FONDAZIONE
DESTINATION
FLORENCE

Procedura di selezione e valutazione dei fornitori di beni e servizi

Approvato dal CdA in data ____

FONDAZIONE
DESTINATION
FLORENCE

SCHEDA CONTROLLO DOCUMENTO

IDENTIFICAZIONE

TITOLO DEL DOCUMENTO	**Procedura di selezione dei fornitori di beni e servizi**

REVISIONI

Versione	Data emissione	Commento	Firma
V.01		Prima emissione	

INDICE

1. Finalità della procedura ed ambito di applicazione

Lo scopo della presente procedura è quello di definire, nel rispetto del piano strategico determinato dal Consiglio di Amministrazione, i criteri e le modalità utilizzate dalla Fondazione Destination Florence Convention & Visitors Bureau (di seguito "Destination Florence" o "Fondazione") per l'attività di selezione e valutazione dei fornitori ai fini dell'approvvigionamento di prodotti, servizi, prestazioni professionali o lavori, di valore inferiore alle soglie di rilevanza europea di cui all'art. 14, D.Lgs. n. 36/2023 (di seguito il "Codice"), che hanno influenza sulla qualità del servizio erogato e/o sulla qualità dei processi aziendali, definendone le relative responsabilità. Il presente documento si prefigge inoltre lo scopo di includere all'interno di un'unica procedura tutte le attività di valutazione dei fornitori e della gestione degli approvvigionamenti di valore inferiore alle soglie eurounitarie.

La presente procedura si applica ai fornitori dei beni e servizi che hanno diretta o indiretta influenza sulla qualità dei servizi forniti da Destination Florence ai suoi clienti. Sono esclusi, di conseguenza, i fornitori di quei beni e servizi le cui caratteristiche non trovano riscontro nei servizi forniti dalla Fondazione: tipicamente il materiale di cancelleria, etc.

2. Principi

La presente Procedura si ispira ai principi di rotazione negli affidamenti, trasparenza, parità di trattamento, proporzionalità, non discriminazione, buona fede e tutela della concorrenza; persegue, inoltre, l'obiettivo da parte della Fondazione di raggiungere con la massima tempestività il migliore rapporto possibile tra qualità e prezzo.
La Fondazione, in linea col disposto normativo dell'art. 1 del Codice, attua tale finalità nel rispetto dei principi di legalità, trasparenza, risultato e concorrenza.
Trasparenza in quanto funzionale alla massima celerità nella corretta applicazione del T.U. appalti e concorrenza quale mezzo per conseguire il miglior risultato nell'affidamento dei contratti.

Questi sono i valori che la Fondazione decide di attuare e perseguire nella valutazione e scelta dei propri fornitori.

3. Modalità operative

3.1. L'affidamento dei servizi e forniture di valore inferiore alle soglie eurounitarie di cui all'art. 14, D.Lgs. n. 36/2023.

L'affidamento di lavori, beni o servizi viene svolta dalla Fondazione nel rispetto dei principi di trasparenza, rotazione, parità di trattamento secondo le regole e le modalità di cui alla Parte I, Libro II, D.Lgs. n. 36/2023 (artt. 49 e ss.).

Salvo quanto previsto dagli articoli 62 e 63 del Codice, la Fondazione procede all'affidamento dei contratti di lavori, servizi e forniture di importo inferiore alle soglie di cui all'articolo 14 del Codice con le seguenti modalità:

A. affidamento diretto per lavori di importo inferiore a 150.000 euro anche senza consultazione di più operatori economici, previa valutazione di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali;
B. affidamento diretto dei servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro;
C. procedura negoziata senza bando, previa consultazione di almeno cinque operatori economici, ove esistenti, per i lavori di importo pari o superiore a 150.000 euro e inferiore a 1 milione di euro;
D. procedura negoziata senza bando, previa consultazione di almeno dieci operatori economici, ove esistenti, individuati in base a indagini di mercato o tramite elenchi di operatori economici, per lavori di importo pari o superiore a 1 milione di euro e fino alle soglie di cui all'articolo 14, salva la possibilità di ricorrere alle procedure di scelta del contraente di cui alla Parte IV del presente Libro;
E. procedura negoziata senza bando, previa consultazione di almeno cinque operatori economici, ove esistenti, individuati in base ad indagini di mercato o tramite elenchi di operatori economici, per l'affidamento di servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo pari o superiore a 140.000 euro e fino alle soglie di cui all'articolo 14.

Nelle procedure di affidamento di cui all'articolo 50, comma 1, lettere a) e b), di importo inferiore a 40.000,00 euro, gli operatori economici attestano con dichiarazione sostitutiva di atto di notorietà il possesso dei requisiti di partecipazione e di qualificazione richiesti nell'invito e dalla normativa vigente. La Fondazione verifica le dichiarazioni, anche previo sorteggio di un campione individuato con modalità predeterminate ogni anno.

Nelle procedure di affidamento di cui all'articolo 50, comma 1, non sono richieste garanzie provvisorie di cui all'articolo 106 del Codice ad esclusione delle procedure di cui alle lettere c), d) ed e) dello stesso comma 1 dell'articolo 50, in considerazione della tipologia e specificità della singola procedura, ricorrano particolari esigenze indicate nei documenti di gara.

Quando è richiesta la garanzia provvisoria, il relativo ammontare non può superare l'uno per cento dell'importo previsto nell'avviso o nell'invito per il contratto oggetto di affidamento.

- La garanzia provvisoria può essere costituita sotto forma di cauzione oppure di fideiussione con le modalità di cui all'articolo 106 del Codice.
- In casi debitamente motivati è facoltà della Fondazione non richiedere la garanzia definitiva per l'esecuzione dei contratti di cui alla presente Parte oppure per i contratti di pari importo a valere su un accordo quadro. Quando richiesta, la garanzia definitiva è pari al 5 per cento dell'importo contrattuale.

In ogni caso, si precisa che la Fondazione, una volta vagliata la possibilità di ricorrere al mercato attraverso l'indizione di una procedura di selezione del fornitore aperta o ristretta, può valutare l'opportunità di procedere ad un affidamento interno ai propri soci, purché ricorrano i requisiti eccezionali di necessità ed urgenza.

In quest'ultimo caso sarà necessario indicare in maniera specifica le motivazioni che hanno portato alla scelta di affidare internamente la fornitura di beni e/o servizi.

Rimandandosi alla normativa cogente richiamata quale riferimento imprescindibile ai fini della corretta gestione dell'approvvigionamento di beni, servizi e lavori, si procede e specificare le modalità approvvigionamento di beni e servizi e lavori di valore inferiore alla soglia di euro 140.000,00, con particolare riferimento alla modalità con cui la Fondazione procede alla selezione e valutazione dei fornitori.

