Ordine dei Dottori Commercialisti e degli Esperti Contabili Trento Rovereto

COMITATO SCIENTIFICO GRUPPO ODCEC AREA LAVORO

I VOLONTARI E IL RAPPORTO DI LAVORO
Venerdì 22 marzo 2024

Stefano Bacchiocchi
Dottore Commercialista in Brescia
Professore a contratto per l'Università degli Studi di Brescia
DPO

FonAR Com FONDO INTERPROFESSIONALE

CONCERTO.it eLearning per commercialisti

IL NUOVO G.D.P.R.
(Regolamento Europeo 679/2016)
D. Lgs. 4.9.2018 n. 101

pur con qualche criticità data dalla scelta
della forma legislativa:

- Queste due norme hanno novellato il vecchio codice;
- Segnano l'inizio di un nuovo modo di pensare al «dato» ed alla sua protezione;
- La 'privacy' è un processo, un flusso, una creazione di valore;
- La sostanza si sostituisce alla forma;
- Finisce l'era degli adempimenti prestabiliti.

PRINCIPIO DELL'ACCOUNTABILITY (RESPONSABILIZZAZIONE)

Le nuove norme responsabilizzano le figure di riferimento al quale si applica la normativa:

Cioè:

Il titolare del trattamento dovrà adottare un complesso sistema integrato di misure e processi giuridici, organizzativi (anche tecnologici e di formazione del personale) volte alla protezione dei dati personali

E

dovrà essere in grado di dimostrarlo.

PRINCIPIO DELLA 'PRIVACY *BY DESIGN*'

La 'privacy' ora incide anche sull'organizzazione della gerarchia aziendale e sulle modalità di lavoro.

Ad esempio: dovranno essere nominate figure di riferimento, designate per contratto, anche esternamente all'organizzazione.

L'ottemperanza alle norme dovrà essere costruita in MANIERA SARTORIALE.

(NO, non basta acquistare un software)

Non esistono più schemi prestabiliti.

PRINCIPIO DELLA 'PRIVACY *BY DEFAULT*'

l'adeguamento alla normativa dovrà essere un'impostazione predefinita dell'organizzazione aziendale.

Ogni nuovo processo adottato, adempimento, attività svolta ecc. dovrà prevedere la protezione dei dati trattati e l'adeguamento alla normativa vigente di '*default*': si tratteranno solo i dati personali strettamente necessari per le finalità che si intendono perseguire, per il tempo minimo necessario.

Alcuni casi molto banali, per capire: cambio di ufficio o di arredamento, nuove assunzioni, imprese di pulizie, cambio di server, telefoni aziendali ecc.

ALTRI PRINCIPI CHIAVE

- NON ECCEDENZA, ADEGUATEZZA, PERTINENZA, MINIMIZZAZIONE, DATA RETENTION: bisogna ridurre al minimo l'uso di dati personali; devono essere pertinenti ed adeguati rispetto alle finalità perseguite; conservati per il tempo minimo necessario;
- LICEITÀ E CORRETTEZZA: il trattamento deve avvenire in maniera lecita e corretta informando i soggetti interessati circa la raccolta, l'utilizzo e la consultazione dei loro dati o ulteriori tipologie di trattamenti, ecc.
- TRASPARENZA: le informazioni e le comunicazioni devono essere facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro;

QUANDO UN TRATTAMENTO È LECITO?

- (nei casi previsti) è stato ottenuto il consenso dell'interessato;
- vi siano obblighi contrattuali;
- vi siano obblighi di legge cui è soggetto il titolare del trattamento;
- vi sia interesse pubblico o esercizio di pubblici poteri;
- vi sia interesse legittimo prevalente del Titolare o di terzi cui i dati vengono comunicati (sempre che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato).

A CHI SI APPLICA IL REGOLAMENTO:

A CHIUNQUE EFFETTUI UN TRATTAMENTO DEI DATI PERSONALI IN MANIERA NON DOMESTICA, nel territorio dell'Unione, con queste precisazioni:

- Si applica ai Titolari e ai Responsabili del trattamento stabiliti nell'Unione ed indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
- Si applica ai Titolari e ai Responsabili del trattamento non stabiliti nell'Unione che trattano dati di Interessati che si trovano nell'Unione, se le attività di trattamento riguardano:

1. offerta di beni o prestazione di servizi agli Interessati dell'Unione;
2. monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo nell'Unione.

