**APPUNTO SUL REGOLAMENTO (UE) 679/2016 - GDPR**

A partire dal 25 maggio prossimo diventerà obbligatorio il Regolamento (UE) 2016/679 che, come sapete, ha rivoluzionato gli adempienti in materia di trattamento dei dati, accentuando fortemente la responsabilizzazione dei titolari del trattamento (ossia dei soggetti pubblici e privati che determinano finalità e modalità del trattamento), dei responsabili, nonché i diritti degli interessati.

La materia merita di essere approfondita, anche in vista delle sanzioni che l’Autorità Garante per la protezione dei dati personali sarà chiamata ad applicare e che, a seconda dei casi, potranno raggiungere i 20 milioni di euro o il 4% del fatturato annuo.

Sarà più che opportuno, dunque, mettere a punto tutte le misure utili e necessarie per non incorrere in sanzioni civili, penali, amministrative ed evitare, altresì, azioni di risarcimento del danno da parte degli interessati.

1. **DEFINIZIONI**

* **Trattamento**: “qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione”.
* **Dato personale**: “qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale”.
* **Dati sensibili**: nel Regolamento diventano *categorie particolari di dati personali*. Sono informazioni che riguardano aspetti specifici della vita degli Interessati in relazione alle quali gli stessi non possono essere discriminati. Riguardano l’origine razziale o etnica, le convinzioni religiose o filosofiche, l’appartenenza a sindacati, partiti; dati relativi alla vita sessuale, orientamento sessuale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica (es: impronte digitali), dati relativi alla salute fisica o mentale.
* **Trattamento di dati sensibili per finalità politiche**: i dati personali che rivelano le opinioni politiche possono essere trattati ex art. 9, comma 2, lett. d)del Regolamento in quanto il trattamento è effettuato nell’ambito delle legittime attività e con adeguate garanzie da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche. Il tutto, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con il Titolare in ragione delle finalità statutarie dello stesso e che i dati non siano comunicati all’esterno senza il consenso dell’interessato.

**2. PRINCIPI**

* 1. **LICEITA’**:

la violazione della legge è violazione di un principio di liceità.

* 1. **CORRETTEZZA;**
  2. **TRASPARENZA**:

fa da corollario ai doveri di informativa del Titolare ex artt. 13 e 14, all’esercizio dei diritti di accesso dell’interessato ex art. 15, ma anche all’intera architettura dell’accountability ex art. 24 e ss. (rapporti tra titolare e responsabile).

* 1. **LIMITAZIONE DELLE FINALITA’**:

il trattamento può avvenire solo per finalità determinate, esplicite e legittime:

* finalità indicate nell’informativa;
* finalità compatibili con le stesse;
* finalità di archiviazione per pubblico interesse, ricerca strica, statistica o scientifica (DEROGA).
  1. **MINIMIZZAZIONE DEI DATI**:

i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. E’ un principio cardine su cui si costruisce la protezione dei dati e assorbe in sé i principi di necessità e proporzionalità.

E’ il principale parametro da considerare in sede di privacy by design e by default (art. 25) nonché di valutazione dell’impatto sulla protezione dei dati (art. 35).

Tale principio si ricollega direttamente alla tutela dell’identità personale.

* 1. **ESATTEZZA:**

devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per cui sono trattati.

* 1. **LIMITAZIONE DELLA CONSERVAZIONE**:

i dati devono essere conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

* 1. **INTEGRITA’ E RISERVATEZZA:**

i dati devono essere trattati in modo da garantirne un’adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o dal danno accidentali.

* 1. **ACCOUNTABILITY**:

ogni Titolare del trattamento è competente per il rispetto dei principi sopra esplicitati ed è in grado di provarlo.

