Clausole Contrattuali Contitolarità

Data Protection Agreement

1 Scopo del documento

Il presente documento ha per obiettivo quello di fornire un facsimile di accordo Data Protection (Data Protection Agreement) nel caso in cui la relazione che si viene ad instaurare per il trattamento di dati personali sia fra due soggetti o più soggetti, che a norma del GDPR si possano classificare come Contitolari rispetto ai trattamenti nei quali vengono coinvolti dati personali.

Si tratta di due o più soggetti giuridicamente diversi che concorrono ognuno per proprie parti all'interno di una unica finalità e determinano congiuntamente i mezzi attraverso i quali eseguire i trattamenti di dati personali. Questi soggetti pertanto devono sottoscrivere un accordo, nel quale si dà atto degli impegni comuni e comune responsabilità, nell'eseguire trattamenti all'interno di un preciso processo che prevede il trattamento di dati personali.

Il facsimile che segue, deve essere ovviamente compilato e personalizzato sulla base di quanto e come ogni soggetto contribuisce al processo complessivo, pertanto costituisce una linea guida nella formalizzazione dell'accordo.

L'articolato che segue può essere oggetto di uno specifico accordo od essere inserito all'interno di atti convenzionali o protocolli di intesa che vengono sottoscritti per regolare anche altri rapporti oltre alla Data Protection.

1 Fac-simile di Accordo Contitolarità

Accordo di contitolarità
(Data Protection Agreement)

Tra

La REGIONE TOSCANA - Giunta Regionale , con sede in _____, rappresentata dal dirigente del [*Settore/direzione]*_____, Dott._____,nella sua qualità di delegato del titolare del trattamento
E
[Titolare 1], con sede in _____, rappresentata da_____, Dott._____, nella sua qualità di _____
E
[aggiungere altri eventuali contitolari, se presenti]

(di seguito, congiuntamente, i *"Contitolari"*)

Premesso che:

Il Regolamento UE 2016/679 relativo alla protezione dei dati personali prevede la possibilità che in talune circostanze uno o più soggetti possano determinare congiuntamente le finalità e i mezzi del trattamento dei dati. In tal senso si esprime l'art. 26 del Regolamento UE che configura tali soggetti quali "contitolari" del trattamento con rispettive responsabilità da ripartire e definire in modo trasparente in un *accordo* interno;

Le linee guida dell'EDPB n. 7/2020 precisano che sussiste la contitolarità quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti che caratterizzano il titolare del trattamento tenendo conto che la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale*;*

In relazione a quanto delineato dalle citate linee guida, i rapporti tra contitolari possono quindi articolarsi in modo *asimmetrico,* nel senso che in alcune situazioni i soggetti coinvolti possono determinare in misura diversa le finalità e/o i mezzi e conseguentemente ciascuno di essi risponde solo per una parte del trattamento;

Richiamati:
[
Richiamare in elenco la legge/regolamento/atto/contratto/progetto….che definiscono la base di liceità, le finalità e le attività di trattamento oggetto dell'accordo per ciascun contitolare
]

Considerato che:

il Regolamento UE 2016/679 richiede ai Titolari del trattamento di comprovare, in applicazione del principio di accountability*,* anche tramite evidenze le valutazioni, le scelte e le misure adottate a garanzia della protezione dei dati personali;

Il Regolamento UE 2016/679 presuppone quindi la definizione di un modello "organizzativo" con ruoli, compiti e responsabilità dei vari attori coinvolti nelle attività, nonché del perimetro di azione di ciascun soggetto per quanto riguarda il trattamento e la gestione di dati personali, sancito dalla sottoscrizione di un accordo interno tra le parti ex art. 26 GDPR;

SI CONCORDA QUANTO SEGUE:

Art. 1
Premesse, richiami e considerata

1.1 Le premesse, i richiami e i considerata costituiscono parte integrante del presente Accordo.

Art. 2
Oggetto dell'accordo

2.1 Il presente accordo di contitolarità regolamenta l'ambito di azione e le responsabilità dei contitolari del trattamento in merito all'osservanza degli obblighi derivanti dal Regolamento UE 2016/679 , compreso il rapporto con gli interessati. In particolare, l'accordo ha lo scopo di definire i compiti dei contitolari relativamente alle attività di trattamento dei dati personali riconducibili a ciascuno di essi.