3.1.1. Affidamento di beni o servizi o lavori al di sotto della soglia di euro 140.000,00.

In caso di approvvigionamento di servizi e beni di valore superiore alla soglia dei 140.000,00 euro, la Fondazione procede con una procedura aperta ad evidenza pubblica secondo il principio dell'offerta più vantaggiosa salvi i casi di cui al combinato disposto degli artt. 50 e 70 D.Lgs. 36/2023.

Per gli affidamenti al di sotto della soglia dei 140.000,00 euro Destination Florence definisce, come di seguito si espone, diversi scaglioni di riferimento per l'affidamento diretto di beni e/o servizi:

- per gli affidamenti da 50.000,00 a 139.999,00 euro, rispetto ai quali devono essere richiesti almeno 3 preventivi;
- per gli affidamenti da 10.000,00 e 49.999,00 rispetto ai quali devono essere richiesti almeno 2 preventivi;
- al di sotto della soglia di 9.999,00 euro compresi, è consentito l'affidamento diretto in seguito alla richiesta, dunque, di un unico preventivo.

Per gli affidamenti relativi a lavori di valore inferiore alla soglia dei 150.000,00 euro, Destination Florence definisce, come di seguito si espone, diversi scaglioni per l'affidamento diretto di dette commesse:

-per gli affidamenti da 50.000,00 euro a 149.999,00 euro, rispetto ai quali devono essere richiesi almeno 3 preventivi;

- per gli affidamenti da 10.000,00 euro a 49.999,00 euro rispetto ai quali devono essere richiesti almeno 2 preventivi;

- al di sotto della soglia di 9.999,00 euro compresi, è consentito l'affidamento diretto in seguito alla richiesta di un unico preventivo.

Sia nel caso di affidamento diretto per lavori che nel caso di affidamento diretto di beni e servizi di importo inferiore a 5.000 euro, si può procedere ad affidamento diretto senza preventiva consultazione del mercato e derogando al principio di rotazione ai sensi e nei limiti di cui agli artt. 49 e 50 D.Lgs n. 36/2023.

La richiesta di preventivi, inviata contestualmente agli operatori economici, viene effettuata mediante richiesta di offerta via e-mail. Qualora la richiesta sia di modesta entità, per la richiesta di offerta vige il principio di libertà della forma e di sinteticità dei contenuti.

3.1.2. Scelta dei fornitori da invitare a presentare preventivo.

Ai fini dell'individuazione degli operatori economici da invitare a presentare un preventivo nelle procedure di cui sopra, Destination Florence può:

a) attingere dal proprio Elenco Fornitori Qualificati, individuando i fornitori da invitare in base al criterio della rotazione, unito a criteri di valutazione, caso per caso, riguardanti l'entità del lavoro da effettuare, la capacità economica dell'impresa, quella professionale ed ogni altra valutazione che la Direzione Generale riterrà di dover effettuare a seconda del caso concreto, di cui si dirà i*nfra*;
b) utilizzare il mercato elettronico della Pubblica Amministrazione attivato da Consip S.p.a;
c) comunque invitare alle procedure per la scelta del contraente altri operatori

Purchè, in tutti e tre i casi, gli stessi siano stati ritenuti idonei dalla Fondazione: in Fornitori possono essere selezionati, ai fini della consultazione nelle procedure dirette di affidamento, a seguito di opportuna valutazione, da effettuarsi caso per caso, da parte della Direzione Generale, sentita anche la Funzione interessata dall'approvvigionamento, che tenga di conto l'entità e specificità della commessa da realizzare, la capacità economica dell'impresa, quella professionale, pregressi rapporti contrattuali con il fornitore, fermo il rispetto del principio di rotazione ex art. 49 del Codice, ed ogni altra valutazione che la Direzione Generale riterrà di dover effettuare a seconda del caso concreto.
L'iscrizione all'Elenco Fornitori Qualificati è obbligatoria per i *tour operator* e per i fornitori di servizi che vogliano operare tramite la piattaforma online *destinationflorence.com.*

Si ribadisce che la Fondazione, una volta vagliata la possibilità di ricorrere al mercato attraverso l'indizione di una procedura di selezione del fornitore aperta o ristretta, può valutare l'opportunità di procedere ad un affidamento interno ai propri soci, purché ricorrano i requisiti eccezionali di necessità ed urgenza.
In quest'ultimo caso sarà necessario indicare in maniera specifica le motivazioni che hanno portato alla scelta di affidare internamente la fornitura di beni e/o servizi.

In virtù dell'art. 49, comma 4, D.Lgs. n. 36/2023, la Fondazione può reinvitare o individuare come affidatario diretto il contraente uscente in casi debitamente motivati con riferimento (cumulativamente):

1) alla struttura del mercato;
2) effettiva assenza di alternative;
3) accurata esecuzione del pregresso contratto.

Come sopra rappresentato (§3.1.1.), in caso di affidamenti diretti di importo inferiore ad euro pari a 5.000 euro, per i quali non è necessaria una preventiva indagine di mercato ai sensi dell'art. 50, D.Lgs. n. 36/2023, è consentito derogare al principio di rotazione (art. 49, ult. Comma, D.Lgs. n. 36/2023).

L'applicazione del principio di rotazione si intende riferita al contraente uscente.

3.2. Richiesta di preventivo e conclusione del contratto.

La richiesta di preventivo deve contenere:

a) l'oggetto della prestazione e le caratteristiche tecniche/funzionali;

b) i tempi e le modalità di esecuzione e/o consegna;

c) il termine di presentazione delle offerte ed il periodo di validità delle stesse;

d) le eventuali garanzie;

e) i termini di pagamento.;

f) il CCNL applicabile al personale dipendente impiegato nell'appalto (art. 11, D.Lgs. n. 36/2023);

g) la richiesta di produzione di tutti i documenti e/o dichiarazioni prescritte dal D.Lgs. n. 36/2023 ai fini di partecipazione alla procedura di aggiudicazione (es. patto di integrità, dichiarazione sostitutiva 52 D.lgs. n. 36/2023, Comunicazione c/c dedicato e relativi delegati ad operarvi, etc.);

h) le ulteriori indicazioni prescritte dall'allegato II.9 al D.Lgs.n. 36/2023;

i) testo dell'informativa privacy fornitori (appendice 1);

f) tenendo conto del servizio richiesto al fornitore e qualora questo comporti un trattamento di dati personali per conto della Fondazione ai sensi dell'art. 28 del Regolamento UE 2016/679 – sentiti i consulenti privacy e/o il Responsabile della protezione dei dati (DPO) se nominato – la richiesta di preventivo dovrà contenere anche la check list sulle misure tecniche e organizzative adottate dal Fornitore (appendice 2).

