TRATTAMENTO DATI

PARAGRAFO 1 – IDENTIFICAZIONE DEL RESPONSABILE

1) dati identificativi, fiscali e di contatto;
2) estremi identificativi del **Rappresentante** del responsabile del trattamento non stabilito nello Spazio Economico Europeo (nei casi previsti dall'articolo 27 del RGPD);
3) indicazione in merito all'avvenuta designazione del Responsabile per la protezione dei dati personali (**RPD o DPO**), ovvero dichiarazione di non sottostare a tale obbligo;
4) indicazione in merito alla tenuta dei **registri delle attività di trattamento**, ovvero dichiarazione di non sottostare a tale obbligo;
5) indicazione in merito all'avvenuta adozione di un **modello organizzativo gestionale** (od altro documento o procedura similare) per l'attuazione delle prescrizioni e misure in materia di protezione dei dati personali;
6) modalità e procedure di formazione, istruzione ed autorizzazione del **personale** (dipendente o collaboratore o assimilati). In particolare, specificare se, per lo svolgimento del servizio oggetto di affidamento:
- il personale sia in possesso di particolari qualifiche, abilitazioni o titoli professionali;
- il personale sia soggetto a specifici accordi documentati di riservatezza / non divulgazione (ad es. segreto professionale, ecc.);
- sia prevista la designazione di un referente privacy (o figura analoga) con funzioni di coordinamento delle attività con il Titolare;

- in caso di affidamento di servizi a contenuto tecnologico, il personale espleterà funzioni di amministratore di sistema, nell'accezione di cui al Provvedimento generale del Garante per la Protezione dei dati Personali 27/11/2008 (e successivi provvedimenti di modifica e precisazione). In tal caso il Responsabile ne fornisce altresì l'elenco nominativo, unitamente all'attestazione delle conoscenze, dell'esperienza, della capacità e dell'affidabilità degli stessi soggetti e le specifiche istruzioni impartite;

7) indicazione in merito all'avvenuta adozione di una **procedura per la gestione delle violazioni di dati personali** ed all'istituzione ed aggiornamento di un registro delle medesime violazioni;
8) dichiarazione di essere o di non esser stato destinatario di **provvedimenti sanzionatori o correttivi**, divenuti definitivi, ad opera del Garante per la protezione dei dati personali o di altra Autorità di controllo, in relazione al trattamento di dati personali effettuato nel contesto di servizi analoghi o similari. In caso di provvedimenti subìti, indicandone gli estremi;
9) dichiarazione (e documentazione) di adesione a **codici di condotta** ai sensi dell'articolo 40 del RGPD;
10) dichiarazione (e documentazione) di essere in possesso di una **certificazione**, ai sensi dell'articolo 42 del RGPD, in relazione ai trattamenti che si intendono effettuare nello svolgimento del servizio in oggetto;
10) dichiarazione (e documentazione) di essere in possesso di una o più **certificazioni**, con riferimento alla gestione della sicurezza delle informazioni, sicurezza IT, sicurezza cibernetica e protezione dei dati personali (**famiglia ISO/IEC 27000**);
11) in caso di servizio erogato in modalità cloud, dichiarazione e documentazione relativa alla qualificazione e presenza nel catalogo dei servizi cloud qualificati per la PA di AgID (ora ACN).

PARAGRAFO 2 – DESCRIZIONE DEL SERVIZIO

Facendo ricorso alle definizioni contenute nella normativa di protezione dei dati personali, il Responsabile dovrà illustrare le **modalità tecniche, tecnologiche ed organizzative di erogazione del servizio**, dettagliando:
A) le **categorie di dati personali** coinvolte dalle operazioni di trattamento, evidenziando la presenza delle seguenti fattispecie:
- dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- dati di accesso e di identificazione (username, password, customer ID, altro...)
- dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
- dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- dati di profilazione

- dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...)
- dati relativi all'ubicazione
- dati che rivelano l'origine razziale o etnica
- dati che rivelano le opinioni politiche
- dati che rivelano le convinzioni religiose o filosofiche
- dati che rivelano l'appartenenza sindacale
- dati relativi alla vita sessuale o all'orientamento sessuale
- dati relativi alla salute
- dati genetici
- dati biometrici

B) le **categorie di Interessati** coinvolte dalle operazioni di trattamento, evidenziando la presenza delle seguenti fattispecie:
- dipendenti/consulenti
- utenti/contraenti/abbonati/clienti (attuali o potenziali)
- associati, soci, aderenti, simpatizzanti, sostenitori
- soggetti che ricoprono cariche sociali
- beneficiari o assistiti
- pazienti
- minori
- persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)

