Legnano, 24/05/2018
Comunicazioni
Int. ML/GS/GC/af
rif.: Reg. GDPR UE 2016/679 Privacy

Alle imprese assistite
loro sedi

Oggetto: **GDPR (Regolamento UE 2016/679 *"relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati"*) - aggiornamento**

Facendo seguito a quanto anticipato sul periodico *online Newslinet.it* (collegato a questa struttura) ed alla precedenti circolari della scrivente (in *SIT Online* su *www.newslinet.it*). si partecipa quanto segue.

Come noto, domani, 25/05/2018, sarà direttamente applicabile in tutti gli Stati membri dell'Unione Europea il nuovo Regolamento UE 2016/679 *"relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati"*, cd. GDPR[1], il quale abrogherà la Direttiva 95/46/CE oramai superata.

In conseguenza degli adempimenti previsti, i soggetti interpellati a riguardo della responsabilità sul trattamento dei dati e delle misure conseguenti adottate dovranno poter fornire adeguata e motivata risposta con particolare riferimento ai nominativi dei soggetti coinvolti nella gestione. In particolare, un problema si pone a riguardo dell'indicazione di tutti i soggetti che trattano i dati ed i cui nominativi devono essere resi noti all'interessato su richiesta. Tale elenco, evidentemente, non può però essere considerato stabile, in quanto suscettibile di ingressi ed uscite tra personale dipendente, collaboratori e liberi professionisti.

Per ovviare alla necessità di inviare costanti e dispendiosi aggiornamenti dell'organigramma, una soluzione potrebbe consistere nel rinvio ad una pagina specifica del proprio sito internet costantemente aggiornata[2].

Al fine di agevolare l'ottemperanza a tali richieste, questa struttura nell'ambito del SIT GDPR istituito per l'importante adempimento, ha predisposto un modello preimpostato[3] da impiegarsi previa, ovviamente, specifica personalizzazione. Gli interessati[4] potranno richiedere ai *partner* di riferimento sotto indicati il suesposto modello.

Ricordiamo che il SIT GDPR si declina in:

1) ***Basic*: fornitura modulistica;**
2) ***Premium*: assistenza personalizzata alla compilazione.**

Nel merito della vicenda, ricordiamo che il GDPR mira ad assicurare un'applicazione omogenea della normativa sulla *privacy* vigente in tutti gli Stati membri.

Il Regolamento muta e innova l'intera disciplina della protezione dei dati personali, prevedendo una lunga serie di diritti e tutele in capo all'interessato/soggetto passivo. Per contro, amplia notevolmente il novero degli obblighi per i titolari e i responsabili del trattamento, delineando un quadro stringente e oneroso.

[1] *General Data Protection Regulation;*
[2] es. *https://www.consultmedia.it/collaboratori/;*
[3] anche quanto a misure di sicurezza tipiche;
[4] che hanno aderito al SIT GDPR;

In particolare, **è accentuata la responsabilità del titolare e del responsabile attraverso il principio di *accountability*[5]**, permeato di obblighi relativi all'**adozione di adeguate misure di sicurezza - tra cui la pseudonimizzazione[6] e la cifratura dei dati - non solo durante o dopo il trattamento, bensì anche in una fase pregressa.**

Tali misure devono essere poi costantemente monitorate e proporzionate ai rischi, connesse ad un'analisi e ad una **capillare valutazione del rischio *ex ante*** derivante dalle operazioni di trattamento.

Oltre a garantire l'efficacia delle misure adottate, il *titolare* del trattamento deve dimostrare, su richiesta, di aver intrapreso le predette azioni, ovvero l'adozione delle succitate misure di sicurezza e la valutazione preventiva del rischio.

Strettamente collegate al principio di ***accountability*** e, quindi, alla valutazione delle misure di sicurezza per garantire la tutela dei diritti dell'interessato e dimostrare la conformità del trattamento alla normativa, sono, tra le altre, le seguenti nozioni:

1. ***privacy by design e privacy by default***. Tra gli interventi *ex ante* che **impongono** al titolare una prima analisi cautelare dell'impatto del trattamento, l'art. 25 descrive le misure volte a garantire la protezione dei dati personali sin dall'inizio del trattamento - *privacy by design* - e per impostazione predefinita - *privacy by default* -. Nello specifico, il titolare è chiamato a valutare, dal momento della progettazione del trattamento, i possibili rischi per la riservatezza dei dati e l'autodeterminazione informativa del soggetto. Correlativamente, deve mettere in atto le misure di sicurezza adeguate[7]. Inoltre, come stabilisce il comma 2, "*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure*

