



**ALLEGATO N. 1 AL
CAPITOLATO DELLE CLAUSOLE PARTICOLARI (CCP)**

Appalto pubblico del servizio di prevenzione dei rischi professionali (RSPP), ai sensi del decreto legislativo italiano 09/04/2008 N. 81, presso enti francesi presenti in Italia e in Vaticano

RIF. N. 25035

Nell'ambito del presente accordo quadro, le parti si impegnano a rispettare la normativa vigente applicabile al trattamento dei dati personali e, in particolare, il RGPD e la legge n. 78-17 del 6 gennaio 1978 relativa all'informatica, ai file e alle libertà.

Precisazioni terminologiche

Il responsabile del trattamento ai sensi del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "regolamento generale sulla protezione dei dati" o RGPD) è il soggetto pubblico e il responsabile del trattamento è il titolare del presente accordo quadro.

Natura, durata, finalità e descrizione del trattamento dei dati personali

Il titolare è autorizzato a trattare per conto dell'ente pubblico i dati personali necessari per l'esecuzione della prestazione.

I dati personali sono trattati per un periodo di 4 anni.

La finalità del trattamento comprende l'esecuzione ottimale dei servizi richiesti nei casi in cui il trattamento dei dati personali migliora i risultati degli stessi.

I tipi di dati personali trattati possono essere in particolare:

- il cognome;
- il nome;
- la funzione;
- la data di nascita;
- indirizzo di residenza;
- il numero della carta d'identità e/o del passaporto;
- i recapiti professionali;
- il numero di telefono personale;
- la foto tessera;
- l'agenda.

Le categorie di persone interessate sono:

- gli agenti delle entità;
- gli ospiti degli enti.

Attuazione del trattamento

Il titolare dell'accordo quadro si impegna, in particolare, a:

- trattare i dati esclusivamente per le finalità per cui sono stati raccolti;
- nel caso in cui venga impartita un'istruzione in violazione del regolamento generale sulla protezione dei dati o di qualsiasi altra disposizione del diritto dell'Unione o del diritto degli Stati membri in materia di protezione dei dati, informare immediatamente l'ente pubblico;
- nel caso in cui sia tenuto a trasferire dati verso un paese terzo (al di fuori dell'Unione europea) o a un'organizzazione internazionale, in virtù del diritto dell'Unione o del diritto dello Stato membro al quale è soggetto, informare l'ente pubblico di tale obbligo giuridico prima del trattamento, a meno che il diritto in questione non vieti tale informazione;
- i dati trasferiti verso un paese terzo devono beneficiare di un livello di protezione equivalente a quello garantito dal RGPD all'interno dell'Unione europea. È formalmente vietato qualsiasi trasferimento di dati personali a favore di qualsiasi entità, in particolare di paesi terzi o organizzazioni internazionali, che non sia strettamente conforme alla normativa francese o europea. Qualora non sia possibile garantire il rispetto di tali requisiti in caso di trasferimento di dati personali verso un paese terzo, il titolare sospende qualsiasi trasferimento e si rivolge all'ente pubblico per valutare, se del caso, l'adeguamento delle modalità di esecuzione al fine di garantire il rispetto dei requisiti del RGPD.

Se le modalità di esecuzione non possono essere adeguate, l'ente pubblico procede alla risoluzione dell'accordo quadro per motivi di interesse generale alle condizioni previste

dal CCAG di riferimento.

- garantire la riservatezza dei dati personali trattati;
- garantire che le persone autorizzate al trattamento dei dati personali:
 - si impegnino a rispettare la riservatezza o siano soggette a un obbligo legale di riservatezza adeguato;
 - ricevano la formazione necessaria in materia di protezione dei dati personali;
- tengano conto, per quanto riguarda i propri strumenti, prodotti, applicazioni o servizi, dei principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default.

Subappalto delle attività di trattamento

Quando il titolare (subappaltatore ai sensi del RGPD) ricorre a un subappaltatore (ai sensi degli appalti pubblici) per svolgere attività di trattamento specifiche, ne informa preventivamente e per iscritto l'ente pubblico (il responsabile del trattamento ai sensi del RGPD).

