diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La tua realtà economica è davvero conforme al GDPR?

Autore: Mirco Caeran
In: Diritto civile e commerciale

Introduzione: una panoramica sul GDPR

Sono passati ormai 5 anni da quando, il 4 maggio 2016, veniva emanato il Regolamento (UE) 679/2016 avente ad oggetto la Protezione dei Dati. Si tratta del famoso RGDP (o GDPR secondo la dicitura inglese) il quale, in vista della sua applicabilità del 25 maggio 2018, ha rivoluzionato il modo in cui fino a quel momento tutti i soggetti economici si erano relazionati con i dati personali.

Moltissimi professionisti, compreso il sottoscritto, si sono specializzati nella materia per fornire ai propri clienti un valido supporto atto a garantire la loro conformità alle molteplici novità che il Regolamento ha portato con sé.

I soggetti più precoci hanno accolto la necessità dell'adeguamento alla normativa europea nell'arco di tempo dei due anni concessi dall'UE. Altri hanno compreso tale necessità solo recentemente. Altri ancora non si sono adeguati, talvolta per non conoscenza di tale esigenza, talaltra, ed è il caso più comune, nell’errata convinzione della non necessità.

Ciò che l'Unione Europea ha chiesto ai diversi operatori economici, in buona sintesi, è di ridisegnare e strutturare l'intera loro dimensione operativa-produttiva attorno a principi molto importanti. Si parla spesso di "privacy by design" e "privacy by default" proprio per racchiudere questo concetto all'interno di due semplici ed incisive formule[1].

L'intera realtà aziendale è chiamata a rivoluzionarsi a livello strutturale nel modo in cui si relaziona e tratta i dati personali di tutti i soggetti con cui entra in contatto.

Inoltre, i processi aziendali inerenti a qualsiasi dato personale devono essere scanditi da procedure standardizzate in grado di garantire il rispetto di tutte le prescrizioni imposte dal GDPR.

Una delle grandi novità di questo Regolamento, tuttavia, è la modalità con cui L'Unione Europea ha chiesto alle imprese di adeguarsi. Ed è proprio questo aspetto che, credo, possa aver ingenerato il

maggior numero di incertezze.

Si ha spesso l'idea che la legge prescriva comportamenti che se violati comportano una punizione. Si tende, quindi, a cercare di comprendere quali atteggiamenti siano contrari alla legge prima di agire, conformandosi al dettato normativo ed evitando di incorrere nelle relative sanzioni.

L'assetto normativo contenuto nel GDPR, tuttavia, è in parte diverso dalla summenzionata struttura.

Ciò che l'UE ha fatto con il proprio Regolamento è l'aver posto le basi irrinunciabili per la garanzia della corretta circolazione dei dati personali.

Ciò è stato possibile attraverso una serie di definizioni, principi, prescrizioni generali e sanzioni[2].

Quando parlo di "prescrizioni generali" intendo dire che il legislatore europeo non impone specificatamente alcuni comportamenti a chi tratta dati personali o, meglio, non solo. La Commissione e il Parlamento Europeo chiedono ai soggetti di "tendere verso il miglior risultato possibile" lasciando un certo grado di libertà agli operatori sul come realizzare questo obiettivo.

La ragione di ciò è che la molteplicità, varietà, complessità delle realtà esistenti non avrebbe mai permesso di strutturare una norma valevole per tutti in tutti i luoghi. Sono, quindi, i singoli soggetti a dover adeguarsi ai principi e dettati del Regolamento attraverso un'"auto-analisi" della propria realtà operativa e del proprio lavoro.

Tale attività, tuttavia, non si esaurisce in singole definite operazioni, ma delinea un processo continuo in cui il "titolare dei dati personali" è costantemente impegnato, attraverso analisi, rimodulazioni della struttura adottata, revisione dei documenti realizzati e predisposti, valutazioni continue, e via dicendo[3].

Ciò che mi sembra di capire dalla mia esperienza, invece, è che i soggetti economici non hanno ben chiaro questo concetto e credono che una volta realizzati tutta una serie di adempimenti, demandati a professionisti pagati proprio per tale attività, la conformità al Regolamento Europeo sia garantita e il rischio di sanzioni azzerato.

Altro elemento particolarmente delicato, inoltre, è la mancanza di consapevolezza dell'importanza del dato personale.

Le aziende tendono a vivere il DGPR come un ulteriore ostacola alla propria attività. Un nuovo "problema" imposto dall'alto al quale lo Stato chiede di far fronte con i relativi costi.

Anche tale asserzione, tuttavia, è ben lontana dalla realtà.

L'idea di fondo del Regolamento Europeo in materia di trattamento dei dati personali, infatti, è quella di

garantire il corretto sfruttamento economico dei dati trattati.

Essa nasce dalla consapevolezza che "il dato è ricchezza", così come il suo sfruttamento[4].

La circolazione dei dati personali in Europa, dunque, deve avvenire nel modo più libero possibile e deve essere alla base di nuovi modelli di impresa e di produzione di benessere.

L'idea, quindi, è quella di avere una normativa che assicuri un minimo di tutela di un asset che è sinonimo di sviluppo per l'impresa[5].

Fintanto che il GDPR continuerà ad essere visto dagli operatori economici come un ostacolo senza cogliere il vero senso dello stesso, le imprese rimarranno legate ad un modello di business passato, antico, non attuale, perdendo la possibilità di crescere economicamente.

Un'impresa che ancora oggi non è conforme ai GDPR è un'impresa saldamente legata al passato ma senza uno sguardo al futuro.

Basti pensare, infatti, che il Regolamento è stato pensato e redatto nel 2015-2016.

Una delle accuse maggiori che gli sono state mosse è stata quella per cui, già al momento della sua attuazione nel 2018, lo stesso era già vecchio, obsoleto.

Ciò, ovviamente, corrisponde solo parzialmente alla realtà, ma ben ci dà l'idea di come il progresso sia più veloce dell'attività legislativa.

