DOMANDE E RISPOSTE SUL GDPR
(General Data Protection Regulation)

PREMESSA

Il seguente documento è stato prodotto dal gruppo di lavoro AssoSoftware che si occupa di Data Protection e Privacy con l'obiettivo di fornire indicazioni utili alle aziende associate e ai loro clienti in merito all'adeguamento al nuovo GDPR delle soluzioni software e dei processi interni ed esterni alle software house medesime. Come è noto il Regolamento Europeo (UE) 2016/679 sarà pienamente applicabile a partire dal 25 maggio 2018 e non richiede un recepimento nazionale. Tuttavia esistono ancora numerosi aspetti da chiarire nel testo base e parallelamente una Commissione Ministeriale, su delega ricevuta dal Legislatore Italiano, sta preparando un Provvedimento (D.Lgs.) che dovrà armonizzare la previgente normativa rispetto alle nuove regole introdotte dal Regolamento Europeo. Si tratta di un percorso che richiederà necessariamente successivi interventi e affinamenti, per tale motivo anche il presente documento è solo un primo contributo e potrà subire variazioni e/o integrazioni nel tempo. In questo scenario si è cercato quindi di porre le principali domande rispetto alle novità introdotte dal GDPR e di dare a ognuna una risposta compatibile con il quadro normativo attuale, con l'organizzazione delle software house e l'evoluzione tecnologica in atto. Il documento è il risultato di numerosi incontri tra i rappresentanti delle principali aziende associate, coadiuvati da consulenti esperti del settore e con un periodico confronto con i funzionari dell'authority Garante della Protezione dei Dati Personali.

INDICE

1. Registro dei trattamenti

1.1. L'art. 30, comma 2, del Regolamento UE n. 679/2016 (*General Data Protection Regulation*, di seguito "GDPR") prevede che il Registro dei trattamenti tenuto dal responsabile del trattamento contenga "*i nomi e i dati di contatto … di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento*", e che siano indicate "*le categorie di trattamenti svolte per ogni titolare del trattamento*". Al riguardo, si osserva che una *software house* può effettuare in qualità di responsabile trattamenti di dati personali per conto di numerosi clienti quali titolari. Vista anche la possibilità di attivazione ed erogazione dei servizi on line, risulta quindi estremamente difficoltosa l'attività, nell'ambito del Registro, di puntuale indicazione e continuo aggiornamento dei nominativi dei titolari per conto dei quali si opera e di correlazione delle categorie di trattamenti svolti per ognuno di essi. Si chiede pertanto se sia possibile, in questi casi, prevedere alcune semplificazioni nella strutturazione del registro dei trattamenti in modo da renderne più agevole la compilazione e la tenuta da parte della *software house* quale responsabile, prevedendo dunque che il Registro in esame sia compilato facendo rinvio, ad es., a schede o banche dati relative alle anagrafiche clienti, contenenti l'elenco puntuale e aggiornato dei medesimi clienti quali titolari del trattamento?

Risposta - *Il Gruppo di lavoro ritiene che sia possibile una semplificazione nella strutturazione del Registro attraverso le seguenti modalità:*

- *per quanto riguarda l'indicazione dei titolari del trattamento per conto dei quali sono effettuati i trattamenti, il rinvio o, ove si tratti di Registro in formato elettronico, il collegamento a schede o banche dati anagrafiche dei clienti (titolari del trattamento), con i relativi prodotti e/o servizi acquistati;*
- *per quanto concerne gli altri elementi richiesti dall'art. 30, comma 2, la descrizione delle categorie dei trattamenti effettuati dalla software house in qualità di Responsabile con riguardo a ciascun prodotto/servizio erogato, nonché l'indicazione degli eventuali trasferimenti di dati all'estero (ove presenti) e la descrizione generale delle misure di sicurezza,*

Si ritiene, inoltre, che il Registro debba essere mantenuto nella versione aggiornata, senza conservazione delle precedenti versioni (in forma storicizzata).

Va ricordato che, ai sensi dell'art. 30, comma 5, del GDPR l'obbligo di tenuta del suddetto Registro dei trattamenti non trova applicazione nei confronti delle software house con meno di 250 dipendenti, a meno che non siano effettuati trattamenti "rischiosi" o che includono categorie particolari di dati (es.: dati sensibili) o dati penali o che il trattamento dei dati non sia occasionale. Per quest'ultimo aspetto, sentito anche il parere del Garante, si ritiene che i produttori di software, nel momento in cui siano anche Responsabili del Trattamento, siano tenuti alla redazione del Registro dei Trattamenti.

1.2. Nell'ipotesi in cui il titolare del trattamento non sia il nostro cliente, ma un terzo, come è possibile assicurare la corretta tenuta e aggiornamento del Registro dei trattamenti? Ad esempio, si consideri il caso in cui il nostro cliente agisca a sua volta come responsabile del trattamento per

conto di un altro soggetto titolare e la *software house* agisca come ulteriore responsabile o "subresponsabile" (es. studio professionale che utilizza i nostri prodotti per svolgere servizi in favore dei propri clienti finali). È possibile, in tal caso, limitarsi ad indicare nel Registro dei trattamenti i nominativi dei nostri clienti quali responsabili (anziché quelli dei titolari "finali") o, in alternativa, trasferire contrattualmente sul nostro cliente gli obblighi di assunzione delle informazioni necessarie alla corretta tenuta del Registro?