Il Titolare deve tenere conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Deve dunque procedere con un approccio basato sul rischio, con riferimento alla dignità delle persone (diritto alla tutela della vita privata, ma anche libertà di espressione, pensiero, movimento, divieto di discriminazioni, libertà di coscienza e di religione). Tale valutazione si attua sulla base degli eventi verificatisi in passato, ivi comprese le eventuali falle del sistema che si sono manifestate. Ogni Titolare mette in atto misure tecniche e organizzative adeguate: l’organigramma di persone che lavorerà al trattamento dovrà essere competente, consapevole e determinato.

**3. CONTITOLARITA’ DEL TRATTAMENTO SUI DATI DEGLI ISCRITTI**

* Il PD nazionale e le articolazioni territoriali definiscono, in qualità di Contitolari del trattamento rispetto ai dati dei tesserati, il riparto delle funzioni al loro interno.
* Si ha contitolarità ai sensi dell’art. 26 del Regolamento allorché due o più Titolari determinano congiuntamente le finalità e i mezzi del trattamento. La scelta di operare congiuntamente riveste una particolare rilevanza in quanto la condivisione delle informazioni tra Titolare e Contitolare è congiunta. I Contitolari dialogano attraverso un accordo interno con cui definiscono le rispettive responsabilità in merito all’osservanza degli obblighi, all’esercizio dei diritti degli interessati, all’informativa rilasciata agli stessi, alle finalità dei trattamenti. Il contenuto dell’accordo interno è essenziale ed è messo a disposizione degli interessati che avranno facoltà di rivolgersi indifferentemente all’uno o all’altro Contitolare (cfr. successivo punto 7). L’accordo è interno ma non vale a spostare le responsabilità, serve a ripartire le competenze e a decidere su finalità e modalità del trattamento.
* Tutti i Contitolari restano responsabili a livello amministrativo, civile e penale.

La Contitolarità rende i diversi Titolari corresponsabili *ab origine* dei trattamenti, e non responsabili solidalmente. La previsione della contitolarità non può eludere gli obblighi di responsabilità, in virtù del principio dell’*accountability* che informa di sé l’intera disciplina europea. In tale ottica, non sono possibili clausole di manleva le quali sarebbero nulle o annullabili.

* Diversamente, per quanto attiene ai dati dei simpatizzanti, degli elettori delle Primarie e, in generale, di tutti quei soggetti diversi dai tesserati, le articolazioni territoriali di volta in volta individuate saranno nominate responsabili esterni.
* Le articolazioni territoriali devono nominare formalmente gli incaricati dei trattamenti, fornendo loro tutte le istruzioni in merito al trattamento. Tali soggetti saranno gli unici autorizzati a trattare i dati (es: invio di newsletter, inserimento dati nel database, mera presa visione, ecc.). Tutti coloro che non sono espressamente nominati incaricati del trattamento non devono poter accedere in nessun modo ai database, ai moduli cartacei contenenti i dati dei tesserati e, comunque, ai dati stessi.

**4. NOMINA DEL RESPONSABILE PROTEZIONE DATI (DPO o RPD) - Artt. 37-39 GDPR**

* La figura del DPO è obbligatoria per i partiti in quanto effettuano trattamenti di dati sensibili su larga scala. Stante le vigenti disposizioni, non è tuttavia chiaro se il criterio della larga scala possa essere applicato a tutte le articolazioni territoriali o solo a quelle maggiormente rappresentative della realtà locale di riferimento. A tal riguardo, mancando indicazioni specifiche, il Partito si riserva di chiedere un parere al Garante per la Protezione dei Dati Personali in merito all’obbligatorietà della nomina del DPO da parte delle articolazioni territoriali.
* Il DPO può essere un soggetto interno o esterno all’organizzazione del Titolare o del Contitolare. I dati di contatto del DPO devono essere indicati nelle informative pubblicate sui siti; non è necessario indicare il nominativo il quale tuttavia va comunicato all’Autorità di controllo secondo lo schema pubblicato sul sito www.garanteprivacy.it.
* Considerata la specifica natura giuridica dei partiti, anche in relazione alle finalità da questi perseguite, si ritiene di poter procedere alla nomina di un DPO UNICO, indicato dal livello nazionale, il quale è poi formalmente nominato dalle articolazioni territoriali. Nulla vieta che ciascuna articolazione territoriale possa procedere alla nomina autonoma di un proprio DPO.