QUANDO SI EFFETTUA UN «TRATTAMENTO»?

Il trattamento è una qualsiasi operazione (o insieme di operazioni) applicata ai dati personali.

ESEMPI:

la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, l'utilizzo, la comunicazione, la diffusione, la cancellazione ecc.

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA?

Ad ogni informazione concernente una **PERSONA FISICA IDENTIFICATA** o identificabile («INTERESSATO», art. 4.1)

«Sono, pertanto, esclusi dall'ambito di applicazione delle disposizioni del regolamento i trattamenti dei dati relativi alle persone giuridiche: è evidente che in tal caso le disposizioni del GDPR troveranno applicazione con riferimento al trattamento dei dati personali del rappresentante legale.»

(cit. dal documento aprile 2018 Gruppo di Lavoro Privacy FNC)

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA? (CONTINUA)

Dati particolari (sensibili) (art. 9):

dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.

VI È UN DIVIETO GENERALE di trattamento per questi dati ad eccezione di taluni casi espressamente elencati.

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA? (SEGUE)

ECCEZIONI AL DIVIETO:

- Quando c'è il **Consenso** dell'Interessato;
- Il trattamento è necessario per assolvere gli obblighi del titolare o per tutelare i diritti dell'interessato nel rapporto di lavoro;
- Il trattamento è necessario per tutelare un interesse vitale dell'Interessato;
- Il trattamento è necessario per accertare o difendere un diritto
- ecc.

A QUALI DATI SI APPLICA LA NUOVA NORMATIVA? (SEGUE)

DATI PERSONALI RELATIVI A

CONDANNE PENALI E REATI (ART. 10):

Il trattamento deve avvenire soltanto sotto il controllo dell'autorità pubblica; oppure deve essere autorizzato dal diritto dell'Unione o degli Stati membri prevedendo garanzie appropriate per i diritti e le libertà degli interessati.

IL CONSENSO

Deve essere espresso mediante un atto inequivocabile con il quale l'interessato manifesta l'intenzione di accettare il trattamento dei dati personali.

Non è espressione del consenso il silenzio, l'inattività o la **preselezione di caselle**.

Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e neutrale.

LE FIGURE CHIAVE

IL TITOLARE DEL TRATTAMENTO: (art. 24 GDPR)

«È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali»

RESPONSABILE DEL TRATTAMENTO
(art. 28 GDPR)

«Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento».

Deve essere scelto dal Titolare TRA SOGGETTI CHE PRESENTINO GARANZIE SUFFICIENTI per mettere in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati.

Deve essere nominato dal Titolare o da altro Responsabile previa autorizzazione scritta del Titolare.

La nomina dei responsabili «esterni» è obbligatoria, deve essere fatta per contratto.

I SOGGETTI AUTORIZZATI AL TRATTAMENTO

La nuova normativa non prevede espressamente la figura dell'«incaricato» del trattamento (come il vecchio Codice *ex* art. 30). Cita invece le "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (in particolare, art. 4, n. 10).

QUINDI:

L'AUTORIZZATO al trattamento è un soggetto che, agendo su incarico e sotto la diretta responsabilità del Titolare del trattamento (o del Responsabile), dopo essere stato **istruito e formato**, tratta dati personali.

ESEMPIO: dipendenti e collaboratori del Titolare

RESPONSABILE DELLA PROTEZIONE DEI DATI

(DPO)

(artt. 37, 38, 39 GDPR)

È UNA DELLE NOVITA' PIÙ IMPORTANTI

A questa figura sono demandati non solo compiti di controllo in ordine a livello di protezione dei dati all'interno della organizzazione del titolare, ma anche compiti di supporto strategico alle decisioni del Titolare in materia di trattamento dei dati.

SI PROFESSIONALIZZA LA 'PRIVACY'

RESPONSABILE DELLA PROTEZIONE DEI DATI (SEGUE)

La nomina del DPO talvolta è obbligatoria:

- quando il trattamento è effettuato da una Autorità Pubblica, Pubblica Amministrazione (ESCLUSA l'autorità giudiziaria);
- quando vengono posti in essere trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- quando le attività principali del Titolare o del Responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati personali (dati relativi alla salute, dati genetici, dati biometrici, ecc.) o di dati relativi a condanne penali e a reati.

