DIGITAL 360 | Group

Whitepaper

Una guida pratica alla gestione dei contratti

L'esternalizzazione di attività che comportano il trattamento di dati personali alla luce del GDPR

by P4I

Annamaria Italiano
Senior Legal Consultant, Partners4innovation
annamaria.italiano@p4i.it

Gabriele Faggioli
CEO Partners4innovation
gabriele.faggioli@p4i.it

2018

Il General Data Protection Regulation (GDPR), ovvero il Regolamento UE n. 679/2016 sul trattamento e protezione dei dati personali, formalmente in vigore dal 24 maggio 2016, ma pienamente applicabile dal 25 maggio 2018, obbligherà aziende ed enti pubblici non solo a ripensare interamente la gestione e l'approccio alla data protection, ma anche a vagliare, rivedere e aggiornare i contratti in essere con oggetto – o comunque implicanti – un trattamento dei dati personali.
Il nuovo Regolamento stabilisce contenuti contrattuali puntuali e specifici che devono connotare gli accordi tra ogni data controller (l'azienda o ente pubblico titolare del trattamento) che intende esternalizzare un trattamento di dati personali e il data processor incaricato di detto trattamento (il fornitore di servizi esternalizzati, sia esso un outsourcer tradizionale o un cloud service provider).
È pertanto raccomandabile tener conto delle indicazioni del nuovo Regolamento già durante le negoziazioni relative a servizi esternalizzati a oggi in corso, onde evitare di dover rivedere e adeguare i relativi contratti tra qualche mese, in vista della scadenza del 25 maggio 2018. Data entro la quale l'intera documentazione aziendale sulla gestione della privacy (contratti, lettere di nomina, informative agli interessati, richieste di consenso, ecc.) dovrà essere inderogabilmente conforme alla nuova normativa. Parallelamente, occorrerà verificare e aggiornare la documentazione esistente, per garantirne l'allineamento rispetto al Regolamento.

In breve, il GDPR imporrà una formalizzazione più stringente degli obblighi che presiedono al trattamento e comporterà un aggravamento della posizione e delle responsabilità del data processor, in tal modo auspicabilmente creando i presupposti, da un lato, per un innalzamento delle garanzie di sicurezza da parte dell'offerta di servizi, dall'altro lato, per incoraggiare le imprese verso l'esternalizzazione dei propri trattamenti.

Ma cosa prevede il GDPR sulla formalizzazione dei reciproci obblighi e responsabilità tra data controller e data processor?
Di seguito proponiamo una schematizzazione di tutto ciò che andrà fatto per gestire i contratti alla luce del GDPR attraverso una serie di 20 tematiche affrontate in modo molto pratico.

Naturalmente, P4i è a disposizione per ogni attività di supporto nella analisi, stesura e rivisitazione dei contratti.

INDICE

1. Quale sarà l'impatto del GDPR sui contratti sui contratti di outsourcing, cloud e fornitura? 5

2. Quali sono le novità introdotte dal GDPR in relazione ai rapporti contrattuali tra titolare del trattamento (data controller) e responsabile del trattamento (data processor)? 6

3. Apparentemente sembrerebbe che la nuova normativa non faccia che imporre ulteriori oneri rispetto a quelli già esistenti. È così importante la formalizzazione richiesta dal GDPR? 7

4. Come è opportuno orientarsi in relazione ai contratti attualmente in fase di negoziazione e a quelli già in essere? 8

5. L'onere di aggiornamento della documentazione contrattuale in essere sarà significativo? 9

6. In quali casi il GDPR richiede una formalizzazione scritta degli obblighi relativi all'esternalizzazione del trattamento dei dati personali? 10

7. Quali contenuti dovranno necessariamente presentare gli accordi tra data controller e data processor? 11

8. Cosa prevede la nuova normativa con specifico riferimento al ricorso al subappalto da parte di un responsabile del trattamento? 13

9. È necessario che il titolare nomini quali responsabili del trattamento i subappaltatori del proprio responsabile? E come avviene la nomina? 15

10. Quali sono le responsabilità del data controller in ordine al ricorso ad un data processor? 16

11. Quali sono le responsabilità del data processor alla luce del GDPR? 17

12. Quali obblighi il GDPR pone direttamente in capo al data processor? 18

13. Nel contesto della nuova normativa, cosa ne è della figura degli incaricati del trattamento? E di quella del responsabile interno del trattamento? Insomma, cosa cambia nell'organigramma privacy aziendale rispetto al passato? 20

14. Quali sono i danni risarcibili ai sensi dell'articolo 82 GDPR? 21

15. Sono previste per legge ipotesi di esonero da responsabilità risarcitoria verso gli interessati? 22

16. È possibile limitare contrattualmente la responsabilità risarcitoria per danni conseguenti a trattamento illecito di dati personali? 23

17. Come si ripartisce la responsabilità per i danni conseguenti ad un trattamento illecito nei rapporti interni titolare-responsabile? 25

18. Quali sono le conseguenze sanzionatorie in caso di mancato rispetto delle prescrizioni relative ai contenuti degli accordi contrattuali tra data controller e data processor? 26

19. Gli interessati che si ritengano lesi da un illecito trattamento come possono ottenere ristoro del danno patito? 27

20. Esistono dei set di clausole contrattuali standard da adottare per disciplinare i rapporti tra titolare e responsabile del trattamento? 28

Riepilogando 29

Check list dei contenuti contrattuali che devono risultare dagli accordi Titolare e Responsabile del trattamento 30

Partners4Innovation 31

1. Quale sarà l'impatto del GDPR sui contratti di outsourcing, cloud e fornitura?

Il *General Data Protection Regulation* (GDPR), ovvero il Regolamento UE n. 679/2016 in materia di protezione dei dati personali, formalmente in vigore dal 24 maggio 2016, ma pienamente applicabile a partire dal 25 maggio 2018, obbligherà aziende e pubbliche amministrazioni non solo a ripensare interamente la gestione e l'approccio alla *data protection*, ma imporrà anche un **maggiore onere di formalizzazione** rispetto a quanto fatto fino ad oggi.

La nuova normativa stabilisce, infatti, **contenuti contrattuali puntuali e specifici** che devono connotare gli accordi tra ogni data controller (l'azienda o la p.a. titolare del trattamento) che intende esternalizzare un trattamento di propri dati personali e il data processor da essa preposto a detto trattamento (il fornitore di servizi esternalizzati, sia esso un *outsourcer* tradizionale o un *cloud service provider*).