Risposta - *Si tratta di un ulteriore aspetto di non semplice interpretazione, posto che, sul punto, manca un raccordo tra l'art. 28 (che prevede la possibilità di un rapporto diretto, previa autorizzazione del titolare, tra un responsabile e un ulteriore responsabile) e l'art. 30 del GDPR (che non disciplina ai fini del Registro il rapporto responsabile/subresponsabile).*
Al riguardo, il GdL sostiene l'orientamento interpretativo secondo cui nel Registro dei trattamenti, tenuto da una software house quale ulteriore responsabile, sia indicato solo il nominativo del cliente quale responsabile con cui intercorre il contratto di servizi, in linea con l'impostazione desumibile dall'art. 28 del GDPR. Ciò anche perché l'alternativa, cioè l'indicazione nel Registro dei nominativi dei titolari, clienti finali del soggetto che si rivolge alla software house e che opera già quale responsabile per conto di questi ultimi, del resto, sarebbe pressoché impraticabile sul piano pratico e operativo dal momento che non vi è alcun rapporto contrattuale con tali soggetti, che in alcuni casi potrebbero non essere neppure identificati/identificabili dall'erogatore del servizio.
In caso contrario, sarebbe necessario prudenzialmente percorrere l'opzione, piuttosto onerosa e complessa, di prevedere l'obbligo contrattuale per il cliente, laddove agisca quale responsabile del trattamento e dunque utilizzi la software house quale "subresponsabile", di mantenere e mettere a disposizione della software house l'elenco aggiornato dei titolari del trattamento e assicurare il tempestivo aggiornamento di tale indicazione, garantendo e manlevando la software house in ordine a eventuali contestazioni dovute all'inadempimento del cliente medesimo a tali obblighi.

1.3. Quale è il livello di dettaglio delle informazioni da inserire nel Registro dei trattamenti, con particolare riguardo alle misure di sicurezza tecniche e organizzative? Tali misure possono essere descritte mediante rinvio a documenti esterni (ad esempio documenti di valutazione del rischio o della PIA in cui le misure di sicurezza sono già espresse)?

Risposta - *Sì, nel Registro dei trattamenti le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. valutazione del rischio, etc.).*

2. Ruoli e organizzazione

2.1 È corretto ritenere che la *software house* debba essere sempre considerata responsabile del trattamento nel caso di erogazione della licenza d'uso del software in modalità "*on premise*", qualora oltre alla licenza vengano erogati servizi di assistenza, aggiornamento e manutenzione, che comprendono ad esempio:

- attività di migrazione dati finalizzata all'installazione e al collaudo del software;
- servizi di assistenza e aggiornamento che comportano (ancorché occasionalmente) l'accesso remoto ai dati del cliente (es. tramite teamviewer, VPN, etc.);
- analisi di dati (DB, videate, esportazioni di dati, etc.) del cliente per verificare problematiche di carattere tecnico e svolgere attività di manutenzione.

Risposta - *Sì, la software house viene a rivestire il ruolo di responsabile del trattamento anche nei casi di erogazione dei prodotti/servizi in modalità "on premise", qualora siano previste attività di assistenza e manutenzione che comportano, anche solo per scopi tecnici, l'effettuazione di operazioni di trattamento di dati personali "per conto" del cliente. In questi casi, posto che, in realtà, il GDPR non prevede più la formalizzazione di una nomina, ma semmai la stipula di un contratto o di clausole contrattuali in cui sia disciplinato il trattamento dei dati personali svolto dal responsabile per conto del titolare e gli obblighi posti in capo al medesimo responsabile, i vincoli e le responsabilità della software house dovranno essere coerenti e circoscritti alle sole attività di stretta competenza (come sopra sintetizzate) che comportino un trattamento di dati personali, escludendo eventuali richieste del cliente dirette ad estendere gli obblighi ad attività non compatibili con la natura del servizio e delle predette attività.*

2.2 È sempre necessario prevedere il ruolo di responsabile per la software house quando il software è erogato in modalità cloud saas?

Risposta - *Sì, contrariamente al vigente Codice sulla privacy che stabilisce la facoltà per il titolare di nomina del responsabile, il GDPR prevede che il soggetto che svolge le attività di trattamento dei dati per conto del titolare, come avviene di regola nell'ambito della fornitura di un servizio (es.: erogazione di un software in modalità cloud saas), sia da considerare comunque quale responsabile del trattamento, non avendo d'altronde il responsabile (nella specie, la software house) alcun potere decisionale in ordine alle finalità del trattamento e non potendo utilizzare i dati personali di titolarità del cliente per proprie autonome finalità.*
Si ricorda inoltre che, nel ruolo di responsabile, la software house non è tenuta ad adempiere ad una serie di obblighi anche verso gli interessati (come, ad es., l'informativa e la richiesta del consenso) per il trattamento dei dati personali conservati presso le proprie infrastrutture, obblighi che rimangono in capo al cliente quale titolare del trattamento.

