Cristina Vicarelli
Avvocato

Il GDPR per le piccole (e piccolissime) imprese

La Dalle domande che mi sono arrivate nell'ultimo mese, mi sono resa conto che molte piccole realtà si affacciano al GDPR (o RGPD – Regolamento Generale sulla Protezione dei dati, nell'acronimo italiano) senza avere le idee troppo chiare e probabilmente trovano indicazioni riferite a realtà più grandi e strutturate che le lasciano confuse, facendo credere che chissà quali complessi e costosi adempimenti le attendono.

In realtà, il GDPR (o RGPD, che dir si voglia) semplifica l'impianto precedente, adattandosi elasticamente ai trattamenti effettuati all'interno delle diverse strutture. Ho pensato che potrebbe essere utile rispolverare i consigli su come prepararsi al GDPR che avevo provato a dare due anni fa, abbassando un po' il livello dell'asticella in modo da poterli adattare a chi si sente schiacciato dal Regolamento come da un incomprensibile gigantesco meteorite piovuto dal cielo per spazzare via la civiltà come la conosciamo ora.

1. Consapevolezza

La chiave di tutto l'impianto è la consapevolezza. Questo è l'unico vero sforzo che ci richiede il RGPD: imparare cos'è la protezione dei dati.

Innanzi tutto partiamo da cosa non è, o, tradizionalmente, non era: non è esattamente la stessa cosa che definiamo privacy; la privacy trovava tutela per lo più in altri rami dell'ordinamento, che proteggono la riservatezza del domicilio o la segretezza della corrispondenza. Possiamo rinunciare alla nostra riservatezza, nell'epoca dei social possiamo decidere cosa mostrare di noi e cosa tenere per noi, ma è una nostra scelta; e non è diritto dei fornitori di servizi ai quali affidiamo i nostri dati abusarne per lucrarci sopra a

nostra insaputa: ed è questo che, in estrema sintesi, dice il Regolamento generale sulla protezione dei dati.

Come dobbiamo attenderci che gli altri proteggano i dati che gli affidiamo (anche se glieli affidiamo per pubblicarli sul web, rinunciando alla nostra privacy), così dobbiamo proteggere i dati che ci vengono affidati. Il mondo cambia e negli anni i dati personali sono diventati una "merce" di valore, e i criminali informatici, ad esempio, saccheggiano i siti web per "raccattare" dati personali da rivendere (qui un elenco delle violazioni di dati più importanti).

Non solo però, c'è anche un mercato legale delle informazioni personali, ed è su quello che il GDPR va a incidere, nel tentativo di regolamentare l'uso dei dati personali senza comprimere i diritti alla riservatezza e alla protezione dei dati personali, che sono diritti fondamentali per l'UE (cfr, artt. 7 e 8 della Carta).

E' anche vero che la differenza tra riservatezza e privacy sfuma nel mondo tecnologico: assistenti domestici, giocattoli, persino lampadine sono in grado di percepire suoni o movimenti. Talvolta alscoltando e conservando anche conversazioni familiari.

La "tua privacy è importante" è lo slogan con cui molti di noi aprono le informative con cui spiegano la protezione dei dati in riferimento ai trattamenti che opereranno: non è uno slogan vuoto ma una esortazione, l'invito ad averne consapevolezza: privacy e protezione dei dati si confondono sempre più con l'avvento dell'intelligenza artificiale e con l'analisi algoritmica e spesso predittiva che viene costantemente operata sulla nostre vite.

In soldoni ciò si traduce:

1. nel capire cosa sono i dati personali: e qui è importante capire che la definizione è più ampia del mero nome e cognome. Può essere d'aiuto la spiegazione semplice della Commissione UE che si trova qui, ma in generale consiglio la lettura di tutta la sezione dedicata al GDPR.

2. Capire quali dati personali "abbiamo" (di quali trattamenti di dati siamo, cioè, Titolari o Responsabili) e qui passiamo al secondo step. La mappatura.

2. Mappare i dati e i trattamenti:

Una seconda domanda che ognuno dovrebbe farsi è: "perché tratto o conservo questi dati?

A cosa mi servono?" Se conserviamo dati che non ci servono, o che non ci servono più, probabilmente stiamo sbagliando qualcosa e quei dati vanno cancellati.

Attenzione, perché i dati personali non sono qualcosa di astratto e scollegato dall'ordinamento giuridico: a volte è la legge che ne impone la conservazione, anche se, apparentemente, hanno esaurito la loro funzione, perché abbiamo raggiunto lo scopo per cui li avevamo raccolti.

