CONFAPI
CONFEDERAZIONE ITALIANA
PICCOLA E MEDIA INDUSTRIA PRIVATA

I QUADERNI DELLA PRIVACY

L'APPLICAZIONE DEL NUOVO REGOLAMENTO EUROPEO 2016/679

Il 04 maggio 2016, è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea (G.U.U.E.), L 119, il testo del Regolamento europeo 2016/679 in materia di protezione dei dati personali.

Il Regolamento europeo sulla privacy è entrato in vigore il 24 maggio 2016 e si applica negli Stati membri dell'Unione europea dal 25 maggio 2018.

Una componente importante del Regolamento europeo è la forte correlazione fra elementi del trattamento e della protezione dei dati personali con quelli del mondo della sicurezza informatica.

Con i presenti quaderni Confapi intende agevolare le imprese associate a comprendere al meglio il cambiamento normativo in atto fornendo bozze esemplificative, consigli pratici ed informazioni utili affinché le stesse possano adempiere agli obblighi imposti dal Regolamento europeo. Nel fornire ciò, Confapi si avvarrà delle modalità di attuazione che il Garante della privacy italiano (Autorità di controllo italiana) ha inteso suggerire per facilitare l'adeguamento delle imprese alla nuova normativa ed il processo di trasformazione della documentazione aziendale.

SOMMARIO

QUADERNO I

IL PASSAGGIO DAL CODICE DELLA PRIVACY ITALIANO (DECRETO LEGISLATIVO N. 196/2003) AL REGOLAMENTO EUROPEO SULLA PRIVACY 2016/679

Il **Regolamento europeo, in quanto tale, è vincolante e direttamente applicabile negli ordinamenti degli Stati membri**, prevalendo sulle normative nazionali. Tuttavia, non abroga formalmente la normativa italiana vigente in materia, ossia il c.d. Codice privacy (decreto legislativo n. 196/2003).

Infatti, **per tutte le questioni non disciplinate dal Regolamento e per tutte quelle ove il Regolamento rinvia alla legislazione degli Stati membri si applica ancora la normativa nazionale**, fermo restando il rispetto dei principi base del Regolamento stesso.

Sul punto, il Governo italiano, per effetto della legge di delegazione europea del Parlamento italiano, ha il compito di pubblicare i decreti legislativi necessari all'adeguamento della normativa nazionale esistente alle disposizioni del Regolamento e quindi consentire una corretta traslazione delle norme del Codice privacy italiano non incompatibili con il Regolamento stesso.

A tal proposito, il primo decreto di coordinamento adottato dal Governo ha ottenuto il parere favorevole del Garante della privacy italiano e, beneficiando della proroga al 21 agosto 2018, ha intrapreso l'iter dei pareri parlamentari necessari per l'approvazione definitiva.

Tale imminente traslazione normativa pone la necessità di evidenziare le principali differenze tra il Codice della privacy italiano ed il Regolamento europeo.

PRIMI ASPETTI COMPARATIVI

- RESPONSABILE DEL TRATTAMENTO DEI DATI → ha nuovi compiti e funzioni;

- CONTITOLARE → nuovo soggetto che determina, congiuntamente ad altro titolare del trattamento dei dati, le finalità e i mezzi del trattamento;

- RESPONSABILE DELLA PROTEZIONE DEI DATI → nuovo soggetto che con indipendenza e autonomia deve principalmente: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento europeo; b) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento. Si differenzia dal Responsabile del trattamento poiché quest'ultimo deve agire seguendo le istruzioni del titolare del trattamento avendo, pertanto, un vincolo che impedisce di godere di ampia indipendenza, tipica invece del Responsabile della protezione dei dati.

-RESPONSABILIZZAZIONE -> Si passa da un concetto di tutele imposte (misure minime) ad un concetto di tutele disposte dal Titolare del Trattamento (misure necessarie).

QUADERNO II

I NUOVI PRINCIPI

AMBITO TERRITORIALE DI APPLICAZIONE:

I) IL PRINCIPIO DI STABILIMENTO

Sarà sufficiente che lo stabilimento dell'impresa titolare o responsabile del trattamento si trovi nel territorio dell'Unione europea per far scattare le tutele previste dal Regolamento europeo.

