Anno 3 - Numero 3 - Ottobre 2018

ASSOSOFTWARE 24

PERIODICO DI INFORMAZIONE DELL'ASSOCIAZIONE NAZIONALE PRODUTTORI DI SOFTWARE GESTIONALE E FISCALE

VISTO DAL PRESIDENTE

GDPR: il produttore di software non è il titolare del trattamento dei dati

*di Bonfiglio Mariotti**

Sono passati poco più di quattro mesi dal 25 maggio 2018, data dalla quale è pienamente applicabile il GDPR (General Data Protection Regulation), ovvero il nuovo Regolamento Europeo per la Privacy, e con esso i relativi obblighi in capo a imprese e soggetti pubblici. In questo numero di AssoSoftware24 facciamo il punto sulle attività che i Produttori di Software e l'Associazione che li rappresenta hanno svolto in questi mesi per accompagnare aziende e clienti sull'adeguamento degli strumenti software e dei processi a essi correlati.

Il nuovo regolamento Europeo, pur essendo particolarmente innovativo in alcuni ambiti e, in particolare, per quei Paesi dell'Unione ancora senza un proprio Codice Privacy, non stravolge invece l'impianto normativo delle nazioni, Italia compresa, in cui da tempo era in vigore una regolamentazione della gestione dei dati personali già avanzata.

Chiariamo subito che il produttore di software non potrà mai essere considerato titolare del trattamento, non potendo lo stesso definire le specifiche finalità per cui i dati sono trattati; casomai, come leggerete sotto, al produttore spettano quasi sempre gli obblighi previsti per il responsabile del trattamento dei dati. Ciò premesso, il produttore effettuerà sui prodotti software gli adeguamenti e gli interventi che riterrà più opportuni per renderli compliant *al GDPR, senza alcun obbligo specifico; sarà sempre cura del cliente, in qualità di titolare del trattamento dei dati, verificare se l'applicativo acquistato risponde alle proprie esigenze; qualora questo non si verificasse, secondo le regole contrattuali, potrà eventualmente recedere dal contratto e scegliere un altro prodotto. Rimane inteso che il cliente potrà chiedere al proprio fornitore, concordando uno specifico compenso, ulteriori modifiche e adeguamenti.*

** Presidente AssoSoftware e Chairman Bluenext*

Da AssoSoftware linee guida e best practice per le software house

di Roberto Bellini Direttore Generale AssoSoftware

Per presidiare questo importante settore, AssoSoftware, da circa un anno, ha costituito uno specifico gruppo di lavoro GDPR (GdL) che si occupa di "data protection" e che ha il compito di definire linee guida e best practice a favore delle aziende associate e dell'intero mercato. L'attività viene svolta con periodici incontri tra le aziende associate, con l'ausilio di esperti di settore e con il confronto continuo con i rappresentanti dell'Authority Garante. Il primo documento prodotto dal GdL, già pubblicato sul sito dell'Associazione, riguarda una raccolta di domande e risposte (FAQ) sul nuovo GDPR contenente indicazioni di grande utilità per tutti i produttori di software per affrontare correttamente l'adeguamento dei propri applicativi e per rispondere nel migliore dei modi alle richieste provenienti dai propri clienti. Il documento FAQ affronta diverse problematiche tecniche e procedurali di grande interesse, dando per ciascuna il punto di vista autorevole dell'Associazione. Esaminiamo alcuni punti, mentre per un maggior approfondimento vi invitiamo a consultare il documento integrale sul sito AssoSoftware.

REGISTRO DEI TRATTAMENTI

Sono da poco giunte dal Garante indicazioni per la tenuta del Registro dei trattamenti che confermano quanto già comunicato da AssoSoftware. Infatti il GdL ritiene che lo stesso possa essere gestito in forma elettronica e modulare, rimandando a schede e archivi anagrafici separati con appositi riferimenti. Così anche la tipologia dei trattamenti si valuta che possa essere elencata in forma schematica per ciascun prodotto/servizio erogato dalla software house. Si ritiene inoltre che il Registro possa essere mantenuto sempre nella versione aggiornata, senza la necessità di storicizzare le variazioni intervenute nel tempo. Per i prodotti/servizi paghe e stipendi sembra possibile organizzare un registro "virtuale" che attinga informazioni sia dall'anagrafica dei clienti della software house, sia dall'archivio dei prodotti/servizi opportunamente arricchito dei trattamenti correlati. In merito all'obbligo o meno per i produttori di software di provvedere alla redazione del Registro dei Trattamenti, considerato l'art.30 c.5 del GDPR, il GdL reputa che sarebbe opportuno procedere in tal senso qualora il Produttore sia anche Responsabile del Trattamento dei dati forniti dai propri clienti.