2.3 L'art. 28, comma 2 del GDPR prevede che il responsabile del trattamento non possa ricorrere ad un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare. Nel caso di autorizzazione generale, è comunque necessario informare il titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili, dando così al titolare la possibilità di opporsi a tali modifiche. Il requisito della specifica indicazione del sub-responsabile richiede necessariamente la indicazione nominativa dello stesso (es. Il titolare prende atto e acconsente sin d'ora che il responsabile si avvalga, per l'esecuzione dei servizi, dei servizi di data center forniti da Microsoft presso la server farm sita in XYW, etc.), o è possibile fare riferimento a categorie di fornitori e localizzazioni geografiche in termini più generali (es. Il titolare prende atto e acconsente sin d'ora che il responsabile sia avvalga, per l'esecuzione dei servizi, di un fornitore di servizi di data center con server localizzati nel territorio dell'Unione Europea)?

Risposta - *Quando l'autorizzazione preventiva del cliente quale titolare è espressa in termini generali potrebbe essere riferita a categorie di titolari ed, ove possibile rinviare ad un elenco aggiornato di subresponsabili della software house, la quale dovrà eventualmente informare il titolare di eventuali aggiunte o sostituzioni di tali subresponsabili, in modo di permettergli di opporsi a tali modifiche.*

Il Gruppo di Lavoro ritiene auspicabile che l'art. 28 possa essere interpretato nel senso di considerare legittime anche le autorizzazioni preventive rilasciate dal cliente finale per categorie di subfornitori senza indicazione specifica delle loro denominazioni (ferma la possibilità per il cliente di richiedere alla software house ulteriori informazioni in proposito), al fine di rendere meno oneroso sul piano operativo l'adempimento dell'informativa degli eventuali cambiamenti e assicurare, in prima battuta, la protezione di informazioni strategiche e coperte da riservatezza commerciale per la software house. A tale proposito, il GdL ritiene inoltre che dovrebbe essere evidenziata la differenza tra soggetti che forniscono prodotti e/o servizi infrastrutturali senza legame specifico con il singolo contratto cliente (es. Microsoft, Google, ecc…) e soggetti che sono invece coinvolti direttamente nel trattamento dei dati dello specifico Cliente e che quindi appartengono alla filiera del sub appalto (es. Subappaltatori, Partner, ecc.).

Resta invece ferma la possibilità per la software house di indicare in termini generali le localizzazioni dei subresponsabili per aree geografiche (facendo ad es. riferimento all'ubicazione in Paese della UE) e di dover scendere in un maggiore dettaglio solo qualora si tratti di soggetti che effettuino i trattamenti di dati personali con strumenti o sistemi ubicati in Paesi terzi al di fuori della U.E., ciò anche al fine di permettere una verifica dell'esistenza di condizioni e garanzie adeguate per il trasferimento di dati all'estero.

2.4 Per adempiere a quanto previsto dall'art. 28, comma 2 del GDPR, è possibile mantenere l'elenco nominativo aggiornato dei subfornitori operanti quali ulteriori responsabili, ad esempio in una sezione dedicata del sito internet, invitando i clienti a consultare periodicamente le suddette informazioni?

Risposta - *Sì, questa forma di comunicazione appare possibile, ma è consigliabile prevedere almeno l'invio di un avviso ai clienti sull'intervenuto aggiornamento dell'elenco, con aggiunta o sostituzione di sub responsabili.*

2.5 Sempre con riguardo all'art. 28 del GDPR, è possibile circoscrivere/limitare contrattualmente il diritto del titolare di opporsi all'aggiunta o sostituzione di sub-responsabili (es. limitarla ai soli casi in cui vi siano "ragionevoli motivi" connessi alla sicurezza)?

Risposta - *Sì, è possibile introdurre alcune cautele a livello contrattuale in modo da prevedere che l'eventuale opposizione del cliente quale titolare debba essere comunque motivata, in conformità anche con i principi di correttezza e buona fede nell'esecuzione dei contratti, facendo riferimento, per esempio, alla carenza oggettiva di requisiti e/o garanzie sufficienti del subresponsabile in materia di protezione e sicurezza dei dati personali.*

2.6 Considerato che spetta al cliente quale titolare disciplinare il rapporto con il responsabile del trattamento (anche se tipicamente la clausola viene inserita in modo "standardizzato" nei contratti di fornitura), che cosa accade se il committente non intende considerare il fornitore quale responsabile del trattamento, pur in situazioni in cui tale nomina sia necessaria (es. servizi di data center)?