Art. 3
Attività di trattamento dei dati personali di ciascun contitolare

3.1 Il Regolamento UE 2016/679 insiste sulla necessità di delineare con chiarezza i ruoli, i compiti e le responsabilità per garantire principalmente i diritti delle persone interessate (soggetti a cui si riferiscono i dati personali).
3.2 Come descritto in premessa, quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento essi sono *contitolari* e in quanto tali sono tenuti, ciascuno per la propria parte, ad adottare le relative misure, tecniche e organizzative, per garantire la protezione dei dati personali.
3.3 I Contitolari svolgono i propri compiti nel rispetto dei principi di finalità, di proporzionalità e di minimizzazione dei dati personali trattati e trattano i dati degli interessati (persone fisiche) congiuntamente come di seguito descritto per una migliore gestione delle attività finalizzate alla realizzazione delle finalità di ciascuno.

A tal fine si specifica quanto segue (se necessario suddividere in fasi il trattamento):

La **Regione toscana - Giunta regionale** nell'ambito del presente accordo di contitolarità ha il compito di:

[
Descrivere i compiti svolti

]

Tali funzioni comportano il trattamento dei seguenti dati personali (specificare la tipologia di dati, le categorie degli interessati e la loro numerosità atta ad individuare se trattasi di trattamento su larga scala):

[

…..
…..
….

]
e lo svolgimento delle seguenti operazioni di trattamento:
[
…..
…..
….

]

Il [Titolare 1] nell'ambito del presente accordo di contitolarità ha il compito di:
[
Descrivere i compiti svolti

]
Tali funzioni comportano il trattamento dei seguenti dati personali (specificare la tipologia di dati, le categorie degli interessati e la loro numerosità atta ad individuare se trattasi di trattamento su larga scala)::
[
…..
…..
….

]
e lo svolgimento delle seguenti operazioni di trattamento:
[
…..
…..
….

]

[ripetere per ogni titolare che concorre all'accordo di contitolarità]

Art. 4
Modalità di trattamento

4.1 La **Regione toscana - Giunta regionale** tratterà i dati con modalità Cartacea [*descrizione sommaria del processo e dei trattamenti di cui è composto*] e/o digitale, attraverso il seguente applicativo _____ *[descrizione sommaria del processo di trattamento]*_____

4.2 Il *[titolare 1]* tratterà i dati con modalità Cartacea [*descrizione sommaria del processo e dei trattamenti di cui è composto*] e/o digitale, attraverso il seguente applicativo _____ [*descrizione sommaria del processo di trattamento*]_____

[ripetere per ogni titolare che concorre all'accordo di contitolarità]

Schema riassuntivo dei dati trattati, delle finalità e modalità del trattamento

Contitolarità del trattamento	**Categoria di interessati**	**Tipologia dei Dati**	**Finalità del trattamento**	**Modalità del trattamento**

Art. 5
Soggetti designati al trattamento e destinatari dei dati

5.1 I contitolari si impegnano ad istruire ed autorizzare il personale facente parte della propria organizzazione a trattare i dati personali e a nominare, laddove sussistono i presupposti, come responsabili del trattamento i soggetti esterni che potrebbero eventualmente intervenire nelle operazioni di trattamento per conto dei contitolari stessi.

5.2 Inoltre, i dati di natura personale potranno essere trasmessi a soggetti terzi appartenenti alle seguenti categorie:

[indicare le categorie di persone fisiche o giuridiche, le autorità pubbliche, il servizio o altro organismo che riceve comunicazione di dati]:

- ….
- ….
- ….

Art. 6
Informativa Privacy

6.1 Il [*indicare il contitolare/i che raccoglie i dati]si impegna a fornire, in sede di raccolta del dato, le informazioni di cui all'art. 13 del Regolamento UE 2016/679 in forma concisa, trasparente, intellegibile e facilmente accessibile, scritta con linguaggio chiaro e semplice. Nello specifico l'informativa privacy verrà inserita nella piattaforma/sito web/modulo cartaceo/ affissa in luogo accessibile al pubblico…,* consentendo ai soggetti interessati di prenderne visione.