"Il registro dei trattamenti è il punto di partenza di qualunque sistema di gestione della privacy e ne è assolutamente raccomandata l'adozione, a prescindere dalle dimensioni aziendali o dalla rischiosità dei trattamenti"

Anna Paola Lenzi - Dpo in Teamsystem

RESPONSABILE DEL TRATTAMENTO DEI DATI PER PRODOTTI "CLOUD" O "ON PREMISE"

Con il nuovo GDPR il soggetto che raccoglie ed elabora dati di terzi assume automaticamente il ruolo di "Responsabile del trattamento", anche nel caso in cui i dati siano trasmessi per sola attività di assistenza, verifica o migrazione. Per tale motivo si ritiene che normalmente il Produttore che eroga anche assistenza sui prodotti

>> continua a pag. 7

IN QUESTO NUMERO

LA PAROLA AL GARANTE

Nuova Privacy: per il Titolare l'accento è sull'accountability

di Cosimo Comella - Dirigente del Dipartimento Tecnologie digitali e Sicurezza informatica del Garante per la Protezione dei dati personali

Il quadro normativo della *privacy*, dominato per un ventennio dalla Direttiva 95/46/CE[1] che introdusse a livello comunitario la protezione dei dati personali, e che attivò negli Stati membri dell'Unione europea i diversi (e molto variegati) percorsi per il suo recepimento negli ordinamenti nazionali degli Stati membri, ha lasciato il campo, dal 2016, al nuovo Regolamento sulla protezione dei dati personali[2], universalmente noto con l'acronimo GDPR (*General data protection regulation*) ed entrato pienamente in vigore, con piena efficacia in tutta l'Europa comunitaria, dal 25 maggio di quest'anno.

L'esigenza di una nuova normativa scaturiva da diverse motivazioni, non ultima quella relativa alla difficoltà di cogliere con un testo di venti anni fa (quando la parola Internet non era mai stata ancora pubblicata, in Italia, da nessun quotidiano nazionale o quando era ancora agli albori, e limitata agli ambienti universitari e di ricerca, la diffusione della "rete delle reti", il *World Wide Web*), pur integrato dalla successiva direttiva *ePrivacy*[3] del 2002 su "*vita privata nel settore delle comunicazioni elettroniche*", le categorie, i concetti, le complessità derivanti dalla capillare diffusione di tecnologie dell'informazione che tanto influenzano, ormai, una larga parte del nostro agire quotidiano.

La nuova normativa europea presenta diverse innovazioni sotto molteplici profili connessi, da una parte, all'espansione dei diritti degli interessati (persone fisiche) e, dall'altra, all'ampliamento dei doveri in capo ai soggetti titolari o responsabili dei trattamenti: aspetti che non è possibile trattare esaurientemente in poche righe.

È possibile tuttavia evidenziare, in relazione soprattutto al ruolo degli operatori del settore *software* rispetto alla protezione dei dati, alcune peculiarità di un Regolamento che pone fortemente l'accento sul concetto di *responsabilizzazione*, termine con cui si è tradotto, senza renderne pienamente il significato, l'originale inglese *accountability*. L'*accountability* consiste nell'adozione di comportamenti *proattivi* e tali da poter dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano sul punto gli artt. 23-25, in particolare, e l'intero Capo IV del Regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nella norma. Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*" citata dall'art. 25 Gdpr per definire la necessità di predisporre i trattamenti prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati. Tali garanzie terranno conto del contesto complessivo in cui il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati che esso comporta. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono tradursi in una serie di attività specifiche e dimostrabili. Proprio l'applicazione dei principi di *data protection by default and by design* è di grande interesse per quei soggetti che, non partecipando necessariamente al trattamento, ne influenzano le caratteristiche e le modalità di svolgimento: il progettista o il produttore di *software* sono quindi fortemente coinvolti, ancorché non necessariamente giuridicamente responsabili riguardo alla protezione dei dati. A questo proposito è auspicabile che la produzione industriale del *software* integri nelle proprie metodologie di sviluppo, fin dalle fasi più precoci di progetto, la formulazione di vincoli e requisiti relativi alla protezione dei dati personali per assicurarne la possibilità di utilizzazione in conformità al Regolamento.

Fondamentali, inoltre, sono le attività connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari, ovvero il rischio inerente al trattamento. Questo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati, che dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano gli artt. 35-36 Gdpr) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi[4]. All'esito di tale valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigarne sufficientemente il rischio) ovvero consultare la *Supervisor Authority* competente per ottenere indicazioni sulla gestione del rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì quello di indicare le eventuali ulteriori misure e accorgimenti che il titolare dovrà prevedere e potrà, laddove necessario, adottare tutte le azioni correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trat-

1. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

2. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

3. Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

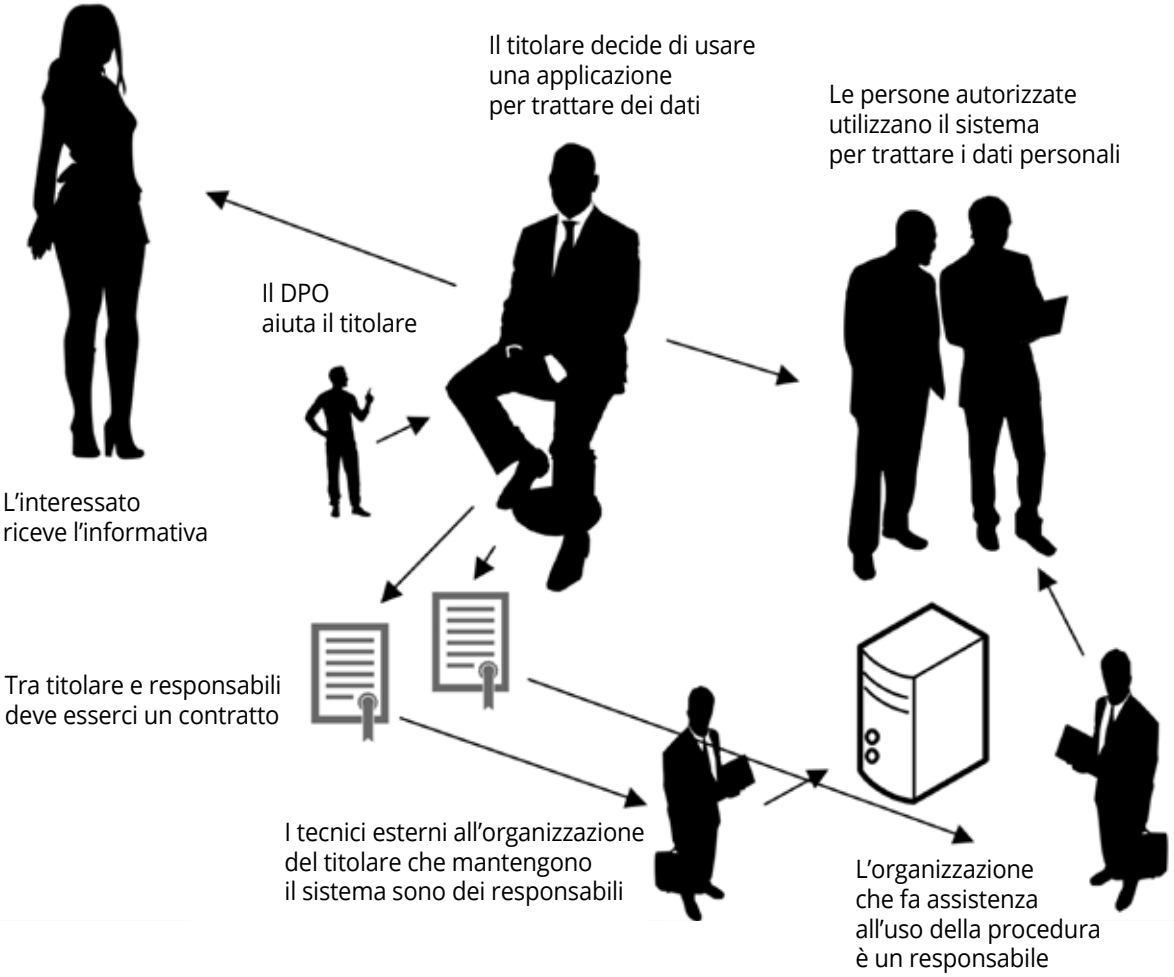
4. Si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo *Articolo 29*, qui disponibili: www.gpdp.it/regolamentoue/DPIA)

tamento. Dunque, l'intervento delle autorità di controllo sarà principalmente *ex post*, collocandosi successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notificazione preventiva dei trattamenti e il cosiddetto *prior checking* (Art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti e di effettuazione di valutazioni di impatto in piena autonomia, con eventuale successiva consultazione dell'Autorità (tranne alcune specifiche situazioni riguardanti lo svolgimento di compiti di interesse pubblico, di cui all'art. 36, paragrafo 5 del Regolamento). Peraltro, alle autorità di controllo, e in particolare al *Comitato europeo della protezione dei dati* (erede del Gruppo "*Article 29*") spetterà un ruolo fondamentale per garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre *linee-guida* e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

I ruoli nell'erogazione dei servizi on premise e cloud

LO SCENARIO "ON PREMISE"