Risposta - *Come detto, il GDPR non prevede per il titolare alcuna facoltà di nomina del responsabile, ma attribuisce di fatto il ruolo di responsabile al soggetto che, in base all'impostazione del rapporto o contratto, effettua il trattamento per conto del titolare. Mentre un responsabile del trattamento dei dati può essere considerato come titolare solo laddove determini autonomamente finalità e mezzi di tale trattamento (v. l'art. 28, comma 10).*

2.7 È corretto ritenere che nel caso descritto al precedente punto 2.6 (fornitore che esegue un trattamento per conto del titolare, pur in assenza di una specifica attribuzione del ruolo di responsabile e conseguente disciplina contrattuale), il fornitore che accetti comunque di eseguire il servizio possa essere ritenuto esso stesso "titolare del trattamento", e come tale tenuto ad adempiere ai relativi obblighi anche, ad es., di informativa agli interessati?

Risposta - *Si richiamano le osservazioni di cui al punto precedente. L'operatività sopra descritta costituirebbe una violazione del GDPR, con conseguente possibile applicazione di rilevanti sanzioni pecuniarie a carico del titolare del trattamento. In casistiche di questo tipo, pertanto si rende necessario prevedere a livello contrattuale specifiche garanzie e manleve per il fornitore, con esclusione della necessità di adempimento di eventuali obblighi facenti capo al committente e con conferma della loro idoneità a coprire anche l'attività richiesta al fornitore.*

2.8 Una volta riviste le vecchie lettere di nomina a responsabile del trattamento per adeguarle nella forma e nei contenuti del GDPR, è opportuno richiedere la loro accettazione anche ai clienti preesistenti? In caso affermativo, quali sarebbero le modalità di accettazione necessarie?

Risposta - *Sì, è necessario sottoporre le nuove clausole contrattuali o contratti/accordi in relazione alla disciplina degli obblighi del fornitore quale responsabile del trattamento (scambiati pure per corrispondenza, come le precedenti lettere), anche ai clienti preesistenti (ove il rapporto perduri al 25 maggio 2018, data di entrata in vigore del GDPR e non vi siano stati rinnovi o modifiche prima).*
Posto che non dovrebbe trattarsi di contratti per i quali è richiesta la forma scritta, ove si tratti di documenti in formato elettronico, possono essere utilizzate modalità semplificate di accettazione anche "on line" (es. point & click con cristallizzazione dei log di accettazione), ove questa sia la prassi normalmente seguita con il cliente anche per altre variazioni contrattuali.

2.9 Con le modifiche introdotte dal GDPR, continuerà a esistere la figura del responsabile "interno" del trattamento?

Risposta - *No, nell'ambito del GDPR la definizione di "responsabile del trattamento" appare riconducibile e utilizzabile solo nei confronti di soggetti esterni all'organizzazione del titolare (posto che i responsabili sono tenuti a tenere un proprio registro dei trattamenti, a nominare eventualmente un DPO, ecc.). Resta ferma la possibilità di mantenere forme di delega e sub-delega interne al Titolare per l'attuazione degli obblighi normativi, ma tali figure di "delegato" non sarebbe inquadrabile in quella del Responsabile ex art. 28 (GDPR), con conseguente inapplicabilità dei relativi obblighi, come sopra ricordati (es. tenuta del Registro dei trattamenti).*

2.10 E quella dell'incaricato? Nel caso di sub-affidamento di parte del trattamento a persone fisiche esterne all'organizzazione i (es. lavoratori autonomi, consulenti, partner), è sufficiente fornire a tali soggetti istruzioni (riconducendoli alla figura di "*incaricati*") o è sempre necessario nominarli come sub-responsabili (con conseguente necessità di chiedere l'autorizzazione del cliente/titolare)?

Risposta - *Sì, anche se il GDPR non prevede la definizione formale di "incaricato", permangono gli obblighi di individuare le "persone autorizzate" a trattare i dati sotto l'autorità del titolare o del responsabile del trattamento e di impartirgli adeguate e documentate istruzioni, anche in tema di sicurezza dei dati, nonché di garantire il loro impegno a mantenere la riservatezza sui dati di cui vengono a conoscenza. Per quanto riguarda l'affidamento di attività a persone fisiche esterne all'organizzazione della software house (es. consulenti a partita IVA o dipendenti di Fornitori), è possibile inquadrarli come "incaricati" o "persone autorizzate" in tutti i casi in cui, dal punto di vista operativo, svolgano tali attività sotto l'autorità della software house (ossia, ad es., quando operino presso le relative sedi, sotto comunque la vigilanza di responsabili/referenti di quest'ultima, ecc.), mentre appare più difficile applicare tale impostazione per soggetti che operano in modo autonomo e in ambiti esterni rispetto ai quali la*

software house non sia in grado di esercitare un effettivo controllo (in quest'ultima ipotesi, sarebbe meglio procedere eventualmente a considerarli quali subresponsabili).

2.11 L'art. 37, comma 1, lett. c) riporta: "*Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta* ***le attività principali*** *del titolare del trattamento o* ***del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali*** *di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10…".* Nel caso di trattamenti che abbiano ad oggetto dati sensibili eseguiti in qualità di responsabile per conto di un titolare, il fornitore che eroga il servizio rientra in questa casistica? Ad esempio, un'azienda che eroga servizi di elaborazione paghe mediante un software in SaaS per un elevato numero di clienti, risulta per ciò solo tenuta alla nomina del DPO?

