GDPR - Tabella ragionata

Con questa tabella si offre a disposizione dell'utenza uno schema sintetico degli obblighi / adempimenti / cautele di spettanza del titolare del trattamento in base alle norme del GDPR - UE 2016/679 (relativo alla *protezione delle persone fisiche con riguardo al trattamento dei dati personali*).

Per una esigenza di articolazione e maggiore significatività della tabella, gli obblighi/adempimenti/cautele sono classificati come di seguito:

1. COLORE VERDE, quelli che riguardano concretamente un nucleo incomprimibile di attività di trattamento di dati, in assenza di incidenti/violazioni delle norme;
2. COLORE ARANCIONE, quelli che hanno a che fare con trattamenti di particolari categorie di dati o con determinate modalità di svolgimento delle attività ovvero si legano al verificarsi di specifiche circostanze (ad es., esercizio congiunto con altro titolare delle decisioni fondamentali sui trattamenti, trattamento di dati relativi alla salute, trattamento ad elevato rischio per i diritti e le libertà delle persone fisiche, raccolta on line di dati di minori di anni 16, organizzazione del titolare con più di 250 dipendenti, incarico ad un soggetto professionale di gestire trattamenti per conto del titolare, trasferimento dei dati in un Paese extra-UE, ecc.);
3. COLORE ROSSO, obblighi/adempimenti gravanti sul titolare in presenza di incidenti/violazioni di dati o a fronte di richieste dell'autorità di controllo;
4. COLORE CELESTE decisioni volontarie del titolare.

A fianco di ciascun argomento/voce la tabella riporta il riferimento (capo, articolo/i) nel testo del Regolamento.

REGOLAMENTO UE 2016/679: TABELLA RAGIONATA *degli OBBLIGHI / ADEMPIMENTI / CAUTELE DEL TITOLARE*	
ADEMPIMENTO	**CAPO, ARTICOLO**
I principi applicabili al trattamento dei dati personali I dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime; i dati: adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantirne un'adeguata sicurezza.	**II - 5**
Acquisizione del consenso da parte dell'interessato e casistica di esonero dal relativo obbligo Ciascun titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) consenso dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.	**II - 6, 7**
Il consenso dei minori a fronte di servizi ICT Nei casi in cui è richiesto il consenso, il trattamento di dati relativo all'offerta diretta di servizi della società dell'informazione ai minori è lecito se il minore che ha prestato il consenso ha compiuto 16 anni. In caso di minori di 16 anni, deve essere acquisito il consenso di colui/coloro che ha/hanno la responsabilità genitoriale del minore e il titolare deve adoperarsi in ogni modo ragionevole, in considerazione delle tecnologie disponibili, per verificare la detta circostanza.	**II - 8**

Trattamento di particolari categorie di dati E' formalizzato il divieto generale del trattamento dei dati corrispondenti a quelli attualmente definiti 'sensibili', oltre che dei dati genetici e biometrici. Dopodiché sono disposte specifiche eccezioni al divieto, come quelle relative alle ipotesi in cui: l'interessato ha prestato il consenso; i dati sono trattati per eseguire un contratto di lavoro e per le connesse esigenze di sicurezza/protezione sociale; i dati sono trattati a fini di tutela di un interesse vitale dell'interessato; i dati personali sono stati resi pubblici dall'interessato, ecc.	**II - 9**
Trattamento di dati relativi a condanne penali e reati Il trattamento dei dati personali sostanzialmente corrispondenti a quelli oggi definiti 'giudiziari' deve avvenire, alternativamente, sotto il controllo della autorità pubblica ovvero previa autorizzazione proveniente da norme dell'Unione e del singolo Stato membro che prevedano garanzie appropriate per i diritti e le libertà degli interessati.	**II - 10**
Trasparenza nella gestione dei trattamenti Il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).	**III - 12**
Informativa all'interessato Adempimento basilare per qualsiasi titolare, si giova necessariamente di una buona capacità di analisi (in particolare) dei flussi dei trattamenti. L'informativa richiesta dal Regolamento UE è più ricca di informazioni di quella attuale e la sua redazione è operazione niente affatto banale: per esempio, il titolare deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo. Non in ultimo, il linguaggio dell'informativa deve essere semplice e chiaro. Si distinguono le due fattispecie in cui la comunicazione delle informazioni è da correlare alla raccolta dei dati presso l'interessato ovvero presso un soggetto diverso.	**III - 13, 14**
Il rispetto dei diritti dell'interessato Il Regolamento formalizza un ampio catalogo di diritti che spettano all'interessato. Si tratta del diritto di accesso, del diritto di rettifica, del diritto alla cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul titolare.	**III - 15, 16, 17, 18, 20, 21**