Oggi è il tempo del lavoro in cloud, della blockchain e degli smart contracts, dei big data e di forme contrattuali, di impresa e di lavoro ben diverse da quelle esistenti nel 2016 e al tempo nemmeno ipotizzabili.

Un'impresa che non si adegua correttamente ai GDPR è un'impresa che sta mancando dell'opportunità di restare al passo con i tempi in quanto dimostra di non essere nemmeno arrivata a strutturarsi secondo gli schemi del 2015, figuriamoci secondo quelli del 2021.

Il perché di un white paper

Negli ultimi tre anni ho presentato alle aziende la necessità di adeguarsi ai GDPR manifestando l’importanza di avere un registro dei dati personali, della modulistica in materia di privacy, di gestione del dato, di trattamento, della formazione di tutti i lavoratori e soggetti coinvolti. E ancora del concetto di dato sensibile e della valutazione di impatto (DPIA), della nomina o meno di un DPO, e via dicendo.

Diritto & Diritti ISSN 1127-8579

Un lavoro che ho svolto con passione assieme a numerosissimi colleghi.

Un lavoro necessario ma non esaustivo. Anzi.

Posso dire con assoluta serenità che gli adempimenti in materia GDPR che tutti ci siamo premurati di presentare e vendere non sono che la base o, ancor meglio, l'inizio di un percorso.

Una volta conclusa questa "prima fase di conformità ai GDPR" il mio lavoro si sarebbe potuto concludere.

Per dovere di correttezza professionale, nonché per onestà intellettuale, tuttavia, non mi sono mai sottratto dall'informare che quanto appena realizzato con e per l'azienda per la quale avevo lavorato non era che l'inizio.

Io avevo solo dato l'impulso, all'impresa sarebbe toccato il restante, ben più impegnativo, compito di adeguamento ai GDPR.

Ma come, mi è stato spesso chiesto, "dopo tutto questo lavoro lo Stato mi chiede altre "scocciature"? Altre "carte"? Ancora adempimenti"?

Ecco, in quei momenti ho compreso che la realtà che avevo davanti non aveva ancora compreso nulla dell'importanza e della struttura dei GDPR.

Di qui la ragione di questo White Paper con il quale mi auguro di aprire gli occhi a molte di quelle realtà aziendali.

In primo luogo mi preme rasserenare il cliente sul fatto che, concluso il mio lavoro di "adeguamento", l'impresa può tranquillamente fare a meno di me.

Così almeno fino al momento di un eventuale controllo da parte del Garante per la protezione dei dati personali.

Le aziende che seguo, però, devono necessariamente essere avvertite del fatto che il mio secondo intervento può essere benissimo evitato attraverso una corretta gestione dei dati personali in loro possesso.

Ma perché mai dovrei consigliare una cosa del genere? Non andrebbe contro il mio stesso interesse?

In realtà no.

Sono profondamente convinto che una società che anziché investire sulla cura investe in prevenzione, oltre ad ottenere un risparmio, ha la possibilità di veicolare la ricchezza in investimenti differenti i quali,

ancora una volta, potranno riguardare me e le mie consulenze.

Perché è necessario mettere in evidenza un punto molto importante: nessuno è in salvo dall'occhio del Garante Privacy.

Le realtà economiche, infatti, si trovano costantemente nella condizione di dover rispondere a richieste di chiarimenti da parte del Garante il quale, ove ravvisi una violazione della normativa GDPR, ha il potere di infliggere pesanti sanzioni.

Non pensiamo che questa sia solo una remota possibilità.

Il Garante non ha, infatti, sanzionato solo grandi società con la TIM, la Vodafone, Iliad, WindTre (così citandole tutte e quattro), ma anche realtà molto più "comuni" e con sanzioni ben più "leggere" rispetto alla famosa sanzione del 1° febbraio 2020 pari a € 27.802.946,00 di TIM.

Ciò che vorrei far capire all'impresa cliente, tuttavia, è che con le giuste accortezze ed investimenti, le risorse possono essere spese in altri modi ben più produttivi.

Il costo della sanzione amministrativa, in effetti, è solo uno e il più evidente dei costi relativi all'inadempimento ai GDPR.

Si dimentica spesso, invece, che per rispondere alle richieste di chiarimento del Garante è spesso necessario avvalersi di tutta una serie di professionisti, anche avvocati, con lo scopo di evitare quanto più possibile la sanzione.

Ma quante risorse e quante energie questo processo comporta?

Non sarebbe meglio strutturarsi e adottare i progetti di "privacy by design" e "privacy by default" richiesti dalla normativa europea?

Tralasciando la possibile rilevanza in sede penale[6] delle violazioni in materia privacy (sebbene altrettanto rilevanti) vorrei mantenere alta l'attenzione anche su un ulteriore aspetto, per così dire, "venale". Si tratta della responsabilità in sede civile[7].

Come dimostra la più recente giurisprudenza, le cause che soggetti comuni intentano nei confronti delle aziende per asserita violazione dei loro dati personali sono in costante aumento. Tutto ciò comporta ulteriori costi e perdita di tempo che può anch'esso essere risparmiato o più produttivamente impiegato.

Il messaggio che vorrei passasse forte e chiaro è che l'aver nominato un DPO o aver redatto un registro di trattamento dei dati personali o aver correttamente utilizzato i moduli privacy che sono stati "confezionati" dal nostro professionista di fiducia non è sufficiente.

Il dato personale, qualunque esso sia, una volta raccolto va tutelato, protetto, utilizzato secondo quanto previsto dalla normativa.

Il lavoro dell'impresa che vuole operare nel rispetto della legge e in conformità dei GDPR non si limita, quindi, ad un atteggiamento "statico", impresso su carta, ma richiede uno sforzo costante.

Le soluzioni per ottimizzare questi processi a livello informatico esistono e sono, ad oggi, estremamente economiche in relazione ai costi che il mancato adeguamento alla normativa comporta.