**5. REGISTRO TRATTAMENTI - Art. 30 GDPR**

* E’ una sorta di “diario di bordo” sul quale tutti i Titolari (o suoi incaricati) dovranno annotare i trattamenti effettuati raggruppandoli per grandi categorie, specificando: finalità del trattamento, tipologia di dati trattati, categorie di destinatari e una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
* Per i partiti si ritiene che tale adempimento sia obbligatorio. Considerato che le articolazioni territoriali, in qualità di Contitolari, potranno procedere a trattamenti autonomi sui dati dei tesserati, le stesse si impegnano a compilare un registro in autonomia, secondo il modello trasmesso unitamente alle presente circolare.

**6. VALUTAZIONE DELL’IMPATTO DEL TRATTAMENTO (Privacy Impact Assessment) - Art. 35 GDPR**

* E’ obbligatoria per i partiti. E’ posta in essere dal nazionale sulla base delle specifiche tecniche del software utilizzato.
* E’ richiesta ogni qualvolta il trattamento possa presentare un rischio per i diritti e le libertà delle persone fisiche.

**7. Protezione dei dati fin dalla progettazione e per impostazione predefinita - Art. 25 GDPR**

Il Titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (*by default*), solo i dati personali necessari per ogni specifica finalità del trattamento (quantità dei dati raccolti, portata del trattamento, periodo di conservazione e accessibilità limitata ai dati a un numero definito di persone fisiche). Sia al momento di determinare i mezzi del trattamento (*by design*) sia all'atto del trattamento stesso, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati.

Tali misure fanno parte integrante del software utilizzato per la gestione dei dati trattati.

**8. Gestione delle richieste di cancellazione**

Qualora un Interessato (*rectius*, tesserato) dovesse rivolgersi ad una articolazione territoriale chiedendo la cancellazione dei propri dati e/o esercitando qualunque altro diritto previsto dal Codice Privacy (art. 7) e/o dal Regolamento (rettifica, aggiornamento, opposizione, blocco, ecc. – artt. 15-22), l’articolazione competente dovrà provvedere entro 7 giorni, informandone il livello nazionale ai seguenti indirizzi email: [privacy@partitodemocratico.it](mailto:privacy@partitodemocratico.it) e tesoreria@partitodemocratico.it.

L’articolazione territoriale dovrà provvedere nello stesso termine sopra indicato qualora la richiesta di cancellazione provenga direttamente dal nazionale.

E’ di fondamentale importanza che la cancellazione dei dati richiesta sia posta in essere senza indugio, al fine di tutelare i diritti fondamentali degli interessati ed evitare, altresì, di incorrere nelle pesanti sanzioni previste dal nuovo Regolamento europeo.

**9. DATA BREACH: notifica al Garante e all’interessato delle eventuali violazioni dei dati - Artt. 33 e 34 GDPR**

Qualora venga registrata una violazione dei dati, il Contitolare dovrà darne notifica al Garante entro 72 ore e agli interessati senza indebito ritardo.

Tale adempimento, quindi, compete anche alle articolazioni territoriali singolarmente.

**10. INFORMATIVE, PRIVACY POLICY e COOKIE POLICY**

Vi preghiamo di pubblicare sui siti di rispettiva competenza le informative aggiornate al nuovo Regolamento 2016/679 sul modello di quella pubblicata sul sito del Partito Democratico.

Si allegano:

1. Regolamento (UE) 679/2016;
2. D.Lgs. 196/2003 (c.d. Codice Privacy);
3. Registro dei trattamenti.