Risposta - *Il Gruppo di lavoro ritiene che non possa essere data un risposta generalizzata per tutti i servizi, in quanto, come indicato anche nelle linee guida sul DPO del Gruppo Art. 29, va valutato caso per caso, a seconda del servizio/prodotto, se il trattamento di dati sensibili possa rientrare o meno nella nozione di "attività principali", ovvero costituisca un componente inscindibile per la fornitura del medesimo servizio (che ove erogato ad un numero elevato di clienti sul territorio nazionale può sicuramente configurare il requisito del "larga scala").*
E' possibile dunque escludere l'obbligo di nomina del DPO per la fornitura del software "on premise" e i correlati servizi tecnici di assistenza o manutenzione, mentre occorre procedere ad una più attenta verifica della tipologia dei servizi erogati in modalità cloud saas, come l'elaborazione paghe e anche la conservazione sostitutiva, che includono necessariamente per gli adempimenti amministrativi gestiti per conto del titolare e in modo non meramente occasionale/incidentale il trattamento di dati sensibili (riguardo, ad es., alle assenze per malattie dei dipendenti o alla trattenuta in busta paga per versamento ad organizzazione sindacale di appartenenza), che, in considerazione del numero e dimensioni di clienti, potrebbero rendere possibile nell'ambito del cloud saas di una software house, un trattamento di dati sensibili su larga scala .
Anche su questo profilo il Gruppo di Lavoro auspica che sia comunque possibile prevedere semplificazioni e riduzione degli oneri soprattutto per le piccole e medie software house, tuttavia, sentito anche il Garante sul punto ritiene che, in assenza di ulteriori indicazioni, sia comunque consigliabile per i Produttori di Software prevedere un DPO.
Il Gruppo di lavoro suggerisce di valutare comunque l'opzione per i casi sopra evidenziati di prevedere la designazione di un DPO nell'ambito dell'associazione di categoria rappresentante le software house responsabile del trattamento (es.: Assosoftware potrebbe offrire un servizio di DPO agli associati, soprattutto ove si tratti di pmi).

3. Informativa e Consenso

3.1 Il GDPR prescrive che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di modulistica (che, ad es., può essere utilizzata da una software house quale titolare nei confronti dei clienti per legittimare l'uso dei loro dati a fini di marketing. Alla luce di tali indicazioni, quali possono essere delle valide modalità di acquisizione di un consenso nel contesto della stipulazione di un contratto con l'interessato?

Risposta *- I requisiti dell'informativa e del consenso rimangono sostanzialmente identici a quelli previsti dalla normativa attualmente vigente in Italia e dai provvedimenti del Garante in materia. L'informativa privacy deve essere chiara e sintetica e agevolmente individuabile e leggibile per gli interessati nel corpo di un contratto, modulo o form o in un separato o apposito documento a cui può rinviarsi. Per quanto riguarda le modalità di acquisizione del consenso, fermi i casi di esclusione (ove il trattamento sia necessario per l'esecuzione del contratto e l'adempimento di obblighi legali), occorre prevedere una specifica dichiarazione od opzione da valorizzare o firmare per l'espressione del consenso privacy, ove necessario (ad esempio per finalità di marketing), separata dalle altre dichiarazioni od opzioni relative all'accettazione del contratto.*

3.2 Con riferimento ai casi in cui la software house operi quale titolare del trattamento dei dati (riferiti ad es. a clienti persone fisiche), ci sono novità apportate dal GDPR in merito alle modalità di acquisizione del consenso on-line? In particolare, è possibile l'accettazione tramite "point & click" o tramite altri comportamenti positivi dell'utente (es. chiudere una finestra, proseguire la navigazione, cliccare "ok").

Risposta *- Sì, per i dati personali comuni il consenso può essere espresso in modo inequivocabile (quindi anche attraverso un'azione o comportamento positivo dell'interessato purché correlata chiaramente e univocamente ad una ben precisa finalità di trattamento dei dati), mentre per i dati sensibili deve essere comunque esplicito, restando però per il titolare l'obbligo di dimostrare di averlo acquisito, attraverso idonea documentazione, anche attraverso modalità point & click o analoga (v. considerando 32 e art. 7 del GDPR).*

3.3 Nel caso di trattamenti di dati personali per cui occorre il consenso (es. sensibili o ad eseguire le profilazioni), il fornitore esterno che agisce come responsabile del trattamento per conto del Titolare può pattuire contrattualmente che il titolare assolva gli obblighi di informativa e richiesta di consenso degli interessati? In altre partole, il Responsabile è tenuto ad ottenere in proprio il consenso espresso degli interessati o il consenso dato per quella finalità al Titolare basta ad autorizzare il Responsabile al trattamento?

