GDPR sta per General Data Protection Regulametation e, in parole povere, è la nuova normativa europea sulla privacy che a cascata cade sull'Italia e sugli enti di qualsiasi tipo e dimensione, incluse le piccole organizzazioni non profit come la tua.

Questo tema e questi cambiamenti sono assolutamente centrali per te che fai fundraising in una piccola organizzazione, perché tutto il fundraising, dall'alba al tramonto, è fondato sui dati dei tuoi sostenitori. **Dati anagrafici, indirizzi e contatti, ma anche dati personali meno tipici che sono però fondamentali per le azioni di raccolta fondi** personalizzate.

La questione non è "quanti dati ho?", ma "Ho DI SICURO dei dati altrui da qualche parte e quindi **devo adeguare la mia piccola realtà a quel che chiede il GDPR**".

Si, è l'ennesima incombenza – senza scadenza, perché una volta fatto, questo adeguamento va mantenuto vivo e aggiornato – che grava sugli enti non profit in Italia, e la cosa difficile in questa fase è **orientarsi e sistemarsi... entro il 25 maggio 2018**! (NOTA: se ancora non l'hai fatto, non ti verranno a cercare coi segugi… ma non attendere oltre!).

Confesso: come un po' tutti in questa fase di transizione, mi ci perdo anche io, ma… (NOTA: dopo aver reso "compliant 3 piccole organizzazioni e questo blog, fidati che ci vuole un po' di tempo, ma resta una cosa semplice!).

per caso, grazie al cielo, sulla mia strada **ho trovato un grande esperto che ho l'immenso piacere di presentarti: Alberto Pattono.**

L'ho scoperto attraverso un suo FANTASTICO manuale operativo per l'autoadeguamento al GDPR dedicato ai piccoli enti non profit con pochi o praticamente nessun soldo da parte per queso scopo (e in questo articolo, ti avviso, troverai alcuni rimandi a questo manuale, secondo me fondamentale, da avere assolutamente! – *NOTA: NON ho rapporti commerciali di alcun genere con Alberto Pattono o con Amazon. Ti consiglio questo libro perché è ottimo, tutto qua!*).

Adesso, lascio la parola ad Alberto per andare ad affrontare *in pratica* alcuni dei molti nodi che riguardano direttamente e in modo trasversale la tua piccola organizzazione, il tuo fundraising e, soprattutto, i dati dei sostenitori, donatori e volontari che sostengono la vostra buona causa!

Buongiorno Alberto, grazie di aver accettato questa intervista!

Cominciamo dalle cose brutte, così poi non ci pensiamo più

La scadenza del 25 maggio 2018 è davvero vicina. E' un bene o un male?

La normativa del governo che raccorda la normativa europea a quella italiana arriverà in Parlamento 2 giorni prima del 25 maggio, che è la data di entrata in vigore di questa nuova disciplina… e così.

La fortuna, da un certo punto di vista, è che la legge europea e italiana non ci fornirà dei moduli da compilare. Quello che ci indica è il senso del da farsi, per tutelare al meglio le informazioni altrui che conserviamo nelle nostre organizzazioni, piccole, medie o grandi che siano.

Diciamo che, anche se c'è un bel po' da fare, siamo di fronte a un'opportunità nuova per gli enti del terzo settore.

Quindi niente cataclismi per chi al 25 maggio non sarà ancora adeguato? Oppure guai in vista?

Ma no, non cade il mondo! In Francia, si sa già che non verranno applicate sanzioni fino a fine anno, nel frattempo **basterà documentare che si sta lavorando in modo serio e rigoroso sul problema**. A mio giudizio, qualche forma di proroga arriverà anche in Italia, magari a favore delle piccole realtà.

Questo però non deve portare a pensare: "Ah ok, allora non c'è da preoccuparsi!".

Anche una chiesa e una parrocchia finiscono dentro a tutto questo! Se mando un bollettino, una circolare, una richiesta di offerte, devo rivedere tutto alla luce del GDPR. Lo stesso vale per organizzazioni tipicamente "innocenti": pensa ai boyscout! Per loro è anche peggio, perché in mano hanno una marea di dati di minorenni. Idem le ASD, ma anche chi fa cooperazione allo sviluppo…

Già, un bel groviglio! Ma quindi, secondo te, visto che ci sono anche delle situazioni oggettivamente più delicate e complesse da adeguare, quanti al 25 maggio saranno di fatto "fuori legge"?