[5] Si tratta del c.d. principio di responsabilizzazione;
[6] l'art. 4, comma 1 del Regolamento fornisce una serie di definizioni innovative; tra queste:
n. 5) Pseudonimizzazione: *"Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"*. È dunque un trattamento volto a mascherare l'identità, ad esempio rendendo impossibile la ri-identificazione tramite strumenti quali la crittografia unidirezionale, in grado di creare dati anonimi.
n. 4) Profilazione: *"qualsiasi forma di trattamento automatizzato di dati personali, consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione, gli spostamenti di detta persona fisica"*. Per meglio definire il trattamento automatizzato, il Regolamento rinvia all'art. 1, par. 1, lett. b) della Direttiva (UE) 2015/1535 che identifica tale trattamento, da intendersi come *"qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per:*
i) «a distanza»: un servizio fornito senza la presenza simultanea delle parti;
ii) «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici;
iii) «a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale."
n. 12) Violazione dei dati: *"Violazione di sicurezza che comporta 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"*. È definizione ampia in quanto ricomprende qualsiasi evento che metta a rischio, anche in maniera accidentale i dati personali trattati. È di rilievo questa definizione legata al termine sicurezza, in quanto si collega alla nozione di *data breach*;
[7] tra cui la pseudonimizzazione e la minimizzazione del trattamento dei dati;

garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica";

2. ***data protection officer (DPO)***. *Ex* art. 37 ss., inserendosi nell'ambito del presidio del rischio, questa nuova figura professionale è caratterizzata da ampia autonomia, riferisce direttamente al vertice gerarchico del titolare o del responsabile del trattamento. Tale soggetto è altresì individuato più specificamente dal Gruppo "Articolo 29" (WP29), che ha adottato il 13/12/2016 le "*Guidelines on Data Protection Officers* (*DPO*)". Si tratta di un soggetto che è incaricato di vigilare sul rispetto della normativa in materia di *privacy* e di fungere da punto di contatto con l'Autorità di controllo;
3. **le nuove procedure che il titolare del trattamento deve rispettare, tra cui la valutazione di impatto sulla protezione dei dati (*DPIA*)[8], la *data breach notification*[9]** e ancora **l'adesione a meccanismi di certificazione della conformità delle misure adottate**[10], per la cui trattazione si rimanda alle pagine successive.

Ogni trattamento deve trovare fondamento in un'idonea base giuridica. I parametri di liceità sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti dal *Codice privacy* di cui al D. lgs. n. 196/2003.

In particolare, si tratta delle seguenti condizioni di liceità:

a) **consenso**[11], il quale deve essere manifestato attraverso una dichiarazione o un atto positivo inequivocabile[12]. Per i dati sensibili e per decisioni basate su trattamenti automatizzati, compresa la profilazione, deve essere esplicito. Il consenso è valido solo se è effettivamente:
   - **libero**: se si presenta, quindi, come manifestazione del diritto all'autodeterminazione informativa, al riparo da qualsiasi pressione e da qualsiasi imposizione di clausole, cui viene condizionata l'accettazione, che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto;
   - **specifico**: dev'essere comprensibile, riferito chiaramente e precisamente al campo d'applicazione e alle conseguenze del trattamento dei dati. Non può essere totale e riferirsi ad un insieme illimitato di attività di trattamento;
   - **informato:** ossia basato sulla valutazione e comprensione dei fatti e sulle conseguenze di una determinata azione. L'interessato deve ricevere in modo chiaro e comprensibile informazioni precise e complete su tutti gli aspetti rilevanti. Questo implica la consapevolezza delle conseguenze del mancato assenso al trattamento in questione.

   Non è necessariamente richiesta la forma scritta ai fini della validità. Il consenso dei minori è valido a partire dai 16 anni.
   L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
   Incombe in capo al titolare del trattamento l'onere di provare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
   N.B. **Il consenso raccolto precedentemente al 25/05/2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di**

[8] *Data Protection Impact Assessment;*
[9] ai sensi dell'art. 33 ss. nel caso in cui sia avvenuta una violazione dei dati personali, il titolare ha l'obbligo di notificarlo all'Autorità Garante e all'interessato;
[10] ai sensi dell'art. 32, comma 3 del Regolamento: *"L'adesione a un codice di condotta approvato di cui all'art. 40 o a un meccanismo di certificazione approvato di cui all'art. 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti*". Sono obblighi di secondo livello, facoltativi, la cui adozione costituisce elemento per dimostrare la conformità del proprio comportamento e del trattamento effettuato rispetto alla normativa;
[11] il consenso viene definito dall'art. 4, comma 1, n. 11 come *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"*.
[12] non è valido il consenso tacito o presunto;

tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il Regolamento, se si vuole continuare a fare ricorso a tale base giuridica. In particolare, occorre verificare che **la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato**[13]. Anche la formula utilizzata per chiedere il consenso deve presentarsi in maniera comprensibile, semplice e chiara;

b) **esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) **adempimento di un obbligo legale** al quale è soggetto il titolare del trattamento;
d) **interesse vitale** dell'interessato o di un terzo[14];
e) **esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) **interesse legittimo prevalente** di un titolare o di un terzo. Il titolare del trattamento deve effettuare il bilanciamento fra il proprio legittimo interesse e i diritti e le libertà fondamentali dell'interessato[15].

