Come valutare e scegliere un software GDPR

di **Leon Pietro Menicanti** – *Legal Tech - Partner Studio Legale Privacy by Orlandi&Partners*
*(www.studiolegaleprivacy.com)*

Per sistema di gestione s'intende l'insieme di tutte quelle informazioni necessarie ad un'organizzazione per dimostrare il rispetto del principio di accountabiliy.

Un sistema di gestione privacy completo deve contenere, almeno:

- una descrizione della struttura organizzativa e delle responsabilità;
- un organigramma privacy;
- le relazioni periodiche del DPO (ove presente);
- le politiche sulla gestione delle richieste degli interessati;
- gli audit interni;
- l'elenco delle attività formative;
- l'elenco degli asset utilizzati per trattare dati personali;
- l'insieme documentale (lettere di autorizzazione, informative, DPA, procedure, linee guida ecc.);
- i registri delle attività di trattamento;
- le misure di sicurezza implementate;
- le valutazioni d'impatto sulla protezione dei dati (Data Protection Impact Assessment – DPIA);
- il registro delle violazioni;

Come appare già evidente, il numero di informazioni e di evidenze documentali necessarie a dimostrare un corretto modello di gestione, organizzazione e controllo della protezione dei dati personali (e con esso il rispetto del principio di accountability) risulta essere cospicuo anche nelle organizzazioni meno complesse. Se a ciò si aggiunge che tutta questa messe di informazioni sono intrinsecamente collegate tra loro appare evidente che la creazione di un sistema di gestione privacy coerente ed efficace non può più essere effettuato ricorrendo esclusivamente a fogli excel o documenti word.

Questo perché l'apparente flessibilità di questi strumenti rappresenta il loro limite più grande.

È senza dubbio possibile creare, gestire e manutenere un registro dei trattamenti in formato excel (ne avevamo parlato anche **qui**) ma il risultato sarà un registro contenente le informazioni minime ed indispensabili previste dall'art. 30 del GDPR; non è così, però che si rispetta il principio di accountability!

L'art. 24 del GDPR, infatti, prevede che il Titolare debba essere in grado di dimostrare di aver implementato misure tecniche e organizzative tali da garantire che i trattamenti siano effettuati

nel rispetto del Regolamento. Appare lampante, quindi, che il rispetto dell'art. 24 prevede un'attività ben più complessa e completa rispetto alla mera elencazione degli elementi indicati nell'art. 30 del GDPR.

Se si aggiunge poi che il sistema di gestione privacy deve essere mantenuto "vivo" e in costante evoluzione (come viva ed in costante evoluzione dovrebbe essere la vita di un'organizzazione), appaiono evidenti tutti i limiti contenuti negli strumenti di cui sopra.

Per questi motivi oggi è fondamentale dotarsi di strumenti tecnologici che consentano una semplice ma approfondita gestione dei numerosi adempimenti previsti dal GDPR e – cosa più importante – consentano una loro esibizione rapida, organica e completa.

Dall'entrata in vigore (nel 2016) del GDPR, ma ancor di più a seguito della sua applicazione il 25 maggio 2018 sul mercato si sono affacciate numerosissime soluzioni tecnologiche atte a supportare consulenti e aziende nel processo di messa a norma privacy.

Cosa valutare, quindi, quando ci si approccia all'acquisto di uno di questi strumenti?

Senza dubbio il primo elemento da tenere in considerazione è la completezza del tool. Lo strumento che si deciderà di usare dovrà essere in grado di gestire almeno tutte le informazioni indicate in precedenza così come quelle necessarie per la certificazione del sistema di gestione privacy, secondo quanto previsto dalla UNI/PdR 43:2018.

Completezza, dicevamo, ma anche aggiornamento; è fondamentale che il software sia costantemente mantenuto aggiornato. In questo periodo si assiste, infatti, ad una vera e propria proliferazione normativa a più livelli, sia nazionale (con le FAQ, linee guida e provvedimenti del Garante per la protezione dei dati personali), che internazionale con le linee guida, raccomandazioni e prassi emanate dall'EDPB (European Data Protection Board) e i provvedimenti le raccomandazioni o gli strumenti delle autorità garanti dei vari paesi europei.

Un esempio sono le linee guida sulla LIA (Legitimate Interests Assessment) emesse dalla ICO (l'autorità inglese) che propongono una guida ed una metodologia per poter valutare e dimostrare in concreto l'applicabilità del legittimo interesse come base giuridica di un trattamento.

Poter effettuare una LIA, magari in maniera guidata, all'interno del software di gestione privacy consentirà ai Titolari di poter meglio dimostrare il processo che ha portato alla scelta di questa particolare base giuridica.

Lo strumento dovrebbe permettere, poi, una compilazione collaborativa dove, in un'ottica di responsabilizzazione, gli utenti possano compilare le parti di loro competenza. In tal modo sarà possibile coinvolgere nel processo i vari referenti o responsabili d'area, consentendo loro di

descrivere puntualmente le attività di trattamento svolte nei rispettivi settori. Sono rare, infatti, le realtà dove un unico soggetto è a conoscenza di tutti gli elementi che compongono un trattamento.

Dovrebbe, infine, essere abbastanza "smart" da aiutare l'utente nella compilazione, evitando la necessità di imputare nuovamente informazioni precedentemente inserite in altre aree del software; guidare l'utilizzatore nella corretta compilazione degli adempimenti più complessi (come ad esempio le DPIA) e contenere strumenti facili e completi di reportistica che consentano l'estrapolazione anche solo di determinate informazioni (es. report degli assessment, delle DPIA, lista degli autorizzati, ecc.)

Questi sono gli elementi fondamentali che non possono mancare in un software privacy; vi sono però, alcuni strumenti la cui presenza agevola l'utilizzatore nel rispetto degli adempimenti previsti dal GDPR e mi riferisco, nello specifico a:

- creazione automatica dei documenti (lettere di autorizzazione, contratti per i responsabili, informative, ecc.) con la possibilità di poter personalizzare il template di stampa rendendolo coerente con quello della nostra organizzazione;
- gestione delle procedure – la possibilità di attribuire procedure, linee guida, istruzioni e quant'altro ai soggetti autorizzati, in tal modo, quando si andranno a produrre le lettere di autorizzazione ogni documento sarà automaticamente corredato con le relative procedure in allegato;
- gestione automatizzata delle lettere di autorizzazione: uno strumento che consenta la consegna automatica della lettera di autorizzazione (e dei relativi allegati) ai singoli soggetti e che ne conservi la presa visione;
- gestione automatizzata delle informative: analogamente al punto precedente, uno strumento che consenta la consegna automatica delle informative agli interessati e che consenta loro di prestare o negare il consenso, anche in un secondo momento.

Come Studio abbiamo avuto cura che ognuno di questi elementi fosse inserito all'interno del software di compliance GDPR UTOPIA (*www.utopiathesoftware.com*), realizzato in partnership con NSI Nier Soluzioni Informatiche S.r.l. e utilizzabile gratuitamente in versione demo.