

Regolamento UE 2016/679

Concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la loro libera circolazione

In vigore dal 24 maggio 2016

Applicabile dal 25 maggio 2018



CONAST – società cooperativa

Sede Legale ed Operativa: via A. Diaz, 17 – 25121 BRESCIA

Sede Direzionale: Viale Italia, 2 – 25121 BRESCIA

Tel 0303774422 – Fax 0303774497 | www.conast.it – E

mail info@conast.it

C.F. e P.IVA 01654890175 - CCIAA n° 01654890175

Situazione legislativa

Con questo atto legislativo l'Unione Europea ha messo ordine nella materia abolendo la Direttiva Europea del 1995, dalla quale sono derivate le normative nazionali di questi ultimi 22 anni, e – di fatto – abolendo le normative stesse.

Il Regolamento diventerà attuativo dal **25 maggio 2018**.

La forma giuridica del “Regolamento UE” è immediatamente applicabile per tutti i paesi aderenti all'Unione, ma in non pochi punti il Regolamento stesso rimanda all'emanazione di normative nazionali o comunitarie, in particolar modo le semplificazioni per le imprese con meno di 250 dipendenti e per le micro, piccole e medie imprese.

Inoltre non tutte le disposizioni contenute nell'attuale Codice Privacy sono presenti anche nel nuovo Regolamento.

Dovrà quindi essere predisposto a livello nazionale dal legislatore, entro il termine di entrata in vigore del nuovo Regolamento del 25 maggio 2018, un nuovo testo che mantenga in vita tali disposizioni e che le integri con quello che il Regolamento consente ai singoli Stati.

Nel frattempo il Garante, che il Regolamento denomina “Autorità di Controllo”, sta diffondendo le linee guida su alcuni degli argomenti che ritiene di dover chiarire. Questo contribuirà ad una maggior chiarezza, soprattutto sulle fasi di passaggio.


In attesa di questi elementi, è opportuno adottare un approccio prudenziale, adeguandosi alle misure del Regolamento comuni ed applicabili a tutti i tipi di organizzazione.

Questo rimane, a nostro avviso, l'aspetto di maggiore incertezza per chi deve organizzare le prossime attività di conversione delle procedure fra il Codice e il Regolamento.

Le principali novità del Regolamento rispetto al Codice Privacy

Gli obblighi principali ricalcano quelli già presenti nell'attuale Codice Privacy, ma la nuova versione obbliga ad una revisione complessiva anche degli adempimenti già presenti ed attuati.




Gli stessi possono essere sintetizzati e riepilogati nella seguente tabella:


Adempimento	Note
Definizione del titolare del trattamento 	E' prevista la possibilità di assegnare una contitolarità di uno o più trattamenti. Questa nuova figura apre ad alcuni cambiamenti di scenario e valutazioni nell'attribuzione delle responsabilità.
Nomina del responsabile dei trattamenti	Va eventualmente rivista la nomina di responsabile in quanto è previsto che l'incarico assuma la forma di <u>contratto o di altro atto giuridico</u> . Inoltre dovrà essere data evidenza dell'utilizzo, da parte del responsabile nominato, di sub-responsabili del cui operato è direttamente

Adempimento	Note
	responsabile.
Nomina e formazione degli incaricati	Si attendono indicazioni circa l'obbligatorietà della formazione degli addetti. Per ora restano valide le nomine effettuate con il Codice Privacy. Dal testo si desume che sia obbligatoria per quelle strutture per le quali è obbligatoria anche la figura del DPO o RPD. Rientra fra le materie sulle quali il legislatore o le autorità di controllo potranno pronunciarsi.
Revisione dei moduli di informativa e consenso	Nel Regolamento sono state ampliate le informazioni che devono essere contenute nell'informativa. Questo obbligherà alla revisione di tutti i moduli utilizzati per i diversi trattamenti e le formule di consenso.

Il regolamento pone con forza l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari 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 stesso.

Adempimento	Note
Adozione del registro dei trattamenti 	Ogni trattamento va analizzato e descritto mediante schede il cui contenuto è vincolato dal Regolamento. L'autorità di controllo ha annunciato la diffusione di linee guida per la tenuta di questo registro.
Adozione del documento di analisi e valutazione dei rischi 	Il legislatore intende sia i rischi relativi alla disponibilità dei dati che i rischi che impattano sulle libertà e i diritti degli interessati. Nei casi più complessi è prevista anche la consultazione obbligatoria dell'autorità di controllo.
Attivazione del registro degli eventi 	Si attendono indicazioni circa l'obbligatorietà della formazione degli addetti. Per ora restano valide le nomine effettuate con il Codice Privacy. Dal testo si desume che sia obbligatoria per quelle strutture per le quali è obbligatoria anche la figura del DPO o RPD. Rientra fra le materie sulle quali il legislatore o le autorità di controllo potranno pronunciarsi.