Le associazioni piccole e medie sono così "fuori norma" – perché sono tipicamente destrutturate se non un po' confuse su molti aspetti amministrativi e di gestione – che in fondo potrebbero pensare: "Una in più o una in meno non fa differenza".

Ma uno dei grandi problemi che intravedo è un altro, e riguarda i rapporti con enti ed amministrazioni pubbliche. Magari la ASL o il Comune, per via di convenzioni e altri tipi di rapporti formalizzati, mi chiederà di dimostrare che io sia *compliant* con la GDPR e quindi io dovrò dimostrarglielo. E lì son problemi, perché in prossimità del rinnovo di una convenzione, magari mi chiederanno un certificato specifico in cui io lo attesti… **è una richiesta legittima, che potrebbe avanzare l'ente locale di turno in autonomia, in questo senso non è necessaria una legge dello Stato.**

Visto che loro saranno sottoposte per certo e senza sconti, ogni tipo di accordo con l'autorità pubblica e le grandi aziende, probabilmente richiederà agli enti non profit di poter attestare – dicendo il vero! – la compliance al GDRP. Un po' come avviene per l'antiriciclaggio e l'antimafia.

Cominciamo bene! Questo è un risvolto che mi era del tutto sconosciuto, già con questa indicazione se non altro hai fatto alzare le antenne a me!

Passiamo ora ai temi più cari a questo blog, che si chiamano… fundraising e marketing per il sociale! Per scaldare i motori, parto con un caso molto specifico.

Moltissimi fundraiser qui in Italia si stanno facendo questa particolare domanda: con l'entrata in vigore del GDRP in Italia, dovremo ottenere da parte dei donatori che già sostengono la nostra organizzazione l'autorizzazione esplicita per iscritto (ad esempio, con la firma di una informativa specifica) a comunicare e a trattare le loro informazioni?

Dobbiamo prendere a riferimento chi lavora da più tempo e meglio di noi sul tema. Soltanto in Inghilterra si sono interessati a capire e a studiare per bene come la GDPR si applica agli enti del terzo settore.

Osservando il parere dei maggiori esperti inglesi, la riposta è: **no, non ci sarà sempre bisogno o obbligo di chiedere un nuovo (o un primo!) consenso esplicito ai sostenitori.**

Se fai un utilizzo leale della database per il fundraising, cioè se non eccedi in pratiche rischiose, sbagliate o "furbe" come affittare, rivendere o condividere con altre organizzazioni i tuoi archivi, allora **vale la regola del "soft consent" ("consenso leggero")**. Quindi: la tua organizzazione può continuare ad utilizzare il suo database proprio come ha sempre fatto, ma nelle tue prossime comunicazioni devi assicurarti di dare un'informativa completa sul "nuovo" trattamento dei dati personali e di **rendere evidente una procedura di opt-out ("cancellazione dalle liste")** molto semplice, con anche la possibilità di un un opt-out parziale (per chi volesse ricevere comunicazioni solo con alcuni strumenti tra telefono, mail, sms etc).

Quindi, se in questo momento e in prospettiva la tua organizzazione sente di avere la coscienza a posto e contemporaneamente hai preso tutte le misure informatiche che tecnicamente metteranno al sicuro i dati dei donatori, **puoi continuare a fare quello che stavi già facendo.**

Visto che, come dicevi poco prima, "non ci sono moduli" predisposti da compilare, sembra quasi che la tenuta dei dati altrui diventi una questione di buon senso da una parte e dall'altra di protezione documentale dall'altra. Quanto è vero?

Il cardine di tutto il GDRP sta nella chiarezza che l'ente non profit deve assicurare ai suoi donatori (e a tutte le persone di cui possieda le informazioni). Hai delle tipologie di dati? Sono tante, sono poche? Da questo punto di vista è uguale, non è una questione di quantità! **Chiarisci ai tuoi sostenitori cosa vuoi fare di questi dati, chiarisci perché ognuna di queste informazioni è utile se non indispensabile**. A cosa ti serve il mio nome? A cosa mi serve il mio indirizzo postale? A cosa ti serve il mio indirizzo email? A cosa ti serve il mio codice fiscale?