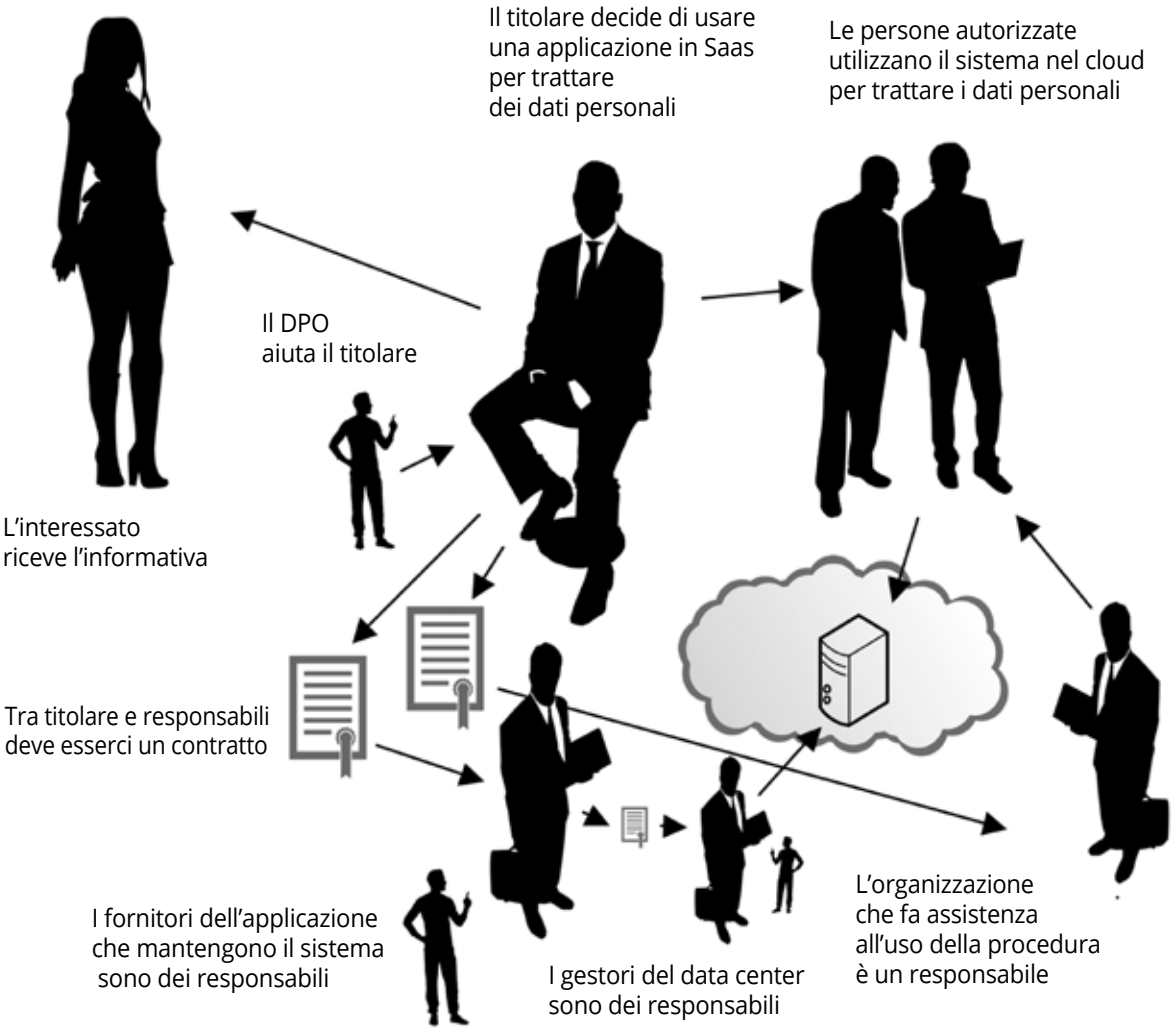
Il titolare gestisce i dati personali utilizzando una applicazione che viene installata nei suoi computer



Il titolare dovrà definire la finalità del trattamento e quindi i rischi derivanti dal trattamento. In questo compito sarà aiutato dal fornitore dell'applicazione, che dovrà comunicare al Titolare le misure di sicurezza implementabili nel software a garanzia di un trattamento sicuro. Le applicazioni poi si inseriscono in workflow aziendali che le estendono e le completano, il Titolare dovrà quindi valutare i rischi connessi con l'uso dei dati originati dall'applicazione e di tutti gli out put che ne derivano.
In questo scenario però è molto probabile che si aggiungano due importanti attori che possono accedere ai dati personali: le **persone che gestiscono l'applicazione ed i sistemi** su cui gira e **le persone che fanno assistenza a chi utilizza l'applicazione**.
Il titolare quindi si trova in questo caso ad avere due organizzazioni che opereranno sui suoi sistemi e che potenzialmente possono accedere ai dati personali. Queste aziende saranno dei responsabili che verranno legati al titolare da un contratto dove devono essere specificati i loro compiti e le misure di sicurezza che devono attuare.
È compito del titolare scegliere dei responsabili che diano adeguate garanzie sul trattamento dei dati. Le due strutture, che attraverso il contratto sono divenute responsabili del trattamento, dovranno a loro volta compilare il "registro dei responsabili" chiarendo quale ruolo svolgono nel trattamento e come prendono in carico la conformità al GDPR delle parti a loro affidate. Poiché si percepisce immediatamente che il fornitore dell'applicazione è quello che conosce meglio i dati trattati e le modalità con cui attivare le misure di sicurezza, il GDPR prevede che i responsabili possano aiutare il titolare a progettare la gestione del trattamento e a stilare i vari registri.

LO SCENARIO "SAAS"

Il titolare gestisce i dati personali utilizzando una applicazione erogata come servizio via Web



Dal punto di vista del GDPR per il titolare cambiano poche cose. Avrà ancora delle persone autorizzate che accedono all'applicazione e trattano i dati personali, vedrà il fornitore dell'applicazione e le persone che fanno assistenza come dei responsabili a cui affida dei compiti ben precisi e normati da un contratto.