Il DPO può essere comunque nominato anche al di fuori dei casi appena citati (CONSIGLIATO!).

LA DOCUMENTAZIONE E LE PRASSI

IL REGISTRO DEI TRATTAMENTI

L'obbligo di redigere il Registro riguarda i titolari o responsabili del trattamento con queste caratteristiche:

- chiunque effettui trattamenti che possano presentare un rischio, anche non elevato, per i diritti e le libertà dell'interessato;
- Chiunque effettui **trattamenti non occasionali**;
- Chiunque effettui trattamenti delle categorie particolari di dati o di dati personali relativi a condanne penali e a reati;
- Chiunque abbia almeno 250 dipendenti.

È quindi chiaro che sono obbligati a tenere e redigere il registro dei trattamenti dei dati personali buona parte di imprese e professionisti.

ANCHE I RESPONSABILI DEL TRATTAMENTO DEVONO TENERE IL REGISTRO

L'INFORMATIVA PRIVACY

Per ogni pratica, processo, adempimento ecc. che porti a trattare dati bisognerà informare l'interessato tramite la cd. «Informativa privacy»:

Consiglio sia in forma scritta, sintetica, chiara e leggibile; dovrà riportare i dati del titolare e l'indicazione dei responsabili del trattamento e, se nominato, i recapiti del DPO.

Dovrà riportare inoltre i diritti dell'interessato e le modalità per esercitarli.

Dovrà contenere inoltre le indicazioni di massima delle caratteristiche dei dati trattati, delle finalità, della base giuridica, delle modalità, degli eventuali trasferimenti, dei processi adottati per la sicurezza, del periodo di conservazione ecc.

IL CONSENSO

L'informativa ha anche lo scopo di permettere che l'interessato possa rendere un valido consenso, se richiesto come base giuridica del trattamento.

In questo caso l'informativa non è solo dovuta in base al principio di trasparenza e correttezza, ma è anche una condizione di legittimità del consenso.

I CONTRATTI DI NOMINA

DOVRANNO ESSERE ADOTTATI, ALMENO:

- nomina degli autorizzati;
- nomina dei responsabili;
- accordo tra contitolari;
- (eventuale) nomina DPO, con comunicazione al Garante.

L'ANALISI DEI RISCHI E LA DPIA

(*Data Protection Impact Assessment)*

Deve essere svolta nell'ambito della valutazione d'impatto sulla protezione dei dati (DPIA).

Cioè: una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una **valutazione dei rischi** per i diritti e le libertà degli interessati; le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla normativa vigente, tenuto conto dei diritti e degli interessi legittimi degli interessati.

LA GESTIONE DEI DATA BREACH

COSA È IL DATA BREACH:

«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» (Art. 4).

La violazione, ad esempio, può essere determinata da accesso abusivo ai sistemi informatici, ovvero da sottrazione o perdita di dati e supporti di memorizzazione.

LA GESTIONE DEI DATA BREACH (SEGUE)

In generale, notificare entro 72 ore al Garante l'avvenuto data breach

TRANNE QUANDO sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; se la probabilità del rischio per gli interessati è elevata, si dovrà informare delle violazioni anche gli interessati senza ingiustificato ritardo.

BISOGNERA' QUINDI:

- mettere in essere procedure standard per il rilevamento e la comunicazione dei data breach;
- valutare il rischio per i diritti e le libertà delle persone;
- tenere traccia delle violazioni e delle valutazioni effettuate;

LA FORMAZIONE

NON SI È OTTEMPERANTI ALLA NORMATIVA SE NON SI EFFETTUA LA CORRETTA FORMAZIONE, anche dei dipendenti e dei collaboratori

ATTENZIONE:

Come già ricordato, per la «nomina» dei responsabili e degli autorizzati al trattamento bisognerà verificare anche questo aspetto.

L' «ANTIVIRUS» DEL FATTORE UMANO È LA FORMAZIONE.

Ordine dei Dottori Commercialisti e degli Esperti Contabili Trento Rovereto

COMITATO SCIENTIFICO GRUPPO ODCEC AREA LAVORO

Grazie dell'attenzione

Stefano Bacchiocchi
Dottore Commercialista in Brescia
Professore a contratto per l'Università degli Studi di Brescia
DPO