Risposta *- Si conferma che il Responsabile possa omettere di informare gli interessati e raccoglierne il consenso essendo peraltro opportuno prevedere opportune tutele contrattuali al riguardo (in quanto si tratta di adempimenti spettanti al cliente quale Titolare).*

3.4 I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del GDPR e in parte sono più ampi rispetto al Codice privacy, richiedendo l'indicazione di alcuni nuovi elementi (dati di contatto del RPD-DPO, ove esistente, **base giuridica** del trattamento, eventuale **interesse legittimo** perseguito dal titolare, eventuale trasferimento di dati in Paesi terzi extra UE e, in caso affermativo, relativi strumenti, periodo di conservazione dei dati, diritto di presentare un reclamo all'autorità di controllo, eventuale presenza di processi decisionali automatizzati, inclusa la profilazione). In particolare, cosa si intende per base giuridica del trattamento e se si può far riferimento in proposito a disposizioni normative, contratti, ecc.? Se sì, è corretto ritenere che sia sufficiente il generico riferimento ai "rapporti contrattuali" o alla normativa in essere (senza puntuale indicazione dei relativi riferimenti)?

Risposta - *Il Gruppo di lavoro ritiene che, in genere, non è necessario specificare gli estremi delle norme di riferimento, ma è sufficiente l'indicazione che il trattamento è effettuato sulla base del contratto in essere con l'interessato e dei correlati obblighi normativi, ove di natura amministrativa e contabile. E' opportuno però che, dal contesto, sia sufficientemente evincibile l'oggetto e natura del rapporto contrattuale (utilizzando eventualmente un riferimento al tipo di contratto o settore di riferimento) ed, ove si faccia riferimento anche a specifici e ulteriori adempimenti normativi, sia ricavabile almeno l'ambito normativo di riferimento (es.: in materia antiriciclaggio).*

3.5 In caso di acquisizione di dati preventivamente anonimizzati da parte di terzi (es. clienti), possiamo utilizzarli liberamente per altre finalità (es. demo) senza alcun consenso del titolare/cliente e senza avviso? E se procediamo noi all'anonimizzazione, dobbiamo informare il titolare? In che modo?

Risposta - *Nel primo caso, se i dati sono acquisiti in forma effettivamente anonima, si è al di fuori dell'ambito di applicazione della normativa in materia di dati personali. Nel secondo caso, laddove è la software house a procedere all'anonimizzazione dei dati personali (che costituisce comunque un'operazione di trattamento) occorrerà comunque informare il cliente e farsi autorizzare in merito a tale utilizzo dei dati (l'autorizzazione del cliente potrebbe risultare necessaria anche per altre profili legali non attinenti alla privacy, ma riguardanti ad es. i possibili diritti in materia di proprietà intellettuale sulla base dati).*
In proposito, è consigliabile e comunque opportuno prevedere, a livello contrattuale, specifiche clausole volte ad evitare eventuali contestazioni da parte del titolare del trattamento.

4. Valutazione del rischio e valutazione di impatto privacy:

4.1 Quali differenze metodologiche esistono tra la valutazione del rischio privacy e la valutazione di impatto privacy?

Risposta - *L'analisi o valutazione dei rischi privacy (ossia dei rischi che un trattamento, per le sue caratteristiche, può presentare per i diritti degli interessati) è un'attività o procedura volta ad individuare il livello di rischiosità dei trattamenti dei dati personali, con particolare riguardo alla gravità e probabilità dei danni di varia natura che, in teoria, tale trattamento, per il tipo di dati, di operazioni effettuate o di tecnologie utilizzate, potrebbe causare agli interessati sotto il profilo del diritto alla riservatezza e di altri diritti della persona.*
Di regola è un'attività che serve per individuare i trattamenti ad "elevato rischio" su cui svolgere la valutazione di impatto privacy e, più in generale, per valutare l'adeguatezza delle misure tecniche, organizzative e di sicurezza per garantire la conformità al GDPR.
La valutazione dei rischi privacy costituisce inoltre una parte rilevante anche della valutazione d'impatto privacy solo nei confronti dei trattamenti di dati ad "elevato rischio" (e non di tutti gli altri per i quali non emergono rischiosità di questo tipo) e una procedura che comprende l'esame e analisi anche di altri aspetti riguardanti, tra l'altro, la proporzionalità e necessità del trattamento rispetto alle finalità perseguite, le misure previste, anche sotto il profilo della sicurezza, e in relazione agli adempimenti posti in essere a garanzie degli interessati (informativa, consenso, diritti, ecc.).

4.2 La valutazione del rischio privacy deve essere effettuata in tutte le realtà che trattano dati?

Risposta - *Di regola si anche se deve essere finalizzata principalmente ad individuare i trattamenti "rischiosi" per i quali vanno innalzati il livello di presidi e accorgimenti, ferme restando le specifiche analisi dei rischi per la sicurezza informativa già svolte in azienda. Si ricorda che il GDPR prevede infatti un approccio basato sul rischio per l'adempimento di diversi obblighi anche in tema di sicurezza (v. l'art. 32 applicabile anche al responsabile del trattamento), consistenti nell'adozione di misure tecniche e organizzative adeguate in base alla rischiosità del trattamento.*

4.3 È corretto affermare che è necessario procedere alla valutazione di impatto privacy solo se dalla valutazione del rischio si evidenziano rischi specifici? I due procedimenti di valutazione possono essere descritti in un unico documento o bisogna procedere con valutazioni separate?