Pertanto, la Fondazione nella valutazione dei preventivi terrà di conto dei seguenti elementi:

- qualità dei prodotti o dei servizi forniti - vengono presi in esame gli elementi necessari per effettuare una valutazione dei prodotti o dei servizi che interessano la Fondazione, come ad esempio: la funzionalità, l'affidabilità, l'efficienza etc.;

- rispetto dei tempi: vengono valutati i tempi di consegna, o di erogazione del servizio, che il fornitore dichiara di attuare e la loro effettiva fattibilità;
- disponibilità - flessibilità: si valuta la capacità del fornitore di rispondere alle esigenze espresse dalla Fondazione;
- prezzi: si valutano i prezzi, gli sconti praticati, il rapporto prezzo/prestazione, modalità di pagamento, etc;
- referenze: vengono valutate le referenze del fornitore, sia quelle fornite dal Fornitore stesso, sia quelle delle quali la Fondazione è venuta a conoscenza;
- rispetto delle norme legislative e regolamentati vigenti in materia di osservanza degli oneri assicurativi e previdenziali, delle norme in materia di sicurezza sul lavoro e di retribuzione dei dipendenti;
- idoneità delle misure tecniche e organizzative (appendice 2), qualora la fornitura rientri nell'ambito di applicazione dell'art. 28 del Regolamento UE 2016/679.

Nella lettera di invito può essere inserita la clausola per cui la richiesta di preventivo non impegna la richiedente, ovvero le riserva di aggiudicare, ove sia vantaggioso per la stessa, anche in presenza di una sola offerta valida o di non aggiudicare motivatamente.

Al ricevimento delle offerte economiche, valutato il possesso dei requisiti di ordine generale e speciale richiesti ex lege (artt. 94 e ss. D.Lgs. n. 36/2023) in capo al fornitore concorrente-la cui carenza determina l'impossibilità dell'aggiudicazione-, valutata l'offerta economica sia dal punto di vista tecnico che economico e, dopo aver individuato l'offerta più congrua, segue, in base all'iter delineato dal combinato disposto di cui agli artt. 17 e 18 del Codice:
- la decisione a contrarre adottata dal Direttore Generale che contiene le informazioni di cui all'art. 17, comma 2, del Codice;
-l'ordine stilato direttamente dall'Ufficio preposto in base alla procedura delineata dal combinato disposto di cui agli artt. 17 e 18 del D.Lgs. n. 36/2023.

Negli affidamenti di beni e servizi di valore inferiore ad euro 40.000, gli operatori economici attestano con dichiarazione sostitutiva di atto di notorietà il possesso dei requisiti di partecipazione e di qualificazione richiesti. La Fondazione verifica le dichiarazioni anche previo sorteggio a campione.

In ossequio all'art. 99 del Codice, la Fondazione verifica l'assenza di cause di esclusione automatiche di cui all'articolo 94 attraverso la consultazione del fascicolo virtuale dell'operatore economico di cui all'articolo 24, la consultazione degli altri documenti allegati dall'operatore economico, nonché tramite l'interoperabilità con la piattaforma digitale nazionale dati di cui all'articolo 50-ter del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e con le banche dati delle pubbliche amministrazioni.

La Fondazione, con le medesime modalità di cui al comma 1, verifica l'assenza delle cause di esclusione non automatica di cui all'articolo 95 e il possesso dei requisiti di partecipazione di cui agli articoli 100 e 103 del Codice.

Agli operatori economici non possono essere richiesti documenti che comprovano il possesso dei requisiti di partecipazione o altra documentazione utile ai fini dell'aggiudicazione, se questi sono presenti nel fascicolo virtuale dell'operatore economico, sono già in possesso della stazione appaltante, per effetto di una precedente aggiudicazione o conclusione di un accordo quadro, ovvero possono essere acquisiti tramite interoperabilità con la piattaforma digitale nazionale dati di cui all'articolo 50-ter del co-dice di cui al decreto legislativo n. 82 del 2005 e con le banche dati delle pubbliche amministrazioni.

Ai sensi dell'art. 99 del D.Lgs 36/2023, la stazione appaltante è dunque tenuta a controllare il possesso dei requisiti da parte dell'operatore economico prescelto, destinatario di un affidamento provvisorio. Tale attività di verifica potrà essere condotta attraverso un collegamento al portale dedicato dell'ANAC.

Prima della sottoscrizione del contratto, qualora la fornitura rientri nell'ambito di applicazione dell'art. 28 del Regolamento UE 2016/679, – sentiti i consulenti privacy e/o il Responsabile della protezione dei dati (DPO) se nominato – la Fondazione trasmette al fornitore l'accordo che disciplina il trattamento dei dati personali da esso derivante (c.d. Nomina del responsabile del trattamento ex art. 28 Regolamento UE 2016/679).

La Fondazione si riserva di aggiornare la presente Procedura ogniqualvolta lo ritenga necessario in ragione dell'intervento di modifiche normative rilevanti ai fini della disciplina di riferimento nonché della sopravvenienza di nuove o mutate esigenze organizzative interne.

APPENDICE 1
INFORMATIVA FORNITORI

Gentile Fornitore, Fondazione Destination Florence Convention & Visitors Bureau (di seguito "DFCVB"), in qualità di Titolare del trattamento, La informa – ai sensi degli artt. 13 e 14 del Regoalmento UE 2016/679 (in seguito "GDPR") - che per l'iscrizione nell'Elenco Fornitori Qualificati e per l'instaurazione ed esecuzione dei rapporti contrattuali di cui Lei è parte potrà venire a conoscenza (o essere già in possesso) di dati personali a Lei riferiti o riferiti ai Suoi dipendenti, collaboratori o amministratori. Tali dati personali saranno trattati come segue:

1. Tipologia di dati trattati

Potranno essere oggetto di trattamento le seguenti tipologie di dati personali:

a) Dati anagrafici, identificativi e di contatto (quali, a titolo di esempio, nome, cognome, data di nascita, codice fiscale, residenza, indirizzi, contatti telefonici, fax, e-mail, pec);
b) informazioni relative a condanne e reati, nonché l'esistenza di procedimenti penali in corso derivanti dai certificati dei carichi pendenti, per i soggetti apicali dell'azienda (art. 94 segg. D.Lgs 36/2023);
c) dati idonei ad attestare il possesso dei requisiti previsti dalla normativa antimafia (D.Lgs. n. 159/2011);
d) Informazioni attestanti qualifiche professionali o a servizi e prestazioni precedentemente svolti, informazioni relative all'attività professionale esercitata, iscrizioni a ordini professionali e certificazioni, posizioni previdenziali e assicurative, estremi bancari.