Ciò vuol dire concretamente che ogni qual volta l'azienda o la p.a. stipuli un contratto con un fornitore esterno che abbia ad oggetto o possa comunque comportare il trattamento, da parte di quest'ultimo, di dati personali di titolarità della prima, oltre alla negoziazione e alla formalizzazione dei contenuti contrattuali strettamente inerenti la prestazione del servizio (diritti e doveri delle parti, durata, garanzie, responsabilità contrattuali, ecc.), **dovranno essere oggetto di discussione ed accordo anche le previsioni inerenti specificamente le attività di trattamento dei dati personali**, secondo quanto previsto dal Regolamento.

Per saperne di più sulle novità introdotte dal GDPR con riferimento alla materia contrattuale, vai alla domanda 2.

Per tornare all'indice, clicca qui.

2. Quali sono le novità introdotte dal GDPR in relazione ai rapporti contrattuali tra titolare del trattamento (*data controller*) e responsabile del trattamento (*data processor*)?

Il GDPR impone una **formalizzazione scritta degli obblighi che presiedono alle attività esternalizzate di trattamento di dati personali**. Tale formalizzazione è, in tutta evidenza, necessaria ogni qual volta abbia luogo una esternalizzazione ovvero una delega di tutte le operazioni di trattamento correlate ad una determinata attività o ad un determinato processo aziendale o anche solo di una parte di esse.

Ciò avviene qualora l'azienda ricorra ad un **fornitore esterno** che agisca in qualità di responsabile del trattamento, nonché ogni qual volta quest'ultimo decida di avvalersi dell'**apporto di uno o più subappaltatori**, che svolgano al contempo il ruolo di sub-responsabili.

Gli obblighi introdotti dal Regolamento in tale materia potranno essere adempiuti tramite l'introduzione di **specifiche clausole nel contratto** che presiede ai rapporti tra l'azienda e il fornitore, ovvero attraverso la predisposizione di specifiche previsioni nell'atto di nomina a responsabile esterno del trattamento (oggi redatto ai sensi dell'articolo 29 del D. lgs. 196/2003 – Codice Privacy; un domani redatto ai sensi dell'articolo 28 del GDPR).

Inoltre, con l'avvento del nuovo Regolamento cambia radicalmente il **regime delle responsabilità risarcitorie** nei confronti degli interessati che abbiano subito un danno in conseguenza di un trattamento illegittimo. Titolare e responsabile, infatti, saranno assoggettati ad un regime di **responsabilità solidale**, che li esporrà nei confronti degli interessati per l'intero ammontare del danno cagionato.

Ciò comporterà, in tutta evidenza, l'esigenza che **il titolare valuti con attenzione le competenze e le caratteristiche organizzative del responsabile cui intende affidare le attività di trattamento** e, per altro verso, l'esigenza che **il responsabile valuti attentamente il contenuto della nomina**.

Per saperne di più:

- sugli obblighi di formalizzazione introdotti dal GDPR, vai alla domanda 6;
- sui contenuti previsti per gli accordi tra data controller e data processor, vai alla domanda 7;
- su cosa prevede la nuova normativa con riferimento al subappalto, vai alla domanda 8;
- sul regime di responsabilità solidale tra data controller e data processor, vai alla domanda 11.

Per tornare all'indice, clicca qui.

3. Apparentemente sembrerebbe che la nuova normativa non faccia che imporre ulteriori oneri rispetto a quelli già esistenti. È così importante la formalizzazione richiesta dal GDPR?

Solo in apparenza gli oneri di formalizzazione richiesti dal Regolamento potrebbero sembrare un appesantimento dei rapporti contrattuali tra le parti.

In realtà, essi rispondono a quel **principio di trasparenza** che costituisce uno dei fondamenti e delle condizioni legittimanti del trattamento e che il nuovo Regolamento impone a tutti "*gli operatori economici, comprese le micro, piccole e medie imprese*" (cfr. considerando n. 13 del Regolamento) al fine di garantire alle persone fisiche un livello coerente di protezione.

I contratti, infatti, definiranno in dettaglio e cristallizzeranno gli obblighi, anche in relazione agli aspetti di sicurezza e le responsabilità del *data processor*, stabilendo certezza tra le parti in ordine ai rispettivi ruoli.

Inoltre, dal momento che i contenuti minimi degli accordi tra *data controller* e *data processor* sono stabiliti dalla normativa, la formalizzazione di tali contenuti:

- Costituirà una **garanzia per il titolare del trattamento** in ordine al proprio livello di conformità formale rispetto al GDPR;
- Potrà essere utilizzata (eventualmente anche in sede di verifiche da parte dell'Autorità) quale **elemento per comprovare l'effettività della protezione** accordata dall'azienda ai dati personali di dipendenti, clienti, fornitori, ecc.;
- Auspicabilmente **accrescerà la fiducia riposta dagli interessati in ordine alle garanzie ad essi assicurate** e, conseguentemente, in ordine alla qualità e all'affidabilità dei servizi offerti.

Per saperne di più sui contenuti previsti per gli accordi tra data controller e data processor, vai alla domanda 7.

Per tornare all'indice, clicca qui.

4. Come è opportuno orientarsi in relazione ai contratti attualmente in fase di negoziazione e a quelli già in essere?

Come già detto, la nuova normativa prevede che i trattamenti affidati da un titolare ad un responsabile siano disciplinati da un contratto o da un altro atto giuridico che enuclei e dettagli specificamente i rispettivi doveri e responsabilità.

Se è scontato che tutti i contratti stipulati dopo la data di piena applicabilità del Regolamento nasceranno già conformi alla nuova normativa, è, tuttavia, altrettanto **raccomandabile tener conto delle indicazioni contenute nel nuovo Regolamento già nel corso delle negoziazioni relative a servizi esternalizzati ad oggi in corso**, onde evitare di dover rivedere ed adeguare i relativi contratti tra qualche mese, in vista della scadenza del 25 maggio 2018, data entro la quale l'intera documentazione aziendale relativa alla gestione della privacy (contratti, lettere di nomina, informative agli interessati, richieste di consenso, ecc.) dovrà essere inderogabilmente *compliant* rispetto alla nuova normativa.

È, quindi, non solo possibile, ma anche **consigliabile ed opportuno inserire già da ora le clausole relative alle tematiche indirizzate dal GDPR nei contratti da stipularsi da adesso fino al 25 maggio 2018**.

Parallelamente, occorrerà **vagliare, rivedere ed aggiornare la documentazione esistente**, relativa ai rapporti in essere la cui durata è destinata a scavalcare la fatidica data di piena applicabilità del Regolamento, al fine di garantirne l'allineamento rispetto a quanto in esso sancito.