Quindi: occorre anche chiedersi se c'è una norma di legge che impone la conservazione (come ad esempio per le fatture) o tra quanto tempo si prescriverà il diritto del cliente di citarci in giudizio per un inadempimento contrattuale, ad esempio.

Un'altra cosa a cui fare attenzione è la modalità con cui conserviamo i dati perché le norme di legge possono disciplinare la conservazione dei documenti che li contengono: ad esempio, per legge occorre conservare ordinatamente anche i contratti e le lettere commerciali.

Quando questi documenti sono archiviati con quelle regole, anche i dati personali eventualmente contenuti seguono le stesse regole e non possono essere cancellati.

Occorre quindi sapere quali dati abbiamo, dove e perché, e, se li conserviamo, se abbiamo un criterio di conservazione.

I dati possono essere trattati e conservati solo in stretta aderenza alla finalità (e alla base giuridica) per cui sono stati raccolti.

Tecnicamente si dice che devono essere pertinenti e non eccedenti, e che devono essere esatti ed aggiornati.

A questo punto possiamo passare alla fase successiva.

3. Analisi dei rischi

Quali rischi corrono i dati che trattiamo? Come li possiamo proteggere al meglio? Quali rischi corre l'interessato (cioè la persona fisica alla quale i dati si riferiscono) se non proteggiamo bene i suoi dati?

Anche qui: buonsenso. Se i dati personali che tratta l'impresa non presentano particolari rischi, ovvero non rientrano nelle categorie descritte dall'articolo 9 del Regolamento generale sulla protezione dei dati (ex dati sensibili, dati biometrici o genetici ecc.), o non rientrano nell'articolo 10 de GDPR, ma sono i dati normalmente utilizzati in una transazione commerciale, l'analisi del rischio non dovrà portare all'adozione di misure spropositate.

Se il trattamento è prevalentemente cartaceo, basterà probabilmente attenersi alle vecchie "misure minime" descritte dall'abrogando allegato B del Codice della privacy.

La stessa valutazione potrà essere fatta per trattamenti informatici che non presentino particolari rischi, magari mantenendo l'aggiornamento automatico dell'antivirus, come già si faceva nella prassi. L'analisi dei rischi non è disciplinata dal Regolamento che si limita a definire i parametri all'articolo 32 del RGPD.

La valutazione dei rischi non si limita alla valutazione del rischio informatico, ma tiene conto del "rischio privacy"; può essere utilità a capire che rischi corrono i dati provare a svolgere qualche considerazione:

1. che tipologia di dati trattiamo?

Qui bisogna capire se si trattano solo dati comuni, se si trattano dati già reperibili in pubblici elenchi o sul web, o se, invece, si trattano dati riferiti a credenziali di accesso, o carte di credito o dati riferiti a categorie svantaggiate o a minori o comunque dati appartenenti a particolari categorie oppure dati giudiziari.

2. I dati possono essere anche combinati tra loro: se ad esempio tratto dati comuni riferiti a minori dovrò prestare maggiore attenzione al trattamento rispetto a dati di adulti appartenenti alla medesima categoria. Se tratto entrambe le tipologie di dati, dovrò applicare al trattamento le protezioni previste per la categoria a maggiore rischio.

Se tratto dati di minori che possono svelare l'orientamento sessuale e il minore appartiene a una categoria debole (magari perché oggetto di pregiudizi da parte della comunità dei consociati, e potrebbe essere vittima di marginalizzazione o discriminazioni, ed esposto a una forte pressione sociale ove i dati venissero diffusi a sua insaputa), è chiaro che dovrò prendere le precauzioni più elevate per evitare questo inconveniente.

A questo punto, infatti, bisogna domandarsi quali rischi corre la persona alla quale i dati si riferiscono se i dati venissero diffusi o appresi senza il suo consenso, o se venisse a mancare la disponibilità di quei dati o se venissero alterati o cancellati.

Più alte saranno le conseguenze sull'interessato più è alto il rischio: le conseguenze possono andare dalla semplice seccatura per l'interessato, fino alla morte (immaginiamo l'indisponibilità di una cartella clinica elettronica che potrebbe comportare la somministrazione di un farmaco al quale il soggetto è allergico).

Il catalogo di conseguenze che si pone tra questi due estremi (danni alla salute, danni economici, furto di credenziali, furto di identità, ecc.) e che non riguarda solo gli aspetti patrimoniali ma anche la sfera psicologica dell'individuo mi darà, a spanne (perché non esistono metriche "fisiche" per la misurazione di questo tipo di effetti) la misura del rischio.