I principi applicabili al trattamento dei dati personali[16] sono:

- **liceità, correttezza e trasparenza;**
- **limitazione della finalità**[17];
- **minimizzazione dei dati**[18];
- **esattezza**[19];
- **limitazione della conservazione**[20];
- **integrità e riservatezza**[21];
- **responsabilizzazione, c.d. *accountability***[22].

***

I soggetti coinvolti nel trattamento sono:

1. **soggetto passivo/interessato**: è la **persona fisica** identificata o identificabile attraverso i c.d. "identificatori"[23].
   Tra gli identificatori, il Regolamento si sofferma in particolare su quelli "*online prodotti da dispositivi, applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, o marcatori temporanei (**cookies**) o a identificativi di altro tipo, come i **tag di identificazione** a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utili per creare profili delle persone fisiche e identificarle*"[24].

[13] ad esempio, all'interno di modulistica;
[14] si può invocare solo se nessun'altra condizione di liceità può trovare applicazione;
[15] l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti;
[16] *ex* art. 5, comma 1;
[17] i dati sono raccolti per finalità determinate, esplicite e legittime;
[18] i dati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
[19] i dati devono essere esatti e, se necessario, aggiornati;
[20] i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
[21] i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
[22] il titolare del trattamento è tenuto a comprovare il rispetto dei principi di cui sopra;
[23] *ex* art. 4, comma 1, n. 1, *"il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*;
[24] considerando n. 30;

2. **soggetti attivi**[25]:
   - **titolare del trattamento**: definito dall'art. 4, comma 1, n. 7 come *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**"*. È il soggetto che dà impulso alle operazioni e alle attività di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto o interconnessione, limitazione, cancellazione o distruzione dei dati. Non è richiesta alcuna specifica attribuzione per legge. Con il termine mezzi si intendono non solo i mezzi tecnici per trattare i dati personali, ma anche le modalità attraverso le quali il trattamento è effettuato;
   - **responsabile del trattamento**: *"La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**"*[26]. Nominato mediante contratto o altro atto giuridico conforme al diritto nazionale, svolge funzione strumentale rispetto all'attività del titolare. Tra i vari obblighi cui è tenuto ad adempiere, si ritrovano la tenuta del registro dei trattamenti svolti, l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti e la designazione del *DPO*;
   - **sub-responsabile**: nominato dal responsabile previa autorizzazione scritta, specifica o generale, del titolare. Anche questa figura, sebbene nominata dal responsabile, dovrà eseguire le attività e le operazioni di trattamento per conto del titolare, nonché agire in via strumentale rispetto alle finalità dal medesimo determinate. **Il responsabile del trattamento mantiene la totale responsabilità nei confronti del titolare anche nel caso in cui l'inadempienza degli obblighi in materia di protezione dei dati derivi dal sub-responsabile da lui nominato**;
   - **contitolare**: figura presente allorché due o più titolari determinino congiuntamente le finalità e i mezzi del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in relazione agli obblighi in materia di protezione dei dati personali, con particolare riguardo all'esercizio dei diritti dell'interessato, le modalità per fornire un'adeguata informativa agli interessati, ai sensi degli artt. 13 e 14, nonché il soggetto che sarà individuato come punto di contatto per gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato;
   - **rappresentante**: "*La persona fisica o giuridica stabilita nell'Unione che, designata per iscritto dal titolare del trattamento o dal responsabile del trattamento, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Regolamento*"[27]. Viene formalmente designato mediante mandato scritto quando il titolare o il responsabile del trattamento non sono stabiliti nell'Unione europea, ma le attività di trattamento sono connesse all'offerta di beni o alla prestazione di servizi o al controllo del comportamento degli interessati situati all'interno dell'Unione. La sua nomina tuttavia non è obbligatoria ove il trattamento sia occasionale, non includa il trattamento, su larga scala, di categorie particolari di dati personali o dati giudiziari, non presenti un rischio per i diritti e le libertà delle persone fisiche, il titolare sia un'autorità pubblica o un organismo pubblico. Esso agisce per conto e in luogo del soggetto rappresentato al fine di assolvere agli obblighi previsti dal Regolamento a carico di quest'ultimo. Esso, infine, rappresenta anche uno strumento di garanzia per gli interessati: questi ultimi possono, infatti, far riferimento a questa figura ove non sia possibile o sia eccessivamente oneroso rivolgersi al titolare o al responsabile del trattamento. La sua presenza non deresponsabilizza il titolare o il responsabile, i quali continuano ad essere imputabili in caso di inosservanza e violazione delle disposizioni del Regolamento;

[25] è importante individuare il ruolo e i compiti affidati alle varie figure che rivestano un ruolo di responsabilità nell'ambito del trattamento dei dati personali al fine di creare una responsabilizzazione maggiore;
[26] definizione *ex* art. 4, comma 1, n. 8, tale soggetto opera in virtù di un mandato ricevuto dal titolare e svolge attività strumentale rispetto al trattamento effettuato dal titolare;
[27] *ex* art. 4, comma 1, n. 17;

- **destinatario**: "*La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi*"[28];
- ***Data Protection Officer* (*DPO*)**: responsabile della protezione dei dati personali, figura autonoma e indipendente la cui nomina è obbligatoria in alcuni casi.