Insomma, per ogni tipologia di informazione **devo saper rispondere alla domanda: perché ti serve questo mio dato, e come la utilizzerai?** Una risposta può anche essere: se non mi autorizzi a trattare questo tuo dato, non riusciremo a fare questa operazione.

Il duro lavoro che il GDRP ci richiede è di questo tipo: rendere noto quali sono i tipi di dati che hai, perché ti servono e come li utilizzi e infine informare su come hai minimizzato il rischio il rischio di alterazione e diffusione di questi dati e con chi li hai condivisi. E quest'ultimo è un aspetto sia di protezione esterna, che di formazione e tutela all'interno dell'organizzazione.

Mi è venuta un'idea improntata alla massima trasparenza, forse eccessiva, ma dimmelo tu… E se con un bel mailing speciale informassi tutti i sostenitori di un mio cliente su questa normativa, mettendo giù anche uno specchietto personalizzato che ricapitola per ognuno tutti i loro dati personali in gestione?

Non è necessario. E' un bel gesto di trasparenza, ma non è dovuto. Come sostenitore magari non te lo aspetti proprio, per cui fa un certo bell'effetto sorpresa. Ma quello che devi comunicare ai tuoi sostenitori è che tipologia di dati sono in tuo possesso, non per forza i dati specifici. Su quelli,

casomai, sarà il donatore a chiederti l'accesso, e tu dovrai garantirlo con mezzi opportuni.

Grazie mille Alberto! Adesso ti propongo un'altra questione pratica e specifica per il settore del fundraising.

Soprattutto nelle piccole realtà, molti fundraiser costruiscono database a partire dalla mappatura delle relazioni dei membri dell'organizzazione, e a volte – penso al caso della profilazione dei grandi donatori – attraverso ricerche in Internet, dalla stampa locale o di settore e via dicendo.

Raccolte tutte queste informazioni – sempre senza il consenso degli interessati! – si lanciano azioni massive (ad esempio: invio una lettera a tutti) o 1 a 1 (es: organizzo un incontro di persona). Conclusione: ci sono interi database costruiti così, senza che l'interessato ne sia a conoscenza in alcun modo. Che si fa?

Da questo punto di vista, il problema di cui dobbiamo preoccuparci non è il consenso in sé e di per sé. E' comunque previsto che tu possa fare una prima comunicazione per capire se la persona che hai in mente sia interessata oppure no a essere ancora contattata.

Quello che sicuramente non può funzionare è l'approccio (che, purtroppo, molti, soprattutto le agenzie di marketing più spinte, promuovo): "Se non agisci in contrasto, se non mi dici di no chiaro e tondo, allora prendo per buono che ti interessa".

Per cui, nei casi che descrivi magari non siamo al massimo della pulizia, e bisogna prestare molte cautele e attenzioni, ma… da qualche parte devi pur iniziare! Se chiedo ai miei consiglieri, volontari, dipendenti, soci di indicare altre persone a loro note, e poi nella lettera che citavi spiego bene perché contatto, cito la persona di riferimento che mi ha indicato il tuo nome e inserisco una chiara informativa sul consenso al trattamento dei dati, siamo a posto.

Torna un attimo sulla profilazione grandi donatori: qui a volte ci sono informazioni davvero personali, private, vorrei dire intime, in gioco. Come fundraiser, potrei aver bisogno di farmi un'idea sulla tua famiglia, sul tuo passato e via dicendo. E questi dati, cosa sono? Posso anche solo tenerli archiviati? Cosa posso o devo farne?

Dipende dal concetto di interesse legittimo e dipende anche da quali sono le tue fonti informative.