2. Finalità del trattamento

I dati personali potranno essere trattati per le seguenti finalità:

a) Acquisizione di informazioni preliminari per consentire la valutazione del Fornitore (referenze per precedenti lavori, solidità finanziaria, struttura organizzativa interna, assenza di elementi ostativi in termini di legge);
b) Valutazione e selezione dei fornitori da interpellare per lo svolgimento delle procedure di acquisto;
c) Accertamento dei requisiti di idoneità derivanti dalle autodichiarazioni prodotte e adempimento degli obblighi di legge previsti, comprendente anche il trattamento di dati personali relativi a condanne penali e ai reati o a connesse misure di sicurezza;
d) Adempimenti connessi agli obblighi derivanti dalle normative vigenti in materia di trasparenza amministrativa;
e) Esecuzione di obblighi derivanti da un contratto del quale il Fornitore è parte, o per adempiere, prima dell'esecuzione del contratto, a Sue specifiche richieste; adempimento di obblighi di legge connessi a disposizioni civilistiche, fiscali e contabili relative ai fornitori; gestione amministrativa dei fornitori (amministrazione dei fornitori; amministrazione di contratti, ordini, spedizioni); gestione dell'eventuale contenzioso (inadempimenti contrattuali, diffide, transazioni, recupero crediti, arbitrati, controversie giudiziarie).

3. Base giuridica

I trattamenti elencati sono connessi ai contratti di fornitura o sono propedeutici all'eventuale instaurazione di rapporti contrattuali (Art. 6, c. 1 lettera b del GDPR). I trattamenti si basano anche sulla necessità di adempiere agli obblighi legali ai quali è soggetto il titolare del trattamento (Art. 6, comma 1 lettera c del GDPR). Nella gestione eventuale del contenzioso la base giuridica è il legittimo interesse del Titolare del trattamento (Art. 6, c. 1 lettera f del GDPR).

4. Conferimento e Tempi di conservazione

Il conferimento dei dati richiesti è obbligatorio per il conseguimento delle finalità di cui sopra; il loro mancato, parziale o inesatto conferimento potrà comportare la mancata validazione dell'iscrizione all'Elenco Fornitori Qualificati, l'esclusione dalle procedure di acquisto o la decadenza dall'eventuale aggiudicazione. I dati relativi all'impresa e quelli necessari ai criteri di validazione potranno essere trattati per il periodo di permanenza nel suddetto Elenco. I dati acquisiti saranno trattati fino alla conclusione del procedimento di selezione e, in caso di affidamento, per tutta la durata del rapporto contrattuale. Esaurite le finalità per cui sono trattati, saranno conservati nel rispetto delle norme vigenti sulla conservazione della documentazione amministrativa.

5. Destinatari dei dati personali

I dati saranno trattati da personale incaricato, opportunamente istruito e operante sotto l'autorità e la responsabilità del titolare. Alcune informazioni potranno esse comunicate, sulla base di quanto stabilito dalle normative vigenti, ad enti pubblici ed Autorità di controllo nei casi previsti dalla legge. Le informazioni potranno inoltre essere trasmesse, nei limiti previsti dalla legge, a concorrenti di gara o ad altri soggetti aventi titolo in base alle normative sul diritto di accesso ai documenti amministrativi.

Alcuni dati potranno essere oggetto di pubblicazione sui siti Web del committente in base a quanto previsto dalle norme relative alla pubblicità legale e alla pubblicità ai fini di assicurare la trasparenza dell'attività dell'Ente.

I dati personali potranno essere trattati, inoltre, da soggetti terzi che forniscono servizi strumentali, tra cui servizi di comunicazione, posta elettronica, recapito della corrispondenza, servizi tecnici informatici, studi legali o di consulenza ai quali il Titolare ha conferito specifico mandato e altri fornitori di servizi inerenti alle finalità sopraccitate. A tali soggetti saranno comunicati solo i dati strettamente necessari per l'espletamento delle relative funzioni. L'elenco dettagliato di tali soggetti è disponibile presso la sede del Titolare del trattamento e verrà fornito su Sua richiesta scrivendo ai recapiti sottoindicati.

6. Diritti dell'interessato

La informiamo, inoltre, che può esercitare in qualsiasi momento i diritti previsti dal CAPO III del GDPR. In particolare, Lei ha diritto di chiedere al Titolare l'accesso ai dati che lo riguardano, la loro rettifica o la cancellazione, l'integrazione dei dati incompleti, la limitazione del trattamento, di opporsi in tutto od in parte, all'utilizzo dei dati, nonché di esercitare gli altri diritti riconosciutigli dalla disciplina applicabile. Tali diritti possono essere esercitati scrivendo ai recapiti sottoindicati.

Ai sensi dell'art. 77 del GDPR, inoltre, l'interessato ha diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali nel caso in cui ritenga che il trattamento violi il citato Regolamento.

7. Dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati (DPO)

Titolare del trattamento è Fondazione Destination Florence Convention & Visitors Bureau, via del Tiratoio, 1 – 50124 Firenze (Italia). Il DPO è contattabile al seguente indirizzo e-mail – privacy@conventionbureau.it

FONDAZIONE
DESTINATION FLORENCE

APPENDICE 2

CHECK LIST MISURE TECNICHE E ORGANIZZATIVE (ART. 28 REGOLAMENTO UE 2016/679)

Il presente allegato contiene la descrizione delle misure tecniche e organizzative messe in atto dal/dai Responsabile/i del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

N°	Controlli	
1	Riservatezza	
1.1	Controllo fisico degli accessi - accesso ai locali e alle strutture in cui vengono trattati i dati. Requisito: *è necessario evitare l'accesso (fisico) di soggetti non autorizzati agli edifici e alle strutture in cui vengono trattati i dati personali del Titolare del trattamento. Il Responsabile del trattamento deve mettere in atto sistemi di controllo degli accessi efficienti (controllo degli accessi tecnologico o mediante personale).*	[Selezionare]
1.1.1	A tal fine vengono messe in atto le seguenti misure tecniche: ☐ Sistemi di allarme ☐ Sistemi antintrusione (barriere fotoelettriche/rilevatori di movimento) ☐ Sistemi automatici di controllo degli accessi ☐ Barriere di accesso biometriche ☐ Sistema di accesso mediante smart card/trasponder ☐ Sistemi di chiusura manuali ☐ Sistemi di chiusura con codice d'accesso ☐ Videosorveglianza dei punti di accesso ☐ *Altro: specificare o inserire spazi*	
1.1.2	A tal fine vengono messe in atto le seguenti misure organizzative. ☐ Controlli del personale tramite portineria/all'accoglienza ☐ Registrazione dei visitatori/libro dei visitatori ☐ Accompagnamento dei visitatori ☐ Registrazione delle chiavi/libro delle chiavi ☐ Obbligo di indossare badge identificativi per dipendenti ☐ Obbligo di indossare badge identificativi per ospiti ☐ Zone di sicurezza con diverse autorizzazioni di accesso ☐ Supervisione del personale esterno ad es. personale per la manutenzione e di servizio ecc. ☐ *Altro: specificare o inserire spazi*	

