <input type="checkbox"/> Documentazione delle regolari procedure di consultazione e trasferimento <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Controllo degli input</b> ( <i>misure idonee a garantire ex post la possibilità di verificare e determinare se e da chi i dati sono stati inseriti, modificati o cancellati</i> ).	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Verbalizzazione di input, modificazioni e cancellazioni <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Identificazione della persona <input type="checkbox"/> Assegnazione dei diritti di lettura e scrittura in base al concetto di autorizzazione <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Controllo del trattamento</b>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Selezione accurata e istruzioni al mandatario <input type="checkbox"/> Controlli periodici presso i locali del mandatario <input type="checkbox"/> Il trattamento è basato su un accordo contrattuale scritto <input type="checkbox"/> Il mandatario è vincolato alle disposizioni <input type="checkbox"/> Penalità contrattuali <input type="checkbox"/> Obbligo contrattuale di cancellazione a fine trattamento

	<input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Controllo della disponibilità e della resilienza</b>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Approvvigionamento ininterrotto di elettricità <input type="checkbox"/> Protezione da fuoco, fumo, alluvioni, umidità, ecc. <input type="checkbox"/> Backup <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)	<input type="checkbox"/> Concetto di backup <input type="checkbox"/> Disaster Recovery Plan <input type="checkbox"/> Esame del Recovery Process <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Verifica, valutazione e analisi periodiche</b>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Soluzioni software per la gestione della protezione dei dati <input type="checkbox"/> Accesso delle collaboratrici e dei collaboratori alle disposizioni interne in materia di protezione dei dati (ad es. intranet) <input type="checkbox"/> Certificazione della sicurezza dei dati informatici secondo ISO 27001, GoodPriv@cy, protezione IT di base BSI, ISIS12 <input type="checkbox"/> Concetto di sicurezza documentato (WIP) <input type="checkbox"/> Verifica della efficacia delle misure di sicurezza tecniche	<input type="checkbox"/> Responsabile della protezione dei dati (interno ed esterno): Dati di contatto <input type="checkbox"/> Formazione delle collaboratrici e dei collaboratori relativamente a: riservatezza, segretezza e protezione dei dati <input type="checkbox"/> Sensibilizzazione delle collaboratrici e dei collaboratori <input type="checkbox"/> Responsabile della sicurezza delle informazioni (interno ed esterno): Dati di contatto <input type="checkbox"/> Esecuzione di una valutazione d'impatto sulla protezione dei dati (DPIA) <input type="checkbox"/> L'organizzazione rispetta gli obblighi di informazione <input type="checkbox"/> Procedura per l'elaborazione di richieste di accesso alle informazioni da parte delle persone interessate <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)

<b>Incident-Response-Management</b>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Utilizzo di Firewall, aggiornamento periodico <input type="checkbox"/> Utilizzo di filtri spam, aggiornamento periodico <input type="checkbox"/> Utilizzo di antivirus, aggiornamento periodico <input type="checkbox"/> Intrusion Detective System (IDS) <input type="checkbox"/> Intrusion Prevention System (IPS)	<input type="checkbox"/> Processo per identificare e notificare gli incidenti legati alla sicurezza <input type="checkbox"/> Procedura documentata nel gestire gli incidenti legati alla sicurezza dei dati <input type="checkbox"/> Coinvolgere il responsabile della sicurezza dei dati <input type="checkbox"/> Coinvolgere il responsabile della sicurezza delle informazioni <input type="checkbox"/> Documentazione di incidenti legati alla sicurezza <input type="checkbox"/> Processo e responsabilità negli interventi correttivi per gli incidenti legati alla sicurezza <input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Impostazioni predefinite nel rispetto della protezione dei dati: Privacy by design / Privacy by default</b>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Raccolta dei dati personali solo se compatibili con le finalità prestabilite <input type="checkbox"/> Facilitare il diritto di recesso delle persone interessate attraverso l'attuazione di misure tecniche	<input type="checkbox"/> Altri: (si prega di fornire una descrizione generale)
<b>Ulteriori misure</b> <i>(Qualora si intenda sottoscrivere anche le SCC, occorre prima verificare se siano state adottate o meno le seguenti misure).</i>	
<b>Misure tecniche</b>	<b>Misure organizzative</b>
<input type="checkbox"/> Misure a garanzia dei principi inerenti il trattamento dei dati <input type="checkbox"/> Misure a garanzia dei diritti delle persone interessate	<input type="checkbox"/> Misure a garanzia dei principi inerenti il trattamento dei dati <input type="checkbox"/> Misure a garanzia dei diritti delle persone interessate

<input type="checkbox"/> Misure per la qualità dei dati	<input type="checkbox"/> Misure per la qualità dei dati
<input type="checkbox"/> Misure per limitare l'archiviazione	<input type="checkbox"/> Misure per limitare l'archiviazione
<input type="checkbox"/> Misure per minimizzare i dati	<input type="checkbox"/> Misure per minimizzare i dati
<input type="checkbox"/> Misure di responsabilità	<input type="checkbox"/> Misure di responsabilità