Ci potrebbero però essere delle differenze: il fornitore potrebbe avvalersi di strutture esterne alla sua organizzazione per l'erogazione del servizio; nel caso "on premise" il produttore del software non trattava i dati del Titolare se non a seguito di richiesta dello stesso, nella soluzione "cloud" il gestore del servizio ha accesso a un enorme volume di dati personali, dato dall'unione di tutti i dati dei suoi clienti.

Nel primo caso il Fornitore dovrà verificare le misure di sicurezza che il fornitore del servizio di Data center garantisce nell'erogazione del servizio. Tali misure di sicurezza dovranno essere comunicate al Titolare in modo chiaro e preciso in modo che lo stesso possa decidere se le misure di sicurezza prospettate siano conformi rispetto alla sua valutazione dei rischi. Anche il fornitore dei servizi di Data center dovrà essere contrattualizzato e dovranno essere previste garanzie e responsabilità a tutela dei dati personali trattati.

Il secondo caso deve essere analizzato attentamente: il rischio che viene percepito dal titolare è più basso di quello che risulta dall'architettura gestita dal responsabile. Nel primo caso i dati sono quelli che raccoglie il titolare, che spesso non rientrano nei trattamenti su larga scala che prevedono ulteriori adempimenti specifici in capo al Titolare (ad esempio nomina DPO o esecuzione DPIA).

Il Fornitore ha concentrato tutti i dati di tutti i suoi clienti, creando così un "honeypot" per gli attaccanti che possono essere ingolositi dalla massa dei dati gestiti.

È evidente che un "data breach" dei soli dati di un singolo titolare, come nel caso "on premise", è molto meno pericoloso che non un "data breach" di una grande server farm.

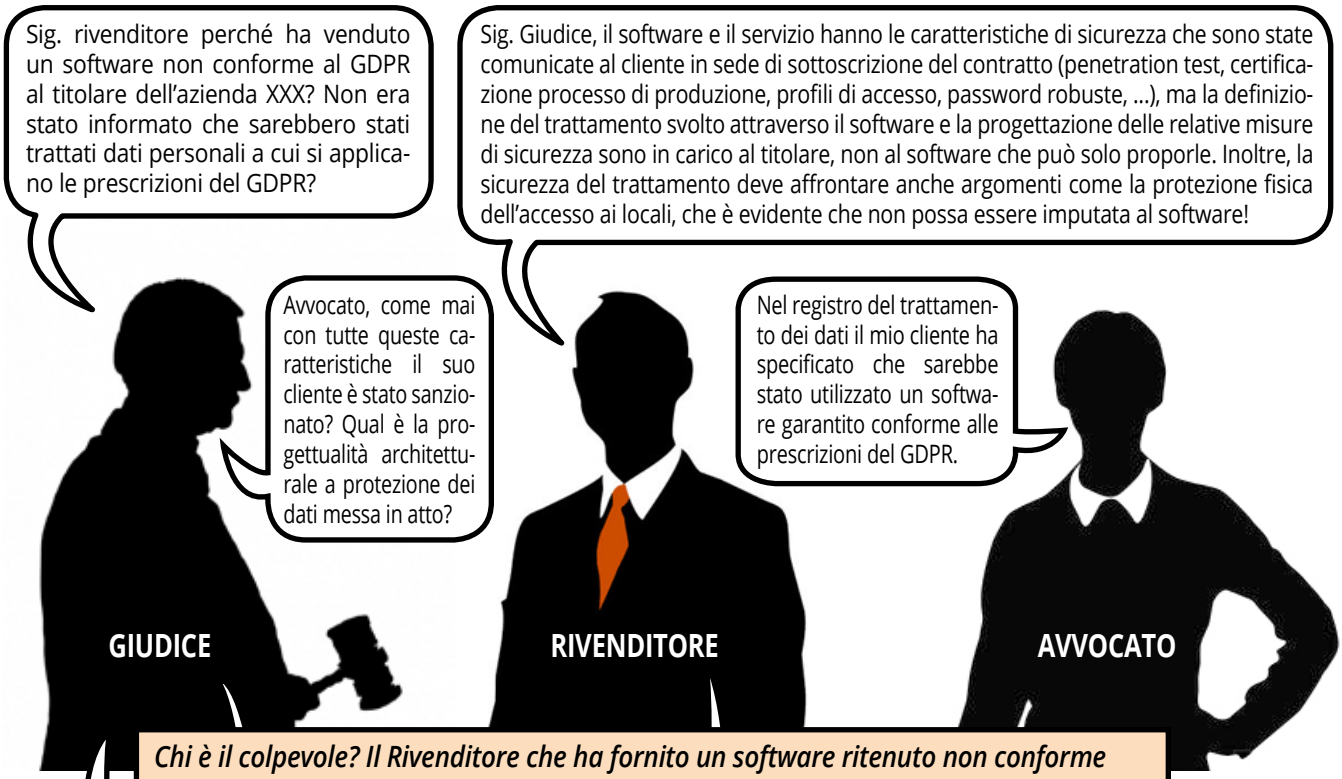
In questo caso il responsabile dovrà svolgere una propria valutazione dei rischi e addirittura valutare il caso in cui risulti a sua volta titolare di un trattamento che supera il trattamento che gli è stato affidato.