1.2	**Controllo logico degli accessi** - L'accesso logico ai sistemi di trattamento, alle applicazioni e ai dati deve essere riservato esclusivamente ai soggetti autorizzati. **Requisito**: *è necessario evitare l'accesso non autorizzato ai sistemi IT. Devono essere messe in atto misure tecniche e organizzative per l'identificazione e l'autenticazione degli utenti.* *L'accesso ai sistemi IT del Responsabile del trattamento deve essere limitato agli utenti autorizzati mediante un processo di autenticazione sicuro. Ogni utente deve avere un ID utente univoco. La condivisione degli account non è consentita.* *L'accesso ai sistemi IT e alle applicazioni del Responsabile del trattamento deve essere accessibile tramite sistemi di autenticazione che prevedono come requisito minimo l'utilizzo di credenziali composte da nome utente e password. Tale protezione deve includere, ma non essere limitata a una policy per la password sicura, una disconnessione automatica dopo un determinato periodo di tempo, il blocco in seguito a diversi tentativi di accesso falliti, una procedura di ripristino della password affidabile, una modifica periodica delle password. Le password devono essere sempre conservate e trasmesse in modo sicuro, ad es. mediante crittografia e funzione hash. Il Responsabile del trattamento ha definito i requisiti, le regole e gli standard delle linee guida per le password in una politica conosciuta dagli utenti e supportata a livello tecnico. Le password devono essere assegnate a una singola persona, conservate e trasmesse in modo sicuro, devono essere sufficientemente lunghe e complesse, modificate su base regolare, limitate in termini di validità, bloccate e successivamente eliminate se inattive per un lungo periodo di tempo e modificate immediatamente qualora compromesse. Ove possibile, in particolare per le utenze con privilegi elevati e per i sistemi e le applicazioni che ospitano dati particolari, si predilige l'utilizzazione di sistemi di autenticazione a più fattori*	. [Selezionare]
1.2.1	A tal fine vengono messe in atto le seguenti **misure tecniche**: ☐ Autenticazione con username e password ☐ Autenticazione a due fattori ☐ Autenticazione con dati biometrici ☐ Utilizzo di certificati digitali per l'autenticazione ☐ Identity and Access Management centralizzato ☐ Sistemi di Single Sign On ☐ Sistemi di controllo scadenza password ☐ Sistemi di controllo robustezza e complessità password ☐ Sistemi di blocco account dopo numero predefinito di tentativi falliti ☐ Sistemi di controllo dell'utilizzo contemporaneo dello stesso account sulle applicazioni ☐ Utilizzo di VPN autenticata crittografata per accesso da remoto ☐ Utilizzo password o pin per i dispositivi mobili ☐ Utilizzo di salvaschermi automatici ☐ Time-out sessione per le applicazioni ☐ *Altro: specificare o inserire spazi*	
1.2.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedure di assegnazione degli account ☐ Inventario aggiornato degli account assegnati ☐ Inventario aggiornato degli account di servizio utilizzati dalle applicazioni ☐ Cancellazione o disabilitazione degli account non utilizzati dopo un periodo di tempo definito ☐ Formazione del personale sull'uso degli account aziendali ☐ Regolamenti o politiche per gli account aziendali e la robustezza delle password ☐ Procedure di azzeramento o ripristino password ☐ *Altro: specificare o inserire spazi*	

1.3	**Profili di autorizzazione e controllo delle autorizzazioni** – Nessuna lettura, copia, modifica o rimozione non autorizzata all'interno del sistema informatico o per il trattamento di dati su supporti cartacei. **Requisito:** *Il Responsabile del trattamento deve definire specifici profili di autorizzazione per i soggetti che accedono ai dati e mettere in atto soluzioni per il controllo dei diritti di accesso e le necessarie autorizzazioni, che devono essere strettamente limitate a consentire l'attività delegata al soggetto autorizzato. Il controllo delle autorizzazioni prevede anche politiche e strumenti di monitoraggio e di registrazione degli accessi ai dati. Particolare attenzione deve essere posta all'assegnazione di privilegi elevati, che devono essere riservati ai tecnici che effettuano operazioni di amministrazione dei sistemi, delle banche dati e delle applicazioni (cd. Amministratori di sistema). Gli amministratori di sistema devono avere un account con privilegi elevati individuale per eseguire le loro attività di amministrazione diverso da quello utilizzato per le attività che non richiedono diritti particolari. I dischi e le memorie destinate allo smaltimento o riutilizzo devono essere distrutti o soggetti a cancellazione sicura*	[Selezionare]
1.3.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Profili utente con accesso limitato alla rete ed alle applicazioni ☐ Ruoli e autorizzazioni basati sul principio della necessità di accesso ai dati ☐ Configurazione dei file server con aree ad accesso limitato in base alle autorizzazioni assegnate ☐ Configurazione delle applicazioni per l'assegnazione di privilegi minimi per eseguire l'attività assegnata all'utente ☐ Sistema di registrazione (log) delle modifiche dei privilegi assegnati ☐ Sistema di alert delle modifiche dei privilegi assegnati ☐ Sistema di registrazione (log) dell'accesso ai sistemi da parte degli amministratori di sistema ☐ Sistema di registrazione (log) dell'accesso ai sistemi da parte degli utenti ☐ Sistema di registrazione (log) dell'accesso alle applicazioni o ai database da parte degli amministratori di sistema ☐ Sistema di registrazione (log) dell'accesso alle applicazioni da parte degli utenti ☐ Registrazione delle attività di inserimento, modifica o cancellazione di dati ☐ Profili di accesso a scanner, fotocopiatrici e stampanti di rete ☐ Meccanismi di cancellazione sicura dei dati (quali wiping program e formattazione a basso livello) per i dischi e le unità di memoria destinati a riutilizzo o smaltimento ☐ *Altro: specificare o inserire spazi*	