Tale informazione deve indicare chiaramente la natura delle attività di trattamento subordinate, l'identità e i recapiti del subappaltatore e le date del contratto di subappalto. Il subappalto può essere effettuato solo se l'ente pubblico non ha sollevato obiezioni entro il termine di 21 giorni dalla data di ricezione della richiesta, in applicazione delle disposizioni dell'articolo R.2193-4 del Codice degli appalti pubblici.

Al fine di ottenere l'accettazione e l'approvazione dell'ente pubblico, il titolare deve presentare il proprio subappaltatore mediante un atto speciale di subappalto, le cui formalità sono contenute nel modulo DC4 o in qualsiasi altro documento equivalente (scaricabile dal sito <https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat>).

Il subappaltatore è tenuto a rispettare gli obblighi del presente accordo quadro per conto e secondo le istruzioni dell'ente pubblico. Spetta al titolare assicurarsi che il subappaltatore presenti le stesse garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti della legislazione e della normativa vigente in materia di protezione dei dati.

Il titolare rimane pienamente responsabile nei confronti dell'ente pubblico dell'adempimento degli obblighi del subappaltatore in conformità al contratto stipulato con il subappaltatore. Il titolare informa l'ente pubblico di qualsiasi inadempimento da parte del subappaltatore dei suoi obblighi contrattuali.

Diritto di informazione ed esercizio dei diritti degli interessati al trattamento

Spetta al titolare fornire le informazioni alle persone interessate dalle operazioni di trattamento al momento della raccolta dei dati.

La formulazione e il formato delle informazioni devono essere concordati con l'ente pubblico prima della raccolta dei dati.

Il titolare deve rispondere, a nome e per conto dell'ente pubblico e nei termini previsti dal regolamento generale sulla protezione dei dati, alle richieste degli interessati in caso di esercizio dei loro diritti.

Il titolare deve essere in grado di garantire, per tutta la durata dei servizi, che tutti i dati personali o le informazioni che tratta nell'ambito dell'esecuzione dell'accordo quadro in qualità di responsabile del trattamento ai sensi del RGPD siano trattati e, più in generale, resi

accessibili esclusivamente all'interno:

- dello Spazio economico europeo;
- di un paese terzo che beneficia di una decisione di adeguatezza ai sensi dell'articolo 45 del RGPD;
- o, in mancanza di ciò, che i trasferimenti risultanti dall'esecuzione delle prestazioni siano disciplinati da garanzie adeguate o da norme aziendali vincolanti ai sensi degli articoli 46 e 47 del RGPD, eventualmente integrate da misure supplementari volte a garantire che non possano essere eluse nello Stato terzo di destinazione, nel rigoroso rispetto della giurisprudenza.

La garanzia del titolare su questo punto deve coprire non solo l'hosting dei dati, ma anche tutte le operazioni di trattamento effettuate dal titolare o dai successivi responsabili del trattamento RGPD ai quali potrebbero essere affidate, se del caso, alcune operazioni di trattamento (in particolare la manutenzione e l'assistenza).

Il titolare deve quindi essere in grado di garantire che i dati trattati non possano essere resi accessibili a destinatari, comprese le autorità amministrative o giudiziarie, situati al di fuori dello Spazio economico europeo senza che sia rispettato il diritto applicabile, in particolare il RGPD. Il titolare descrive in dettaglio i mezzi messi in atto per garantire tale rispetto.

Notifica delle violazioni dei dati personali

Il titolare notifica all'ente pubblico qualsiasi violazione dei dati personali entro 24 ore dalla sua scoperta e tramite e-mail. Tale notifica è accompagnata da tutta la documentazione utile per consentire all'ente pubblico, se necessario, di notificare la violazione all'autorità di controllo competente (nella fattispecie, alla Commissione nazionale dell'informatica e delle libertà, CNIL) se possibile entro 72 ore dal momento in cui ne è venuto a conoscenza.

Previo consenso scritto dell'ente pubblico, il titolare notifica all'autorità di controllo competente, a nome e per conto dell'ente pubblico, le violazioni dei dati personali entro un termine massimo di 24 ore, a meno che la violazione in questione non sia suscettibile di comportare un rischio per i diritti e le libertà delle persone fisiche.