II) L'ECCEZIONE

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nell'Unione europea esclusivamente nel caso in cui le attività di trattamento riguardino:
- l'offerta di beni o la prestazione di servizi agli interessati, oppure
- il monitoraggio del comportamento degli interessati all'interno dell'Unione europea.
In tal senso, tutte le imprese, ovunque stabilite, dovranno quindi rispettare le regole fissate dal Regolamento europeo.

IL PRINCIPIO DI RESPONSABILIZZAZIONE (ACCOUNTABILITY)

Il Titolare del trattamento dovrà:

1) adottare politiche ed attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme (fin dalla fase embrionale) a tutte le disposizioni del Regolamento;

2) assicurare che tutta la documentazione richiesta sia conforme alle prescrizioni di legge;

3) analizzare e valutare in maniera responsabile le attività che incidono sulla protezione dei dati apportando ad esse tutte le contromisure che lo stesso titolare ritiene necessarie per abbassare i rischi alle libertà degli interessati dalle operazioni di trattamento;

4) progettare fin dalla nascita, ossia "by design", operazioni di trattamento che dovranno avere come impostazione predefinita quella di tutelare i diritti dell'interessato nell'attività di trattamento per l'intera gestione del ciclo di vita dei dati;

5) progettare sistemi privacy che abbiano impostazioni "by default", ossia configurazioni "chiuse" e ristrette in punto privacy, per poi gradualmente ampliarle solo dopo avere valutato l'impatto su questi dati di eventuali aperture del sistema.

IL PRINCIPIO DELLE BASI GIURIDICHE PER IL TRATTAMENTO DEI DATI

Il regolamento conferma che ogni trattamento deve trovare fondamento almeno in una delle seguenti idonee basi giuridiche: **CONSENSO, CONTRATTO, OBBLIGO DI LEGGE, LEGITTIMO INTERESSE DEL TITOLARE DEL TRATTAMENTO E SALVAGUARDIA INTERESSE VITALE**.

• IL CONSENSO COME BASE GIURIDICA:

1. il consenso è da considerare una base giuridica similare alle altre;

2. laddove sia prescritto il consenso questo deve essere "esplicito". Un caso particolare di consenso chiaramente richiesto in forma esplicita è quello che riguarda i trattamenti automatizzati;

3. il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

4. non è ammesso il consenso tacito o presunto (esempio: NO a caselle pre-spuntate nei moduli).

FOCUS ON: il consenso raccolto precedentemente al 25 maggio 2018 resta valido?

Esso resterà valido solamente se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il Regolamento, se si vuole continuare a fare ricorso alla base giuridica del consenso.

LA RICHIESTA DEL CONSENSO:

a) dovrà essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato;
b) dovrà essere comprensibile, semplice e chiara.

IL LEGITTIMO INTERESSE COME BASE GIURIDICA:

Tale previsione attua il principio di responsabilizzazione (accountability) indicando che il titolare del trattamento dovrà verificare l'esistenza di un valido fondamento di liceità e quindi un legittimo interesse che consenta di trattare il dato. Potrebbero sussistere tali legittimi interessi quando:

- esista una relazione pertinente e appropriata tra l'interessato ed il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento;

- il titolare del trattamento debba trattare dati personali strettamente necessari a fini di prevenzione delle frodi;
- il titolare del trattamento debba trattare dati personali per finalità di marketing diretto.

Il Garante della Privacy, nelle sue raccomandazioni fornisce una serie di indicazioni per considerare valido il principio del bilanciamento di interessi ad esempio con riguardo ad alcune tipologie di trattamento di dati biometrici, con riguardo all'utilizzo della videosorveglianza, in merito all'utilizzo di sistemi di rilevazione informatica anti-frode.

QUADERNO III

I NUOVI PERSONAGGI

Interessato

L'interessato al trattamento è la **persona fisica** a cui si riferiscono i dati personali. Ai fini di comprendere chi sia l'interessato è necessario comprendere cosa sia un dato personale.

Per DATO PERSONALE si intende qualsiasi informazione riguardante una persona fisica vivente (interessato), identificata o identificabile.

