

GDPR E SANZIONI: le fiamme gialle scottano i consulenti del lavoro?

Lo strano periodo transitorio in cui si consigliava ai controllori di avere un atteggiamento soffice nel comminare le sanzioni e, al Garante per la protezione dei dati personali (nel prosieguo amichevolmente solo Garante), di produrre adeguamenti operativi e facilitazioni fumose, si è concluso. Ora anche in Italia il Regolamento EU n. 679/2016 è totalmente e irrimediabilmente operativo ma, giacché ho avuto il piacere di ritrovare qualche *dispencer* di timori sanzionatori, disbrigo subito la pratica multe, più avanti le questioni importanti.

SANZIONI E GUARDIA DI FINANZA

C'è chi punta al secondo comma dell'art. 83 del GDPR ricordando che *“Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso [...]”* calcando sull'interpretazione (corretta) che ciò vale anche in merito a prescrizioni, regolamenti generali e provvedimenti del Garante; altri invece si tuffano direttamente nei commi 4, 5 e 6 nuotando nella tempesta di dieci o venti milioni di euro, con moto ondoso al 2 o 4 per cento del fatturato (magari omettendo *“del fatturato mondiale annuo”* che già rende meglio l'idea rispetto a chi vuole riferirsi il Legislatore). In sostanza possiamo aspettarci che con la primavera spunteranno da ogni dove fioriture di Finanziari che:

1. Ispezioneranno ogni panettiere (chiedo scusa: panificio pasticceria con caffetteria e annesso ufficio finanziamenti) che fa trovare già pronti i sacchetti del pane dei clienti abituali, con sopra scritto a pennarello indelebile il cognome dell'avventore corrispondente, condannandolo per: mancata anonimizzazione, violazione per diffusione dei dati personali e raccolta di dati per la profilazione dell'interessato in merito alle sue abitudini alimentari, senza richiesta di consenso.
2. Entreranno in tutti gli studi dei consulenti del lavoro contestando la liceità del tratta-

mento dei dati personali di natura particolare (precedentemente conosciuti come dati sensibili), per la decadenza dell'Autorizzazione Generale n. 1/2016 del Garante.

Propendo per escludere entrambe le fattispecie ma esaminiamo la seconda (per la quale, tra l'altro, ci sono maggiori sicurezze normative), visto l'ambito di pubblicazione di questo intervento, per la prima attenderò che si faccia avanti *Conformai*.

Il Garante, con la newsletter del 7 febbraio 2019, n. 449, ha chiarito che i consulenti del lavoro sono Titolari quando trattano, in piena autonomia e indipendenza, i dati dei propri dipendenti oppure dei propri clienti quando siano persone fisiche, come per esempio i liberi professionisti, determinando puntualmente le finalità e i mezzi del trattamento. Sono, viceversa, Responsabili quando trattano i dati dei dipendenti dei loro clienti sulla base dell'incarico ricevuto, che contiene anche le istruzioni sui trattamenti da effettuare. Sempre il Garante, con il Provvedimento n. 497 del 13 dicembre 2018, individua le prescrizioni contenute nell'Autorizzazione Generale n. 1/2016 che risultano compatibili con il Regolamento EU n. 679/2016 e con il D.lgs. n. 101/2018 di adeguamento del Codice Privacy (D.lgs. n. 196/2003), che confermano la liceità del trattamento da parte dei consulenti del lavoro (Allegato 1, par. 1.1, lettera e), ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro.

A chiudere il quadro e per porre un pietrone tombale su disquisizioni in punta di fioretto legale, c'è sempre il caro e semplice GDPR che, all'art. 88, stabilisce che *“Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti* ➤

GDPR E SANZIONI: LE FIAMME GIALLE SCOTTANO I CONSULENTI DEL LAVORO?

dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.”

INFORMATIVE, SICUREZZA E DIMOSTRAZIONI

Affianchiamo alla normativa le notizie di stampa (Italia Oggi Sette del 19 aprile 2019): ci sono 7.219 reclami e 946 notificazioni di violazioni della privacy registrati dal Garante nel periodo dal 25 maggio 2018 al 31 marzo 2019 di cui occuparsi. Aggiungiamo le deliberazioni del Garante, nonché le esternazioni pubbliche del Comandante del Nucleo Privacy della Guardia di Finanza, inerenti le attività ispettive che saranno finalizzate principalmente a:

1. trattamenti di dati effettuati da società/enti che gestiscono banche dati di rilevanti dimensioni;
2. trattamenti di dati personali effettuati presso istituti di credito relativamente alla legittimità della consultazione e del successivo utilizzo di dati da parte di soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
3. trattamenti di dati personali effettuati da società per attività di *telemarketing*;
4. controlli nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee sui presupposti di liceità del trattamento e alle condizioni per il consenso qualora il trattamento sia basato su tale presupposto, sul rispetto dell'obbligo di informativa nonché sulla durata della conservazione dei dati. Pertanto gli organi ispettivi difficilmente

varcheranno la soglia degli studi, se non per reclami importanti o segnalazioni di gravi inadempimenti, quindi, semplificando:

- è necessario formare, formalizzandone l'erogazione, gli addetti in quanto autorizzati al trattamento, sia per l'obbligo proveniente da GDPR (artt. 29 e 32) sia per dimostrare di aver fronteggiato il maggior rischio di violazione dei dati: l'umano distratto, inconsapevole o stolto;
- bisogna avere e mettere a disposizione informative scritte precisamente per la propria realtà e finalizzate ai clienti, ai lavoratori dei clienti e ai propri lavoratori: quindi non genericamente copiate e incollate dall'internet (qui personificato nel compagno di banco, che mostra sicumera e fiera determinazione, a cui ci sia aggrappa per svogliatezza o disperazione, onde poi scoprire, al momento del voto, che ne sapeva ancor meno di noi);
- si è costretti a pensare a modalità operative e mezzi di comunicazione che non trasferiscano dati particolari a chiunque e ad alta visibilità (non è detto che servano per forza sistemi di criptazione da Cia, magari possono bastare *software* semplici, oppure distribuzioni controllate di documenti protetti da *password* sicure), nonché a tecnologie di sicurezza informatica che non prevedano l'alabarda lanzichenecca o l'archibugio visconteo, ma accolgano strumenti moderni di protezione;
- consiglio di avere sempre aggiornata una valutazione dei rischi, finanche non redatta da professori ISO (anche se una lettura delle 27014 e 27016 potrebbe non fare male, sicuramente meno nociva del consiglio di un cugino scaduto), ma redatta come elenco di quello che ho, faccio e voglio migliorare (perfettamente imperfetta come il *wabi-sabi* insegna).

I quattro punti qui sopra potrebbero dimostrare *Privacy By Design* e *By Default*, nonché l'*Accountability*, pilastri e travi portanti del GDPR, chiaramente dirimenti in caso di contestazioni e contenziosi, più di tanta carta firmata, controfirmata e cerallaccata.