Qualsiasi altra persona che agisce sotto l'autorità del titolare del trattamento o del responsabile, che ha accesso ai dati personali, può trattarli solo su istruzione del titolare o se è imposto dalla legge o degli Stati membri dell'UE;

3. **soggetti con funzione di controllo**[29]: Garante per la protezione dei dati e Comitato europeo per la protezione dei dati personali.

***

Il Regolamento stabilisce che il titolare del trattamento debba fornire informazioni agli interessati relative al trattamento posto in essere.

Relativamente all'**obbligo di informazione**, ai sensi degli artt. 13 e 14, i contenuti dell'informativa sono elencati in modo tassativo. In particolare, nel caso in cui la raccolta dei dati avvenga presso l'interessato, il titolare, nel momento in cui tali dati vengono raccolti, fornisce all'interessato le seguenti informazioni:

a) l'identità e i suoi dati di contatto e, ove applicabile, del rappresentante e del responsabile della protezione dei dati (*DPO*);
b) le finalità del trattamento, nonché la base giuridica del trattamento;
c) gli eventuali destinatari o categorie di destinatari dei dati personali;
d) l'intenzione di trasferire i dati personali in Paesi terzi o ad organizzazioni internazionali e attraverso quali strumenti.

Il titolare del trattamento fornisce, inoltre, nel momento in cui i dati personali sono ottenuti, ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente, tra cui:

e) il periodo di conservazione dei dati o i criteri seguiti utilizzati per determinare tale periodo;
f) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento che lo riguardano, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
g) l'esistenza del diritto di revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento nel caso in cui lo stesso si fondi sul consenso espresso dell'interessato;
h) il diritto di presentare reclamo a un'Autorità di controllo;
i) la comunicazione dei dati personali risponde ad un obbligo legale o contrattuale oppure è da considerarsi un requisito necessario per la conclusione di un contratto, inoltre, se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
j) l'esistenza di un processo decisionale automatizzato - compresa la profilazione - e indicazioni sulla logica utilizzata da tali processi decisionali, oltre alle conseguenze previste per l'interessato.

Nel caso i dati non siano raccolti direttamente presso l'interessato, la suddetta informativa deve essere fornita **entro un termine ragionevole che non deve superare un mese dall'ottenimento dei dati personali, oppure al momento della prima comunicazione con l'interessato o con terzi.**

[28] *ex* art. 4, comma 1, n. 9;
[29] sono autorità pubbliche indipendenti incaricate di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche;

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico. Il regolamento ammette l'utilizzo di icone[30] standardizzate in combinazione, però, con l'informativa estesa.

Si hanno casi di esclusione dell'obbligo di informativa quando:

a) l'interessato già dispone di tali informazioni;
b) la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato;
c) i dati personali devono rimanere riservati, conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri o ad un obbligo di segretezza previsto per legge.

***

Gli adempimenti previsti dal Regolamento, ossia le fasi di adeguamento delle aziende suddivise in step, sono:

1. **mappatura dei trattamenti;**
2. **individuazione dei ruoli, delle responsabilità e dei compiti;**
3. **definizione e attuazione degli adempimenti per priorità d'azione e definizione di misure di sicurezza adeguate;**
4. **definizione di una procedura di *data breach*;**
5. **definizione di *policy* e procedure organizzative interne;**
6. **documentazione delle attività di trattamento per provare la conformità al Regolamento.**

1. <u>Mappatura</u> – Tenuta del registro dei trattamenti

Ai sensi dell'art. 30: *"Ogni titolare del trattamento e, ove applicabile, il suo rappresentante[31] tengono un registro delle attività di trattamento svolte sotto la propria responsabilità"*. Tale **registro** deve contenere le seguenti informazioni:

a) i riferimenti del titolare del trattamento e, ove applicabile, del contitolare, del rappresentante e del responsabile della protezione dei dati (*DPO*);
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e dei dati personali trattati;
d) le categorie di destinatari a cui i dati sono stati o saranno comunicati, anche soggetti di Paesi terzi od organizzazioni internazionali;
e) il flusso di dati, in caso di trasferimento di dati extra UE;
f) il tempo di conservazione per ciascuna categoria di dati;
g) una descrizione delle misure di sicurezza tecniche e organizzative adottate per minimizzare i rischi.