FOCUS ON:

Esempi di dati personali

• nome e cognome;
• foto;
• indirizzo di residenza;

• targa veicolo;
• indirizzo e-mail, come nome.cognome@azienda.com;
• numero della carta d'identità;
• dati sulla posizione (ad es. quella su un telefono cellulare);
• un indirizzo IP (Internet Protocol);
• un ID cookie;
• l'identificativo pubblicitario del proprio telefono;
• i dati conservati in un ospedale o da un medico, che possono essere un simbolo che identifica univocamente una persona.

Esempi di dati non considerati personali:

• indirizzo e-mail, come info@azienda.com;
• numero di iscrizione al registro delle imprese di una società;
• dati resi anonimi

Al fianco dei dati personali sopra individuati, qualificabili genericamente come comuni, vi sono altre tipologie di dati che possono riguardare l'interessato e che assumono una rilevanza centrale soprattutto in riferimento alle conseguenze sulla dignità e libertà dello stesso interessato. Si tratta dei Dati Particolari e dei Dati Giudiziari.

Per DATO PARTICOLARE ci si riferisce al dato personale che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, lo stato di salute o la vita/orientamento sessuale della persona (cosiddetti dati sensibili), nonché il dato genetico ed il dato biometrico.

Per DATO GIUDIZIARIO ci si riferisce al dato personale relativo alle condanne penali ed ai reati o a connesse misure di sicurezza.

FOCUS ON:

Esempi di dati particolari

• informazioni relative a fruizioni permessi per festività religiose/attività politica/attività sindacale;
• dati relativi a categorie protette;
• informazioni inerenti la salute (non è necessaria la patologia);
• informazioni relative a matrimoni e forme particolari di convivenze;

Titolare e Contitolare del trattamento

Il titolare del trattamento dei dati è:

• il soggetto che determina le finalità del trattamento e ne stabilisce i mezzi;

• può essere una persona fisica o giuridica, un'autorità pubblica o altro organismo.

La sua funzione è:

• quella di mettere in atto tutte le misure tecniche ed organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Regolamento europeo.

FOCUS ON: possono esserci più titolari del trattamento?

Il Regolamento rende evidente la possibilità che ci siano più "Titolari del Trattamento" e allora si avrà la figura dei "Contitolari del trattamento" che potranno anche essere più di due e, laddove esistenti, dovranno determinare congiuntamente le finalità ed i mezzi del trattamento.

Si ipotizza quindi la necessità di una codecisione in merito alle finalità (ossia il perché) ed ai mezzi (ossia il come) di un determinato trattamento.

La contitolarità deve essere resa riconoscibile agli interessati attraverso un accordo interno con cui i contitolari hanno l'obbligo di determinare, in modo trasparente, le rispettive responsabilità e compiti sull'osservanza degli obblighi derivanti dal Regolamento europeo con particolare riferimento ai diritti dell'interessato e agli obblighi di fornire le informazioni previste al momento della raccolta (Art.13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; Art.14 – Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato) > **ALLEGATO 1**.

Da un punto di vista pratico, per l'individuazione del contitolare del trattamento non vi sono differenze con le modalità di identificazione del titolare del trattamento.

Se il titolare o il contitolare del trattamento è una persona giuridica, sarà quest'ultima ad acquisire autonomo rilievo e non il legale rappresentante della stessa che solo temporaneamente la rappresenta (vedi Cassazione, VI Sezione Civile 2 – Ordinanza 18 marzo – 8 aprile 2014, n. 8184).

Responsabile del trattamento

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

L'affidamento del Trattamento può essere operato solo se ci sia un contratto o un altro atto giuridico, stipulato in forma scritta, anche in formato elettronico > **ALLEGATO 2**.

FOCUS ON: IL Responsabile del trattamento può avvalersi di altri delegati?

È possibile solamente previa autorizzazione scritta, specifica o generale, del titolare del trattamento e nel caso di autorizzazione scritta generale, il responsabile del trattamento dovrà informare il titolare del trattamento di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Si prevede altresì che tali atti giuridici dovrebbero essere adottati in conformità a schemi tipo predisposti dal Garante.

Altra sostanziale modifica riguarda l'obbligo del responsabile di attenersi alle istruzioni impartite dal titolare e di sottostare alle verifiche periodiche che il Titolare dovrà effettuare su di lui.

