

Responsabile Esterno del
Trattamento dei Dati
- ISTRUZIONI PER IL TRATTAMENTO -

Allegato 1

Compiti del responsabile - Articolo 28 - Regolamento Europeo 2016/679

1. Termini relativi al Trattamento dei Dati

1.1. Nel corso della fornitura dei Servizi e / o dei Prodotti al TITOLARE in conformità all'affidamento, il RESPONSABILE può trattare i dati personali per conto del TITOLARE secondo i termini del presente Documento.

1.2. Nella misura richiesta dalle Leggi sulla Protezione dei Dati applicabili, il RESPONSABILE dovrà ottenere e mantenere tutte le licenze, autorizzazioni e permessi necessari per il trattamento dei dati personali, compresi i dati personali inerenti al presente accordo.

1.3. Il Responsabile manterrà tutte le misure tecniche e organizzative per soddisfare i requisiti stabiliti dal presente accordo ed altri eventuali allegati.

2. Comunicazione dei Dati

2.1. Il Responsabile al Trattamento tratta i Dati personali del Titolare del Trattamento solo ai fini dell'esecuzione dell'incarico ricevuto. Il Responsabile del Trattamento non deve trattare, trasferire, modificare, correggere o alterare i Dati personali del Titolare del Trattamento o divulgare o consentirne la divulgazione a terzi se non in conformità alle istruzioni documentate dal Titolare del Trattamento, a meno che il trattamento non sia richiesto dall'UE e/o dalle leggi dello Stato Membro a cui è soggetto il Responsabile e/o una qualsiasi legislazione anche sovranazionale a cui è soggetto il Responsabile. Il Responsabile del Trattamento dovrà, nella misura consentita da tali leggi, informare il Titolare del Trattamento di tale requisiti legali prima di trattare i Dati Personali e attenersi alle istruzioni del Titolare del Trattamento per ridurre al minimo, per quanto possibile, l'ambito della divulgazione.

3. Affidabilità e Non-Divulgazione

3.1. Il Responsabile del Trattamento adotterà misure ragionevoli per garantire l'affidabilità di qualsiasi addetto che possa avere accesso ai dati personali interessati al trattamento.

3.2. Il Responsabile del Trattamento garantisce che tutti gli addetti:

3.2.1. Siano informati della natura confidenziale dei Dati personali trattati per conto del Titolare del Trattamento e siano a conoscenza degli obblighi del Responsabile del Trattamento;

3.2.2. Siano stati adeguatamente formati/ certificazioni appropriate in relazione al GDPR o qualsiasi altra formazione / certificazione eventualmente richiesta dal Titolare del Trattamento;

3.2.3. Siano soggetti a impegni di riservatezza o obblighi professionali o normativi di riservatezza;

3.2.4. Siano soggetti all'autenticazione dell'utente e alle procedure di accesso quando accedono ai Dati personali del Titolare del Trattamento in conformità al presente Accordo, all'affidamento ed alle Leggi sulla Protezione dei Dati applicabili.

4. Sicurezza - Articolo 32 Regolamento Europeo 2016/679

4.1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del Trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

4.1.1. la pseudonimizzazione e la cifratura dei dati personali;

4.1.2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

4.1.3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali del Titolare del Trattamento in caso di incidente fisico o tecnico;

4.1.4. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il responsabile del trattamento deve garantire l'applicazione degli adempimenti inerenti l'attività degli "Amministratori di sistema" in riferimento al Prov. del 27/11/2008 del Garante della Privacy, ove applicabili, ed in particolare all'autenticazione dell'utente mediante valide credenziali di accesso per ciascuna persona fisica, e ciascun amministratore di sistema che prevedano la registrazione degli accessi mediante conservazione inalterabile dei LOG degli stessi e delle attività di trattamento per almeno 6 mesi.