Qual è la responsabilità della Software house nell'erogazione dei servizi?

Il cliente ritiene che sia il software a dover essere conforme al GDPR, ma la legge prescrive che sia il cliente/Titolare del trattamento a progettare il trattamento.

UN CASO ESEMPLARE: SOFTWARE NON CONFORME?

Il cliente, titolare dell'azienda XXX, è stato sottoposto a procedimento sanzionatorio a seguito di una segnalazione per trattamento illecito del dato.
Il cliente chiede di essere risarcito dal rivenditore che, secondo lui, ha venduto un software non conforme al GDPR.



Chi è il colpevole? Il Rivenditore che ha fornito un software ritenuto non conforme o il Titolare che non ha attivato le misure di sicurezza?

Dove veniva utilizzato? Chi aveva accesso alla sala server? Che protezione avete messo in atto per i backup o per le stampe? Quale delle misure offerte dal software sono state attivate?

Ma lei rivenditore del software, in qualità di responsabile della fornitura, non ha consigliato il titolare come impostare le misure di sicurezza a tutela dei dati?

Non saprei... nel registro del titolare non trovo traccia di come siano stati affrontati questi problemi... ma il mio cliente ha sempre agito in buona fede!

La progettazione del trattamento è responsabilità del titolare del trattamento. Il software è un anello della catena, ci sono poi l'organizzazione aziendale, le misure di sicurezza fisica e molti altri aspetti da considerare.

Un software non può essere "conforme" al GDPR, può esserlo un trattamento. Il titolare può scegliere un software che dia delle garanzie e fornisca delle opzioni, che poi potrà utilizzare per progettare un trattamento "conforme" al GDPR.

>> prosegue da pag. 1

software da lui forniti sia da considerare "Responsabile del trattamento" a prescindere che i medesimi siano venduti nella modalità "on premise" (installati presso il cliente), ovvero in "cloud" su piattaforme del Produttore.

"L'attribuzione di responsabilità nei confronti di un fornitore esterno richiede la stipula di un contratto che regoli la materia disciplinata, la durata del trattamento, la natura e finalità, il tipo di dati personali e le categorie di interessati, specificando i compiti attribuiti al Responsabile in relazione ai rischi che il trattamento comporta e definendo le responsabilità effettive del fornitore."

Mario Brocca - Dpo in Zucchetti"

SERVIZI EROGATI DALLE SOFTWARE HOUSE E NOMINA DPO (DATA PROTECTION OFFICER)

Non è possibile dare indicazioni generali per l'obbligo o meno di provvedere alla nomina di un DPO all'interno della Software House; la cosa andrà valutata caso per caso a seconda del servizio/prodotto erogato e del trattamento dati effettuato. Tuttavia mentre nel caso di vendita e assistenza di soli prodotti "on premise" si può escludere a priori l'obbligo, nel caso di servizi erogati in SaaS Cloud, si ritiene che la cosa vada attentamente valutata e che sarebbe comunque consigliabile la nomina di un DPO.

"In realtà multinazionali come la nostra già esistevano funzioni dedicate alla protezione dei dati personali. L'istituzione della figura del DPO da parte del GDPR ha fornito lo spunto per riorganizzare le funzioni e suddividere i compiti. La scelta di costituire un Data Protection Office italiano, composto da professionisti con competenze giuridiche e tecniche, che opera sotto la supervisione di un DPO europeo, consente di rispondere prontamente alle richieste dei dipartimenti aziendali e, nel caso, dell'autorità di controllo."

Andrea Barone - Ufficio Privacy Wolters Kluwer Italia"

DIRITTO ALL'OBLIO E CANCELLAZIONE DEI DATI NEI BACKUP

Sul punto non ci sono particolari novità essendo la cancellazione dei dati già prevista dall'art.7 c.3, lett.b del Codice Privacy, quindi, qualora la stessa sia formulata in termini generali, si ritiene che andrebbe applicata anche ai backup. Tuttavia si reputa che debbano essere previste determinate deroghe qualora il processo di individuazione dei dati da cancellare dai backup sia particolarmente difficoltoso e/o oneroso e comporti costi significativi per il Titolare e per il Responsabile. Un esempio calato sulla realtà dell'elaborazione paghe e stipendi riguarda il salvataggio degli archivi dell'anagrafica dipendenti e percipienti, spesso univoca per più datori di lavoro; ne consegue che la cancellazione dei dati anagrafici del titolare del trattamento (datore di lavoro) e dei soggetti interessati (dipendenti) non potrebbe avvenire senza coinvolgere i dati di altri soggetti e di conseguenza non sarebbe attuabile.

"Bisogna porre attenzione a quanto esprimerà il Garante, che è consapevole della problematica e potrebbe, come ha fatto l'Authority francese, accettare come misura quella di informare preventivamente l'interessato degli ineluttabili tempi tecnici di conservazione dei backup."