La gestione dei consensi e dei dati personali è un punto troppo trascurato dalle nostre imprese.

Alcune domande meritano una risposta.

Dinnanzi ad una moltitudine di dati necessariamente raccolti nel corso del tempo, l'impresa è effettivamente in grado di rispondere correttamente alle domande eventualmente poste dal Garante in caso di ispezione?

L'impresa è in grado di raccogliere e di rispondere prontamente e positivamente alle istanze a lei poste dal privato in relazione ai dati personali da lui concessi? Pensiamo al diritto all'accesso o all'oblio, alla portabilità dei dati.

Altra domanda fondamentale è la seguente: l'impresa sta adeguatamente trattando i dati come "new oil" (nuovo petrolio)?

Ai miei clienti ricordo sempre come i dati siano ricchezza e il fatto che non lo siano oggi non significa che non lo possano essere un domani.

Una gestione scorretta dei dati personali può determinare la loro inutilizzabilità.

Il che risulterebbe paradossale allorquando l'impresa avesse comunque adottato per anni delle misure di protezione dei dati, salvo scoprire solo al momento del loro uso che le stesse sono state insufficienti.

Ecco un ulteriore costo economico che vorrei i miei clienti evitassero.

Un dato mal raccolto o mal gestito è un dato inutile, anzi dannoso perché espone la società a possibili sanzioni.

Da ultimo ricordo sempre ai miei clienti che l'appetibilità di una società medio-grande si misura anche in termini di asset immateriali in proprio possesso, tra i quali compaiono sicuramente anche i dati personali.

Una società che ancora non si è adeguata ai GDPR, o che lo ha fatto male, perde una grande opportunità

Diritto & Diritti ISSN 1127-8579

di esser ancor più appetibile in termini di acquisizione o investimenti.

Sicuramente le summenzionate considerazioni paiono essere pur sempre personali, seppur date da un professionista.

La sanzione amministrativa conseguente al mancato adeguamento ai GDPR rappresenta, invece, ancora oggi lo strumento più efficace per convincere le imprese della bontà delle mie parole.

L'attività delle Autorità di regolamentazione Privacy da maggio 2018 a marzo 2021.

L'attività delle Autorità di regolamentazione designate dai singoli paesi europei al controllo del rispetto della normativa GDPR ha visto una progressiva impennata nel corso dei mesi trascorsi dalla data di applicabilità del Regolamento 679/2016.

Lo Studio Legale CMS ha cercato di tradurre in dati visibili questa "presa di coscienza" del proprio ruolo, dei poteri, delle proprie capacità di queste Autorità, rappresentandoli nel proprio sito www.enforcementtracker.com.

L'idea che mi sono fatto personalmente è che nel corso dei prossimi anni quest'attività non potrà che conoscere un ulteriore sviluppo, con progressivo aumento sia del numero delle sanzioni che del loro ammontare.

I dati parlano chiaro.

Dalla prima sanzione del 2018 (per un valore di € 400.000,00) si è passati alle totali 584 sanzioni del marzo 2021 per un controvalore pari a € 277.217.088,00 totali[8].

Anche il trend delle singole sanzioni emesse per mese sembra in costante aumento. Dall'unica sanzione emessa nel luglio 2018, si passa alle 34 del mese di marzo 2021, con un picco di 55 sanzioni/mese del mese di dicembre 2020.

Per quanto riguarda specificamente l'Italia, l'Autorità Garante per la protezione dei dati personali ha emesso 67 sanzioni per un totale di € 76.065.601, divenendo la seconda Autorità in Europa per numero totale di sanzioni e la prima per valore totale in euro di sanzioni inflitte. (Si badi che la Spagna, prima con le sue 213 sanzioni, è solo quinta per valore totale in euro). Insomma, un buon primato.

Diritto & Diritti ISSN 1127-8579

La curiosità, a questo punto, è d'obbligo e ci spinge a chiederci quali siano le ragioni più comuni per le quali gli operatori economici europei sono stati sanzionati.

- Insufficiente base giuridica per il trattamento dei dati: € 164,764,848 (su 229 sanzioni)
- Insufficienti misure tecniche ed organizzative volte ad assicurare la sicurezza delle informazioni: € 65,904,419 (su 138 sanzioni)
- Non conformità ai principi generali per il trattamento dei dati: € 24,620,264 (su 114 sanzioni)
- Mancanza di rispetto dei diritti soggettivi in materia di dati: € 16,024,025 (su 59 sanzioni)
- Mancanza di rispetto degli obblighi di informazione: € 5,660,445 (su 35 sanzioni)
- Mancanza di rispetto degli obblighi di notificazione di un data breach: € 1,238,291 (su 17 sanzioni)
- Mancata nomina di un DPO: € 186,000 (su 5 sanzioni)
- Insufficiente cooperazione con l'Autorità di controllo: € 183,229 (su 25 sanzioni)
- Data processing agreement (contratto tra titolare e responsabile del trattamento) insufficiente: € 89,380 (su 3 sanzioni)
- Sconosciuta: € 500 (su 1 sanzioni)

Su 626 sanzioni totali, il 36,58% riguardano un' "Insufficiente base giuridica per il trattamento dei dati"; il 22% le "Insufficienti misure tecniche ed organizzative volte ad assicurare la sicurezza delle informazioni"; il 18,21 % la "Non conformità ai principi generali per il trattamento dei dati"; il 9,45 % la "Mancanza di rispetto dei diritti soggettivi in materia di dati"; il 5,6 % la "Mancanza di rispetto degli obblighi di informazione"; il 4 % un'"Insufficiente cooperazione con l'Autorità di controllo"; il 2,72 % la "Mancanza di rispetto degli obblighi di notificazione di un data breach"; lo 0,8 % la "Mancata nomina di un DPO"; lo 0,48 % un "Data processing agreement (accordo per il consenso) insufficiente" e il restante 0,16 % per ragioni non note.