A questo punto dovrò misurare i rischi fisici e informatici ai quali è sottoposta le mia strumentazione e decidere la misura per farvi fronte.

Più i rischi saranno alti, più farò bene a rivolgermi a un professionista capace di indicarmi le misure di sicurezza necessarie e opportune in base ai rischi.

Chiaramente, al contrario, se il "rischio privacy" è davvero basso per il numero dei soggetti coinvolti e la tipologia dei dati e dei trattamenti, probabilmente basterà appoggiarsi al catalogo delle misure minime delle quali abbiamo recente memoria.

Con due precisazioni: non sempre le misure minime prendevano in considerazione gli strumenti del trattamento: ad esempio, non venivano presi in considerazione i siti web, che sono tra le aree a maggiore rischio di sottrazione o intrusione. Teniamo in considerazione anche questi aspetti.

Inoltre, teniamo presente che non sempre le informazioni presentano gli stessi rischi: ad esempio il nome di una persona, pur essendo un dato identificativo, dice poco se viene considerato a sé; abbinato al cognome dice di più; abbinato al codice di avviamento postale ancora di più, all'indirizzo di residenza di più ancora, e così via. Consideriamo quindi non i dati a sé, ma anche l'insieme delle informazioni disponibili (non solo a noi) e alle relazioni che le legano, prima di decidere se il rischio è alto, medio basso o massimo.

All'esito di queste valutazioni in ordine ai rischi relativi ai diritti e alle libertà dell'interessato e dello stato dell'arte -ovvero delle migliori soluzioni offerte dalla tecnologia si potranno prendere le misure più adeguate tenendo conto di tutti i parametri definiti dall'articolo 32 del Regolamento.

In genere è preferibile tenere traccia di questa valutazione, per tenere a mente il criterio seguito, e rendere più facili le revisioni o la difesa in caso di controlli.

Ma non è obbligatorio, e se l'impresa è davvero piccola e i trattamenti sono a rischio davvero basso potrebbe essere superfluo.

Questa valutazione deve essere operata anche rispetto ai dati dei dipendenti o dei collaboratori, se ci sono.

Può essere utile a questo scopo il manuale pubblicato dall'ENISA, ne ho parlato in ordine ai tool gratuiti relativi alla sicurezza dei trattamenti.

4. Individuare il proprio "ruolo"

Il soggetto che decide le finalità (perché tratto questi dati?) e le modalità del trattamento (e, quindi, anche se esternalizzare un trattamento) è il titolare.

Se, io titolare, queste decisioni le prendo, anche solo in parte, insieme a un altro soggetto, quello che decide insieme a me è contitolare.

Se, invece, delego il trattamento a un altro soggetto che non ha potere decisionale e devo dargli istruzioni, perché tratta i dati per mio conto, quello è il responsabile del trattamento. Il Responsabile del trattamento è un soggetto esterno e va vincolato con un contratto ai sensi dell'articolo 28 del RGPD.

Se invece il soggetto al quale ho esternalizzato il servizio non tratta i dati per mio conto, ma decide da solo le modalità e le finalità del trattamento, e non posso dargli istruzioni, è un titolare come me, e per distinguerlo dalle altre figure a volte si indica come "autonomo" (ma è una convenzione di comodo, si tratta semplicemente di un soggetto che rientra nella definizione di titolare ex art. 4 del RGPD, che determina da solo finalità e mezzi del trattamento).

Degli obblighi del Responsabile del trattamento ho scritto qui.

Della differenza tra responsabile della protezione dei dati e responsabile del trattamento, invece, qui.

5. La base giuridica del trattamento

Il consenso è una delle basi giuridiche del trattamento, ma non è l'unica;

non ho bisogno di acquisire il consenso (e, a volte, se provassi ad acquisirlo non sarebbe valido) se il trattamento poggia su una diversa base giuridica e fintanto che resto aderente alla finalità connessa a quella base.

La base giuridica determina la liceità del trattamento (è lecito solo il trattamento sostenuto da una base giuridica) e mentre la finalità rappresenta lo scopo per cui tratto i dati, la base

giuridica è la ragione o il motivo del trattamento. Ogni trattamento si radica su una base giuridica e da lì si proietta verso la finalità.