Il registro deve avere forma scritta, anche elettronica[32], e deve essere esibito su richiesta al Garante per la protezione dei dati personali.

<u>Tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano presenti un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di categorie particolari di dati, o dati relativi a condanne penali e a reati.</u>

[30] queste icone dovranno essere identiche in tutta l'UE e saranno prossimamente definite dalla Commissione europea;
[31] e anche il responsabile del trattamento;
[32] in strutture complesse di titolari e responsabili del trattamento è ipotizzabile l'utilizzo di software e formulari automatizzati;

2. Individuazione dei ruoli, delle responsabilità e dei compiti

Il **titolare del trattamento** è tenuto a:

- implementare opportune misure di sicurezza[33], *"tenendo conto della natura dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche"*;
- dimostrare la conformità delle operazioni di trattamento rispetto ai principi sanciti dal Regolamento, adempiendo a tutte le procedure di *assessment* previste dal Regolamento e aderendo ad un meccanismo di certificazione o a codici di condotta approvati.

Il Regolamento stabilisce che il soggetto può richiedere al titolare il **risarcimento dei danni** subiti da un trattamento; in tal caso **il titolare è tenuto a risponderne direttamente e interamente.**

Il **responsabile del trattamento** tratta i dati per conto del titolare. I trattamenti eseguiti dal responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. L'atto di designazione[34] deve sancire precisi **doveri in capo al responsabile**, tra cui:

- trattare i dati personali eseguendo le istruzioni fornite dal titolare;
- assicurare che le persone autorizzate a trattare i dati si siano impegnate a rispettare vincoli di riservatezza;
- implementare e mantenere tutte le misure tecniche e organizzative adeguate;
- assistere il titolare del trattamento per la gestione delle richieste di diritto di accesso e per gli altri obblighi imposti;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36[35], tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su richiesta del titolare cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;
- fornire al titolare qualsiasi informazione necessaria per dimostrare il rispetto del Regolamento;
- tenere un registro delle categorie di attività di trattamento dei dati personali svolte per conto del titolare;
- cooperare con l'Autorità di controllo;
- avvertire il titolare del trattamento immediatamente dopo aver riscontrato il verificarsi di una violazione dei dati;
- designare un Responsabile della protezione dei dati (*DPO*) nei casi in cui è richiesto.

Il **responsabile della protezione dei dati (*DPO*)**, *ex* art. 37, viene designato dal titolare e dal responsabile del trattamento e ha funzione di informazione, di consiglio e di controllo interno. Questa nuova figura introdotta dalla normativa europea agisce in modo indipendente e riferisce direttamente ai vertici. La sua nomina è **obbligatoria** ogniqualvolta:

[33] misure tecniche e organizzative, adeguate politiche in materia di protezione dei dati, protezione dei dati dalla progettazione e di *default*;
[34] contratto o altro atto giuridico;
[35] le norme richiamate sono quelle che impongono al titolare del trattamento di adottare adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio; la procedura di *data breach*, ossia la notifica al Garante *privacy* di una violazione dei dati personali; la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva;

a) il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni;
b) le attività principali del titolare o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
c) le attività principali del titolare o del responsabile del trattamento consistano nel trattamento, su larga scala, di categorie particolari di dati personali o di dati giudiziari.

Al di là di questi casi tassativi, il titolare del trattamento può comunque valutare l'opportunità di nominarlo.

Ai sensi dell'art. 39, il *DPO* è incaricato di:

a) informare e consigliare il titolare o il responsabile del trattamento sugli obblighi concernenti il Regolamento;
b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e a sorvegliarne lo svolgimento;
d) cooperare con l'Autorità di controllo;
e) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Responsabilità del *DPO*: il controllo del rispetto del Regolamento non significa che il *DPO* sia personalmente responsabile in caso di inosservanza. Il Regolamento chiarisce che il rispetto delle norme in materia di protezione dei dati fa parte della **responsabilità d'impresa** del titolare del trattamento, non del *DPO*. **In caso di inadempimenti derivanti da colpa o dolo del *DPO*, il titolare o il responsabile potrà avanzare pretese risarcitorie a titolo di responsabilità contrattuale.**

Assenza di conflitti di interesse: il *DPO* può essere un soggetto interno o esterno[36] all'azienda. Il regolamento consente al *DPO* di svolgere anche altri compiti e funzioni, a condizione che il titolare del trattamento o il responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un **conflitto di interessi**. Ciò significa che **il *DPO* non può rivestire all'interno dell'organizzazione del titolare o del responsabile del trattamento un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali.** Le Linee Guida delle Autorità Garanti forniscono alcuni esempi di soggetti che, per il ruolo che rivestono in azienda, **non possono essere nominati *DPO*:**

- amministratore delegato;
- responsabile operativo;
- direttore finanziario;
- direttore sanitario;
- responsabile marketing;
- responsabile HR;
- responsabile IT.