Le violazioni del GDPR nel 2020: una panoramica

L'osservatorio di Federprivacy ha pubblicato un interessante dossier analizzando le fonti istituzionali dei trenta paesi dello Spazio Economico Europeo e realizzando un quadro statistico dei provvedimenti sanzionatori amministrativi emessi nel corso del 2020 sulla base di diverse variabili come il tempo, il valore economico, la tipologia di violazione ed il settore[9].

I diversi dati raccolti e i grafici proposti confermano il medesimo trend precedentemente illustrato.

Inoltre, dimostrano come le sanzioni del 2020, diversamente che da quelle del 2018 e del 2019, abbiano avuto ad oggetto maggiormente il modo con cui le realtà economiche si sono concretamente approcciate con i dati personali piuttosto che il mancato adeguamento ai GDPR dal punto di vista più formale (ossia nella predisposizione di tutti quegli aspetti preliminari, come la documentazione, l'informativa, il registro dei trattamenti, etc…)

Passiamo all'analisi di qualche dato.

L'Italia si classifica al secondo posto sia per numero di sanzioni che per valore economico di esse.

Per quanto riguarda la tipologia di violazioni e la relativa incidenza economica emerge che il 59,2 % delle sanzioni hanno riguardato trattamenti illeciti, il 20,8 % le misure di sicurezza, nel 9,1 % dei casi hanno riguardato i diritti dell'interessato, mentre le violazioni sulle informative sono state il 3,8% del totale.

Infine, dando uno sguardo ai settori maggiormente sanzionati nel 2020, emerge come tra i primi 10 settori più sanzionati il più colpito per numero di procedimenti nel 2020 è stato quello delle telecomunicazioni con 69 multe, seguito da quello dei servizi e da quello del commercio, rispettivamente con 47 e 45 sanzioni, mentre la pubblica amministrazione è stata oggetto di 41 multe delle autorità di controllo.

Guardando però il valore economico complessivo delle sanzioni, il settore più colpito è quello di internet ed e-commerce con 144,9 milioni di euro di multe (pari al 47% del totale), e a seguire quello delle telecomunicazioni con 62,4 milioni di euro, e poi quello di commercio e attività produttive con 38,1 milioni di euro di sanzioni.

GDPR: le due grandi tipologie di violazioni

Tra le tipologie di sanzioni ritengo sia possibile operare una divisione in due grandi gruppi: il primo avente ad oggetto le sanzioni derivanti da una mancata predisposizione degli strumenti-base necessari per poter conformarsi al GDPR (Insufficienti misure tecniche ed organizzative volte ad assicurare la sicurezza delle informazioni; Mancanza di rispetto degli obblighi di informazione; Mancata nomina di un DPO; Data processing agreement (contratto tra titolare e responsabile del trattamento) insufficiente).

Diritto & Diritti ISSN 1127-8579

Con essi mi riferisco, ad esempio, alla nomina del DPO, alla creazione di un registro per il trattamento dei dati e a tutti quei documenti necessari per raccogliere il consenso dei soggetti.

Si tratta di tutte quelle operazioni "prodromiche" che nell'incipit di questo white paper spiegavo essere state l'oggetto principale di tutti i professionisti che hanno proposto alle aziende di "adeguarsi" al nuovo GDPR.

Il secondo gruppo, invece, comprende tutte quelle sanzioni inflitte per il modo in cui il consenso raccolto è stato gestito (Insufficiente base giuridica per il trattamento dei dati; Non conformità ai principi generali per il trattamento dei dati; Mancanza di rispetto dei diritti soggettivi in materia di dati;

Mancanza di rispetto degli obblighi di notificazione di un data breach; Insufficiente cooperazione con l'Autorità di controllo;

Data processing agreement (contratto tra titolare e responsabile del trattamento) insufficiente).

Tali sanzioni riguardano l'attività di costante controllo, sorveglianza, monitoraggio e corretto uso dei dati raccolti.

A ben vedere, pare che sia proprio una scorretta gestione dei dati la ragione principale della stragrande maggioranza delle sanzioni che hanno colpito gli operatori economici.

Da ciò ricaviamo due possibili letture: la prima è che, forse, le aziende europee si sono preparate correttamente all'avvento dei GDPR, adottando tutta una serie di documenti e strumenti.

La seconda è che, molto probabilmente, tali strumenti sono rimasti sulla carta e che, una volta predisposti, le aziende hanno continuato ad operare senza curarsi realmente di gestire correttamente tutta la mole di dati in loro possesso.

A conferma di ciò è proprio il fatto che il secondo gruppo raccoglie il 71,04 % della totalità delle sanzioni [10](se si esclude lo 0,16 % della ragione non nota).

Il significato delle violazioni

Cerchiamo di capire quale sia la relazione tra sanzione e quella che ho definita essere una scorretta gestione dei consensi, analizzando le singole diciture:

- Insufficiente base giuridica per il trattamento dei dati.

Ogni dato va trattato in modo lecito, corretto e trasparente. Per poter adempiere a ciò, l'art. **6 (coordinato con i successivi art. 7-8)** dei GDPR impone l'esistenza di una valida base giuridica per il trattamento dei dati.

Le sei basi giuridiche per il trattamento dei dati previste dal GDPR sono:

Si tratta del consenso che il soggetto interessato dà al fine che i suoi dati personali possano essere trattati.

Il consenso deve essere dato liberamente, inequivocabile, e deve essere facilmente revocabile.

Poiché in caso di controlli è il titolare dei dati a dover dimostrare tutto ciò, è abbastanza semplice comprendere che l'operatore economico deve essere in possesso di una struttura in grado, ad esempio, di ordinare e catalogare i consensi, permettendo inoltre a chi ha prestato il consenso di poterlo revocare in qualsiasi momento (nonché di conoscere di quali dati l'azienda è in possesso e, in caso di domande, rispondere prontamente entro 30 giorni).

Una raccolta e una sistemazione dei dati caotica rende impossibile tutte queste operazioni.