Antonio Campodipietro
Responsabile Infrastrutture e Sicurezza ICT in ADS

DIRITTO ALLA PORTABILITÀ DEI DATI E FUNZIONI DI EXPORT

Il diritto alla portabilità dei dati riguarda unicamente i dati forniti dall'interessato e non tutti i dati derivati e risultanti da elaborazioni del software. I dati presenti sui cedolini paga o sui dichiarativi fiscali e contributivi non sono forniti dall'interessato ma frutto di un'elaborazione del software, e per tale motivo non soggetti alla portabilità. Qualora sia richiesta, la portabilità potrà avvenire su formato standard e potrà essere pattuito un compenso per l'attività richiesta.

"La 'portabilità' come strumento di controllo degli interessati sui propri dati e sulla diffusione degli stessi favorirà nuovi servizi nel mercato digitale".

Fabio Torrengo - Responsabile IT in Sistemi"

Questi sono solo alcuni dei punti affrontati dal documento e in ogni caso, vista la complessità della materia e la mancanza alla data di chiarimenti ufficiali, su molti aspetti si dovrà ritornare con ulteriori approfondimenti da parte del gruppo di lavoro associativo.

Fornitori e GDPR: quali garanzie?

Ai sensi dell'art. 28 GDPR, il Titolare che affida a un terzo operazioni di trattamento di dati personali «ricorre unicamente a **responsabili del trattamento** che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate». Ma quali sono queste garanzie e a quali aspetti è necessario prestare più attenzione quando si seleziona un fornitore?

01 **SICUREZZA**
Il responsabile del trattamento deve adottare misure tecniche e organizzative adeguate, tenuto conto della natura e della finalità del trattamento, ma anche dei costi di attuazione. Può essere utile rifarsi alla documentazione tecnica predisposta dal fornitore e valutarne l'adeguatezza rispetto alle proprie finalità.

02 **CONTRATTI**
L'attività del responsabile deve essere regolata da uno specifico contratto (Data Processing Agreement) che definisca obblighi e diritti del Titolare. Il DPA può fare parte delle condizioni di contratto predisposte dal Fornitore e deve contenere tutti i contenuti di cui all'art. 28, comma 3 GDPR.

03 **LIMITAZIONE ALL'UTILIZZO DEI DATI**
Il responsabile tratta i dati solamente per finalità e nella misura necessaria a svolgere i servizi affidati, attraverso personale autorizzato e vincolato da specifici obblighi di riservatezza. Al termine dei servizi, i dati devono essere cancellati o restituiti al Titolare e le eventuali copie cancellate.

04 **TRASFERIMENTO EXTRA UE**
È necessario verificare il luogo di conservazione dei dati e, soprattutto, se vi è un trasferimento dei dati al di fuori dello Spazio Economico Europeo. In tal caso, il fornitore deve Fornire specifiche garanzie in merito al rispetto dei limiti e requisiti del trasferimento.

05 **ASSISTENZA ALLA CONFORMITA'**
Il responsabile del trattamento deve fornire supporto nell'adempimento degli obblighi che la normativa pone a carico del Titolare (es. richieste di esercizio dei diritti, DPIA, etc.), fermo restando che tali attività potranno essere oggetto di specifici accordi ove non compresi nel prezzo base del servizio.

06 **DATA BREACH**
In caso di violazioni di sicurezza, il responsabile deve darne tempestiva comunicazione al titolare, in modo da consentirgli di adempiere agli obblighi di notifica, e adottare ragionevoli misure per porre rimedio alla violazione e limitare i possibili effetti negativi.