La nuova disciplina specifica in maniera dettagliata gli elementi del contratto (o altro atto giuridico conforme al diritto nazionale):

1) la materia disciplinata;
2) la durata del trattamento;
3) la natura;
4) la finalità del trattamento;
5) il tipo di dati personali;
6) le categorie di interessati cui si riferiscono i dati;
7) gli obblighi e i diritti del titolare del trattamento;
8) le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite.

Incaricato del trattamento

A differenza della normativa italiana sulla privacy, il Regolamento europeo non menziona espressamente tale figura.

Tuttavia, il Regolamento europeo pur non prevedendo espressamente la figura dell'"incaricato" del trattamento, non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento".

FOCUS ON: è ancora utile quindi la figura dell'incaricato del trattamento?

In ragione del principio di "responsabilizzazione" (accountability), si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante della privacy italiano > **ALLEGATO 3**.

Responsabile della protezione dei dati (Data protection officer – D.P.O.)

È **la figura maggiormente innovativa** nel panorama del Regolamento europeo.

È obbligatoria esclusivamente in presenza di uno o più dei seguenti presupposti:

1) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

2) le attività principali consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;

3) le attività principali consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Nelle faq pubblicate sulla guida del Garante della Privacy è poi chiaramente indicato che "Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

Al di fuori dei suddetti presupposti, la designazione del responsabile del trattamento **non è obbligatoria** (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; **imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti)**.

Al netto di queste ipotesi la nomina è volontaria.

FOCUS ON: È IN OGNI CASO CONSIGLIABILE NOMINARE IL D.P.O.?

Nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla sua designazione.

Il DPO (Data Protection Officer) può essere paragonato ad un manager che dovrà avere approfondite conoscenze:

• in campo normativo;

• in materia di sicurezza informatica.

Il DPO non dovrà avere conflitti di interesse in azienda e dovrà essere coinvolto preventivamente nelle decisioni della direzione aziendale (management).

Il Responsabile della protezione dei dati personali, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

• possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;

• adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;

• operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio.

I COMPITI DEL D.P.O.:

1. Informare il titolare e gli incaricati, circa gli obblighi derivanti dai dati trattati;

2. monitorare l'implementazione e l'applicazione delle politiche adottate dal titolare in materia di protezione dei dati, l'assegnazione delle responsabilità e la formazione del personale aziendale;

3. monitorare che accessi illeciti ai dati siano notificati, nel rispetto della norma, all'autorità Garante;

4. monitorare l'efficacia, l'adeguatezza e l'applicazione del DPIA (Data protection impact assessment, ovvero l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati personali), nonché la sistematica autorizzazione e consultazione del titolare al trattamento prima di adottare una decisione che coinvolga il trattamento dei dati e la privacy.

Il DPO rimarrà in carica, come minimo, due anni, rinnovabili alla scadenza. Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati personali le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

QUADERNO IV

GLI ADEMPIMENTI

INFORMAZIONE AGLI INTERESSATI

L'informativa è un atto con cui chi tratta i dati altrui, innanzitutto, si identifica; inoltre rende noto agli interessati le caratteristiche del trattamento e illustra i diritti che spettano per legge. Tale incombente è già previsto nel Codice italiano della Privacy e quindi è adempimento già a carico del Titolare del Trattamento.

Con il Regolamento europeo i contenuti dell'informativa vengono in parti ampliati rispetto al Codice italiano.

In particolare, oggi si prescrive che il Titolare all'interno dell'informativa debba:

1) Indicare la base giuridica del trattamento;

2) specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;

3) indicare se il trattamento comporta processi decisionali automatizzati (anche la profilazione) e indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato;

4) specificare i dati di contatto del Responsabile del Trattamento dei dati;

5) indicare se i dati personali saranno trasferiti in Paesi terzi ed, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano norme aziendali vincolanti tra società facenti parte dello stesso gruppo d'impresa - BCR di gruppo).

Una importante novità del Regolamento rispetto alle regole già esistenti nel Codice riguarda i Tempi dell'informativa.