- Esecuzione di un contratto.

Significa che i dati possono essere trattati allorché siano necessari per dare esecuzione ad un contratto voluto dall'interessato.

Anche in questo caso è importante porre molta attenzione sul fatto che tutti i dati raccolti che non hanno una correlazione con una qualche previsione contrattuale devono avere una base giuridica differente per poter essere trattati.

Ancora una volta, quindi, il modo in cui vengono ordinati, catalogati, sistemati i dati ottenuti può avere una importante funzione di autocontrollo funzionale ad evitare di essere sanzionati.

- Obbligo legale.

Ad esempio perché richiesto dalla normativa in materia di lavoro, sicurezza, diritti del consumatore, etc…

- Interesse vitale.

Diritto & Diritti ISSN 1127-8579

Si tratta del caso in cui il trattamento dei dati personali risulti necessario per tutelare il bene vita del destinatario. (Molto più comune in ambito medico che in quello commerciale).

- Pubblico interesse.

Si ha laddove il trattamento è necessario per finalità decise da un'Autorità Pubblica.

- legittimo interesse.

Come spiegato dalle autorità europee: "un'azienda/organizzazione ha un interesse legittimo quando il trattamento avviene all'interno di una relazione con il cliente, quando si trattano dati personali per scopi di marketing diretto, per prevenire frodi o per garantire la sicurezza della rete e dei dati dei sistemi informatici dell'azienda". Inoltre, "La tua azienda/organizzazione deve anche verificare che, perseguendo i propri legittimi interessi, i diritti e le libertà di tali persone non siano seriamente pregiudicate[11]"

Occorre porre particolare attenzione alla scelta della base giuridica per il trattamento dei dati per diverse ragioni:

- ci può essere una sola base giuridica per ogni trattamento e la scelta deve essere fatta prima del trattamento stesso.

Ciò significa che non ci possono essere "trattamenti correttivi postumi".

Una volta fatta la scelta, questa deve essere mantenuta e non può essere modificata o alternata con altre, pena la non utilizzabilità del dato.

- Qualsiasi sia la scelta deve poter essere dimostrata in qualsiasi momento, sia agli interessati che alle autorità di controllo, quale base giuridica è stata scelta per ogni singolo dato.

Ad esempio, un'azienda dovrà sempre essere in grado di dimostrare quando e come un soggetto ha dato il consenso all'esecuzione del contratto.

Anche in questo caso, una mancanza di organizzazione e strutturazione interna dei sistemi di gestione del consenso rende difficile, se non impossibile, tale operazione, comportando una violazione del GDPR.

Diritto & Diritti ISSN 1127-8579

- La scelta della base giuridica ha un impatto significativo nel modo in cui l'azienda/società è chiamata a rispondere alle richieste da parte del destinatario qualora costui voglia esercitare un proprio diritto (ad es. il diritto all'oblio).

Esistono condizioni, eccezioni e limitazioni che possono differire a seconda del tipo di trattamento scelto.

- Sempre connesso al punto precedente, se un'azienda/società tratta differenti dati con differenti basi giuridiche, deve sempre essere in grado di distinguere per ogni dato quale base giuridica è stata scelta per adempiere alle richieste del destinatario.

- Alcuni dati (come quelli inerenti alla religione, all'etnia, alla salute, etc…) hanno un'unica base giuridica. (cfr. **9-10** GDPR)

È bene precisare che non esiste una base giuridica superiore ad un'altra.

La scelta deve essere fatta in base allo scopo del trattamento, del tipo di dato personale e della relazione con il dato.

La non conformità tra scelta e gestione può comportare una violazione di numerosi aspetti del GDPR: la mancanza di base giuridica del trattamento, l'insufficiente organizzazione, la violazione dei diritti personali, la mancanza di controllo dei dati, etc…

- Non conformità ai principi generali per il trattamento dei dati.

Si tratta in particolar modo dell'art. **5** GDPR (ma anche degli artt. **44-45-46-47-48-49** sulle cautele per il trasferimento dei dati in Paesi terzi).

Si rammenta che dati debbono essere **trattati** in modo lecito, corretto e trasparente nei confronti dell'interessato.

Le **finalità** devono essere determinate, esplicite e legittime; **i dati:** adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantirne un'adeguata sicurezza.

L'art. 5 GDPR ha un'interferenza con tutti gli altri articoli, essendo il cuore dell'intera normativa.

Diritto & Diritti ISSN 1127-8579

Anche quest'articolo dimostra che la gestione dei dati raccolti è un'operazione "insidiosa" e che richiede una certa dedizione ed impegno.

Senza una corretta organizzazione com'è possibile, ad esempio, pensare di limitare la conservazione del dato raccolto?

Come riuscire a capire se, come e quando è necessario limitare l'uso di un dato o cancellarlo (al fine di garantire il diritto all'oblio)?

- Mancanza di rispetto dei diritti soggettivi in materia di dati.

Il Regolamento formalizza un ampio catalogo di diritti che spettano all'interessato.

Si tratta del diritto di **accesso**, del diritto di **rettifica**, del diritto alla **cancellazione** (più noto come diritto all'oblio), del diritto di **limitazione del trattamento**, del diritto alla **portabilità dei dati**, del diritto di **opposizione al trattamento**, con gli eventuali connessi obblighi di **notifica/comunicazione gravanti sul titolare**. (Si tratta degli artt. **15-16-17-18-20-21** GDPR, ma anche dell'art. **22** sui processi decisionali automatizzati).

Anche in questo caso una cattiva gestione del consenso rende impossibile per l'operatore economico provvedere a consentire l'accesso dei dati al destinatario; la rettifica dei suoi dati ove richiesta; la loro cancellazione; provvedere alla portabilità dei dati oppure, come al punto sotto, notificare un data breach (o anche solo riconoscere l'esistenza di un data breach e per quali dati e con quale impatto).