I SOCI DI ASSOSOFTWARE

01 INFORMATICA SRL	DEVPROJECT SRL	KALYOS SRL	SEASOFT SPA
01SISTEMI SRL	DIEFFE INFORMATICA SRL	KIBERNETES SRL	SELCO SNC
2 BIT SRL	DNR INFORMATICA SRL	LASERSOFT SRL	SESAMO SOFTWARE SPA
ABAS BUSINESS SOLUTIONS SRL	DOLPHIN SRL	LUCUS INFORMATICA SRL	SI.EL.CO. SRL
ABC SOLUTIONS SRL	DYLOG ITALIA SPA	M.A.P. CONSULTING SRL	SIA SRL
ABLE TECH SRL	EDISOFTWARE SRL	MAIN OFFICE SRL	SIAC SRL
ACCENTURE HR SERVICES SPA	ELABORA SRL	MATISSE SRL	SICOM SRL
ADP SOFTWARE SOLUTIONS ITALIA SRL	ELEA SRL	MAXI-DATA SRL	SIGMA SISTEMI SRL
ADRIATICA SISTEMI SOC. COOP.	ELMAS SOFTWARE SPA	MEDIASOFT SNC	SINTEL SRL
ADS AUTOMATED DATA SYSTEMS SPA	EST SAS	METHEOS INFORMATICA SAS	SINTEM SRL
ALA DATA SYSTEM SRL	EURO ARPA SRL	METODO SRL	SISCOM SPA
ALBALOG SRL	EVIN SRL	MICROAREA SPA	SISTEMI INFORMATICI SRL
ALMA INFORMATICA SRL	EVOLUTION SRL	MICROMATICA SRL	SISTEMI SPA
AMBIENTE.IT SRL	E-WIN SRL	MIDA 4 SRL	SIWEB SPA
ANTEX SERVIZI DI ASSISTENZA FISCALE SRL	FILOSOFIA FISCALE SRL	MODI NUOVI SAS	SIXTEMA SPA
APOGEO SRL	FINSON.COM SRL	MULTIDATA SRL (PRATO)	SOFT SYSTEM SRL
APRA SPA	FORGHIERI INFORMATICA	MULTIDATA SRL (ROSIGNANO MARITTIMO)	SOFTGROUP SRL
BF SOLUZIONI INFORMATICHE	GBSOFTWARE SPA	NAMIRIAL SPA	SOFTONE SRL
BI ELLE SRL	GENESYS SRL	NEW SYSTEM SRL	SOGEA SRL
BITECH SRL	GESAG SRL	OPEN DOT COM SPA	SONAR ITALIA SRL
BLUDATA INFORMATICA SRL	GL ITALIA SRL	OPEN SOURCE ITALIA SRL	SOPRA HR SOFTWARE
BLUENEXT SRL	GOLDENPRO SRL	ORGANIZZAZIONE COLOMBO PAGHE MONZA INFORMATICA SRL	SPAZIO INFORMATICO SNC
BRAINWARE SNC	GRUPPO BUFFETTI SPA	OTELIA SRL	SPEED INFORMATICA SRL
CBA INFORMATICA SRL	GRUPPO FORMULA SPA	PA DIGITALE SPA	STRUTTURA INFORMATICA SPA
CEP SOLUTIONS SRL	GRUPPO SERVIZI AZIENDALI SNC	PAL INFORMATICA SRL	STUDIO 74 SRL
CINECA	HALLEY INFORMATICA SRL	PASSEPARTOUT SPA	STUDIO CENTRO SRL
CL SYSTEM INFORMATICA SRL	HAWK AML SRL	PERO SOLUTION SAS	STUDIO PRAGMA SAS
CNR SERVICE SRL	HIVE SRL	PLUS INFORMATICA SNC	STUDIO ZIVERI SRL
CODICE SRL	I. E O. INFORMATICA E ORGANIZZAZIONE SRL	PNG SRLS	SYS-THEMA SRL
CODIVIN SRL	ICE SRL	POLYMATIC SRL	TEAMSYSTEM SPA
CONCEPT SOFTWARE SNC	INAZ SRL	PRO CONSULTING SRL	TECHNE CONSULTING SRL
CONSULT DATA SRL	INF.OR. SRL	PRO.SY.T SRL	TELE.MA.CO.
COPPOLA LUIGI	INFO-BIT SRL	PRODATA SRL	THESMA SRL
CORE SOLUTION SRL	INFOCOM SRL	PROGETTO AUTOMAZIONE SRL	TNX SRL
CRP SOFTWARE SRL	INFOMEDICA SRL	PUBLISYS SPA	TPC & JOIN SRL
CSC SRL	INFOMINDS SPA	RANOCCHI COM SRL	UNIMEDIA SOFT SRL
DANEA SOFT SRL	INFORMATICA 80 SOFTWARE SRL	RAVOTTI EMILIO	VM SISTEMI SPA
DATA FLOW SRL	INFORMATICA EDP SRL	RDV NETWORK SRL	WEB2S SNC
DATA MANAGEMENT HRM SPA	INFOTEL SRL	REGOLD SRL	WIN SOFTWARE SRL
DATA PRINT GRAFIK SPA	INNOVAZIONE & SOFTWARE SRL	REPLICA SISTEMI SPA	WINDEX SRL
DATA SERVICES SRL	IT TOSCANA SRL	RICERCHE E METODI SRL	WOLTERS KLUWER ITALIA SRL
DATA SYSTEM ITALIA SRL	ITACME INFORMATICA SRL	RIEDMANN SRL	WOODOO SRL
DATALOG SRL	ITALPAGHE SRL	S.E.LE.D. SOC. COOP.	WORK MANAGEMENT CONSULTING SRL
DATEV.IT SPA	ITALSOFT SOFTWARE PRODUCTION SRL	S.I.R.A.C. SRL	WT SRLS
DEDALUS SPA	ITWORKING SRL	SAN MARCO INFORMATICA SRL	ZUCCHETTI SOFTWARE GIURIDICO SRL
DELTA PHI SIGLA SRL	IVM INFORMATICA SRL	SAP ITALIA SPA	ZUCCHETTI SPA
DENTAL TREY SRL	J-SOFTWARE SRL	SEAC SPA	

Radiocor AGENZIA D'INFORMAZIONE

Direttore responsabile: Lorenzo Lanfrancone
In redazione: Maurilio Fina
Proprietario ed Editore: Il Sole 24 ORE Spa
Registrazione: n° 274 dell'11-11-2016 presso il Tribunale di Milano

Sede Legale e redazione: Via Monte Rosa n. 91 20149 Milano -Tel: 02.3022.4602-3 - Fax: 02.3022.481
Progetto editoriale, grafico e artwork: Il Sole 24 ORE Radiocor Agenzia d'informazione