Per saperne di più sull'aggiornamento dei contratti in essere, vai alla domanda 5.

Per tornare all'indice, clicca qui.

5. L'onere di aggiornamento della documentazione contrattuale in essere sarà significativo?

Non necessariamente. Dipenderà da cosa statuiscono i contratti in essere e dal livello di profondità con cui essi dettaglieranno gli obblighi in capo ai responsabili esterni del trattamento.

La normativa attuale già stabilisce che "*i compiti affidati al responsabile siano analiticamente specificati per iscritto dal titolare*" (articolo 28, comma quarto, Codice Privacy); inoltre, da un lato, si impone al responsabile di effettuare il trattamento attendendosi alle istruzioni impartite dal titolare e nei limiti delle stesse, dall'altro lato si stabilisce, in capo al titolare, il potere-dovere di vigilare sul responsabile, anche tramite verifiche periodiche, sulla puntuale osservanza delle norme in materia di trattamento dei dati personali e delle istruzioni ricevute (articolo 29, comma quinto, Codice Privacy).

A ciò si aggiunga, poi, ai sensi dell'articolo 31 dell'attuale Codice Privacy, "*i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*". Il concetto di idoneità, che, nell'impianto del nuovo Regolamento, è destinato a improntare sull'intera materia della sicurezza non è, dunque, una nozione sconosciuta all'attuale vigente normativa.

È, quindi, ben possibile che le attuali lettere di nomina a responsabile esterno del trattamento, così come i *Data Processing Agreement* proposti da molti fornitori di servizi informatici a corredo degli accordi di servizio, contengano già molte delle previsioni oggi previste espressamente ed obbligatoriamente dal GDPR.

Per saperne di più:

- sui contenuti previsti per gli accordi tra data controller e data processor, vai alla domanda 7;
- su cosa prevede la nuova normativa con riferimento al subappalto, vai alla domanda 8.

Per tornare all'indice, clicca qui.

6. In quali casi il GDPR richiede una formalizzazione scritta degli obblighi relativi all'esternalizzazione del trattamento dei dati personali?

Le ipotesi prese in considerazione dalla normativa sono fondamentalmente due:

- **Qualora il titolare affidi uno specifico trattamento ad un responsabile** (articolo 28, comma terzo, del GDPR);
- **Qualora un responsabile del trattamento intenda ricorrere ad un altro responsabile del trattamento dell'esecuzione di specifiche attività di trattamento** per conto del titolare (articolo 28 comma quarto, del GDPR).

In entrambi i suddetti casi, la normativa prevede che le parti siano tenute a stipulare un "*contratto*" o un "*altro atto giuridico a norma del diritto dell'Unione o degli Stati membri*" che vincoli il soggetto preposto alle attività di trattamento, definendone modalità, condizioni, durata, natura e finalità e chiarendo espressamente il tipo di dati personali trattati, le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento.
Il riferimento contenuto nella normativa ad un mero "*atto giuridico*" lascia intendere che **tale formalizzazione, in continuità con quanto sinora avvenuto, possa essere adempiuta anche mediante le lettere di nomina a responsabile esterno del trattamento, ai sensi dell'articolo 29 del Codice Privacy, purché provviste dei contenuti minimi indicati dall'articolo 28 del GDPR**.

Per saperne di più:

- sui contenuti previsti per gli accordi tra data controller e data processor, vai alla domanda 7;
- su cosa prevede la nuova normativa con riferimento al subappalto, vai alla domanda 8.

Per tornare all'indice, clicca qui.

7. Quali contenuti dovranno necessariamente presentare gli accordi tra data controller e data processor?

Così come già oggi avviene con le lettere di nomina a responsabile esterno del trattamento redatte ai sensi dell'articolo 29 del Codice Privacy, l'accordo vincolante tra il *data controller* ed il *data processor* dovrà disciplinare la materia considerata, **definendo la durata, la natura e le finalità del trattamento, il tipo di dati personali trattati, le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento**.

In aggiunta a tali informazioni, la normativa stabilisce poi un elenco dettagliato di **contenuti minimi** che dovranno essere presidiati attraverso gli accordi.

In particolare, l'articolo 28, comma terzo, del GDPR dispone che l'accordo vincolante per il responsabile del trattamento debba prevedere in particolare:

- **L'obbligo di trattare i dati solo in conformità alle istruzioni** – che dovranno essere adeguatamente documentate – **ricevute dal titolare**, anche in ipotesi di trasferimento dei dati al di fuori dell'Unione Europea;
- L'obbligo di garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da **obblighi di riservatezza,** contrattualmente assunti o stabiliti per legge;
- L'obbligo di adottare le misure richieste ai sensi dell'articolo 32 del Regolamento medesimo, vale a dire le **misure tecniche ed organizzative a protezione dei dati ritenuti idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento**;
- Che in ipotesi di ricorso al **subappalto**, il responsabile si renda adempiente a tutte le condizioni di cui all'articolo 28, comma quarto del GDPR (v. domanda 8);
- L'obbligo di **assistere il titolare**, mediante misure tecniche ed organizzative adeguate e, nella misura in cui ciò sia possibile, **nel dar seguito alle eventuali richieste provenienti dagli interessati** (accesso, rettifica, cancellazione, portabilità, opposizione);
- Tenendo conto della natura del trattamento e delle informazioni a sua disposizione, l'obbligo di **assistere il titolare**:

    - Nell'assicurare protezione ai dati attraverso **misure tecniche ed organizzative adeguate**, ai sensi dell'articolo 32 del Regolamento;
    - Nel **notificare all'Autorità eventuali** *data breaches* **occorsi,** ai sensi dell'articolo 33 del Regolamento;

- Nel **comunicare agli interessati gli eventuali data breaches occorsi**, nei casi previsti dall'articolo 34 del Regolamento;
- Nell'**effettuare la valutazione di impatto** richiesta dall'articolo 35 del Regolamento;
- Nel **consultare l'Autorità**, qualora la valutazione di impatto effettuata indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

- L'obbligo **di cancellazione o restituzione dei dati**, su scelta del titolare, al momento della cessazione del rapporto, salvo che la legge non imponga specifici obblighi di conservazione;
- L'obbligo di **mettere a disposizione del titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi** di cui al presente elenco;
- L'obbligo di **consentire al titolare di effettuare attività di audit**, direttamente o per il tramite di terze parti all'uopo incaricate.