1.3.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Creazione di profili utente con autorizzazioni in base al ruolo e a compiti assegnati (Segregation of duty, need to know e least privilege) ☐ Procedure di autorizzazione documentate (richiesta, assegnazione, revoca delle autorizzazioni) ☐ Riesame regolare delle autorizzazioni ☐ Account con privilegi amministrativi individuali e utilizzati solo quando necessario ☐ Account individuali anche per i tecnici esterni che necessitano di credenziali amministrative ☐ Verifica delle caratteristiche soggettive di esperienza, capacità e affidabilità degli amministratori di sistema ☐ Elenco aggiornato degli amministratori di sistema, con il dettaglio dei compiti assegnati ☐ Verifica periodica delle attività degli amministratori di sistema ☐ Presidio, controllo e verifica delle attività degli interventi tecnici effettuati da personale esterno ☐ Distruzione dei supporti di memorizzazione destinati allo smaltimento ☐ Regole e policy su utilizzo di scanner, fotocopiatrici e stampanti di rete ☐ Utilizzo di tritadocumenti per la distruzione di documenti cartacei non più necessari ☐ Triturazione certificata dei documenti cartacei non più necessari ☐ *Altro: specificare o inserire spazi*	
1.**4**	**Pseudonimizzazione e cifratura** – Per i dati più critici è opportuno adottare ulteriori misure di sicurezza per evitare la comprensibilità e l'usabilità dei dati anche in caso di furto o accesso non autorizzato. **Requisito:** *Nei casi in cui il trattamento riguardi dati particolari o relativi a condanne penali o reati, nonché per i dispositivi a maggiore mobilità e quindi più soggetti a furti e smarrimenti, è opportuno applicare misure tecniche e organizzative per limitare la possibilità di utilizzo dai dati da parte di soggetti non autorizzati.*	[Selezionare]
1.4.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Sistemi di crittografia dei database ☐ Cifratura dei dischi dei server ☐ Cifratura dei dischi dei dispositivi ☐ Cifratura dei dati in cloud ☐ Cifratura dei supporti removibili ☐ Cifratura dei backup ☐ Cifratura delle memorie dei dispositivi mobili ☐ Nel caso di dati pseudonimizzati: separazione dei campi identificativi su sistemi separati protetti ☐ Abbreviazione dei record di dati per limitare le possibilità di identificazione (es. indirizzo IP) ☐ *Altro: specificare o inserire spazi*	
1.4.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Politiche di conservazione e gestione delle chiavi di cifratura ☐ Utilizzo di dati pseudonimizzati (codici) nelle fasi di trattamento in cui non è necessaria l'identificazione degli interessati ☐ Rimozione degli elementi identificativi degli interessati ove non necessari (fasi di sviluppo, rendicontazione, uso o comunicazione di dati aggregati) ☐ *Altro: specificare o inserire spazi*	

1.5	**Protezione dei dati durante la trasmissione** – È necessario garantire la sicurezza dei dati nella trasmissione tra sistemi, nel trasporto tra diverse sedi e nelle fasi di comunicazione. **Requisito:** *Nei casi di trasmissione di dati tra sistemi, di trasporto di dati tra diverse sedi e nei casi di comunicazione autorizzata a terze parti è necessario garantire la sicurezza dei canali di trasmissione. I canali di trasmissione elettronica devono essere sicuri, crittografati e garantiti. Va tutelata anche la sicurezza dei dati nel caso di trasporto e consegna di documenti cartacei.*	[Selezionare]
1.5.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Configurazione di tunnel VPN ☐ Crittografia delle e-mail ☐ Crittografia degli allegati ☐ Trasmissione di dati, documenti o allegati con password trasmessa su alto canale ☐ Utilizzo di https nei sistemi web based ☐ Protocolli TLS 1.2 o successivi su web server ☐ Crittografia delle reti WI-FI (almeno WPA2) ☐ Utilizzo di crittografia nei server ftp (FTPS o SFTP) ☐ Contenitori/involucri sicuri per la spedizione ☐ Istruzioni chiare riguardo ai destinatari autorizzati ☐ Altro: *Specificare misure previste*	
1.5.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Trasferimento dei dati in forma pseudonimizzata ☐ Elenchi dei destinatari autorizzati ☐ Regole e Istruzioni di trasferimento ai destinatari autorizzati ☐ Regole per il trasporto di documenti ☐ Verifica e controllo delle consegne ai destinatari autorizzati ☐ *Altro: specificare o inserire spazi*	
2	Integrità	
2.1	**Controllo delle modifiche –** Determinare se i dati personali sono stati inseriti, modificati o rimossi dai sistemi che trattano i dati e da chi. **Requisito:** *è necessario conservare la documentazione completa relativa alla gestione delle modifiche e alla manutenzione dei dati. Si devono garantire la tracciabilità e/o la documentazione del trattamento dei dati. Ove possibile è opportuno implementare misure tecniche che permettano la revisione successiva mediante sistemi di registrazione al fine di determinare i dettagli relativi all'immissione, alla modifica o alla rimozione di dati.*	[Selezionare]
2.1.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Registrazione (log) di inserimento, modifica, eliminazione dati dalle basi dati ☐ Sistemi di autorizzazione da parte di supervisori per la modifica o la cancellazione dei dati ☐ Avvisi di conferma(double-check) per la modifica o la cancellazione dei dati nelle applicazioni ☐ Altro: *Specificare misure previste*	