Infatti si prescrive che laddove i dati personali non siano raccolti direttamente presso l'interessato l'informativa debba essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

Laddove, invece, i dati siano acquisiti direttamente presso l'interessato l'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati.

L'informativa dovrà essere resa in forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, con un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee.

Si incentiva l'uso di informative in formato elettronico anche se sono ammessi altri mezzi. **Potenzialmente l'informativa può essere fornita anche oralmente (cosa che evidentemente però si sconsiglia).**

Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo in combinazione con l'informativa estesa.
Queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

FOCUS ON: l'informativa resa precedentemente al 25 maggio 2018 resta valida?

Essa resterà valido solamente se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per effettuare le dovute modifiche e/o integrazioni necessarie.

TABELLA COMPARATIVA:

L' INFORMATIVA AI SENSI DEL CODICE DELLA PRIVACY ITALIANO E AI SENSI DEL REGOLAMENTO EUROPEO SULLA PRIVACY

	Art. 13 Codice della Privacy italiano	**Art. 13 e 14 Regolamento europeo sulla privacy n. 679/2016**
Cosa deve essere indicato	1) I dati del Titolare del Trattamento; 2)le finalità del trattamento; 3) le modalità del trattamento; 4) se il conferimento dei dati è obbligatorio o facoltativo; 5) quali sono le conseguenze del rifiuto di fornire i dati da parte dell'interessato; 6) i soggetti cui saranno comunicati i dati raccolti; 7) i diritti spettanti all'interessato; 8) i dati del Responsabile del Trattamento se nominato	1) i dati del Titolare del Trattamento; 2) le finalità del trattamento; 3) **per ogni finalità del trattamento la base giuridica dello stesso**; 4) se l'interessato è obbligato a fornire i dati; 5) quali sono le conseguenze del rifiuto di fornire i dati da parte dell'interessato; 6) gli eventuali destinatari (o le eventuali categorie di destinatari) dei dati; 7) **il periodo di conservazione dei dati oppure, se non possibile, i criteri utilizzati per determinare tale periodo;** 8) **se è previsto il trasferimento dei dati in paesi extra-UE o ad organizzazioni internazionali e se si quali sono gli strumenti utilizzati;** **9) i diritti spettanti all'interessato;** 10) **l' esistenza di un processo decisionale automatizzato, ivi inclusa la profilazione;** 11) **i dati del Responsabile per la Protezione dei dati se nominato (attenzione si sta parlando della figura del DPO)**
Quando deve essere fornita	1) Se i dati sono raccolti presso l'interessato l'obbligo va adempiuto prima o al massimo al momento di dare avvio alla raccolta per il trattamento di dati personali. 2) Nel caso di raccolta dei dati presso il terzo, l'informativa è data all'interessato: • nel momento in cui i dati sono registrati; • (quando è prevista la loro comunicazione) al momento della prima comunicazione.	1) Se i dati sono raccolti presso l'interessato l'obbligo va adempiuto prima o al massimo al momento di dare avvio alla raccolta per il trattamento di dati personali. 2) Nel caso di raccolta dei dati presso il terzo, l'informativa è data all'interessato: • entro un termine "ragionevole" e comunque entro 1 mese; • quando è prevista la loro comunicazione ai terzi o all'interessato non oltre la prima comunicazione a quest'ultimo o ad altro destinatario.
Come deve essere l'informativa	L'informativa può essere fornita in forma scritta o orale. La forma scritta costituisce prova obiettiva dell'assolvimento dell'obbligo da parte del titolare.	L'informativa deve essere resa in forma: • concisa • trasparente • intelligibile • facilmente accessibile • con un linguaggio semplice e chiaro (in particolare per il caso di minori). L'informativa deve essere resa per iscritto o con altri mezzi (anche elettronici, come per es., la posta elettronica). Ove richiesto dall'interessato, l'informativa è da rendere oralmente (purché sia comprovata con altri mezzi l'identità dell'interessato). E' comunque opportuno che il titolare si procuri e conservi una evidenza del rilascio dell'informativa.

Di rilevante importanza nell'era della Responsabilizzazione è l'inesistenza di Informazioni agli Interessati valide per tutte le occasioni.