Per saperne di più:

- su cosa prevede la nuova normativa con riferimento al subappalto, vai alla domanda 8;
- sulle conseguenze sanzionatorie previste in caso di mancato rispetto dell'articolo 28 del GDPR, vai alla domanda 18.

Per tornare all'indice, clicca qui.

8. Cosa prevede la nuova normativa con specifico riferimento al ricorso al subappalto da parte di un responsabile del trattamento?

A norma dell'articolo 28, comma secondo, del GDPR, **è fatto divieto al responsabile del trattamento di ricorrere, a propria volta, ad un altro responsabile senza previa autorizzazione scritta da parte del titolare** del trattamento.

Ciò vuol dire che, in ipotesi di subappalto, i contratti e gli accordi vincolanti tra *data controller* e *data processor* dovranno necessariamente normare la materia, prevedendo espressamente il consenso del primo al ricorso a terze parti per lo svolgimento delle attività di trattamento.

La **preventiva autorizzazione scritta da parte del titolare** potrà essere **generale** (in tal caso, il contratto o l'atto di nomina del responsabile sancirà genericamente la possibilità del *data processor* di ricorrere ad ulteriori responsabili per l'esecuzione di tutte o di parte delle attività di trattamento oggetto di accordo alle condizioni e nei limiti di cui alla normativa), ovvero **specifica** (in tal caso, il contratto o l'atto di nomina dovrà riportare l'elenco specifico e dettagliato dei subresponsabili autorizzati ad intervenire nelle attività di trattamento).

Il Regolamento prevede anche che, in caso di autorizzazione scritta generale (ma si tratta di una cautela che è consigliabile adottare contrattualmente anche in relazione alle ipotesi di autorizzazioni specifiche), il responsabile del trattamento sia tenuto ad **informare il titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento**, in modo da permettere al titolare che dissenta rispetto alle suddette modifiche di opporvisi.

È, inoltre, indispensabile, che i medesimi obblighi di formalizzazione imposti nei rapporti tra titolare e responsabile trovino applicazione e vengano ribaltati anche nei rapporti sottostanti tra quest'ultimo ed il subresponsabile.

Infatti, a norma dell'articolo 28, comma quarto del GDPR, occorre che il **responsabile imponga al proprio subresponsabile, mediante un contratto o un altro atto scritto, gli stessi obblighi di cui all'articolo 28.3 del GDPR contenuti nell'accordo tra il primo ed il titolare del trattamento**, in particolare sotto il profilo delle misure di sicurezza adeguate al trattamento.

Resta inteso che l'**originario** *data processor* **conserva l'intera responsabilità nei confronti del data controller**, rispondendo direttamente e personalmente nei confronti di quest'ultimo in relazione ad eventuali inadempimenti o violazioni della propria catena di subfornitura.

Per saperne di più:

- sulla nomina a data processor dei subappaltatori, vai alla domanda 9;
- sulle conseguenze sanzionatorie previste in caso di mancato rispetto dell'articolo 28 del GDPR, vai alla domanda 18.

Per tornare all'indice, clicca qui.

9. È necessario che il titolare nomini quali responsabili del trattamento i subappaltatori del proprio responsabile? E come avviene la nomina?

Se nell'impostazione disegnata dal Codice Privacy la nomina a responsabile del trattamento ai sensi dell'articolo 29 è un atto facoltativo (sebbene comunque fortemente caldeggiato anche dall'Autorità Garante), nella nuova impostazione disegnata dal GDPR la nomina del responsabile (o la stipula di uno specifico contratto con esso) diviene un **adempimento vincolante**, dovuto ogni qual volta abbia luogo un'attività di trattamento da parte di un terzo.

Per cui, sì: **ogni subappaltatore che interviene nelle operazioni di trattamento dovrà formalmente assumere la qualifica di data processor**. Senonché, una delle novità introdotte dal GDPR è costituita dalla possibilità, accordata al responsabile del trattamento, previa autorizzazione da parte del titolare, di procedere alle **cc.dd. nomine a cascata**, vale a dire, la possibilità che il data processor nomini a propria volta i responsabili del trattamento. In tal modo, una facoltà da sempre accordata al solo titolare del trattamento (la nomina di un altro soggetto in qualità di responsabile concretamente preposto alle attività di trattamento) diviene oggetto di possibile delega, in linea con la nuova ripartizione degli obblighi prevista dal Regolamento e con lo spostamento del baricentro delle responsabilità un po' più verso il **data processor** e un po' meno verso il *data controller*. D'altra parte, l'originario responsabile continua a rispondere direttamente nei confronti del titolare e viene così assoggettato tanto ad un obbligo di diligenza "*in eligendo*", quanto ad un obbligo di diligenza "*in vigilando*" sui propri subappaltatori/subresponsabili che fa da contrappeso al minor rigore con cui è possibile esternalizzare in tutto o in parte le attività di trattamento rispetto al passato. Se, dunque, oggigiorno, sotto la vigenza del Codice Privacy, il titolare è tenuto a **nominare direttamente**, quali responsabili del trattamento, tutti i subappaltatori ai quali il proprio fornitore demandi specifiche attività di trattamento, ovvero a conferire a quest'ultimo un **mandato con rappresentanza ai sensi dell'articolo 1704 c.c.**, affinché questi nomini i propri subappaltatori responsabili del trattamento in nome e per conto del titolare, un domani, con l'applicabilità del GDPR, i rapporti e le procedure di nomina verranno enormemente semplificate. Ciò costituirà **un'evidente facilitazione in relazione ai servizi caratterizzati da lunghe catene di subfornitura e da una certa complessità delle relazioni contrattuali multilivello sottostanti al trattamento dei dati personali** (si pensi, ad esempio, ai servizi di cloud computing).

Per tornare all'indice, clicca qui.

10. Quali sono le responsabilità del *data controller* in ordine al ricorso ad un *data processor*?

Per garantire che siano rispettate tutte le prescrizioni di legge relative al trattamento dei dati personali che il responsabile deve eseguire per conto del titolare del trattamento, in caso di esternalizzazione di servizi, il titolare dovrebbe ricorrere unicamente a responsabili che presentino garanzie sufficienti, in particolare in termini di **conoscenza specialistica, affidabilità e risorse**, così garantendo la possibilità di mettere in atto misure di sicurezza che soddisfino le esigenze di protezione espresse dalla nuova normativa. Il ricorso, da parte del responsabile a **codici di condotta o meccanismi di certificazione,** può certamente costituire un indice di garanzia ed affidabilità e, quindi, un elemento attraverso il quale il titolare può dimostrare il rispetto degli obblighi relativi alla diligenza "*in eligendo*" dei propri data processor.