Per prima cosa: per quanto riguarda gli enti non profit, il cuore pulsante del GDRP non è il consenso di per sé, perché come enti che svolgono attività e perseguono missioni di pubblico interesse, possiamo dire – ma va verificato di volta in volta, nel caso di specie – che **dalla nostra parte c'è un interesse legittimo a informare, sensibilizzare, cercare di coinvolgere dei soggetti che ancora non sono archiviati nei nostri database.**

Seconda cosa: **se il dato è pubblico, non vuol dire anche che sia utilizzabile! Tu hai certamente il diritto di fare la raccolta dei dati resi pubblici o nei modi che vuoi**, ma devi farlo in una maniera strutturata, informatizzata oppure anche cartacea… ma devi fare molta attenzione alla loro conservazione, e a che non siano ceduti o riutilizzati in maniera impropria.

Fatti questa domanda: tu saresti stupito di ricevere una comunicazione da cui si palesa che io possiedo informazioni personali che ti riguardano?

Ti faccio un esempio: se sono il più ricco della città, in un certo senso me lo devo aspettare che mi arrivi la lettera del parroco per le campane, anche se non ho nulla a che fare con la chiesa, anche se non sono credente. Perché in quel contesto locale, sono comunque il più ricco della città: tutti lo sanno, sono un personaggio pubblico, scrivono di me, mi espongo in convegni, momenti pubblici e via dicendo.

Ma il discorso cambia e non poco se mi scrive una realtà che è troppo estranea alle mia abitudini, al mio stile, ai miei interessi, ma che comunque riesce ad avere informazioni che mi riguardano e che su queste fonda il suo approccio. Un esempio: se sostengo bambini palestinesi ammalati, non vuol automaticamente dire che sono di sinistra! E quindi, un'organizzazione politica che mi inviasse una lettera indirizzata chiedendo sostegno per il suo programma, adducendo argomenti a "prova" del mio interesse che sono solo ipotetici e non fondati, di fatto sta utilizzando in modo illegittimo informazioni che comunque, se fatto lecitamente, aveva diritto di ricercare e archiviare.

E ora passo a uno dei rompicapi che assillano me e i miei colleghi: il DPO (data protection officer). Una creatura mitologica! Visto che nessuno sa dire dove trovarlo, cosa si può fare finché non salta fuori da solo?

La figura del DPO è prevista in effetti dal GDPR. E' sicuramente obbligatorio per le realtà che fanno utilizzo su larga scala di dati sensibili, quindi sembrerebbe di certo obbligatorio per le medie e grandi organizzazioni del terzo settore. Soprattutto quelle che fanno del marketing massivo il loro pane quotidiano.

Dove si trova un DPO fatto e finito? La risposta é: saperlo, visto che ancora non si sa come diventa DPO! La legge lascia libero spazio.

Per iniziare a orientarsi, meglio cercare in Google quali sono gli enti di formazione di grandi dimensioni che stanno certificando con corsi specializzanti. Io sono socio di Federprivacy e Clusit, ma c0è anche Assoprivacy e forse altre associaizoni e 'albi informali'.

Una valida alternativa è rivolgersi ad avvocati da tempo specializzati sulla normativa privacy, perché di fatto se vai a vedere le competenze tecniche previsti dalla legge per il DPO, di fatto loro lo sono già

E tutto questo, giustamente (soprattutto per il DPO!) non viene a gratis…

Una grande-media realtà, deve mettere in conto un budget di almeno 20.000€ per il primo anno "di impianto" + 5.000€ per ogni anno seguente.

Belle botte! Una piccola semplicemente non riesce a tirarle fuori. E

quindi, che facciamo?

Beh, del DPO una piccola realtà, dalla sportiva paesana a qualsiasi altra non profit locale, potrebbe farne a meno… ma non so dirti in base a quale norma del regolamento! E' un'interpretazione che fornisco io, sulla base di quel che osservo nella discussione europea in corso, che a volte è verticale sul settore non profit.

L'orientamento, che anche io promuovo, è: se sei in grado di fare da solo, perché no?

Ripeto: la normativa sul GDPR ti chiede di adeguarti a una nuova disciplina, ma allo stesso tempo di da abbastanza carta bianca sul *come*.

Quindi, in questa fase di transizione che trova tantissime organizzazioni disinformate e impreparate, il consiglio è questo: **qualunque passo nella direzione dell'adeguamento fai, comunicalo prima di tutto all'interno! Documenta cosa sta accadendo e traccia il flusso di comunicazioni interne**.