L'informativa dovrà essere, infatti, adottata almeno per singole fasce di interessati (ad es. , dipendenti > **ALLEGATO 4**, candidati > **ALLEGATO 4A** navigatori del sito > **ALLEGATO 4B**, dipendenti di clienti/fornitori > **ALLEGATO 4C** e per fasce di finalità (ad es. misure precontrattuali/contratti in corso/profilazione su sito).

DIRITTI DEGLI INTERESSATI

Già con il Codice della Privacy italiano all'interessato, ossia alla persona fisica cui si riferiscono i dati personali, sono riconosciuti taluni diritti ai sensi dell'art. 7. In particolare questo articolo dispone che "L'interessato ha diritto di ottenere la conferma dell'esistenza o meno dei dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile".

L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale."

Con il Regolamento si prevedono in generale:

1) Diritto di accesso (art. 15)

2) Diritto di rettifica (art. 16)

3) Diritto di cancellazione (diritto all'oblio) (art.17)

4) Diritto di limitazione del trattamento (art. 18)

5) Diritto alla portabilità dei dati (art. 20)

ANALISI DEI RISCHI E APPROCCIO BASATO SUL RISCHIO

MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE)

Il Codice della Privacy italiano disciplina in maniera puntuale l'obbligo del Titolare del trattamento di porre in sicurezza i dati.

Con il Regolamento europeo, l'approccio del Codice italiano viene superato e si passa da una serie di misure imposte (le misure minime) alle misure scelte dal Titolare.

Il Regolamento nel richiamare il principio di "responsabilizzazione" invita tutti i Titolari del Trattamento all'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Il Regolamento stabilisce, in questo senso, i criteri per effettuare l'Analisi dei Rischi e verificare quali siano le misure tecniche e organizzative adeguate per garantire, **ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al Regolamento.

Si dovrà tenere conto di:
1) natura, ambito di applicazione, contesto e finalità del trattamento,
2) rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai Titolari del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento europeo.

Alla conclusione dell'analisi dei rischi il Titolare quindi dovrà applicare le misure di sicurezza previste quali, fra le altre:

a) la pseudonimizzazione delle informazioni (uso di codici e pseudonimi) e la cifratura dei dati personali (algoritmo che rende incomprensibile i dati a coloro che non hanno i codici crittografici per accedervi);

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tale lista non è esaustiva. Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.

FOCUS ON: una rilevantissima parte dell'Analisi dei Rischi deve riguardare sicuramente il riesame e l'aggiornamento costante.

VALUTAZIONE D'IMPATTO
PRIVACY BY DESIGN
PRIVACY BY DEFAULT

Come sopra indicato, il nuovo approccio del Regolamento europeo crea un onere in capo al Titolare di effettuare una valutazione d'impatto del trattamento in modo da renderlo sin dall'inizio sempre conforme alle prescrizioni del Regolamento.

Tale obbligo posto in capo al Titolare si esprime con l'espressione inglese "data protection by default and by design" che viene previsto all'art. 25 del Regolamento.

In base a tale norma il Titolare dovrà valutare la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, i rischi aventi probabilità e gravità diverse per i diritti e lo stato dell'arte e dei costi di attuazione, e mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati.

Questo onere deve essere attuato prima di procedere al trattamento dei dati vero e proprio e quindi al momento di determinare i mezzi del trattamento e deve durare per tutto il trattamento.

L'applicazione delle misure organizzative e tecniche adeguate devono essere realizzate per impostazione predefinita, ossia in modo da non essere resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

FOCUS ON: con la circolare n. 5 del 19 febbraio 2018 l'Ispettorato nazionale del lavoro ha reso immediatamente applicativo tale onere relativamente agli strumenti di controllo a distanza dei lavoratori.
Si dispone, in particolare, che chi chiede l'autorizzazione dovrà dare prova all'Ente della necessità di installazione dell'impianto

da cui può indirettamente derivare il controllo fra le finalità previste e dimostrare attraverso la consegna di un progetto dettagliato che il sistema sia conforme ai requisiti richiesti dal regolamento (privacy by design) e che sia sin dall'inizio dotato di misure tecniche e organizzative per evitare che i dati siano accessibili ad un numero indefinito di persone senza l'intervento di persone fisiche.