2.1.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Conservazione dei moduli cartacei da cui sono stati trasferiti i dati per il trattamento automatizzato ☐ Conservazione dei dati originali in caso di importazione da altre fonti ☐ Assegnazione di diritti separati per l'immissione, la modificazione e la cancellazione di dati ☐ *Altro: specificare o inserire spazi*	
2.2	**Controllo dell'esattezza e dell'aggiornamento dei dati –** devono essere adottate tutte le misure ragionevoli per aggiornare, cancellare o rettificare tempestivamente i dati inesatti o obsoleti rispetto alle finalità per le quali sono trattati. **Requisito:** Il Responsabile è tenuto a monitorare per tutto il loro ciclo di vita i dati personali raccolti o gestiti, dal momento dell'acquisizione e fino alla loro cancellazione, mediante misure che limitino il più possibile la possibilità di errore	Not Applicable
2.2.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Applicazioni con campi predefiniti o sistemi di controllo nell'inserimento dei dati ☐ Sistemi di allineamento con altre banche dati / applicazioni ☐ Sistemi di aggiornamento automatico dei dati ☐ Sistemi di cancellazione automatica dei dati alla scadenza ☐ Altro: *Specificare misure previste*	
2.2.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedure di validazione dei dati ☐ Procedure di controllo periodico dell'esattezza dei dati inseriti nelle banche dati ☐ Procedure di controllo periodico dell'aggiornamento dei dati inseriti nelle banche dati ☐ Immediato aggiornamento / rettifica dei dati su tutti i sistemi in caso di segnalazione / rilevamento di errori o necessità di aggiornamento in uno specifico dataset ☐ Procedure – regole di data retention definite ☐ Cancellazione dei dati obsoleti ☐ *Altro: specificare o inserire spazi*	
3.	**Disponibilità e resilienza**	
3.1	**Sistemi di sicurezza nelle sale server -** Protezione da distruzione/perdita accidentale di dati e misure per la disponibilità dei servizi **Requisito:** *il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità dei dati. I dati devono essere protetti dalla distruzione o dalla perdita accidentale (ad esempio dovuta a blackout, incidenti o eventi naturali). In particolare le macchine e le sale server che le ospitano devono essere protette da influenze ambientali esterne e sabotaggi.*	[Selezionare]
3.1.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Estintori nelle sale server con estinguenti adatti ☐ Aria condizionata nelle sale server ☐ Dispositivi per il monitoraggio di temperatura e umidità nelle sale server ☐ Sistemi di rilevamento di fiamme e fumo ☐ Sistemi di controllo e alert per parametri server e dispostivi di rete (uptime, temperatura, carico, errori, anomalie ecc.) ☐ Sistemi automatic di spegnimento incendi ☐ Alimentazione elettrica ininterrotta (UPS e gruppi di continuità) ☐ Infrastruttura IT duale (ridondanza) ☐ Sistemi di protezione fisica per l'accesso alle sale server ☐ Sistemi di accesso alle sale server con smart card / pin / trasponder / identificatori biometrici ☐ Videosorveglianza delle sale server ☐ *Altro: specificare o inserire spazi*	

3.1.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Notifica di allarme in caso di accesso alle stanze server ☐ Notifica di allarme in caso di superamento dei parametri di temperatura/umidità/fumo ☐ Divieto di accesso al personale non autorizzato al perimetro fisico dell'infrastruttura del sistema IT ☐ Controllo dell'ubicazione delle sale server in relazione alle condutture idriche ☐ Le sale server si trovano ai piani rialzati se in una zona soggetta a inondazioni ☐ *Altro: specificare o inserire spazi*	
3.2	**Protezione della rete e dei dispositivi –** La rete, gli host e i dispostivi collegati in rete devono disporre di misure di protezione da attacchi di malintenzionati e da software malevolo. **Requisito:** *il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità (oltre alla riservatezza e l'integrità) dei dati trattati proteggendo la rete, i dispositivi e i dati conservati, elaborati o in transito, da effetti dovuti a software malevolo o attacchi di malintenzionati. I dati devono essere elaborati, trasmessi e conservati con strumenti la cui sicurezza è implementata secondo gli standard di settore*	[Selezionare]
3.2.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Protezione tramite sistemi firewall ☐ Appliance UTM (Unified Threat Management) ☐ Sistemi IDS, IPS o IDPS ☐ Sistemi NAC (Network Access Control) ☐ Sistemi DLP ☐ Sistemi SIEM ☐ DMZ per i servizi esposti ☐ WAF (Web Application Firewall) per i servizi esposti ☐ Software antimalware aggiornato a livello di rete ☐ Software antimalware aggiornato a livello di host ☐ Software antimalware aggiornato su tutti i dispostivi ☐ *Altro: specificare o inserire spazi*	
3.2.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ SOC (Security Operations Center) ☐ Servizi di MSS (Managed Security Services) ☐ Segmentazione delle reti ☐ Controllo e aggiornamento periodico delle policy dei firewall ☐ Analisi dei log e degli avvisi di sicurezza ☐ Test hardware su base regolare (ciclo di vita, prestazioni) ☐ Test di penetrazione su base regolare ☐ Regolamento / Disciplinare/ Policy sull'utilizzo della rete e degli strumenti informatici da parte degli utenti ☐ Formazione degli utenti in merito ad attacchi di phishing e social engineering ☐ *Altro: specificare o inserire spazi*	
3.3	**Controllo delle disponibilità e controllo della recuperabilità –** Salvataggio periodico dei dati e procedure per recuperare i dati il prima possibile. **Requisito:** *I dati devono essere conservati i più copie su reti/sistemi/sedi separate. Il Responsabile del trattamento deve mettere in atto una politica di backup e di ripristino che garantisce il recupero del sistema e dei dati.*	[Selezionare]

3.3.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Sistemi di backup automatizzato ☐ Sistemi di backup in cloud ☐ Sistemi di disaster recovery con infrastrutture proprie ☐ Sistemi di disaster recovery con piattaforme DRaaS in cloud ☐ *Altro: specificare o inserire spazi*	
3.3.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Contratti con i fornitori per la fornitura di hardware sostitutivo con tempi definiti (SLA) ☐ Piani di backup e di recovery del software, delle configurazioni e dei dati ☐ Procedure di continuità operativa ☐ Procedure di ripristino dei dati ☐ Test di ripristino periodici ☐ Esercitazioni di simulazione di crisi/emergenza su base regolare con prove di ripristino ☐ *Altro: specificare o inserire spazi*	
3.4	**Gestione e Controllo delle Risorse informatiche e del software:** *Il Responsabile del trattamento deve garantire la sicurezza dell'ambiente di trattamento e degli strumenti utilizzati.* **Requisito:** *È necessaria una gestione globale e attiva (inventariare, abilitare, tracciare, aggiornare) di tutti gli strumenti utilizzati per il trattamento dei dati, compresi gli strumenti non direttamente attivi nel trattamento ma connessi alle reti o ai sistemi utilizzati per la conservazione, il transito o l'elaborazione dei dati. Questi comprendono i sistemi di rete, i sistemi di protezione, i sistemi server di elaborazione e archiviazione, i sistemi di comunicazione e trasmissione dei dati, i dispositivi dell'utente autorizzato, mobili e portatili inclusi, i dispositivi di rete, i dispositivi IoT connessi all'infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette.* *Parimenti è necessario gestire attivamente (inventariare, tracciare e aggiornare) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito, adottando politiche o misure per impedire l'istallazione o l'esecuzione di software non autorizzato*	[Selezionare]
3.4.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Strumenti di rilevamento attivo delle risorse connesse alla/e rete/i ☐ Strumenti di rilevamento passivo delle risorse connesse alla/e rete/i ☐ Strumenti di inventario dei dispositivi ad alimentazione manuale ☐ Strumenti automatici di rilevamento dei software utilizzati a livello di rete ☐ Strumenti di inventario dei software installati ad alimentazione manuale ☐ Sistemi di aggiornamento automatico del software ☐ Vulnerability assessment periodici ☐ Altro: *Specificare misure previste*	
3.4.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati ☐ Procedure per la gestione delle risorse non autorizzate (rimozione, blocco, quarantena) ☐ Inventario accurato, dettagliato e aggiornato di tutti software utilizzati a livello aziendale ☐ Registrazione e monitoraggio di tutte le modifiche alle configurazioni di risorse, apparati e sistemi IT ☐ Procedure per l'aggiornamento e l'applicazione delle correzioni di sicurezza nei software ☐ Verifica periodica dei bollettini di sicurezza per le vulnerabilità rilevate ☐ Altro: *Specificare misure previste*	