La metto all'estremo: anche se ti troverai a fare tutto da solo, anche a costo di mandare PEC su PEC a tutti i membri del direttivo, documenta che si sta parlando e procedendo e agendo sull'adeguamento al GDRP, in un modo che renda chiaro che questo cambiamento sta coinvolgendo i dirigenti, i decisori, i dipendenti… chiunque abbia un ruolo, un compito e delle responsabilità all'interno dell'organizzazione. Parlane nel prossimo bilancio sociale, documenta che c'è stato un percorso condiviso con al centro l'adeguamento alla GDPR.

Quanto alla protezione dei dati a mezzo sistemi informatici, cosa consigli di fare? Molte organizzazioni dipendono da fornitori esterni (per le newsletter, il database, spazi di archiviazione in cloud etc)…

La norma prevede che il Titolare del trattamento, cioè l'organizzazione non profit, svolga la sua attività attraverso dei fornitori.

Se questi hanno una certa autonomia nel mettere in atto il trattamento, sono 'Responsabili del trattamento', una figura espressamente prevista dal GDPR che pone in capo a loro obblighi precisi. Il Responsabile può avere dei subfornitori, per esempio chi mette i dati sul cloud.

Tutti questi soggetti devono stipulare con il Titolare accordi precisi e mettere nero su bianco tutto quello che hanno fatto, fatto e faranno (e quello che non hanno fatto o faranno) con ciascuna tipologia di dati.

[*NOTA: nel manuale scritto da Alberto Pattono, trovi esempi ANCHE – non solo – di questo tipo di accordo, da prendere, personalizzare e portare al tavolo dei tuoi fornitori!*]

Puoi indicarci, in modo molto pratico e operativo, i primi passi da fare per mettere ordine in questa bella matassa?

Senz'altro. Dunque:

1) Risolvi i problemi e le preoccupazioni con i tuoi fornitori di servizi informatici siglando con loro un contratto d'acciaio. Il senso di questo contratto dev'essere: "Mi aspetto che tu faccia questo e questo e questo, a tutela della protezione dei dati che riguardano i nostri donatori, volontari, beneficiari." In questo modo attribuisci a loro con certezza la piena responsabilità per

malfunzionamenti, anomalie e effrazioni con oggetto queste informazioni.

2) Procedi a un censimento dei dati in possesso. Dove sono? Come sono archiviati? Quando sono stati acquisiti? Per che scopi? Quindi passo ad omologare e armonizzare questa archiviazione in maniera chiara, organizzata, comprensibile, protetta.

3) Chiedo a me stesso: ma questi dati mi servono tutti? Davvero? Perché mi servono? Che utilizzo devo farne? Mi sento in diritto di usarli? E di possederli? Cosa ne farò quest'anno? Cosa ne stanno facendo altri? Che problemi nascerebbero se questi dati scappassero di mano? Quale sarebbe sugli interessati l'impatto della diffusione dei loro dati?

In questo modo hai composto il "Registro dei Dati". A norma di legge è vero che potresti farne a meno come piccola azienda, ma nella pratica è meglio farlo.

A questo punto in mano hai:

- **una valutazione del possibile impatto** in caso di problemi
- **una valutazione sui flussi di trattamento** dei dati
- **una valutazione generale che parte da un giudizio di equità**

Arriva allora il momento di redigere una privacy policy, una semplice lettera che deve restare sempre a disposizione dell'interessato e dalla quale discendono i moduli per la conferma del consenso.

A questo punto, comunico per chiedere il consenso, sviluppando supporti di comunicazione adatti allo scopo.

Per come tu sei capace di esporre la questione, sembra tutto davvero molto più facile del previsto, anche se articolato. Ma quindi, alla fine si può fare a meno di consulenti esterni?

Domani di sicuro ci saranno quelli che diranno: *"Pagami che ti certifico la compliance alla GDPR!"*.

I casi sono due: ne avrai bisogno se hai fatto il lavoro male. Ma se invece l'hai fatto bene, visto che **non esiste l'adeguamento perfetto o ideale, ma solo quello ben svolto sotto la guida del buon senso e del giudizio di equità**, puoi andare da quello che vorrebbe "obbligarti" e gli smacchi sul tavolo tutto quello che hai documentato!