Il mancato rispetto dei diritti si connette, infine, anche alla disposizione di cui all'art. **12 GDPR** in materia di "Trasparenza nella gestione dei trattamenti".

Il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima.

- Mancanza di rispetto degli obblighi di notificazione di un data breach. (Art. **33-34** GDPR)

- Insufficiente cooperazione con l'Autorità di controllo. (artt. **31-58** GDPR)

Diritto & Diritti ISSN 1127-8579

La domanda va da sé: com'è possibile riuscire a cooperare con il Garante Privacy se, dopo aver raccolto i consensi, questi sono stati abbandonati a loro stessi nel caos più totale? Anche in questo caso scatterà la sanzione.

Ma cosa hanno in comune tutte queste violazioni?

A me sembra che condividano l'errato modo con cui il titolare dei dati ha concretamente utilizzato, manipolato, conservato, lavorato, in una parola sola "gestito" i dati che gli interessati gli hanno affidato.

Vediamo ora le restanti violazioni, che abbiamo individuato come parte di un altro grande gruppo di adempimenti cosiddetti "preparatori" al GDPR. Tra queste troviamo:

- Insufficienti misure tecniche ed organizzative volte ad assicurare la sicurezza delle informazioni. **24, 25, 29, 30, 32, 35, 36 GDPR.**
- Mancanza di rispetto degli obblighi di informazione. Artt. **13-14** GDPR
- Mancata nomina di un DPO. (artt. **37-39** GDPR)
- Data processing agreement (contratto tra titolare e responsabile del trattamento) insufficiente. **28 GDPR**.

Ponendoci la stessa domanda fatta per il gruppo di violazioni precedenti: cosa condividono queste violazioni?

Credo di poter sostenere che siano tutte violazioni "preparatorie"-"strutturali" che, molto spesso, sono adempiute con una corretta preparazione "sulla carta".

Non riguardano, infatti, tanto il modo in cui i dati sono "gestiti" concretamente dal titolare, ma il modo in cui sono "prelevati" e "archiviati" e "protetti".

Esse riguardano il primo aspetto fondamentale della famosa "privacy by design and by default".

Tuttavia, costituiscono solo il primo adempimento, quello più semplice, ossia quello che negli ultimi anni è stato il più proposto alle realtà economiche dai diversi professionisti in materia di GDPR.

Questi articoli appena menzionati sono "il punto di partenza" per adempiere correttamente al GDPR.

Diritto & Diritti ISSN 1127-8579

Purtroppo, però, vengono spesso intesi come la condizione necessaria e sufficiente.

Come visto, però, così non è assolutamente.

Violazioni articolo per articolo: una statistica.

Nelle prime pagine di questo white paper mi sono servito delle statistiche realizzate dal "GDPR Enforcement Track" di CMS Law per dimostrare la crescente attività delle Autorità Garanti della Privacy in Europa dall'entrata in vigore del GDPR ad oggi.

Vorrei provare, ora, a prendere in analisi un più limitato periodo di tempo per comprendere quali articoli in particolare sono stati oggetto di sanzione per la loro violazione.

Passerò in rassegna, dunque, un periodo di tempo che va dal marzo 2020 (inizio della pandemia dovuta al Covid-19) a metà aprile 2021 (più o meno i giorni nostri).

Per prima cosa cercherò di capire quali articoli sono stati maggiormente oggetto di attenzione in Europa e, successivamente, farò lo stesso concentrando l'attenione sul nostro Paese[12].

EUROPA. Marzo 2020 – Aprile 2021

Numero di sanzioni: 380

Numero di articoli violati: 832

Analisi articolo per articolo:

Diritto & Diritti ISSN 1127-8579

- 5: articolo violato 243 volte
- 6: articolo violato 160 volte
- 7: articolo violato 11 volte
- 8: articolo violato 2 volte
- 9: articolo violato 24 volte
- 12: articolo violato 33 volte
- 13: articolo violato 52 volte
- 14: articolo violato 22 volte
- 15: articolo violato 26 volte
- 16: articolo violato 1 volta
- 17: articolo violato 11 volte
- 18: articolo violato 1 volta
- 21: articolo violato 15 volte
- 24: articolo violato 12 volte
- 25: articolo violato 13 volte
- 28: articolo violato 12 volte
- 29: articolo violato 3 volte
- 30: articolo violato 2 volte
- 31: articolo violato 14 volte
- 32: articolo violato 100 volte
- 33: articolo violato 21 volte

Diritto & Diritti ISSN 1127-8579

- 34: articolo violato 9 volte
- 35: articolo violato 9 volte
- 36: articolo violato 1 volte
- 37: articolo violato 6 volte
- 44: articolo violato 1 volta
- 48: articolo violato 1 volta
- 58: articolo violato 26 volte

ITALIA. Marzo 2020 – Marzo 2021

Numero di sanzioni: 57

Numero di articoli violati: 165

Analisi articolo per articolo:

- 5: articolo violato 50 volte
- 6: articolo violato 28 volte
- 7: articolo violato 4 volte
- 8
- 9: articolo violato 14 volte
- 12: articolo violato 9 volte
- 13: articolo violato 11 volte
- 14: articolo violato 2 volte

- 15: articolo violato 6 volte
- 16: articolo violato 1 volta
- 17: articolo violato 2 volte
- 18
- 21: articolo violato 2 volte
- 24: articolo violato 3 volte
- 25: articolo violato 5 volte
- 28: articolo violato 7 volte
- 29: articolo violato 1 volta
- 30: articolo violato 1 volta
- 31
- 32: articolo violato 12 volte
- 33: articolo violato 2 volte
- 34: articolo violato 1 volta
- 35: articolo violato 2 volte
- 36
- 37: articolo violato 2 volte
- 44
- 48
- 58

Una volta raccolti i dati ho proceduto a dividere ancora una volta tra violazioni “strutturali-preparatorie” (in verde) e violazioni della “gestione dei consensi” (in giallo).