Oltre all'obbligo di stipulare con i propri responsabili accordi scritti che presentino i contenuti minimi di cui si è detto, incombe sul titolare il dovere di **fornire loro dettagliate istruzioni scritte** in ordine alle modalità del trattamento. Stabilisce, infatti, a questo proposito, l'articolo 29 del GDPR che "*il responsabile del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

Tale obbligo è particolarmente importante, poiché quanto più puntuali e dettagliate saranno le istruzioni trasmesse al responsabile, quanto più agevole e pacifica sarà la ripartizione della responsabilità civile e dell'onere della prova in ipotesi di violazioni normative, inadempimenti contrattuali e danni cagionati agli interessati. Resta inteso che l'eventuale esternalizzazione totale o parziale del trattamento non implica alcuna deresponsabilizzazione per il titolare, il quale risponderà direttamente, per ciò che ad egli compete, in ordine alla conformità normativa delle proprie attività di trattamento dati.

Per saperne di più:

- sulla responsabilità risarcitoria del titolare del trattamento, vai alla domanda 14;
- sulla ripartizione della responsabilità per i danni conseguenti ad un trattamento illecito nei rapporti interni titolare – responsabile, vai alla domanda 17.

Per tornare all'indice, clicca qui.

11. Quali sono le responsabilità del *data processor* alla luce del GDPR?

L'aggravamento della posizione del *data processor* e la sua **maggiore responsabilizzazione** costituiscono una novità assoluta introdotta dalla nuova normativa.

Nella vigenza della normativa attuale, infatti, le conseguenze sanzionatorie derivanti da un illecito trattamento dei dati personali sono fondamentalmente poste a carico del solo titolare, il quale potrà agire in rivalsa nei confronti del responsabile per le eventuali violazioni poste in essere rispetto alle istruzioni ricevute.

Questa impostazione cambia radicalmente con il GDPR.

Infatti, a norma dell'articolo 82 del Regolamento, e salvo che non dimostri che l'evento dannoso non possa essergli in alcun modo imputato, **il responsabile risponde, in solido con il titolare e per l'intero ammontare, del danno cagionato** da un trattamento non conforme a normativa se:

- **ha agito in modo difforme o contrario rispetto alle istruzioni** legittime ricevute dal titolare; ovvero
- **non ha adempiuto agli obblighi che il GDPR pone direttamente in capo ai responsabili**.

Oltre all'esonero di responsabilità che la norma accorda nell'ipotesi in cui il responsabile riesca a dimostrare che l'evento dannoso non gli è in alcun modo imputabile e che, pertanto, nessun rimprovero, nemmeno a titolo di colpa, possa essergli mosso (per esempio, in caso di violazione intenzionale dei dati, nonostante l'adozione di tutte le misure di sicurezza adeguate rispetto al trattamento ed il puntuale rispetto di tutte le istruzioni ricevute), è importante tenere a mente anche quanto disposto dall'articolo 28.3, ultimo periodo, del GDPR, a norma del quale "*il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati*".

Pertanto, il dovere del *data processor* di conformarsi alle istruzioni ricevute viene meno in ipotesi di istruzione illegittima o *contra legem* proveniente dal titolare, a condizione, tuttavia, che tale illegittimità venga prontamente comunicata al titolare medesimo, anche allo scopo di porre quest'ultimo in condizione di porre in essere gli opportuni correttivi, rettificando così anche eventuali accordi con il *data processor.*

Per saperne di più:

- su quali sono gli obblighi che il GDPR pone direttamente in capo ai data processor, vai alla domanda 12;
- sulle conseguenze sanzionatorie previste in caso di mancato rispetto dell'articolo 28 del GDPR, vai alla domanda 18.

Per tornare all'indice, clicca qui.

12. Quali obblighi il GDPR pone direttamente in capo al *data processor*?

La nuova normativa, come già detto, prevede, in capo ai responsabili del trattamento specifici adempimenti, la cui violazione è suscettibile di dar luogo a responsabilità diretta di questi ultimi (il che vuol dire, esposizione risarcitoria nei confronti degli interessati in relazione ai danni cagionati e eventuali conseguenze sanzionatorie derivanti dagli inadempimenti alla normativa).

Tra le prescrizioni specificamente indirizzate ai responsabili, si segnalano in particolare:

- L'obbligo di **designare un proprio rappresentante all'interno dell'Unione Europea**, qualora il responsabile, pur essendo stabilito al di fuori dell'Unione, tratti dati di interessati che si trovino nell'Unione e le sue attività di trattamento siano connesse all'offerta di beni o servizi (anche a titolo gratuito) a tali interessati nell'Unione ovvero comportino il monitoraggio del comportamento di tali interessati, nella misura in cui tale comportamento ha luogo nell'Unione (cfr. articolo 27 GDPR);
- Gli obblighi relativi al **subappalto** (cfr. articolo 28 GDPR);
- Il **divieto di trattare i dati** cui il responsabile ha accesso **in mancanza di istruzioni del titolare** in tal senso e salvo che ciò non sia richiesto dal diritto dell'Unione o degli Stati Membri (cfr. articolo 29 GDPR);
- L'obbligo di **istituire ed aggiornare il registro delle attività di trattamento** effettate per conto del titolare (cfr. articolo 30 GDPR);
- Gli **obblighi di cooperazione con le Autorità di controllo**, che si concretizzano nel dovere di dar seguito alle richieste da esse provenienti, tanto nell'esercizio dei loro poteri di indagine, quanto nell'esercizio dei loro poteri correttivi (cfr. articoli 30, 31 e 58 GDPR);
- Gli **obblighi relativi alla sicurezza** e, in particolare, l'obbligo di adottare misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio (che comprendono, tra le altre, se del caso: la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecnico-organizzative per garantire la sicurezza del trattamento)

(cfr. articolo 32 GDPR);

- L'**obbligo di istruire gli incaricati** che agiscono sotto la sua autorità ed abbiano accesso ai dati personali (cfr. articolo 32 GDPR);
- L'**obbligo di informare senza giustificato ritardo il titolare di ogni evento di violazione della sicurezza** (c.d. data breach) di cui sia venuto a conoscenza (cfr. articolo 33 GDPR);
- L'**obbligo di nominare un DPO**, laddove richiesto per legge (cfr. articolo 37 GDPR);
- L'**obbligo di fornire le garanzie adeguate** previste dal Regolamento in ogni ipotesi in cui il responsabile intenda **trasferire dati personali al di fuori dell'Unione** (cfr. articoli 30 e 46 GDPR).