Ad esempio: se devo rispondere a una richiesta dell'interessato, o adempiere a un contratto del quale è parte l'interessato la base giuridica sarà rappresentata dal contratto o dalla necessità di dare seguito alla richiesta dell'interessato.

Una volta adempiuta la prestazione concordata, dovrò conservare il contratto e la fattura per legge. Questo trattamento (relativo alla conservazione) si basa sulla necessità di adempiere a un obbligo di legge.

Se voglio invece fare marketing al mio cliente via sms, dovrò anche acquisire il suo consenso, che mi servirà solo per questo tipo di attività.

Le basi giuridiche sono descritte dall'articolo 6 del RGPD.

Quello che ci appare come un unico trattamento (contatto, preventivo, conclusione del contratto, erogazione della prestazione, fattura, conservazione, cancellazione dei dati, marketing via sms) in realtà è una concatenazione di azioni che si distinguono in diversi trattamenti, contraddistinti da diverse finalità e che poggiano su diverse basi giuridiche.

Se l'interessato mi domanda la cancellazione dei suoi dati e si oppone al trattamento per finalità di marketing via sms o mi revoca il consenso precedentemente prestato per quel tipo di trattamento, la sua richiesta non si estenderà (e non potrebbe) ai trattamenti che poggiano su altre basi giuridiche o miranti a conseguire diverse finalità: vale infatti anche la regola che il consenso , quando necessario (e abbiamo visto che non sempre lo è) si presta per singole finalità, secondo il rapporto: una finalità / un consenso.

6. L'informativa

Una volta che abbiamo individuato i dati, i trattamenti, i ruoli, le basi giuridiche e le finalità del trattamento siamo pronti a scrivere l'informativa.

Infatti, occorre obbligatoriamente dare alcune informazioni all'interessato, e quali sono queste informazioni ce lo dicono gli articoli 13 e 14 del RGPD.

Quali informazioni vanno rese?

Molto dipende dai trattamenti e dagli obblighi che gravano concretamente sull'impresa. Se l'impresa è piccola e non ha trattamenti "su larga scala", potrà evitare alcuni adempimenti, come ad esempio la nomina del DPO e, se e non ha trattamenti particolarmente rischiosi da effettuare con nuove tecnologie, potrà evitarsi anche la valutazione di impatto sulla protezione dei dati (che è cosa diversa dalla valutazione dei rischi).

Se l'impresa neppure trasferisce dati in Paesi che si trovano fuori dall'UE (qui attenzione a servizi cloud, servizi di email marketing, servizi email, siti web e plugin o altri strumenti usati per il sito web che potrebbero importare il trasferimento dei dati in server situati fuori dall'UE) e non fa profilazione e non prende decisioni con strumenti automatizzati, nell'informativa potrà limitarsi a indicare:

1. il suo nome o la sua denominazione (il titolare) e i dati di contatto;
2. le finalità del trattamento;
3. la base giuridica del trattamento, e nel caso di trattamento basato su legittimo interesse quale interesse sta soddisfacendo;
4. Le finalità del trattamento;
5. Eventuali destinatari o categorie di destinatari a cui comunicherà i dati (es. società di recupero credito, commercialisti e altri consulenti esterni, società di servizi ICT);
6. il periodo di conservazione o i criteri utilizzati per determinarlo;
7. nel caso in cui venga chiesto il consenso, che il consenso si può revocare in ogni momento e senza costi;
8. se fornire i dati è obbligatorio per legge o per contratto, o se sono necessari per concludere il contratto, e che succede se l'interessato non fornisce i dati;
9. I diritti dell'interessato: accesso, rettifica, cancellazione, limitazione del trattamento, diritto alla portabilità dei dati;

10. Il diritto di opporsi al trattamento che deve essere evidenziato e separato dal corpo del restante testo;
11. Il diritto di proporre reclamo all'autorità.

Il titolare può evitare di fornire all'interessato le informazioni che l'interessato possiede già.

Se invece i dati non sono raccolti direttamente presso l'interessato, ci sono degli elementi in più da fornire, e sono descritti dall'articolo 14 del RGPD.

Ovviamente, se invece si trasferiscono dati all'estero o si fanno altri trattamenti che comportano la nomina del DPO, l'informativa cambia un po', perché occorrerà aggiungere anche questo tipo di informazioni.