Adempimento	Note
Revisione dei moduli di informativa e consenso	Devono essere annotati tutti gli eventi che mettono a rischio i dati. In alcuni casi la comunicazione va inoltrata immediatamente all'autorità di controllo.
Attivazione del ruolo di responsabile della protezione dei dati (RPD) o data protection officer (DPO) 	<p>L'RDP può essere un dipendente del titolare o del responsabile o un collaboratore con un contratto di servizio.</p> <p>I compiti del RPD sono:</p> <p><u>Articolo 39 del Regolamento</u></p> <p>a) <i>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 presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;</i></p> <p>b) <i>sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;</i></p> <p>c) <i>fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;</i></p> <p>d) <i>cooperare con l'autorità di controllo;</i></p> <p>e) <i>fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.</i></p> <p>Le modalità adottate dal titolare del trattamento e dal responsabile del trattamento per la sua nomina e quelle della sua attività sono:</p> <ol style="list-style-type: none"> 1) assicurare che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali; 2) fornire al RPD le risorse necessarie per assolvere i compiti di cui all'art. 39 e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica; 3) assicurare che il RPD non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il RPD non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il RPD riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Adempimento	Note
	<p>4) Gli interessati possono contattare il RPD per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.</p> <p>5) Il RPD è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.</p> <p>6) Il RPD può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.</p>
Verifica delle misure di sicurezza	<p>Con la futura abolizione del Codice vengono abolite anche le misure minime di sicurezza obbligatorie. La responsabilità delle misure adottate sarà TOTALMENTE in carico al titolare (gli amministratori di sistema sono "semplici" incaricati) che risponde in caso di adozione di misure poco efficaci.</p> <p>Anche in questo caso l'autorità di controllo ha annunciato l'emanazione di linee guida o buone prassi.</p>
Documento riepilogativo delle misure adottate	<p>Non è formalmente previsto un documento descrittivo delle misure adottate ma l'obbligo generale contenuto nel Regolamento di documentabilità delle attività intraprese dal titolare o dal responsabile lo rende "di fatto" obbligatorio.</p>



Restano esclusi gli adempimenti, oggi in vigore, legati alla figura dell'**amministratore di sistema**. Questa figura non era inserita nel Codice Privacy e non è prevista nemmeno dal nuovo Regolamento UE. Fa parte di quegli adempimenti introdotti o comunque descritti, nei provvedimenti a carattere generale emanati dal Garante. Questi provvedimenti resteranno in vigore.

Nel caso dell'amministratore di sistema il ruolo è compatibile, non in contrasto, con il Regolamento. Bisogna quindi considerarlo una "precisazione" che la normativa nazionale potrà contemplare.

Inoltre nel Regolamento sono contenute anche nuove indicazioni che regolano la possibilità per l'interessato di avanzare richieste:

- di accesso,
- di cancellazione,
- di limitazione del trattamento,
- di opposizione,
- di portabilità,
- di oblio.

Questo comporta la necessità di dotarsi preventivamente delle procedure idonee a soddisfare le richieste che potrebbero pervenire.

I nostri consigli su come procedere

E' necessario muoversi passo-passo seguendo gli interventi legislativi, linee guida e buone prassi che il Garante ha dichiarato di voler emanare.

Essendo ancora in vigore l'attuale Codice Privacy non si ritiene al momento opportuno modificare le procedure di nomina o i moduli.

Nell'adeguamento del proprio sistema Privacy al nuovo Regolamento, è consigliabile aggiornare i **vecchi adempimenti (informativa e consenso) nelle nuove forme previste dal Regolamento** seguendo l'ordine indicato in tabella.

Una volta completata la parte relativa alle **nomine**, con particolare attenzione alle **con-titolarietà** e alla revisione dei **ruoli dei responsabili**, dovrà essere formalizzato il **ruolo del RPD o DPO** che, a richiesta, **potrà essere ricoperto anche da Conast stessa**, definendo le condizioni di autonomia e risorse, anche finanziarie, che la legge impone il titolare conceda al DPO.

La fase più invasiva per l'organizzazione sarà quella di valutazione dei trattamenti finalizzata alla costituzione del registro dei trattamenti.

E' stata annunciata la diffusione di schemi tipo e linee guida per **l'analisi dei trattamenti e la redazione del registro**. In attesa dell'emanazione di tali linee guida, suggeriamo di iniziare la raccolta delle informazioni necessarie a tale analisi contestualmente a quella per la **valutazione dei rischi**.

Contatti

Conast società cooperativa può affiancare ed assistere l'organizzazione nell'adeguamento dei propri adempimenti e offrire un supporto consulenziale continuativo nel tempo.

Per maggiori informazioni è possibile contattare il ns. referente tecnico area Privacy:

Gianfausto Vincenzi

030 3774422

privacy@conast.it