Poiché i trattamenti dati affidati riguardano la Pubblica Amministrazione, il RESPONSABILE mette in atto le medesime misure minime di sicurezza richieste alla PA, in riferimento alle misure dell'AGID - CIRCOLARE 18 aprile 2017, n. 2/2017.

4.2. Nel valutare l'adeguato livello di sicurezza, il Responsabile del Trattamento tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

5. Catena di Responsabilità

5.1. A partire dalla Data di Validità del Presente accordo, il Titolare del Trattamento autorizza il Responsabile del Trattamento a coinvolgere altri Responsabili (autorizzazione generale). Il Responsabile del Trattamento si impegna a comunicare i dati solamente previo consenso scritto da parte del Titolare del Trattamento.

5.2. il Responsabile del Trattamento dovrà:

5.2.1. Su richiesta da parte del Titolare, fornire i dettagli completi relativi al trattamento dei dati da parte di altri Responsabili (sub-responsabili - Allegato 2).

5.2.2. Effettuare un'adeguata "due diligence" su ciascun responsabile aggiunto (sub-responsabile) per garantire che possa fornire il livello di protezione dei Dati personali definito sulle istruzioni fornite dal Titolare del Trattamento. In ogni caso il Responsabile deve assicurare che il responsabile aggiunto (sub-responsabile) adotti misure tecniche e organizzative appropriate e/o ulteriori in modo tale che il Trattamento soddisfi i requisiti del GDPR ed il presente Accordo.

5.2.3. Su richiesta, il Responsabile del Trattamento dovrà fornire al Titolare del Trattamento una copia dei suoi accordi con altri Responsabili, per la sua revisione.

5.2.4. Se e quando tale contratto comporti il trasferimento dei Dati del Titolare in Paesi Extra - Ue, dovranno essere incorporate le clausole di riservatezza o qualsiasi altro meccanismo adottato per garantire l'adeguata protezione dei Dati personali del Titolare del Trattamento.

5.2.5. Rimanere pienamente responsabile nei confronti del Titolare del Trattamento per qualsiasi mancanza da parte di ciascun altro Responsabile (sub - responsabile) nell'adempiere ai propri obblighi in relazione al trattamento dei Dati personali del Titolare del Trattamento.

6. I Diritti degli Interessati - Articoli 15 - 16 - 17 - 18 - 19 - 20 - 21 - 22 - 23

6.1. Tenuto conto della natura del Trattamento, il Responsabile del Trattamento assisterà il Titolare del Trattamento implementando le misure tecniche ed organizzative appropriate. Se e quando possibile, supporterà il Titolare per l'adempimento dell'obbligo di quest'ultimo di garantire l'esercizio dei diritti degli interessati come previsto dal Regolamento Europeo 2016/679

6.2. Il Responsabile del Trattamento dovrà informare tempestivamente il Titolare del Trattamento se riceve una richiesta da un interessato, dall'Autorità di controllo e / o altra autorità competente ai sensi delle leggi sulla protezione dei dati applicabili in relazione ai Dati Personali del Titolare del Trattamento.

6.3. Il Responsabile del Trattamento dovrà cooperare come richiesto dal Titolare del Trattamento per consentire:

6.3.1. La fornitura di tutti i dati richiesti dal Titolare entro un ragionevole periodo di tempo specificato in ciascun caso dal Titolare stesso. Tale procedura dovrà essere rispettata per tutte le informazioni comprese le copie del reclamo, la comunicazione o la richiesta e qualsiasi Dato Personale che il Titolare del Trattamento conserva relativo ad un Interessato.

6.3.2. Ove applicabile, fornire l'assistenza richiesta dal Titolare del Trattamento per consentirgli di soddisfare la relativa richiesta entro i termini prescritti dalla Legge.

6.3.3. Implementare eventuali misure tecniche ed organizzative aggiuntive che possano essere ragionevolmente richieste dal Titolare del Trattamento per consentire di rispondere in modo efficace a reclami, comunicazioni o richieste pertinenti.