3. Definire e attuare gli adempimenti e determinare le misure di sicurezza adeguate

[36] nominato in base a un contratto di servizi;

Dopo aver mappato i trattamenti è necessario identificare per ciascuno di questi le attività da effettuare per essere conformi al Regolamento. Le procedure di *assessment* sono suddivise secondo moduli scalari **per priorità in base ai rischi** per i diritti e le libertà dei soggetti[37].

Tali procedure di *assessment* vengono di seguito elencate ed esaminate.

- **Analisi generica del potenziale impatto** sui dati personali

Ai sensi dell'art. 32, intitolato "Sicurezza del trattamento":

*"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 titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate **per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:*

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si 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".

L'articolo richiama l'attenzione anche sulla possibilità di aderire a specifici codici di condotta approvati dall'Autorità Garante competente[38] o a schemi di certificazione approvati da appositi organismi qualificati e riconosciuti per dimostrare la conformità ai requisiti stabiliti dalla disposizione e attestare l'adeguatezza delle misure di sicurezza adottate.

- **Valutazione d'impatto sulla protezione dei dati (*DPIA*)**

Ai sensi dell'art. 35:

*"1. **Quando un tipo di trattamento**, allorché prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, **il titolare del trattamento effettua prima di procedere al trattamento, una valutazione d'impatto dei trattamenti** previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati.

*3. **La valutazione d'impatto è richiesta in particolare nei casi seguenti**:*

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si

[37] nel definire la tipologia di adempimenti richiesti, il Regolamento fa infatti riferimento al valore soglia del "**rischio elevato**";

[38] l'elaborazione dei codici di condotta spetterà alle associazioni o ad altri organismi rappresentanti le categorie di titolari del trattamento;

fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali o dati giudiziari;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati[39].

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato (...)."

La valutazione d'impatto deve contenere:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La valutazione d'impatto deve essere periodicamente aggiornata, in particolar modo tutte le volte che vi sia un mutamento significativo circa la natura, la finalità o le modalità di trattamento, compresa l'introduzione di nuove tecnologie.

- **<u>Consultazione preventiva</u>**

Ai sensi dell'art. 36: *"Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 indichi che* ***<u>il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio</u>***.*"*

Si ricorre a questo strumento qualora si verifichino due condizioni:

- quando, a seguito della valutazione d'impatto, emerge che il trattamento presenti comunque un rischio elevato;
- quando le misure per mitigare il rischio sono impraticabili per il titolare a causa della tecnologia prevista e dei costi di attuazione.

[39] le Linee Guida del Gruppo "Articolo 29", in materia di valutazione di impatto sulla protezione dei dati (WP248), hanno fornito alcuni criteri in vista dell'elaborazione degli elenchi dei trattamenti più rischiosi, ossia: *i*) trattamenti valutativi, inclusa la profilazione o l'assegnazione di punteggi, in particolare, in considerazione di *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"*; *ii*) processi decisionali automatizzati che producono significativi effetti giuridici o di analoga natura (assunzioni, concessioni di prestiti, stipula di assicurazioni); *iii*) monitoraggio sistematico (videosorveglianza); *iv*) dati sensibili o aventi carattere altamente personale, categoria prevista dagli artt. 9 e 10 del Regolamento; *v*) trattamento di dati "su larga scala", tenendo conto del numero di soggetti interessati dal trattamento (in termini assoluti ovvero espressi in percentuale della popolazione di riferimento), il volume di dati oggetto di trattamento, la durata del trattamento e la portata geografica dell'attività di trattamento; *vi*) creazione di corrispondenze o combinazione di insieme di dati; *vii*) dati relativi a interessi vulnerabili; *viii*) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative (quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale); *ix*) quando il trattamento in sé *"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"*, comprendente quei trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto;

In questi casi, dunque, occorre un parere preventivo delle Autorità di controllo per valutare la situazione alla luce degli interessi in gioco. L'Autorità di controllo fornisce, entro 8 settimane[40] dal ricevimento della richiesta di consultazione, un parere scritto al titolare e al responsabile del trattamento.

Al momento di consultare l'Autorità di controllo il titolare del trattamento comunica:

a) le rispettive responsabilità del titolare, dei contitolari e dei responsabili del trattamento;
b) le finalità e i mezzi del trattamento;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
d) ove applicabile, i dati di contatto del responsabile della protezione dei dati (*DPO*);
e) la valutazione d'impatto sulla protezione dei dati;
f) ogni altra informazione richiesta dall'Autorità di controllo.