La notifica contiene almeno:

- la descrizione della natura della violazione dei dati personali, comprese, se possibile, le categorie e il numero approssimativo di persone interessate dalla violazione e le categorie e il numero approssimativo di registrazioni di dati personali interessati;
- il nome e le coordinate del responsabile della protezione dei dati o di un altro referente presso il quale è possibile ottenere ulteriori informazioni;
- la descrizione delle conseguenze probabili della violazione dei dati personali;
- la descrizione delle misure adottate o che l'ente pubblico intende adottare per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure volte ad attenuare le eventuali conseguenze negative.

Se e nella misura in cui non è possibile fornire tutte queste informazioni in un'unica notifica, le informazioni possono essere comunicate in modo scaglionato senza indebito ritardo.

Previo consenso scritto dell'ente pubblico, il titolare comunica, a nome e per conto dell'ente pubblico, la violazione dei dati personali all'interessato nel più breve tempo possibile, qualora tale violazione possa comportare un rischio elevato per i diritti e le libertà di una persona fisica.

La comunicazione all'interessato descrive, in termini chiari e semplici, la natura della violazione dei dati personali e contiene almeno:

- la descrizione della natura della violazione dei dati personali, comprese, se possibile, le categorie e il numero approssimativo di persone interessate dalla violazione e le categorie e il numero approssimativo di registrazioni di dati personali interessati;
- il nome e le coordinate del responsabile della protezione dei dati o di un altro punto di contatto presso il quale è possibile ottenere ulteriori informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o che il soggetto pubblico intende adottare per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure volte a mitigarne le eventuali conseguenze negative.

Assistenza del titolare nell'ambito dell'adempimento degli obblighi da parte dell'ente pubblico

Il titolare assiste l'ente pubblico:

- a effettuare analisi d'impatto relative alla protezione dei dati;
- alla consultazione preventiva dell'autorità di controllo.

Il titolare mette a disposizione dell'ente pubblico la documentazione necessaria per dimostrare il rispetto di tutti i suoi obblighi e per consentire, se del caso, lo svolgimento di audit, comprese le ispezioni, da parte dell'ente pubblico o di un revisore da esso incaricato, e contribuisce a tali audit.

Misure di sicurezza

Il titolare attua le seguenti misure di sicurezza:

- pseudonimizzazione e crittografia dei dati personali;
- i mezzi per garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;
- i mezzi per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in tempi adeguati in caso di incidente fisico o tecnico;
- una procedura per testare, analizzare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

Destinazione dei dati

Al termine dell'esecuzione del presente accordo quadro, l'ente pubblico informa il titolare della sua decisione in merito al destino dei dati. L'ente pubblico può chiedere al titolare di:

- distruggere tutti i dati personali;
- restituire tutti i dati personali all'ente pubblico o al terzo da esso designato.

Il rinvio deve essere accompagnato dalla distruzione di tutte le copie esistenti nei sistemi informativi del responsabile del trattamento. Una volta distrutti, il responsabile del trattamento deve giustificare per iscritto la distruzione

Responsabile della protezione dei dati

Non appena riceve la notifica dell'accordo quadro, l'ente pubblico comunica al titolare il nome e i recapiti del proprio responsabile della protezione dei dati.

Registro delle attività di trattamento

Il titolare tiene un registro scritto di tutte le attività di trattamento effettuate per conto dell'ente pubblico, comprendente:

1. il nome e i recapiti dell'ente pubblico per conto del quale agisce, degli eventuali subappaltatori e, se del caso, del responsabile della protezione dei dati;
2. le categorie di trattamenti effettuati per conto dell'ente pubblico;
3. se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione di tale paese terzo o organizzazione internazionale e, nel caso dei trasferimenti di cui all'articolo 49, paragrafo 1, secondo comma, del regolamento generale sulla protezione dei dati, i documenti che attestano l'esistenza di garanzie adeguate;
4. per quanto possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative, in particolare, se necessario:
 - la pseudonimizzazione e la crittografia dei dati personali;
 - mezzi per garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;
 - mezzi per ripristinare la disponibilità dei dati personali e l'accesso agli stessi entro un termine adeguato in caso di incidente fisico o tecnico;
 - una procedura volta a verificare, analizzare e valutare regolarmente l'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del trattamento.