Se vuoi cercare comunque un parere esterno, ti serve una persona che ti indirizzi nella documentazione dei processi, che siano abituate a descriverli ogni giorno.

Facciamo che prendiamo la via dell'autoadeguamento. Quanto tempo stimi che vada dedicato per andare da cime a fondo? Internamente, chi ci deve mettere la testa per velocizzare e lavorare al meglio? Chi coinvolgeresti da fuori?

Molte associazioni sono in difficoltà anche solo a censire i propri dati. Negli archivi, di qualsiasi genere, si vede purtroppo di tutto! Rischi così che molto tempo vada via nei primissimi passi.

Ma in realtà, se sono messe meglio, in 30-40 ore di lavoro dedicato e ordinato, si può fare tutto. E' un lavoraccio perché devi scrivere tantissimo e descrivere accuratamente fasi e processi. Ecco, diciamo che questa seconda parte non fa propriamente parte delle abitudini mentali e quotidiane di tutti!

Un buon team di lavoro interno è: all'inizio tutti, cioè ex presidenti, ex tesorieri, volontari particolarmente impegnati, se possibili ex dirigenti retribuiti, dipendenti e collaboratori in particolari posizioni di contatto col pubblico e che abbiano avuto a che fare con l'archiviazione di dati. **Assieme a loro ricostruisci lo storico, perché bisogna capire dove sono tutti i dati possibili.**

Poi parli col tuo webmaster o chi ne capisce di più sul piano informatico, perché questi aspetti interni sono collegati quasi sempre anche a rapporti con fornitori esterni di servizi.

Alla fine comunque bisogna contare su **un paio di teste dedicate a coordinare, documentare e stendere procedure.**

Ok, direi che sei stato quasi fin troppo generoso! Alberto, tutto quello che ci hai spiegato e indicato è preziosissimo per parte col piede giusto. Ti chiedo ancora una cosa però: qual è l'approccio giusto da tenere di fronte a questa strana avventura?

Consiglio: non schivare il GDPR! Non partire col piglio: "Oh no, e adesso come me la sfango?". Piuttosto, mettiti in questa lunghezza d'onda: **"Come colgo l'opportunità di sistemarmi di fronte a un problema che non avevo mai esaminato?"**.

E' l'opportunità di capire perché e se faccio bene a lavorare in un certo modo, oppure perché e se è caso di non farlo più, insomma, se è caso di cambiare, a volte anche in maniera profonda, il mio modus operandi nella gestione dei dati personali.

Mettiti nei panni degli altri: "Se fossi dalla parte di chi riceve il messaggio, o se questi dati fossero diffusi per errore, per dolo, per colpa… come mi sentirei? Cosa proverei? Cosa penserei di quell'organizzazione"?

Grazie di cuore Alberto! Ti dobbiamo molto, lo dico sinceramente! Alla prossima!

Alberto Pattono, giornalista e divulgatore si è occupato di finanza e di salute. Ha lavorato con le Associazioni di pazienti e Società scientifiche soprattutto nel campo del diabete.
E' socio di Federprivacy e membro del Clusit – Associazione italiana per la sicurezza informatica.
Ha scritto recentemente: "GDPR. Lo stretto indispensabile per le Associazioni di Volontariato: Cosa devono davvero fare le realtà del no-profit per adeguarsi al Regolamento europeo per la privacy (RGDP 2016/679)" e "GDPR. Lo stretto indispensabile per le PMI: Cosa devono davvero fare le piccole imprese per adeguarsi al Regolamento europeo per la protezione dei dati personali (RGPD 2016/679)."

Condividi generosamente su

- Fai clic per condividere su Facebook (Si apre in una nuova finestra)
- Fai clic qui per condividere su Twitter (Si apre in una nuova finestra)
- Fai clic qui per condividere su LinkedIn (Si apre in una nuova finestra)
- Fai clic per condividere su WhatsApp (Si apre in una nuova finestra)
- Fai clic per condividere su Telegram (Si apre in una nuova finestra)