4	Politiche e procedure per la gestione della tutela dei dati personali, per l'esame periodico del sistema di trattamento, per la valutazione e per la verifica su base regolare, nonché per l'assistenza al Titolare del trattamento	
4.1	Politiche di protezione dei dati personali Requisito: *Il Responsabile del trattamento deve implementare un proprio sistema di tutela dei dati personali.* *Gli elementi includono:* – *Una struttura organizzativa vigente per la protezione dei dati con responsabilità definite (incluso la nomina di un responsabile della protezione dei dati, qualora richiesto a livello legale)* – *Conformità a tutti i requisiti legali per la protezione dei dati personali* – *Sistema di gestione dei contratti vigenti per la conservazione di tutti gli accordi relativi alla protezione dei dati (es. accordi per il trattamento dei dati, accordi con sub-responsabili del trattamento ecc.)* – *Formazione sulla tutela dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento* – *Accordi sulla riservatezza dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento* – *Una procedura che garantisce i diritti dei soggetti interessati (in cooperazione con il Titolare del trattamento)* – *L'adozione di certificazioni sulla sicurezza dei dati e l'adesione a codici di condotta possono essere validi strumenti di controllo delle politiche di protezione*	[Selezionare]
4.1.1	A tal fine vengono messe in atto le seguenti misure organizzative. ☐ Registro del trattamento in qualità di responsabile ☐ Analisi dei rischi che incombono sugli interessati in relazione ai trattamenti effettuati ☐ Nomina di un responsabile della protezione dei dati (se richiesto a livello legale) ☐ Adozione di un sistema di gestione o di un Modello Organizzativo per la tutala dei dati personali ☐ Adesione a codici di condotta in relazione al trattamento di dati personali ☐ Certificazioni relative alla sicurezza dei dati (es. ISO/IEC 27001 e 27701) ☐ Contratti con i fornitori che svolgono parte dei trattamenti affidati (sub-responsabili) che prevedono meccanismi di tutela dei dati personali e relativi accordi di riservatezza ☐ Piano di formazione del personale in relazione alla tutela dei dati personali ☐ Autorizzazione formale al personale incaricato del trattamento dei dati personali affidati ☐ Adozione di un accordo di riservatezza per il personale a cui è affidato il trattamento ☐ Procedura per la risposta alle richieste di esercizio dei diritti degli interessati ☐ Registrazione delle richieste di esercizio dei diritti degli interessati ☐ *Altro: specificare o inserire spazi*	
4.2	Gestione delle risposte agli incidenti che possono comportare violazioni dei dati personali / data breach Requisito: *Il Responsabile del trattamento deve implementare un proprio sistema di gestione degli incidenti e delle violazioni dei dati personali (cd. Data breach).* *Gli elementi includono:* – *Un processo per segnalare violazioni della protezione dei dati personali (in particolare in cooperazione con il Titolare del trattamento)* – *Una procedura per la gestione degli incidenti che possono comportare violazioni dei dati personali*	[Selezionare]

4.2.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedura per la risposta ad incidenti di sicurezza ☐ Procedura per la gestione e la notifica delle violazioni dei dati (data breach) ☐ Adozione di un registro dei data breach ☐ Assegnazione dei ruoli di valutazione degli incidenti di sicurezza ☐ Procedure o meccanismi di risposta agli incidenti di sicurezza, comprensivi dell'assegnazione di compiti e ruoli ☐ Regole o procedure di segnalazione delle anomalie o degli incidenti di sicurezza da parte degli utenti ☐ *Altro: specificare o inserire spazi*	
4.3	**Protezione dei dati by design e by default** **Requisito:** *il Responsabile del trattamento è obbligato a mettere in atto misure tecniche e organizzative nelle fasi iniziali della progettazione delle operazioni del trattamento, in modo da rispettare i principi della privacy e della protezione dei dati fin dall'inizio. Inoltre, il Responsabile del trattamento deve garantire che i dati personali vengano trattati con il massimo livello di protezione, in modo che i dati personali non siano accessibili a un numero indefinito di persone by default.*	[Selezionare]
4.3.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedura di privacy by design e by default ☐ Adozione di controlli preventivi per la minimizzazione dei dati in fase di raccolta ☐ Adozione di controlli preventivi per la minimizzazione dei dati in fase di elaborazione ☐ Adozione di controlli preventivi per la minimizzazione dei dati in fase di comunicazione ☐ Controllo delle caratteristiche di sicurezza e funzionalità nella tutela dei dati in fase di adozione di nuovi software ☐ Valutazione delle esigenze di tutela dei dati (comprese valutazioni su necessità, riduzione al minimo dei dati utilizzati, valutazione della necessità di pseudonimizzazione o di adozione di altre misure sicurezza) per ogni fase del flusso di dati necessaria all'attività delegata ☐ Altro: *Specificare misure previste*	
4.4	**Procedure di controllo** **Requisito:** *il Responsabile deve mettere in atto politiche e procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*	[Selezionare]
4.4.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Revisione periodica del sistema di trattamento dati e delle misure di sicurezza implementate ☐ Audit interni periodici documentati ☐ Audit del Responsabile della Protezione dei Dati (DPO) periodici documentati ☐ Audit di seconda parte documentati ☐ Audit di terza parte (es. come parte di procedure di certificazione o revisione di certificazioni) ☐ Altro: *Altro: specificare o inserire spazi*	
4.5	**Assistenza al Titolare del trattamento** **Requisito**: *Il Responsabile del trattamento ha l'obbligo di fornire assistenza al Titolare tenendo conto della natura del trattamento. Tale obbligo di assistenza riguarda anche gli eventuali sub-responsabili ove presenti e ove necessario.*	[Selezionare]
4.5.1	Se per l'assistenza vengono implementate specifiche misure tecniche e organizzative ulteriori rispetto a quelle indicate nel presente allegato, elencarle di seguito: ☐ ☐ ☐ ☐ ☐ ☐	

Qualora il fornitore si avvalga di (sub-)responsabili del trattamento specificare la ragione sociale, la sede legale e il servizio svolto:

RAGIONE SOCIALE	SEDE LEGALE	SERVIZIO SVOLTO