7. Violazione dei Dati Personali - Articoli 33 e 34 - Regolamento Europeo 2016/679

7.1. Il Responsabile del Trattamento dovrà inviare una notifica al Titolare del Trattamento senza indebito ritardo e, in ogni caso, entro ventiquattro (24) ore dall'essere venuto a conoscenza o aver ragionevolmente sospettato di una violazione dei dati personali. Il Responsabile del Trattamento fornirà al Titolare del Trattamento informazioni sufficienti per consentire al Titolare del Trattamento di adempiere a qualsiasi obbligo di segnalare (Autorità di controllo e/o interessati) una violazione dei Dati Personali ai sensi del Regolamento Europeo 2016/679. Tale notifica deve contenere:

7.1.1. La descrizione, la natura della violazione dei dati personali, le categorie ed il numero dei soggetti interessati, nonché le categorie ed il numero di dati personali colpiti dalla violazione;

7.1.2. Comunicare il nome e le informazioni di contatto del Responsabile della protezione dei dati o di altri contatti rilevanti dai quali possono essere ottenute ulteriori informazioni;

7.1.3. Descrivere il rischio stimato e le probabili conseguenze della Violazione dei Dati Personali;

7.1.4. Descrivere le misure adottate o proposte per gestire la Violazione dei Dati Personali.

7.1.5. Mantenere un registro per l'annotazione degli incidenti.

7.2. Il Responsabile del Trattamento dovrà cooperare con il Titolare del Trattamento ed intraprendere le misure ragionevoli per assisterlo nelle indagini, nella mitigazione e risoluzione di ogni violazione.

7.3. In caso di violazione dei dati personali, il Responsabile del Trattamento non deve informare terzi senza prima ottenere il consenso scritto del Titolare del Trattamento, salvo che lo richieda il diritto dell'Unione o una legge dello stato cui è soggetto il Responsabile. In tal caso, il Responsabile del Trattamento dovrà informare il Titolare del Trattamento circa tale obbligo giuridico, fornire una copia della notifica proposta e considerare eventuali commenti formulati dal Titolare del Trattamento prima di notificare la Violazione dei dati personali.

8. Valutazione d'Impatto sulla Protezione dei Dati e Consultazione Preventiva - Articoli 35 e 36 - Regolamento Europeo 2016/679

8.1. Il Responsabile del Trattamento fornirà al Titolare del Trattamento un'assistenza ragionevole per qualsiasi trattamento oggetto di una valutazione d'impatto sulla protezione dei dati richiesta dall'articolo 35 del GDPR e previa consultazione con qualsiasi autorità di controllo da parte del Titolare del Trattamento che sia richiesta ai sensi dell'articolo 36 del GDPR, in ogni caso unicamente in relazione al trattamento dei dati personali oggetto del presente accordo.

9. Cancellazione o restituzione dei Dati Personali

9.1. Il Responsabile del Trattamento dovrà prontamente e, in ogni caso, entro e non oltre 72 ore: (i) cessare il Trattamento dei Dati Personali del Titolare del Trattamento da parte del Responsabile; o (ii) risolvere l'Accordo, a scelta del Titolare del Trattamento (tale scelta deve essere notificata al Responsabile del Trattamento per iscritto). Dovrà inoltre:

9.1.1. Restituire una copia completa di tutti i Dati al Titolare del Trattamento stesso mediante trasferimento sicuro di file nel formato indicato dal Titolare del Trattamento, cancellare in modo sicuro tutte le altre copie dei Dati personali elaborati dal Responsabile del Trattamento;

9.1.2. Cancellare in modo sicuro tutte le copie dei dati personali del Titolare del Trattamento trattati dal Responsabile del Trattamento o da qualsiasi sub Responsabile autorizzato e, in ogni caso, fornire una certificazione scritta al Titolare del Trattamento attestante che ha rispettato pienamente i requisiti della sezione Cancellazione o Restituzione dei Dati Personali del Titolare del Trattamento.