Risposta - *Sì, come detto, la valutazione d'impatto è obbligatoria solo nei confronti dei trattamenti ad "elevato rischio". La valutazione dei rischi privacy è in genere una parte obbligatoria della valutazione d'impatto che, come detto, deve essere effettuata dal titolare (cliente), eventualmente con l'assistenza del responsabile (software house o fornitore) che per la specifica prestazione potrà prevedere anche un compenso.*

4.4 Qualora a seguito della valutazione di impatto risulti la presenza di un rischio residuale elevato, in caso di incertezza ci si potrà rivolgere all'autorità di controllo?

Risposta - *Sì, come la valutazione d'impatto, in tali casi la consultazione preventiva dell'autorità di controllo (il ns. Garante) è obbligatoria per il titolare del trattamento e il responsabile che, alle condizioni economiche concordate, può essere chiamato, per quanto di competenza, ad assistere il titolare in tale procedura che prevede in prima battuta il rilascio di un parere o eventualmente anche l'esercizio dei poteri di indagine, correttivi, ecc. da parte dell'Autorità nei termini indicati all'art. 36 del GDPR.*

4.5 In considerazione di quanto previsto dalle recenti linee guida del Gruppo Art. 29 in materia di valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment* o *DPIA* - WP248), è possibile che tutti i produttori di software per gli stessi servizi che erogano facciano la stessa valutazione d'impatto? O utilizzino la stessa metodologia?

Risposta - *Sì, in linea di massima, è stato confermato che è possibile per i titolari utilizzare un'unica DPIA per valutare più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. In caso, per esempio, di nuovi prodotti hardware o software, impiegabili da titolari diversi è possibile utilizzare la stessa metodologia o anche DPIA da parte di più fornitori purché i prodotti software abbiano le stesse caratteristiche nei termini sopra ricordati.*

4.6 Il principio di Privacy by design, secondo cui i prodotti devono tenere conto dei requisiti previsti dalla normativa privacy sin dalla loro progettazione, ha delle ricadute anche sui prodotti già presenti sul mercato (fermo restando che l'art. 25 pone obblighi a carico del titolare e non dell'azienda produttrice del software)?

Risposta - *Il GdL ritiene che la Privacy by design sia un concetto che riguarda il processo di progettazione e sviluppo di una nuova soluzione applicativa (non di applicativi esistenti, già in uso da parte dei clienti) e comunque trattasi di obblighi che ricadono sul titolare che quindi è sempre responsabile, al momento dell'acquisizione di un nuovo prodotto/servizio, di verificare e integrare le misure adeguate, per rispettare il GDPR.*

4.7 È necessario/opportuno in vista dell'entrata in vigore del GDPR procedere alla revisione di tutti i contratti standard allo scopo di assicurarne la *compliance* alla nuova normativa?

Risposta - *Sì, il Gruppo di lavoro ritiene che la revisione dei contratti sia necessaria e comunque utile.*

5. Diritti dell'interessato

5.1 Il titolare deve dare riscontro agli interessati gratuitamente. Il Responsabile del trattamento deve supportare il titolare nel riscontro all'interessato. Mentre nel caso del Titolare è specificato che le informazioni devono essere rese gratuitamente, salvo casi particolari, nel caso del Responsabile/fornitore è possibile pattuire contrattualmente degli oneri per le spese sostenute in relazione alle attività svolte per conto del Titolare?

Risposta - *In base all'art. 28 del GDPR, deve essere previsto contrattualmente che il responsabile assista il titolare con misure tecniche e organizzative adeguate per dare riscontro alle richieste degli interessati ed è chiaro che questo impegno e le spese correlate potrà essere oggetto di quotazione nell'ambito dei complessivi compensi pattuiti per le attività oggetto del contratto.*

5.2 L'art. 17 ("*diritto all'oblio*") consente all'interessato il diritto di ottenere la cancellazione dei dati personali quando non ci sia più motivo per conservarli. Con riguardo a dati storici contenuti sui backup, cosa comporta l'applicazione di tale diritto? Sarà necessario implementare anche procedure di cancellazione nell'ambito delle policy di backup?

Risposta - *In realtà, sotto questo profilo, non ci sono particolari cambiamenti e viene confermato il diritto di cancellazione dei dati che non è necessario conservare ulteriormente per le finalità perseguite, come già previsto dall'art. 7, comma 3, lett. b), del Codice privacy. Resta fermo che se la richiesta di cancellazione dei dati è formulata in termini generali e non con riferimento a specifici sistemi o archivi, in tal caso occorrerà implementare procedure per la cancellazione dei dati anche sui backup. A tal proposito il Gruppo di Lavoro ritiene che debbano essere previste alcune deroghe qualora il processo di individuazione e cancellazione dei dati dai supporti di backup sia particolarmente difficile e oneroso e comporti costi significativi per il Titolare e per il Responsabile. (Ad esempio su un unico backup possono essere memorizzati più db o file di più clienti che sono salvati come unico salvataggio; altro esempio è che le richieste di cancellazione riguardano gli interessati che sono salvati nei backup insieme ai dati di tanti altri interessati a cui la software house non può accedere in quanto il servizio riguarda la semplice conservazione dei dati e non la visualizzazione, la modifica etc. In sostanza il backup è rivolto per i servizi che eroghiamo non a conservare i dati dei singoli interessati bensì i dati dei clienti considerati come unità a cui la sw house non può accedere ma deve solo ripristinare per motivi di sicurezza in caso di necessità. Per questo motivo e per come sono fatti oggi i sistemi di backup, che spesso non salvano i dati ma immagini di dischi, non è possibile prevedere una cancellazione puntuale di un singolo dato personale di una o più tabelle di un db o di un file).*