Per saperne di più sulla responsabilità solidale tra titolare e responsabile, vai alla domanda 11.

Per tornare all'indice, clicca qui.

13. Nel contesto della nuova normativa, cosa ne è della figura degli incaricati del trattamento? E di quella del responsabile interno del trattamento? Insomma, cosa cambia nell'organigramma privacy aziendale rispetto al passato?

Pur non prevedendo espressamente la figura dell'incaricato del trattamento di cui all'articolo 30 del Codice Privacy, il GDPR non ne esclude la presenza. Al contrario, all'articolo 4 n. 10 fa espressamente riferimento a "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*"; mentre all'articolo 32 fa obbligo al titolare e al responsabile del trattamento di istruire "*chiunque agisca sotto la loro autorità e abbia accesso ai dati personali*". Inoltre, secondo quanto precisato dal Garante Privacy nella "*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*", **le disposizioni del Codice Privacy in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del Regolamento**, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili, che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del Regolamento. Di conseguenza, **è consigliabile mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento**, così come delineatesi negli anni anche attraverso gli interventi del Garante, in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al Regolamento.

Discorso diverso vale, invece, per la figura del responsabile interno del trattamento. Da un lato, infatti, il nuovo impianto normativo lascia **presupporre la terzietà del** *data processor* rispetto all'azienda che agisca in qualità di titolare del trattamento. Ciò è evidente, ad esempio, nell'elenco degli elementi contrattuali obbligatori di cui all'articolo 28.3, alcuni dei quali appaiono applicabili esclusivamente a soggetti esterni all'azienda (come l'impegno alla riservatezza dei propri dipendenti e collaboratori).

Dall'altro lato, il sensibile aggravamento della responsabilità gravante sui data processor, chiamati – in specifiche ipotesi – a rispondere per l'intero ammontare del danno in via solidale con il data controller, farà sì che difficilmente si trovino persone fisiche, all'interno dell'organizzazione aziendale, disposte ad accollarsi una responsabilità così gravosa. Pertanto, è presumibile che, all'indomani della data di piena applicabilità del Regolamento, la figura del responsabile interno del trattamento, sviluppatasi nella prassi italiana (ad esempio, il responsabile HR, IT, Marketing, ecc.) verosimilmente sparirà.

Per tornare all'indice, clicca qui.

14. Quali sono i danni risarcibili ai sensi dell'articolo 82 GDPR?

Sotto il profilo del risarcimento del danno, l'impostazione del nuovo Regolamento conferma quella già vigente con il Codice Privacy, ove il trattamento dei dati personali è civilisticamente qualificabile quale attività pericolosa, ai sensi dell'articolo 2050 c.c., con il conseguente obbligo in capo a colui che tale attività effettui di risarcire all'interessato tanto i **danni patrimoniali**, quanto i **danni non patrimoniali** cagionati in conseguenza del trattamento.

A conferma di ciò, anche l'articolo 81, comma primo, stabilisce che "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

Con riferimento alla responsabilità per danni derivanti da attività pericolose, l'articolo 2050 c.c. stabilisce che chiunque cagiona un danno è tenuto al suo risarcimento "*se non prova di avere adottato tutte le misure idonee*" ad evitarlo.

In relazione all'onere della prova, pertanto, mentre l'interessato che si pretenda leso nei propri diritti avrà il solo onere di allegare e provare in giudizio il nesso di causalità tra il trattamento dei dati ad egli riferiti ed il danno subito, a carico del titolare o del responsabile del trattamento vige una presunzione di responsabilità particolarmente gravosa, che può essere superata solo dimostrando di aver adottato tutte le misure tecniche ed organizzative che ex ante potevano ritenersi idonee a prevenire il danno causato.

Per saperne di più:

- sulle ipotesi di esonero da responsabilità verso gli interessati, vai alla domanda 15;
- sulla possibilità di limitare contrattualmente l'esposizione risarcitoria nei confronti degli interessati, vai alla domanda 16;
- sulla ripartizione della responsabilità nei rapporti interni tra titolare e responsabile, vai alla domanda 17.

Per tornare all'indice, clicca qui.

15. Sono previste per legge ipotesi di esonero da responsabilità risarcitoria verso gli interessati?

A norma dell'articolo 82, comma terzo, il titolare o il responsabile del trattamento sono **esonerati** da responsabilità verso gli interessati se dimostrano che **l'evento dannoso non gli è in alcun modo imputabile**.

Il che vuol dire, per entrambi, riuscire a dimostrare di aver adottato tutte le misure di sicurezza adeguate rispetto al rischio insito nel trattamento e volte a prevenire il danno causato e, per il responsabile in particolare, provare di avere correttamente adempiuto ai propri obblighi e alle istruzioni legittime ricevute dal titolare.

Dal momento, inoltre, che la norma che sancisce la responsabilità diretta del *data processor* fa espresso riferimento alle "istruzioni legittime" ricevute dal titolare, è da ritenersi che un'ulteriore ipotesi di esonero da responsabilità possa essere configurata in caso di istruzione illegittima o *contra legem*, a condizione che il *data processor* abbia prontamente informato il data controller del fatto che, a suo parere, un'istruzione ricevuta si ponga in violazione della legge nazionale o dell'Unione relativa alla protezione dei dati (così come stabilito dall'articolo 28 del Regolamento), in tal mondo consentendo al controller di porre in essere gli opportuni correttivi.

Per saperne di più:

- su quali sono i danni risarcibili in conseguenza di un trattamento illecito, vai alla domanda 14;
- sulla possibilità di limitare contrattualmente l'esposizione risarcitoria nei confronti degli interessati, vai alla domanda 16.

Per tornare all'indice, clicca qui.

16. È possibile limitare contrattualmente la responsabilità risarcitoria per danni conseguenti a trattamento illecito di dati personali?

Dipende.

Il Regolamento stabilisce che *"gli interessati dovrebbero ottenere pieno ed effettivo risarcimento del danno subito"*. A rafforzamento di tale principio, l'articolo 82 fa obbligo al titolare ed al responsabile di rispondere nei confronti dell'interessato *"per l'intero ammontare del danno, al fine di garantire un risarcimento effettivo"*.