Aggregando i dati è emerso che, quanto all’interno dell’UE, su 832 articoli del GDPR violati, 232 hanno riguardato previsioni “strutturali-preparatorie” (27.88%), mentre 600 la “gestione dei consensi” (72,12%).

In Italia, invece, in un anno, su 165 articoli del GDPR violati, 46 hanno riguardato previsioni “strutturali-preparatorie” (27.88%), mentre 119 la “gestione dei consensi” (72,12%).

Il risultato, abbastanza sorprendente quanto all’esattezza della percentuale, è che l’Italia risulta perfettamente in linea con la media europea.

Come da ipotesi, sia in Europa che in Italia, la stragrande maggioranza delle sanzioni dell’ultimo anno non hanno avuto ad oggetto gli aspetti “preparatori-strutturali” di conformità al GDPR, ma la scorretta gestione dei consensi.

Sicuramente è un dato su cui bisognerebbe riflettere e, possibilmente, spingere gli operatori economici ad attività di “prevenzione” a questa falla.

Se ancora non bastasse…

Finora ho parlato solamente delle sanzioni amministrative in quanto più immediatamente “evidenti”.

È importate ricordare, tuttavia, che non tutti i procedimenti aperti dall’Autorità Garante per la privacy sfociano in un provvedimento sanzionatorio pecuniario.

Talvolta, infatti, la procedura si interrompe in medias res.

Ma, a quale prezzo?

Come già detto, dover gestire un’incursione del Garante all’interno della propria realtà economica significa dover premunirsi di esperti, avvocati, tecnici che anziché dedicarsi ad altre attività sono chiamati a concentrarsi sull’evitare la sanzione.

Senza contare che, nel tempo necessario agli approfondimenti, l’Autorità Garante ha il potere di limitare, sospendere o bloccare i trattamenti in corso, paralizzando l’attività economica.

Diritto & Diritti ISSN 1127-8579

Ovviamente, migliore sarà l'organizzazione della gestione dei consensi e minore sarà il tempo da dover dedicare alla dimostrazione della propria conformità.

Ma dicevamo che non ci sono solo sanzioni pecuniarie.

Ebbene sì, perché talvolta, accanto alle (spesso pesanti) sanzioni economiche se ne possono aggiungere delle altre.

In primo luogo, da non sottovalutare, sono le ripercussioni in termine di danno reputazionale della realtà economica, soprattutto se medio-grande.

In un mondo digitalmente connesso, in cui la reputazione e il buon nome sono tutto, la cattiva pubblicità può costare caro e rendere invisa ad investitori e clienti una certa società/impresa in quanto stigmatizzata come "realtà che non rispetta la privacy dei clienti".

Una stigmate che è meglio evitare.

Inoltre, anche ove l'Autorità Garante decidesse di non sanzionare in via amministrativa, esistono le cd. "Sanzioni correttive" che possono consistere nel:

- rivolgere avvertimenti al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare le norme;

- rivolgere ammonimenti al titolare o al responsabile del trattamento ove i trattamenti abbiano violato le norme;

- ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;

- ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle norme, specificando eventualmente le modalità e i termini per la conformità;

- imporre una limitazione provvisoria o definitiva al trattamento, sospendere temporaneamente il trattamento, o vietare del tutto;

- ordinare la rettifica, la cancellazione o l'aggiornamento dei dati personali;

- revocare le certificazioni o ingiungere all'organismo di certificazione di ritirare le certificazioni rilasciate se i requisiti non sono soddisfatti;

- infliggere le sanzioni amministrative pecuniarie;

Diritto & Diritti ISSN 1127-8579

- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Infine, se anche queste sanzioni non bastassero, esiste un altro possibile danno economico per chi viola il GDPR.

Si tratta delle sempre più comuni cause civili in materia di responsabilità extracontrattuale per violazione dei diritti privacy dei soggetti.

Sul punto, senza pretesa di esaustività, si deve rilevare come la giurisprudenza sia sempre più indirizzata nel riconoscere all'illecito trattamento dei dati ex art. 82 GDPR una responsabilità oggettiva per rischio d'impresa derivante dall'attività di trattamento dei dati personali in violazione delle regole di condotta conformative, protettive dell'interessato-danneggiato.

Il risultato è che un soggetto, ove ritenga che una società abbia leso i suoi diritti in materia di privacy dovrà solo allegare il fatto e la violazione della norma per ottenere un risarcimento materiale e immateriale, spettando alla Società, invece, il duro compito di dimostrare il rispetto della normativa contenuta nel GDPR[13].

Conclusioni

Il presente white paper non nasce con l'idea di spaventare gli operatori economici ma di sensibilizzarli sul fatto che il dato personale rappresenta nella nostra economia una grande opportunità ma che, ove non vengano assunte adeguate strumentazioni in grado di "padroneggiarlo" il rischio è che lo scotto da pagare sia davvero importante.

L'invito, quindi, è sempre quello di cercare dei sistemi efficaci ed efficienti atti a prevenire il problema e ad essere pronti ad ogni evenienza.

Non bisogna essere miopi, ma è fondamentale considerare tutte le ripercussioni che un mancato adeguamento alla normativa del GDPR può comportare[14].

Il primo passo che invito ognuno a fare, in conclusione, è quello di porsi alcune domande come: "di quali dati sono in possesso? Perché posso tenerli? Ho un consenso specifico e ho registrato eventuali obiezioni? Come continuerò a monitorare e consentire azioni ed obiezioni? Sto rispettando i diritti del soggetto interessato? Etc…", con l'invito di agire di conseguenza nel più breve tempo possibile.