5.3 L'art. 20 ("*diritto alla portabilità dei dati*") offre all'interessato il diritto di trasferire i propri dati tra diversi fornitori. Il trasferimento di tali dati potrà avvenire anche su formato aperto? È necessario prevedere nel contratto standard un nuovo servizio di export dei dati?

Risposta - *Il diritto alla portabilità può essere esercitato dagli interessati nei confronti del titolare del trattamento (cliente) solo nei casi in cui i dati siano stati forniti direttamente dall'interessato e trattati elettronicamente sulla base del consenso o di un contratto con l'interessato (ad esempio, il diritto alla portabilità non è quindi esercitabile nei confronti dei dati contenuti nelle paghe elaborate tramite i software dei fornitori).*
Nei casi in cui ricorrano le suddette condizioni, la trasmissione dei dati può avvenire su un formato di uso comune, strutturato e leggibile da qualsiasi dispositivo che garantisca massima interoperabilità, come indicato anche dalle linee guida sul tema del Gruppo art. 29 (WP242).
È pertanto opportuno che le software house chiamate quali responsabili a supportare i titolari nel riscontro alle richieste di esercizio di tale diritto, ove applicabile, si attrezzino per poter fornire ai clienti i servizi e le funzionalità necessarie in proposito ed è chiaro che questo impegno e le spese correlate potranno essere oggetto di quotazione nell'ambito dei complessivi compensi pattuiti per le attività oggetto del contratto.

6. Misure di sicurezza

6.1 Quando un dato può dirsi effettivamente "anonimo" o "anonimizzato"? È possibile fare qualche esempio di procedura di anonimizzazione sicura.

Risposta - *A differenza della cifratura e della pseudonimizzazione dei dati personali, che sono considerate delle robuste misure di sicurezza da applicare in relazione, ad es., a trattamenti "ad elevato rischio", l'anonimizzazione è una procedura che, attraverso non solo l'eliminazione dei dati identificativi, ma anche l'aggregazione o generalizzazione degli altri dati personali (ad es., raggruppati per età anziché per data di nascita, per area geografica anzichè per indirizzo di residenza, per variabili o dati riferibili a gruppi, classi o insiemi di persone, dipendenti, utenti ecc.), rende impossibile risalire all'identità delle persone a cui si riferiscono o ri-associare in tutto o in parte, anche a posteriori, i dati o informazioni trattate a singole persone. Sul punto si richiama il parere del Gruppo art. 29 sulle tecniche di anonimizzazione (WP126)*

6.2 Molti clienti in vista dell'entrata in vigore del GDPR chiedono che il prodotto consenta di tracciare tutte le operazioni/audit svolte dagli incaricati/utenti (non solo amministratori di sistema), producendo e conservando adeguati log. Tale richiesta è legittima? O dipende dalla natura del dato?

Risposta - *Il tracciamento degli accessi ai sistemi o delle operazioni effettuate dagli incaricati o utenti è da sempre considerato una preventiva ed idonea misura di sicurezza al fine di prevenire il rischio di accessi non autorizzati o trattamenti non consentiti (ad es., oltre che per gli amministratori di sistema, il tracciamento è già previsto per diversi sistemi utilizzati nel settore delle comunicazioni elettroniche, in ambito sanitario, nelle banche, ecc.).*
Alla luce dei principi di accountability e risk-based approach di cui al GDPR, è chiaro quindi che tale misura può quindi risultare sicuramente adeguata in base alla rischiosità del trattamento dei dati personali che si intende presidiare e particolarmente utile anche nell'ottica di monitorare eventuali data breach. Ma, rispetto alla richiesta di implementazione di tale misura, è comunque necessario contemperare l'esigenza di sicurezza dei trattamenti di dati personali con i limiti in materia di controlli a distanza dei lavoratori previsti dallo statuto dei lavoratori, che richiamano anche i principi della normativa privacy. Per cui, è da escludere a priori la possibilità di un tracciamento generalizzato in relazione a mere esigenze di protezione dati ed occorre ogni volta verificare quale sia l'ambito e livello del possibile tracciamento in relazione alle finalità perseguite dal cliente, i tempi di conservazione dei log, modalità di controllo, soggetti che possono accedervi, adempimenti nei confronti dei dipendenti/utenti interessati, ecc.