Dalla formulazione letterale della norma e dal principio di piena e massima tutela degli interessati che ne è alla base, sembrerebbe, dunque, doversi intendere che **la responsabilità verso gli interessati per danni derivanti da trattamenti illeciti non possa in alcun modo essere limitata, costituendo il diritto alla protezione dei propri dati personali un diritto fondamentale ed incomprimibile dell'individuo**.

Il che pone un problema di legittimità e tenuta giuridica delle clausole di limitazione di responsabilità eventualmente contenute negli accordi che vincolino contrattualmente il titolare ai propri interessati (quando, ad esempio, il trattamento dei dati personali si iscrive nel contesto dell'erogazione di un servizio contrattualmente disciplinato)

In mancanza di un rapporto contrattuale che vincoli titolare ed interessati, invece, l'eventuale responsabilità derivante da illecito trattamento di dati personali avrà **natura extracontrattuale**, con conseguente applicazione dei relativi principi e termini prescrizionali civilistici, nonché piena esposizione risarcitoria del titolare nei confronti dell'interessato, stante quanto disposto dall'articolo 82, comma quarto, GDPR, laddove si stabilisce che, al fine di garantire il risarcimento effettivo dell'interessato, titolare e responsabile rispondono in solido *"per l'intero ammontare del danno"*.

Alla luce della disposizione da ultimo citata, una piena responsabilità è, invece, sempre prevista in capo al responsabile del trattamento, che di regola non è direttamente vincolato agli interessati in virtù di rapporti contrattuali. **La sua responsabilità potrà, se del caso, essere limitata nei rapporti interni titolare-responsabile**, in virtù di apposite **clausole di limitazione di responsabilità**, ma rimarrà comunque piena verso l'esterno, in relazione ad eventuali danni protestati dagli interessati.

Resta inteso che qualsiasi clausola di limitazione di responsabilità contenuta negli accordi interni tra titolare e responsabile dovranno in ogni caso soggiacere al principio generale di cui all'articolo 1229,

primo comma, c.c., a norma del quale *"è nullo qualsiasi patto che esclude o limita preventivamente la responsabilità del debitore per dolo o colpa grave"*.

Per saperne di più:

- su quali sono i danni risarcibili in conseguenza di un trattamento illecito, vai alla domanda 14;
- sulla ripartizione della responsabilità nei rapporti interni tra titolare e responsabile, vai alla domanda 17.

Per tornare all'indice, clicca qui.

17. Come si ripartisce la responsabilità per i danni conseguenti ad un trattamento illecito nei rapporti interni titolare-responsabile?

Se la regola della responsabilità solidale per l'intero ammontare del danno costituisce il criterio che guida l'esposizione risarcitoria di titolare e responsabile nei confronti degli interessati, **nei rapporti interni la regola è quella della responsabilità pro quota**.
Stabilisce, infatti, l'articolo 82, comma quinto, GDPR che "*qualora un titolare del trattamento o un responsabile del trattamento abbia pagato (...) l'intero risarcimento del danno, tale titolare o responsabile del trattamento ha diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte di risarcimento corrispondente alla loro parte di responsabilità per il danno (...)*".
Ne deriva, quindi, che il titolare o responsabile che abbia risarcito l'interessato per l'intero ammontare del danno potrà sempre **agire in regresso** nei confronti del titolare o del responsabile coinvolti nello stesso trattamento, qualora ritenga che vi sia stata una responsabilità esclusiva o concorrente di questi ultimi nella produzione del danno.

Per saperne di più sulla responsabilità solidale tra titolare e responsabile, vai alla domanda 11.

Per tornare all'indice, clicca qui.

18. Quali sono le conseguenze sanzionatorie in caso di mancato rispetto delle prescrizioni relative ai contenuti degli accordi contrattuali tra *data controller* e *data processor*?

Il Regolamento prevede, ai sensi dell'articolo 83, comma quarto, la possibilità per le Autorità nazionali di irrogare sanzioni amministrative pecuniarie fino a € 10.000.000 o, in caso di "*undertaking*" al 2% del fatturato totale mondiale annuo dell'esercizio precedente, a seconda del quale risulti la sanzione più elevata, al ricorrere di una serie di violazioni, tra cui la violazione delle obbligazioni di *controller* e processor, inclusi le prescrizioni contrattuali obbligatorie, gli obblighi di sicurezza e quelli in materia di data *breach notification*.

Sanzioni più pesanti sono previste in relazione a violazioni più gravi (come per esempio, la violazione dei principi di base del trattamento, ivi incluso il consenso, la violazione dei diritti degli interessati o l'illegittimo trasferimento dei dati all'estero).

Occorre comunque ricordare che la nuova normativa prevede solo i massimali delle sanzioni amministrative pecuniarie applicabili, che necessiteranno poi di essere concretamente gradate dai legislatori nazionali.

Per quanto riguarda le sanzioni penali, invece, a norma dell'articolo 83 GDPR e stante la sovranità degli Stati Membri in materia penale, esse saranno concretamente determinate dai parlamenti nazionali, nel rispetto dei principii di effettività, proporzionalità e dissuasività sanciti dalla nuova normativa.

Per tornare all'indice, clicca qui.

19. Gli interessati che si ritengano lesi da un illecito trattamento come possono ottenere ristoro del danno patito?

A norma dell'articolo 79, comma secondo, GDPR ogni interessato ha diritto a proporre un ricorso giurisdizionale effettivo nei confronti del data controller o del data processor, qualora ritenga che i diritti di cui gode siano stati violati a seguito di un trattamento illegittimo. Le azioni nei confronti del data controller o del data processor sono promosse dinanzi alle autorità giurisdizionali dello Stato Membro in cui il controller o il processor ha uno stabilimento. In alternativa, le azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato in cui gli interessati risiedono abitualmente.

Gli interessati potranno inoltre:

- Ai sensi dell'articolo 77 GDPR, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, proporre reclamo a un'Autorità di controllo nello Stato Membro in cui risiedono abitualmente, ovvero lavorano o, in alternativa, nel luogo ove si è verificata la violazione;
- Ai sensi dell'articolo 78, comma secondo, GDPR, fatto salvo ogni altro ricorso amministrativo o extragiudiziale, proporre un ricorso giurisdizionale effettivo nei confronti dell'Autorità di controllo.

Per saperne di più su quali sono i danni risarcibili in conseguenza di un trattamento illecito, vai alla domanda 14.

Per tornare all'indice, clicca qui.

20. Esistono dei set di clausole contrattuali standard da adottare per disciplinare i rapporti tra titolare e responsabile del trattamento?