Volume consigliato

Diritto & Diritti ISSN 1127-8579

Note

[1] Sulla nozione del principio di precauzione e sull'applicazione di tale principio nelle nuove tecniche

di tutela delle cc. dd. privacy by design e privacy by default, anche alla luce del diritto sovranazionale, nonché sull'incidenza che tale principio ha avuto sulla responsabilità civile e, in particolare, sul rafforzamento della sua funzione preventiva, v. Stanzione, Incidenza del principio di precauzione sulla responsabilità civile negli ordinamenti francese e italiano, in Comparazione e Diritto civile, 1-38. Disponibile al link http://www.comparazionedirittocivile.it/prova/files/STANZIONE_PRECAUZIONE_2016.pdf

[2] Letture utili alla comprensione di questi concetti sono, in dottrina, quelle delle opere di: Siano, Art. 24, in Riccio, Scorza, Belisario (a cura di), GDPR e Normativa Privacy, Commentario, Milano, 2018, 236-245. V. anche Lucchini Guastalla, Privacy e Data Protection: principi generali, in Tosi (a cura di), Privacy digitale, Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, Milano, 2019, 82 e segg.; Id., Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori, in Contratto e Impresa, 2018, I, 106-125; Poletti, Causarano, Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, in Tosi (a cura di), Privacy digitale, cit., 377 e segg.; Tosi, La responsabilità civile per trattamento illecito dei dati personali, in ibidem, 639 e segg.; in materia di responsabilità civile, si veda anche Bilotta, La responsabilità civile nel trattamento dei dati personali, in Panetta (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy), Milano, 2019, 460 e segg.

[3] Per approfondimenti in dottrina, E. Faccioli – M. Cassaro, Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design, in Diritto Industriale, 2018, 6, 6561.

[4] Si legga, ad esempio: Commissione Europea, Una strategia europea per i dati, 19 febbraio 2020, p. 15:

«la strategia dei dati europea si basa su un florido ecosistema di soggetti privati per creare valore economico e sociale a partire dai dati. (…) l'Europa dovrebbe offrire un contesto che sostiene l'innovazione basata sui dati e stimola la domanda di prodotti e servizi che dipendono dai dati quale importante fattore di produzione». Per una ricostruzione della crescente importanza di assicurarsi le "materie prime" che consistono nei dati personali e per un'analisi dei modelli economici fondati su questi ultimi si veda: Zuboff, Il capitalismo della sorveglianza: Il futuro dell'umanità nell'era dei nuovi poteri, Roma, 2019, Cap. III e V, rispettivamente 73 ss. e 139 ss.

[5] Il dato personale è spesso raffigurato metaforicamente come il "nuovo petrolio". Tale metafora è ricorrente nei documenti di molte istituzioni. a titolo di esempio, si veda il documento del World Economic forum, secondo cui «personal data will be the new "oil" - a valuable resource ofthe 21st century. It will emerge as a new asset class touching all aspects of society», WEF, PersonalData: the Emergence of a new

Asset Class, 2011, disponibile all'indirizzo: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. Si vedano inoltre i discorsi the big data revolution, del vice-presidente della Commissione europea, del 26 marzo 2013, consultabile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/sPEECH_13_261 e della Commissaria europea Kuneva, Roudtable on online data collection, targeting and profiling, 31 maggio 2009, consultabile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/sPEECH_09_156. Per quanto riguarda la letteratura accademica, si veda, tra i tanti esempi: De Monjoye, Wang e Pentland, On the trusted use of large-scale personal data, in Data Eng., vol. XXXV, n. 4, 2012, 5. Sulla c.d. economia del dato profilato, si rinvia a Ricciuto, La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, in I dati personali nel diritto europeo, a cura di Cuffaro, D'Orazio, Ricciuto, Torino, 2019, 52. Sulla conoscenza dei dati personali quale bene immateriale e, in particolare, sul trasferimento dei dati da parte di Facebook a Cambridge Analytica v. Roppo, Il racconto della legge, Milano, 2019, 364.

[6] Per una disamina sul punto si legga V. Manes – F. Mazzacuva, GDPR e nuove disposizioni penali del codice privacy, in Dir. Pen. e Processo, 2019, 2, 167.

[7] Sulla natura e sul profilo funzionale del modello di responsabilità civile da illecito trattamento dei dati personali quale modello in cui si accentuano i profili di responsabilizzazione degli autori del trattamento e di prevenzione dei danni, v. Gambini, Responsabilità e risarcimento nel trattamento dei dati personali, in V. Cuffaro, R. D'orazio, V. Ricciuto (a cura di). I dati personali nel diritto europeo, Giappichelli, 2019, 1031.

[8] https://www.enforcementtracker.com/?insights

[9] L'intero dossier è disponibile al link: https://www.federprivacy.org/attivita/studi-statistiche?download=393:report-statistico-sanzioni-privacy-see-2020-italiano

[10] Secondo i dati forniti da enforcementtracker.com

[11] Si veda https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_it#:~:text=La%20tua%20azienda%2Forganizzazione%20ha,dei%20sistemi%20informatici%20dell'azienda.

[12] L'analisi è realizzata attraverso un conteggio manuale dei dati raccolti da CMS law e disponibili per la consultazione al sito: https://www.enforcementtracker.com/

[13] Per approfondimenti: E. Tosi, Illecito trattamento dei dati personali, responsabilizzazione,

responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo, in Contratto e Impresa, 2020, 3, 1115.

[14] “Ma la responsabilità del titolare non si esaurisce con la valutazione e l'adozione delle misure di sicurezza. Il titolare deve compiere un'attività di continuo monitoraggio, per verificare che esse siano proporzionate e adeguate ai rischi, anch'essi in continuo mutamento. Occorre dunque una complessa attività di valutazione (tecnica, giuridica e organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di policy interne e quindi un'attività di monitoraggio continuo. Tutto ciò deve essere anche adeguatamente formalizzato e il titolare non soltanto deve attuare la normativa vigente, ma anche essere in grado di dimostrarlo”. Così G. Finocchiaro, GDPR tra novità e discontinuità – il principio di accountability, in Giur. It., 2019,12, 2777.

https://www.diritto.it/la-tua-realta-economica-e-davvero-conforme-al-gdpr/

Diritto & Diritti ISSN 1127-8579