Con l'istituto del "data protection by default and by design" si richiede, quindi, di effettuare una Valutazione d'Impatto.

Tale ultimo adempimento diventa, inoltre, **obbligatorio quando un tipo di trattamento è effettuato con l'uso di nuove tecnologie (es. riconoscimento facciale, etc.).**

Laddove all'esito di questa valutazione di impatto il titolare consideri le misure predisposte idonee a mitigare sufficientemente il rischio, questi potrà effettuare il trattamento. In caso contrario dovrà consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale.

L'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ossia l'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

NOTIFICAZIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Uno dei più importanti adempimenti che a partire dal 25 maggio 2018 tutti i Titolari del trattamento dovranno attuare è la Notifica delle violazioni dei dati personali.

Tale adempimento è collegato alla nuova visione di "responsabilizzazione" del Regolamento europeo che sposta il controllo dell'Autorità dalla fase di inizio del Trattamento, , alla fase di realizzazione del Trattamento, ossia a valle delle determinazioni assunte autonomamente dal titolare. Prova ne è l'abolizione, a partire dal 25 maggio 2018, dell'istituto della notifica preventiva dei trattamenti prevista dal Codice della Privacy italiano.

Il Titolare del Trattamento dovrà realizzare una procedura che consentirà di notificare all'Autorità di controllo le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque senza ingiustificato ritardo, quando si ritiene che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Non si tratta di una notifica obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta sempre al titolare del trattamento.

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del Regolamento europeo.

FOCUS ON: Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati. Si raccomanda, pertanto, ai titolari del trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

REGISTRO DEI TRATTAMENTI

Altro adempimento, in parte nuovo, è il registro dei trattamenti previsto come obbligatorio nei casi espressamente indicati dall'art. 30 del Regolamento, ossia:

1) per gli organismi con più di 250 dipendenti;

2) per gli organismi che effettuano trattamenti che possano presentare un rischio per i diritti e le libertà dell'interessato, qualora il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Si tratta di uno strumento fondamentale > **ALLEGATO 5**, non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

FOCUS ON: il Garante della Privacy ha invitato tutti i titolari di trattamento ed i responsabili, a prescindere dalle dimensioni dell'organizzazione, a dotarsi di tale registro.

Con un parere espresso dal Gruppo di lavoro europeo composto dalle Autorità nazionali di vigilanza e protezione dei dati è

stata specificata la portata del termine "non occasionalità del trattamento dei dati particolari o giudiziari". In tale parere il Gruppo ha chiarito che è probabile che una piccola organizzazione elabori regolarmente i dati relativi ai propri dipendenti e di conseguenza, tale organizzazione effettua un trattamento non "occasionale" anche di dati particolari ed è quindi tenuta alla realizzazione del Registro dei Trattamenti.

I contenuti del registro sono fissati, come detto, nell'art. 30 tuttavia, non è fatto divieto di inserire altre informazioni che saranno ritenute utili nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Al fine di aiutare la redazione del registro dei trattamenti di seguito si riporta:

Tabella comparativa:

indicazioni che era obbligatorio inserire nel Documento Programmatico della Sicurezza secondo quanto disposto dal punto 19 dell'Allegato B del D.lgs. 196/03 – Codice della Privacy italiano e le indicazioni che dovranno essere contenute nel Registro dei Trattamenti.

	Art. 19 Allegato B - Codice della Privacy italiano	**Art. 30 Regolamento europeo sulla privacy n. 679/2016**
Cosa deve essere indicato	19.1. l'elenco dei trattamenti di dati personali; 19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati; 19.3. l'analisi dei rischi che incombono sui dati; 19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità; 19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23; 19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali; 19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare; 19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.	a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
Chi deve redigere?	Il Titolare del Trattamento	Ogni titolare del trattamento o il suo rappresentante sul territorio. Ogni responsabile del trattamento o il suo rappresentante sul territorio.

TRASFERIMENTO I DEI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

Per quanto riguarda il trasferimento dei dati all'estero ci si riferisce principalmente al problema del flusso transfrontaliero dei dati un destinatario soggetto a una giurisdizione straniera.