Il GDPR prevede espressamente che i rapporti tra titolare e responsabile e quelli tra responsabile e subresponsabili possano essere disciplinati tanto sulla base di un contratto individuale, quanto sulla base di clausole contrattuali standard adottate direttamente dalla Commissione ovvero da un'Autorità di controllo in conformità al meccanismo di coerenza di cui agli articoli 63 e ss. del GDPR (cfr. considerando n. 81 e gli articoli 28.7 e 28.8). Al momento, non è ancora stato adottato nessun set di clausole in conformità a tali previsioni, ma non è da escludersi che in futuro la Commissione o le Autorità nazionali intervengano in materia, semplificando la contrattualizzazione degli obblighi di legge tra gli attori del rapporto privacy, in maniera del tutto analoga a quanto già avvenuto in passato con l'approvazione delle Standard Constractual Clauses che, allegate ai contratti che prevedano un trasferimento extra UE di dati personali, costituiscono garanzia di adeguata protezione dei dati medesimi e rendono legittimo il trasferimento. Tali clausole contrattuali potranno costituire, inoltre, parte di un codice di condotta o di uno schema di certificazione, l'adesione ai quali costituirà, per i responsabili del trattamento, un indice presuntivo di rispetto e conformità in relazione alle prescrizioni del nuovo Regolamento.

Occorre, peraltro, ricordare che la legge del 20 novembre 2017, n. 167, "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea*", sono state apportate modifiche all'attuale articolo 28 del Codice Privacy, probabilmente con la finalità di consentire al Garante per la protezione dei dati personali di adottare fin da ora degli schemi tipo.

All'articolo 29, così come da ultimo modificato, è stato, infatti, aggiunto un comma 4-bis ove si dispone che "*fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti sono adottati in conformità a schemi tipo predisposti dal Garante*".

È quindi presumibile che, forse anche a stretto giro, l'Autorità di controllo italiana intervenga in materia.

Per tornare all'indice, clicca qui.

Riepilogando...

- Ogni qual volta il titolare ricorra ad un responsabile per effettuare determinate attività di trattamento, è tenuto a formalizzare per iscritto, attraverso un contratto o un altro atto giuridico vincolante, gli obblighi cui il responsabile deve soggiacere.
- La norma di riferimento che dettaglia i contenuti degli accordi vincolanti tra il *data controller* ed il *data processor* e a alla quale occorre quindi guardare in sede di contrattualizzazione di servizi esternalizzati è l'articolo 28 del GDPR.
- Il GDPR impone al titolare uno specifico obbligo di diligenza in *eligendo* dei propri responsabili, i quali dovranno necessariamente presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative idonee, in modo tale che il trattamento soddisfi le prescrizioni di legge in materia e garantisca l'esercizio o la tutela effettiva dei diritti degli interessati. L'onere di verificare la capacità, l'affidabilità e l'adeguatezza del responsabile incombe sul titolare, fin dal momento delle trattative in ordine alla contrattualizzazione del servizio.
- L'adesione, da parte del responsabile ad un codice di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare la sussistenza di garanzie sufficienti in capo al responsabile e ad eventuali subresponsabili.
- La nuova normativa aggrava la posizione del responsabile del trattamento, stabilendo che egli risponda direttamente, sia sotto il profilo sanzionatorio, sia sotto il profilo degli obblighi risarcitori nei confronti degli interessati, in due ipotesi specifiche: i) mancato adempimento degli obblighi che il Regolamento pone direttamente in capo ai responsabili; ii) condotta difforme o contraria rispetto alle istruzioni legittime ricevute dal titolare.
- Titolare e responsabile sono esonerati da responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile.
- Tanto il titolare, quanto il responsabile, coinvolti nel trattamento rispondono in solido e per l'intero ammontare del danno nei confronti degli interessati che siano stati lesi da un trattamento illegittimo.

Check list dei contenuti contrattuali che devono risultare dagli accordi Titolare e Responsabile del trattamento

- La materia disciplinata e durata del trattamento
- La natura e finalità del trattamento
- Il tipo di dati personali trattati
- Le categorie di interessati
- Gli obblighi e i diritti del titolare del trattamento
- L'obbligo del responsabile di trattare i dati solo su istruzione documentata del Titolare
- L'obbligo del responsabile di garantire l'impegno alla riservatezza da parte delle persone fisiche incaricate delle operazioni di trattamento
- L'adozione da parte del Responsabile delle misure tecniche ed organizzative richieste dall'articolo 32 del GDPR
- In caso di subesternalizzazione delle attività di trattamento, il rispetto delle condizioni previste dal GDPR per il ricorso a subresponsabili
- L'obbligo del Responsabile di assistere il Titolare nel dar seguito alle richieste provenienti dagli interessati
- L'obbligo del Responsabile di assistere il Titolare in relazione agli adempimenti posti a suo carico agli articoli da 32 a 36 del GDPR
- La restituzione e/o cancellazione dei dati alla cessazione dei servizi relativi alle attività di trattamento
- Il diritto di verifica del Titolare ed il corrispondente obbligo del Responsabile di collaborare per consentire tali verifiche

P4I - Partners4Innovation

P4I - Partners4Innovation è la società del Gruppo Digital360 che offre servizi di Advisory e Coaching a supporto dell'Innovazione Digitale e Imprenditoriale ad imprese e Pubbliche Amministrazioni.
L'approccio all'Advisory di Partners4Innovation è reso unico dal ricorso a metodologie, dati e asset di conoscenza distintivi e si caratterizza per una forte attenzione all'empowerment dei decisori interni all'organizzazione cliente, ai quali vengono fornite informazioni, metodologie e strumenti per guidare l'innovazione.

P4I, inoltre, attraverso il suo network di relazioni, offre un confronto con la più grande community d'innovazione digitale e imprenditoriale in Italia trasversalmente a tutte le sue practice – che coprono tutte le aree chiave della Digital Transformation, dallo Smart Working fino all'Industria 4.0.

In particolare, nell'ambito contrattualistico, P4i supporta le aziende e le pubbliche amministrazioni in tutte le fasi del ciclo di vita del contratto, dalla selezione del fornitore e della soluzione tecnologica alla stesura dei capitolati di gara o delle RFP, dalla stesura del contratto e degli allegati tecnici alla loro negoziazione, dalla gestione del contratto una volta stipulato al supporto nelle controversie in caso di contrasti.

annamaria.italiano@p4i.it
gabriele.faggioli@p4i.it

NETWORK DIGITAL 360

VIA COPERNICO, 38 - 20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ

WWW.DIGITAL360.IT © ICT & STRATEGY

DIGITAL 360 | Group