Il particolare caso dei processi decisionali automatizzati E' riconosciuto il diritto dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona (tra le operazioni contemplate dalla norma campeggia la profilazione come definita dall'art. 4.1, n. 4). Il correlativo divieto non si applica ove la decisione si basi sul consenso esplicito dell'interessato, sia necessaria per l'esecuzione di un contratto con l'interessato, ovvero sia autorizzata dal diritto dell'Unione o del singolo Stato membro.	**III - 22**
Misure di sicurezza adeguate Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate.	**IV - 24, 32**
Privacy by design (fin dalla progettazione) Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati.	**IV - 25.1**
Privacy by default (per impostazione predefinita) Il titolare del trattamento attua misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi.	**IV - 25.2**
Contitolarità del trattamento Nel caso in cui due o più titolari operano come contitolari del trattamento (determinando congiuntamente finalità e mezzi del medesimo), concordano in modo trasparente, mediante un contratto, la ripartizione delle responsabilità del trattamento, con particolare riguardo all'esercizio dei diritti degli interessati e ai connessi obblighi informativi. Il contenuto essenziale dell'accordo deve essere messo a disposizione degli interessati.	**IV - 26**
Nomina del Rappresentante del titolare Laddove si applichi l'art. 3.2 (trattamento di dati personali relativi ad interessati che si trovano nell'Unione da parte di titolare/responsabile non stabilito nell'UE), il titolare/responsabile designa per iscritto un proprio rappresentante nell'Unione. Il rappresentante è l'indefettibile interlocutore della competente autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.	**IV - 27**

Nomina del Responsabile del trattamento Il titolare può nominare un responsabile che effettui il trattamento per suo conto. Il titolare ha la responsabilità di scegliere per tale incarico un soggetto/organismo che presenti garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate. Il Regolamento stabilisce un numero cospicuo di requisiti minimi di contenuto del contratto tra titolare e responsabile del trattamento.	**IV - 28**
Obbligo di istruzione da parte del Titolare Il titolare del trattamento deve previamente istruire tutti coloro che siano autorizzati ad accedere ai dati personali, compreso il responsabile del trattamento.	**IV - 29**
Adozione del Registro delle attività di trattamento E' adempimento obbligatorio per il titolare del trattamento con almeno 250 dipendenti o che, anche al di sotto di tale soglia dimensionale, effettui un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici, giudiziari. Cuore del documento è una mappa dettagliata di tutti i trattamenti effettuati dall'organizzazione del titolare.	**IV - 30**
Obbligo di cooperazione con l'autorità di controllo Il titolare è tenuto a cooperare con l'autorità di controllo, quando quella gliene faccia richiesta.	**IV - 31**
Notificazione di una violazione dei dati Rientra tra gli obblighi del titolare anche la notifica all'autorità di controllo (Garante) senza ingiustificato ritardo - e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza -, di ogni violazione della sicurezza dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche.	**IV - 33**
Comunicazione di una violazione dei dati all'interessato Quando la violazione della sicurezza dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve darne notizia all'interessato senza ingiustificato ritardo. La norma fissa i requisiti di contenuto della comunicazione, che deve essere redatta con un linguaggio semplice e chiaro. Altresì la norma individua i casi in cui la detta comunicazione non è richiesta (per semplicità, quando il titolare ha adottato misure tali da scongiurare il rischio o quando la comunicazione richiederebbe sforzi sproporzionati.	**IV - 34**
Redazione della Valutazione d'impatto sulla protezione dati e consultazione dell'autorità di controllo Si tratta di un ulteriore adempimento che grava sul titolare che debba iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche. Ciò si può verificare, in particolare, quando sia implicato l'uso di nuove tecnologie, ovvero in considerazione di altre caratteristiche (natura, oggetto, contesto, finalità) del trattamento. Quando la valutazione di impatto indichi che il trattamento presenta un rischio elevato, prima di procedere al trattamento il titolare è tenuto a consultare l'autorità di controllo.	**IV - 35, 36**

Nomina di un Responsabile della Protezione dei Dati (Data Protection Officer - DPO) La nomina del DPO è adempimento obbligatorio quando il titolare del trattamento: a) è autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali); b) effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. Il DPO ha compiti di informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina 'privacy'. E' anche l'interlocutore dell'autorità di controllo.	**IV, 37-39**
Adesione a codici di condotta/sistemi di certificazione Si tratta di adempimenti volontari del titolare mediante i quali può implementare importanti misure di sicurezza dei trattamenti e dimostrare la conformità delle attività di trattamento ai requisiti stabiliti dal Regolamento.	**IV - 40-42**
Cautele per il trasferimento dei dati in Paesi terzi Il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale deve essere effettuato nel rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento.	**V - 44, 45, 46, 47, 48, 49**
Obbligo di risarcimento del danno Il titolare è tenuto a risarcire il danno materiale o immateriale cagionato da una violazione del Regolamento. Egli è esonerato da tale responsabilità soltanto se dimostra che l'evento dannoso non gli è in alcun modo imputabile.	**VIII - 82**