6.2 I contitolari si impegnano a fornire supporto al contitolare sopra individuato nella redazione dell'informativa.

Art.7
Esercizio dei diritti dell'interessato

7.1 Tutte le richieste di esercizio dei diritti di cui agli artt. 15-22 del Regolamento UE 2016/679 saranno gestite, per conto e nell'interesse di tutti i Contitolari, dal_____(*dati di contatto del contitolare indicato*), rivolgendosi al **Responsabile della Protezione dei Dati (DPO),** contattabile all'indirizzo mail: _____ *[o altro canale di comunicazione/contatto]*.
7.2 Gli interessati potranno esercitare, comunque, i propri diritti anche nei confronti di ciascun contitolare, ai sensi dell'art. 26, comma 3, del GDPR.
7.3 Le parti si impegnano a fornire supporto, per quanto di rispettiva competenza, agli altri contitolari per dare seguito alle richieste degli interessati.

Art. 8
Sicurezza del trattamento

8.1 Nel rispetto dei principi di cui all'art. 32 del Regolamento UE 2016/679 i contitolari nei limiti delle funzioni esercitate e delle rispettive prerogative, tenendo conto anche dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità di trattamento, devono adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati. Le parti stabiliscono che le misure tecniche e organizzative adeguate sono le seguenti *[indicare ,in ragione dell'oggetto del contratto, le misure adeguate per ciascuna categoria che si ritiene di richiedere sotto elencata]*:

- *misure di pseudonimizzazione e cifratura dei dati personali:*_____
- *misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento:*_____
- *misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico:*_____*;*
- *procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*
- *misure di identificazione e autorizzazione dell'utente*
- *misure di protezione dei dati durante la trasmissione*
- *misure di protezione dei dati durante la conservazione*
- *misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati*
- *misure per garantire la registrazione degli eventi*
- *misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita*
- *misure di informatica interna e di gestione e governance della sicurezza informatica*
- *misure di certificazione/garanzia di processi e prodotti*
- *misure per garantire la minimizzazione dei dati*
- *misure per garantire la qualità dei dati*
- *misure per garantire la conservazione limitata dei dati*
- *misure per garantire la responsabilità*

- *misure per consentire la portabilità dei dati e garantire la cancellazione].*

8.2 Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), ciascun Contitolare applica limitazioni specifiche e/o garanzie supplementari.

8.3 Nei casi in cui ciascun Contitolare effettui trattamenti di conservazione dei dati personali nel proprio sistema informativo, deve garantire la separazione di tipo logico di tali dati da quelli trattati per conto di terze parti o per proprio conto e deve adottare misure tecniche ed organizzative adeguate a salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

8.4 Ciascun Contitolare attesta, a mezzo della sottoscrizione del presente accordo, la conformità della propria organizzazione almeno ai parametri di livello minimo di cui alle misure di sicurezza individuate da Agid la circolare n. 2/2017

8.4 I Contitolari, in quanto parti dell'Accordo si impegnano a stabilire, attuare, mantenere e migliorare un sistema di gestione per la sicurezza delle informazioni, sia con riferimento a strumenti, archivi e supporti cartacei, sia con riferimento a strumenti e mezzi digitali e informatici utilizzati.

Art. 9
Data Breach

9.1 Si intende per Data Breach ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal titolare del trattamento.

9.2 Ai sensi e per gli effetti dell'art. 33 Regolamento UE 2016/679, il titolare del trattamento, in caso di violazione di dati personali, notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore è corredata dai motivi di ritardo. Ai sensi e per gli effetti dell'art. 34 Regolamento UE 2016/679, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo qualora la violazione di dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali dell'interessato.

9.3 Titolare del trattamento per la gestione di eventuali Data Breach è _____, il quale si atterrà alla disciplina per la gestione delle violazioni dei dati. Ciascun contitolare dovrà pertanto comunicare tempestivamente al _____ gli eventuali casi di data breach per la valutazione congiunta del fenomeno e per le eventuali comunicazioni al Garante e agli interessati. In caso di valutazioni non concordi tra i contitolari la valutazione ultima sarà rimessa al contitolare su cui insiste la violazione dei dati personali

9.4 Ciascun contitolare si impegna a fornire, per quanto di rispettiva competenza, specifico report relativo alla violazione di sicurezza occorso entro il termine sopra indicato; tale documento dovrà contenere quantomeno:

a) una descrizione relativa alla natura della violazione dei dati personali compresi, ove possibile, dell'indicazione delle categorie e del numero approssimativo di interessati in questione nonché delle categorie e del numero approssimativo di registrazioni dei dati personali in questione;

b) l'indicazione del nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) una descrizione delle probabili conseguenze della violazione dei dati personali;
d) una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Art. 10
DPIA