Il trasferimento in paesi extracomunitari è ammissibile se nel paese di destinazione è garantito un livello di protezione dei dati adeguato a quello europeo. Per valutare l'adeguatezza occorre esaminare diversi aspetti del trattamento: la natura dei dati, la finalità del trattamento, la possibilità che tali dati transitino in altri paesi prima di giungere alla destinazione, le norme di diritto anche settoriali, le misure di sicurezza osservate.

Il requisito dell'adeguatezza, piuttosto che quello dell'equivalenza, consente l'utilizzo di diverse vie per garantire la protezione dei dati e si realizza se:

i) l'adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;

ii) in assenza di decisioni di adeguatezza della Commissione, siano adottate dai titolari coinvolti garanzie adeguate di natura contrattuale o pattizia (fra cui le norme vincolanti d'impresa e clausole contrattuali modello);

iii) in assenza di ogni altro presupposto, si faccia riferimento ad appositi deroghe al divieto di trasferimento applicabili in specifiche situazioni (corrispondenti in parte alle disposizioni dell'art. 43, comma 1, del Codice).

QUADERNO V

LE SANZIONI

Con l'entrata in vigore del Regolamento europeo, il quadro sanzionatorio privacy sarà ben più severo. Va messa in evidenza la scelta del legislatore europeo di uniformare la tipologia e l'entità delle sanzioni, a differenza di quanto accadeva in precedenza.

Sulla base dell'art. 82 del Regolamento europeo, resta la possibilità per l'interessato, che subisca un danno materiale o immateriale, di ottenere il risarcimento del danno, a seconda che la violazione sia stata commessa dal Titolare o dal Responsabile del trattamento dei dati.

Le sanzioni amministrative pecuniarie possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato globale dell'impresa nei casi di,

a. violazione delle condizioni applicabili al consenso dei minori;

b. trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;

c. mancata o errata notificazione e/o comunicazione di una violazione dei dati personali all'Autorità nazionale competente;

d. violazione dell'obbligo di nomina del DPO;

e. mancata applicazione di misure di sicurezza.

Le sanzioni possono aumentare fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato globale dell'impresa, nei casi di:

a. inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;

b. trasferimento illecito di dati personali ad un destinatario in un Paese terzo.

Ai fini dell'applicazione delle sanzioni verranno utilizzati alcuni criteri:

a. "la natura, gravità e durata della violazione";

b. "il carattere doloso o colposo della violazione";

c. "il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi".

Alcune condotte che potranno integrare il suddetto carattere doloso sono riconducibili alle ipotesi di:

a. trattamenti illeciti autorizzati esplicitamente dalla Direzione aziendale, ovvero ignorando i pareri formulati dal DPO;

b. modifica di dati personali, avente la finalità di fornire un'impressione "fuorviante" circa il conseguimento degli obiettivi individuati;

c. vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Inoltre, nel Regolamento europeo è stabilito che gli Stati Membri dovrebbero poter stabilire disposizioni relative a sanzioni penali.

IN DEFINITIVA

Al fine di adempiere in maniera efficace ed efficiente alle disposizioni del nuovo Regolamento europeo il Titolare dovrà:

• mettere in atto misure organizzative, tecniche e tecnologiche adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento al Regolamento.
• tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

• al fine di dimostrare l'efficacia delle misure e della protezione, effettuare una preliminare mappatura dei dati (indicandone in via esemplificativa tipologia, basi giuridiche, finalità e modalità di utilizzo), dei flussi (indicandone in via esemplificativa la provenienza, l'utilizzazione, il destino e l'onere di mantenimento) e infine verificare i rischi che i trattamenti producono tenendo in considerazione degli strumenti che vengono utilizzati nell'attività d'impresa.

Solo attraverso queste azioni l'impresa sarà in grado di avere piena contezza dei dati che tratta e quindi poter determinare, con accordi, procedure, misure tecniche e tecnologiche, le modalità per attuare al meglio il nuovo Regolamento europeo.

A cura di

Barbara Bertoletti (Servizio Legale API Torino)
Moreno Polidori (Servizio Legale Confapi Pesaro Urbino)
Angelo Favaron (Ufficio Affari Legali Confapi)

Maggio - Giugno 2018