C) le **operazioni di trattamento** (a mero titolo esemplificativo, la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione) specificando:
1) quelle a carico del Responsabile e di eventuali altri responsabili (fatto salvo quanto infra previsto in relazione alla possibilità di avvalersene) e quelle a carico del Titolare;
2) per ciascuna operazione, se la medesima avverrà presso la sede del Titolare, del Responsabile (o altri responsabili) o in modalità mista;
3) per ciascuna operazione, se sia necessario e quale sarà il coinvolgimento (o supporto) del Titolare. In particolare, precisando:
- le procedure ed i tempi di acquisizione dei dati personali presso il Titolare del trattamento e di quelle di riconsegna al termine dell'affidamento;
- le procedure di comunicazione dei dati personali con il Titolare (durante lo svolgimento del servizio);
- la necessità di accesso a banche dati del Titolare, formate o detenute da uffici o servizi diversi da quello affidante (con indicazione delle ragioni di necessità, tempi, periodicità, modalità, ecc.);
4) nel caso sia prevista una raccolta di dati personali presso l'interessato o presso terzi, i soggetti presso i quali avverrà la raccolta, i tempi e le relative modalità;
5) in caso di utilizzo, da parte degli interessati, di strumenti elettronici forniti dal Responsabile, la tipologia degli strumenti, i tempi e le modalità;
6) in caso di utilizzo di servizi cloud necessari a rendere il servizio affidato (software gestionali, crm, ecc.), la tipologia dei servizi, i tempi e le modalità;
7) i luoghi e le procedure di conservazione dei dati personali, trattati per conto del Titolare;
8) nel caso sia prevista una comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione di dati personali, i soggetti destinatari, i tempi e le modalità di esecuzione;
9) le procedure e le modalità di distruzione o cancellazione dei dati personali al termine dell'affidamento;
10) nel caso sia prevista l'anonimizzazione dei dati personali, trattati per conto del Titolare, anche successiva alla scadenza dell'affidamento, la descrizione dei tempi e delle modalità di esecuzione;
8) l'esistenza di disposizioni normative o dell'Autorità che impongano una conservazione dei dati personali, trattati per conto del Titolare, anche oltre la scadenza del servizio affidato (e relativi tempi di conservazione);
D) le modalità, tecniche ed organizzative, mediante le quali il fornitore intende rendere disponibili all'utenza le **informazioni prescritte dagli articoli 13 e 14 del RGPD** (il cui contenuto è a carico e sarà fornito dal

Titolare). In particolare dovrà essere indicato se previsto l'utilizzo di modalità informatiche (es. sito web) o di modalità analogiche (cartellonistica presso i luoghi di prestazione del servizio, modulistica cartacea, ecc.);
E) le modalità, tecniche ed organizzative, mediante le quali il fornitore ha previsto l'esercizio dei **diritti dell'interessato** ed il relativo riscontro da parte del Titolare;

PARAGRAFO 3 – MISURE DI SICUREZZA
In relazione allo specifico profilo della sicurezza del trattamento dei dati personali, il fornitore deve fornire:
a) la descrizione (tipologica) delle misure di sicurezza adottate per prevenire perdite di integrità, disponibilità e confidenzialità dei dati personali, con riferimento ai **luoghi fisici** ove avverranno le operazioni di trattamento. La descrizione dovrà evidenziare le misure adottate a garanzia della separazione dei dati personali trattati per conto del Titolare, rispetto a quelli trattati per conto proprio o di terzi;
b) la descrizione (tipologica) delle misure di sicurezza adottate per prevenire perdite di integrità, disponibilità e confidenzialità dei dati personali, con riferimento agli **strumenti elettronici** (hardware e software) utilizzata per il trattamento. La descrizione dovrà riguardare le misure indicate dall'Agenzia per l'Italia Digitale con la Circolare 18 aprile 2017, n. 2/2017 e dovrà evidenziare le scelte adottate a garanzia della separazione logica dei dati personali trattati per conto del Titolare, rispetto a quelli trattati per conto proprio o di terzi;
c) le attività e gli oneri (esclusi quelli di carattere economico), previsti a carico del Titolare e necessari per consentire la sicurezza del trattamento dei dati personali e la sua conformità alla normativa.
d) le modalità, anche tecniche e le procedure mediante le quali il Responsabile intende assicurare **l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza** dei dati personali oggetto di trattamento, per conto del Titolare, rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati;
Qualora, in relazione al trattamento di dati personali effettuato dal Responsabile per conto di altro Titolare, in fattispecie assimilabile a quella oggetto di affidamento, sia già stata effettuata una valutazione d'impatto sulla protezione dei dati personali - ai sensi dell'articolo 35 del RGPD – il Responsabile ne fornisce le informazioni rilevanti, impegnandosi a prestare al Titolare la collaborazione necessaria a condurre la propria valutazione. In caso non sia stata effettuata o non sia disponibile, il fornitore deve relazionare in merito alle soluzioni tecniche ed organizzative adottate con riferimento alle seguenti categorie di rischio (indicando, per ciascuna, quali misure contribuiscono a mitigare il rischio, quale sia la gravità del rischio e come stima la probabilità di verificazione del rischio, tenuto conto delle misure adottate o pianificate):

1) accesso illegittimo ai dati;
2) modifiche indesiderate ai dati;
3) perdita di dati

PARAGRAFO 4 – TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO
Ove il Responsabile intenda trasferire all'estero i dati personali, oggetto di trattamento per conto del Titolare, ne dovrà fare espressa menzione, indicando:
a) il paese nel quale s'intendono trasferire i dati personali;
b) le categorie di dati personali oggetto di trasferimento;
c) le categorie di Interessati i cui dati personali saranno trasferiti;
d) le operazioni di trattamento previste a seguito del trasferimento;
e) ove il trasferimento avvenga verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, l'indicazione circa le modalità ed i termini che garantiscono il rispetto delle disposizioni contenute nel capo V del GDPR.

PARAGRAFO 5 – RICORSO AD ALTRO RESPONSABILE
Nel caso il fornitore intenda ricorrere ad altro soggetto ("Sub-responsabile") per eseguire tutte o parte delle operazioni di trattamento per conto del Titolare, ne deve fare espressa menzione, al fine di consentire al Titolare di compiere le valutazioni necessarie al rilascio della prescritta autorizzazione. A tal fine il Responsabile specifica, per ciascun Sub-responsabile, le informazioni di cui ai precedenti paragrafi (da 1 a 5).