4. **Definire la procedura di *data breach***, disciplinata dagli artt. 33 e 34 del Regolamento. Nel caso si verifichi una violazione dei dati personali, da intendersi come *"violazione di sicurezza che comporta 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"*[41], il Regolamento prevede **due obblighi di notifica**, uno nei confronti dell'Autorità di controllo e l'altro nei confronti degli interessati.

Nel primo caso – notifica al Garante - il titolare del trattamento 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, **soltanto se ritiene probabile che da tale violazione derivino rischi** per i diritti e le libertà delle persone fisiche[42].

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire tempestivamente tutte le informazioni richieste, gli elementi mancanti possono essere forniti in fasi successive senza ingiustificato ritardo.

Il titolare è tenuto a **documentare** qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

[40] termine prorogabile di ulteriori 6 settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il titolare e il responsabile del trattamento ne sono informati entro un mese dal ricevimento della richiesta di consultazione;
[41] *ex* art. 4, comma 1, n. 12;
[42] il Gruppo di lavoro "Articolo 29" ha determinato una serie di fattori che permettono di valutare la rilevanza/gravità di una violazione dei dati: *i*) il tipo di violazione; *ii*) la natura, il numero e il grado di sensibilità dei dati personali violati; *iii*) facilità di associare i dati violati ad una persona fisica; *iv*) gravità delle conseguenze per gli interessati; *v*) numero di interessati esposti al rischio; *vi*) caratteristiche del titolare del trattamento;

Nel secondo caso - notifica agli interessati - essa **è obbligatoria** e da effettuarsi senza ingiustificato ritardo, solo nel caso in cui la violazione presenti un **rischio elevato** per i diritti e le libertà delle persone fisiche.

Anche in presenza di tale elevato rischio, tuttavia, **non si darà luogo alla comunicazione** quando è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica.

5. Definizione di *policy* e procedure organizzative interne

Per garantire un alto livello di protezione dei dati personali è indispensabile porre in essere delle procedure interne che comprendano:

- il rispetto del principio della protezione dei dati già in fase di progettazione;
- la formazione e la sensibilizzazione dei soggetti interni che trattano dati personali;
- la gestione dei reclami e delle richieste di esercizio dei diritti da parte degli interessati;
- la prevenzione e la gestione di violazioni dei dati personali.

6. Documentazione delle attività di trattamento per provare la conformità al Regolamento

È fondamentale la raccolta e la custodia della documentazione necessaria. Tutte le attività e i documenti posti in essere in ogni fase del trattamento dovranno essere **riesaminati e aggiornati regolarmente** per assicurare una protezione dei dati permanente. In particolare, si fa riferimento a:

- documentazione attestante i trattamenti di dati personali svolti[43];
- documentazione attestante il rispetto dei diritti e delle libertà dei soggetti interessati[44];
- documentazione che definisce i ruoli e le responsabilità in materia di protezione dei dati personali[45];
- comprova delle misure di sicurezza tecniche implementate.

***

Regime sanzionatorio per l'illecito trattamento dei dati personali

Gli illeciti in ambito *privacy* possono essere di natura civile, amministrativa e penale. Il Regolamento disciplina le sanzioni amministrative, rimettendo ai singoli Stati membri la disciplina delle sanzioni penali.

[43] registro delle attività di trattamento, valutazione d'impatto, documentazione prevista per il trasferimento dei dati extra UE;
[44] le informative, i moduli di raccolta consensi, l'attestazione dei consensi raccolti, la gestione dei diritti esercitati;
[45] i contratti e le nomine dei responsabili esterni, la gestione degli incaricati del trattamento, le procedure interne, etc.;

Ai sensi dell'art. 83, comma 1, le sanzioni amministrative pecuniarie sono inflitte dall'Autorità di controllo[46] e devono essere effettive, proporzionate e dissuasive.

Le sanzioni pecuniarie possono essere comminate in aggiunta o in luogo delle misure di cui all'art. 58, comma 2, lett. da a) a h) e j) del Regolamento[47].

È possibile dividere e distinguere due livelli sanzionatori:

1) **sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[48];**
2) **sanzioni amministrative pecuniarie fino 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[49].**

Nell'invitare le imprese assistite a consultare frequentemente il sito *www.newslinet.it*, ospitante il periodico telematico *NL Newslinet* (collegato a *Consultmedia*), al fine di conseguire aggiornamenti in tempo reale in ordine ad informazioni rilevanti in materia economica, giuridica, amministrativa, fiscale e tecnica, si partecipa che questa struttura è a disposizione per qualsiasi chiarimento a riguardo di quanto sopra, evidenziando che **i *partner* di riferimento per l'incombenza in parola sono:**

dr.ssa Gloria Siri - tel. 0331/452183 comunicazioni@planetmedia.it
dr.ssa Giulia Cozzi – tel. 0331/593377 social@planetmedia.it

professionisti cui è demandata l'assistenza per le problematiche di specie.