10.1 Per ogni nuova iniziativa che comporti l'utilizzo di nuove tecnologie per il trattamento dei dati, o in caso di modifiche di strumenti del trattamento già adottati, i Contitolari si impegnano a collaborare per la valutazione dei rischi connessi e delle misure tecniche ed organizzative da adottare a tutela dei dati personali, secondo i dettami dell'art. 35 Regolamento UE 2016/679.
10.2 Il punto di contatto _____ individuato dalle parti indicherà la metodologia da adottare e si impegnerà a raccogliere le singole valutazioni d'impatto prodotte dai singoli contitolari.

Art. 11
Le persone di contatto delle Parti

11.1 Qualora risultasse necessario e per ogni evenienza, le Parti forniscono reciprocamente le informazioni richieste sui dati trattati nella relativa area funzionale.
11.2 Le persone di contatto delle Parti sono i rispettivi responsabili _____.
11.3 Le Parti danno immediata comunicazione di qualsiasi cambiamento, es. sostituzione, riguardo la persona individuata come punto di contatto, ovvero ciascun referente per le medesime.
11.4 Le parti si impegnano a comunicare altresì il nominativo e i recapiti del Responsabile per la Protezione dei dati (RPD, ove nominati;

Art. 12
I responsabili del trattamento

12.1 Qualora una della Parti intenda avvalersi di responsabili del trattamento nell'ambito del presente accordo, essa si impegna a stipulare uno specifico contratto ai sensi dell'art. 28 del GDPR e a darne comunicazione in forma scritta alle altre Parti, prima della stipula dello stesso.
12.2 Le Parti si informano reciprocamente e tempestivamente di qualsiasi modifica riguardo la nomina e/o la sostituzione dei responsabili del trattamento e individuano solamente fornitori che garantiscano il rispetto della normativa sulla protezione dei dati e delle disposizioni del presente accordo.
12.3 Non sono considerati servizi, ai sensi del presente articolo, quelli di cui le Parti si avvalgono in forma di supporto accessorio, come ad esempio i servizi di telecomunicazione e manutenzione occasionale.
12.4 In ogni caso, le Parti sono tenute a stipulare opportuni accordi contrattuali in conformità alla legge e ad adottare misure di controllo al fine di garantire la protezione e la sicurezza dei dati personali, anche nel caso di servizi aggiuntivi forniti da terzi.

Art. 13
I registri delle attività di trattamento

13.1 I contitolari tengono e aggiornano, ove previsto, il registro delle attività di trattamento ai sensi dell'art. 30 par. 1 del GDPR e lo comunicano laddove necessario agli altri contitolari.

Art. 14
Trasferimento dei dati verso paesi extra-UE

14.1 Le parti si impegnano a circoscrivere il trattamento dei dati personali all'interno del territorio dell'Unione Europea
14.2 Le Parti si impegnano a rispettare, in caso di trasferimento dei dati all'esterno dell'Unione Europea, i limiti e le condizioni di cui al capo V del Regolamento UE 2016/679.

Art. 15
La responsabilità delle Parti nei confronti degli interessati

15.1 Fermo restando i ruoli identificati e i compiti svolti,le Parti rispondono in solido nei confronti dell'interessato per i danni causati da un trattamento non conforme al GDPR. È fatta salva, in ogni caso, la possibilità di esercizio del diritto di regresso, ai sensi dell'art. 82, comma 5 del GDPR.

Art. 16
Conclusioni

16.1 Le parti si impegnano a revisionare il presente accordo in caso di necessità; a tal fine verrà monitorato e revisionato periodicamente per assicurarne l'attualità e l'allineamento alle novità legislative.
16.2 Il presente accordo viene meno con il conseguimento delle finalità del trattamento da parte dei contitolari o qualora non vi siano più i presupposti di contitolarità.
16.3 Ai sensi dell'articolo 26 comma 2 del Regolamento UE 2016/679, il contenuto essenziale del presente accordo sarà pubblicato sul sito del _____ e in tal modo messo a disposizione degli interessati.

Luogo, data, firme