Come si vede, però, è sufficiente, probabilmente, integrare la precedente informativa con i dati mancanti (e sempre che l'informativa fosse conforme alla precedente normativa e non fosse scritta troppo in "legalese", perché il RGPD impone un lessico semplice)

7 I diritti dell'interessato

Qui è importante la consapevolezza: avere indirizzi dedicati a raccogliere le istanze facilita la loro gestione, comprendere quali sono i diritti che può esercitare l'interessato rispetto al trattamento effettuato (ad esempio la cancellazione, che non sempre è possibile) e conoscere il termine per dare riscontro; una illustrazione del catalogo dei diritti riconosciuti all'interessato si può trovare qui: http://www.garanteprivacy.it/regolamentoue/diritti-degli-interessati

8. Accountability (o responsabilizzazione) e data breach (o violazione di dati personali)

Per dimostrare l'adempimento, il titolare deve documentare gli adempimenti posti in essere, per garantire il rispetto dei principi (elencati all'articolo 5 del RGPD) che presiedono alla protezione dei dati.

In una struttura piccola e che non fa particolari trattamenti, a meno che il trattamento dei dati non sia occasionale (ma non bisogna avere nemmeno dipendenti perché sia occasionale), bisogna tenere il registro dei trattamenti.

Il responsabile, oltre il suo registro, deve tenere anche quello per il Titolare, descritto anch'esso all'articolo 30 del GDPR.

Il registro può consistere in un foglio di calcolo (deve essere in formato elettronico), in cui i campi vengono contrassegnati dagli elementi indicati dall'articolo 30 RGPD.

Quelli indicati dall'articolo sono i soli elementi tassativi.

Molte sono le soluzioni in commercio o gratuite disponibili in rete, è importante controllare che i campi corrispondano esattamente a quelli indicati dal detto articolo.

Possono essere aggiunti campi ulteriori, ma il nucleo minimo tassativo è quello indicato lì (nell'articolo 30 GDPR) e deve essere presente.

Uno degli argomenti più caldi del RGPD è la violazione dei dati personali.

In che consiste?

In breve: la violazione di dati personali è "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Quindi è importante che il titolare impari a riconoscere una violazione, e nel caso avvenga si ricordi di:

- conservare in ogni caso la documentazione relativa; questo è l'unico adempimento se è improbabile che dalla violazione derivi un rischio per i diritti e le libertà dell'interessato.
- fare la notifica al Garante negli altri casi entro 72 ore (poi ci sono eccezioni, ma la regola generale è questa): deve sapere cosa comunicare (è indicato dall'articolo 33 del GDPR) e come (nel momento in cui scrivo non è disponibile una apposita piattaforma sul sito del garante e ogni titolare dovrà predisporre da sé idonea modulistica e conservarla in caso di necessità) e a quale recapito.
- fare la comunicazione anche all'interessato nel caso di rischi gravi (valgono le stesse considerazione operate sopra, con qualche problema in più in ordine alla necessità di fare la comunicazione a una pluralità di interessati e a volte con modalità "pubbliche" che vanno attentamente valutate.

Sarebbe bene scrivere una breve politica aziendale per fissare questi punti con allegata documentazione.

9. L'organizzazione interna

E' importante che le imprese facciano attenzione anche all'organizzazione interna.

I soggetti che trattano i dati devono essere autorizzati e istruiti in tal senso.

Il Regolamento non dice come vadano fate le autorizzazioni e il titolare è libero di riconfermare i vecchi incarichi o predisporre di nuovi, con nuove modalità, lasciandone comunque traccia.

L'importante è vincolare dipendenti e collaboratori alla riservatezza, rispettare il principio di minimizzazione e in particolare di privacy sin dalla progettazione e per impostazione predefinita anche sotto il profilo organizzativo, per cui potranno trattare i dati personali solo i soggetti che è necessario che li trattino.

10. Aggiornamento e formazione

Il regolamento generale sulla protezione dei dati impone al Titolare di verificare periodicamente l'assetto che si è dato.

Questa sommaria analisi è partita dalla consapevolezza del titolare come elemento cardine della conformità alla normativa e si chiude con un richiamo alla formazione che ne è corollario.

Il titolare deve essere in grado di garantire la riservatezza e la sicurezza dei dati e deve poterlo fare anche confrontandosi con un mondo che subisce continua evoluzione sia sotto il profilo tecnologico che sotto il profilo normativo.

Restare aggiornati e preparati è un elemento fondamentale, e la formazione per sé e per i soggetti che operano per lui è un elemento di accountability imprescindibile per ogni imprenditore.

Tutti i contenuti presenti nel blog, ove non diversamente specificato, sono distribuiti con licenza Creative Commons Attribuzione – Condividi allo stesso modo 4.0 Internazionale.