Infine si ricorda che **nell'area riservata agli utenti S.I.T. (*Service Informativo Telematico*) del sito *www.newslinet.it* è presente la raccolta di tutte le circolari inviate dalla struttura Consultmedia da un triennio a questa parte**. Per adesioni al servizio S.I.T. (erogato al costo annuale di euro 100,00 oltre IVA): *annalisa@planetmedia.it* (rif. Annalisa Ferioli 0331/452183).

---

[46] in Italia, dal Garante per la protezione dei dati personali;

[47] l'art. 58, comma 2, elenca i poteri correttivi riconosciuti in capo all'Autorità di controllo. Nello specifico, il Garante può: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del Regolamento; b) rivolgere ammonimenti al titolare del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del Regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal Regolamento; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del Regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli artt. 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'art. 17, par. 2 e dell'art. 19; h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli artt. 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono più soddisfatti; j) ordinare la sospensione dei flussi di dati verso un destinatario in un Paese terzo o un'organizzazione internazionale;

[48] sanzioni applicabili in caso di violazione delle disposizioni che disciplinano: *a*) il consenso dei minori in relazione ai servizi della società dell'informazione; *b*) il trattamento che non richiede identificazione; *c*) la *privacy by design* e la *privacy by default*; *d*) la non presenza all'interno del territorio dell'UE dei titolari e dei responsabili del trattamento; *e*) l'individuazione delle *"responsabilities"* del responsabile del trattamento; *f*) i registri delle attività del trattamento; *g*) l'attività di cooperazione fra titolare e/o responsabile del trattamento e Garante per la protezione dei dati personali; *h*) la designazione del *DPO*; *i*) l'approntamento di misure di sicurezza adeguate; *l*) la notifica di una violazione dei dati personali al Garante; *m*) la predisposizione di codici di condotta; *n*) l'accreditamento degli organismi di certificazione; *o*) la valutazione d'impatto sulla protezione dei dati personali;

[49] sanzioni applicabili in caso di violazione delle disposizioni che disciplinano: *a*) i principi di base del trattamento, comprese le condizioni di liceità, le condizioni per il consenso e il diritto di revoca, il trattamento di categorie particolari di dati personali; i diritti riconosciuti in capo all'interessato; *b*) i trasferimenti di dati extra UE; *c*) l'inosservanza di un ordine da parte dell'Autorità di controllo di cui all'art. 58, comma 2;

È gradita l'occasione per salutare cordialmente.

Consultmedia

1) *Il presente servizio è rivolto esclusivamente alla clientela delle strutture Consultmedia (divisione della s.r.l. Planet) e Tecnomedia (Tecnomedia s.r.l.);*
2) *E' espressamente vietata la trasmissione, riproduzione, distribuzione, elaborazione e/o divulgazione, anche parziale, della presente comunicazione e/o della documentazione ad essa allegata e/o collegata, in assenza di preventiva autorizzazione scritta delle s.r.l. Planet e/o Tecnomedia, che ne detengono tutti i diritti;*
3) *Le s.r.l. Planet e Tecnomedia non rispondono di eventuali involontari errori e/o omissioni nel contenuto delle circolari o di un errato impiego delle indicazioni in esse contenute, a maggior ragione qualora ciò consegua ad arbitrarie interpretazioni analogiche, estensive o riduttive delle informazioni rese, e, pertanto, invitano i destinatari a verificare sempre, e quindi in ogni caso, la fattispecie applicativa, consultando i professionisti indicati in calce oppure soggetti di propria fiducia, esponendo la propria specifica situazione ai fini di una corretta individuazione dell'ambito di applicazione;*
4) *Le modalità di erogazione del servizio di informazione gratuita attraverso posta elettronica, fax o comunque ogni altro mezzo di trasmissione o comunicazione, offerto dalle strutture Consultmedia (e quindi da Planet s.r.l.) e Tecnomedia alla propria clientela e/o ai soggetti da esse Consultmedia (e quindi Planet s.r.l.) e Tecnomedia ritenuti d'interesse, prevedono l'insindacabile facoltà d'esclusione dal novero dei destinatari del servizio del soggetto che non abbia provveduto a conferire incarico consultivo alle strutture Consultmedia (e quindi della Planet s.r.l.) e Tecnomedia per tre adempimenti consecutivi, fatta salva la sottoscrizione, mediante abbonamento, al servizio SIT Online;*
5) *Informazione ai sensi del decreto legislativo 196/2003: il Vs. indirizzo e-mail è utilizzato esclusivamente per questo servizio informativo. Esso non sarà comunicato o diffuso a terzi. Qualora desideraste essere eliminati dall'elenco, inviate un'e-mail con la dicitura "cancellazione dall'elenco" all'indirizzo* info@consultmedia.it*; diversamente ci legittimerete a proseguire nel servizio.*