9.2. Il Responsabile del Trattamento può conservare i Dati solo nella misura e per il periodo richiesto dalla legge dell'Unione o dello Stato Membro, e sempre a condizione che il Responsabile del Trattamento garantisca la riservatezza di tutti i Dati personali e garantisca che gli stessi siano trattati esclusivamente secondo le necessità per gli scopi specificati nelle leggi dell'Unione o degli Stati membri che richiedono la sua conservazione e per nessun'altra finalità.

10. Diritti di audit

10.1. Il Responsabile del Trattamento dovrà mettere a disposizione del Titolare del Trattamento, su richiesta, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del Trattamento o da un altro soggetto da questi incaricato di qualsiasi sede in cui il Trattamento di Dati Personali del Titolare del Trattamento abbia luogo. Il Responsabile del Trattamento consentirà al Titolare del Trattamento o ad altro auditor incaricato di ispezionare, verificare e copiare tutte le registrazioni, processi e sistemi pertinenti in modo che il Titolare del Trattamento possa accertarsi che le disposizioni del presente accordo siano rispettate. Il Responsabile del Trattamento dovrà fornire piena collaborazione al Titolare del Trattamento in relazione a tali audit e fornirà, su richiesta, evidenza del rispetto degli obblighi previsti. Il Responsabile del Trattamento dovrà immediatamente informare il Titolare qualora, a suo parere, un'istruzione ai sensi della presente sezione Audit (Diritti di Audit) violi il Regolamento Europeo 2016/679 o altre disposizioni, nazionali o dell'Unione Europea, relative alla protezione dei dati.

11. Trasferimento dei Dati Personali del Titolare del Trattamento

11.1. Il Responsabile del Trattamento non tratterà i Dati Personali del Titolare del Trattamento né consentirà a nessun Sub-Responsabile Autorizzato di trattare i Dati Personali in un Paese terzo, se non nei confronti di quei destinatari in Paesi Terzi autorizzati per iscritto dal Titolare del Trattamento.

12. Codici di Condotta e Certificazione - Articoli 40 e 42 - Regolamento Europe 2016/679

12.1. Su richiesta del Titolare del Trattamento, il Responsabile del Trattamento dovrà rispettare qualsiasi Codice di condotta approvato ai sensi dell'articolo 40 del GDPR ed ottenere qualsiasi certificazione approvata dall'articolo 42 del GDPR, per quanto riguarda il trattamento dei Dati personali del Titolare del Trattamento.

13. Condizioni generali

13.1. In base a questa sezione, le parti concordano che il presente Accordo e le eventuali/ulteriori clausole contrattuali terminano automaticamente in caso di risoluzione dell'affidamento o alla scadenza o alla risoluzione di tutti i contratti di servizio stipulati dal Responsabile del Trattamento con il Titolare del Trattamento, in riferimento all'affidamento.

13.2. Qualsiasi obbligo imposto al Responsabile del Trattamento ai sensi del presente Contratto in relazione al Trattamento dei Dati personali sopravviverà a qualsiasi risoluzione o scadenza di questo.

13.3. Il presente accordo è regolato dagli articoli di legge previsti nell'affidamento per tutto il tempo in cui tali articoli facciano parte della legislazione di uno Stato membro dell'Unione Europea.

13.4. Qualsiasi violazione di questo Contratto costituirà una violazione sostanziale dell'accordo principale.

13.5. Qualora una qualsiasi disposizione di questo Contratto fosse non valida o inapplicabile, il resto di questo Contratto rimarrà valido e in vigore. La clausola non valida o inapplicabile sarà (i) emendata se necessario per garantirne la validità e l'applicabilità, preservando nel contempo il più strettamente possibile le intenzioni delle parti o, se ciò non fosse possibile, (ii) interpretata in modo tale che la parte non valida o inapplicabile non sia mai stata contenuta in esso.