COMUNE di ORZINUOVI
PROVINCIA DI BRESCIA

Prot. n. 9925 del 23/05/2018

Circolare del Segretario n. 5/2018

Al Sindaco
Agli Assessori
Ai Responsabili di Area
A tutti gli uffici

OGGETTO: ADEMPIMENTI DERIVANTI DAL **REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI -** REGOLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27 APRILE 2016**.**

Il prossimo 25 maggio 2018 diverrà efficace ed entrerà immediatamente in vigore il Regolamento in oggetto, noto come **GDPR** (General Data Protection Regulation) **Regolamento Generale sulla Protezione dei Dati**.

SCHEMA ADEMPIMENTI DA ATTUARE

I soggetti

IL TITOLARE DEL TRATTAMENTO DEI DATI RACCOLTI (l'Ente Comune che opera attraverso il **Sindaco** ovvero un suo delegato). Nell'informativa all'utenza deve essere individuato il titolare indicando "Comune di Orzinuovi".

- ✓ E' responsabile del rispetto dei principi, applicabili al trattamento di tutti i dati personali raccolti o conservati dall'ente: correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.
- ✓ Ha l'obbligo di porre in essere e aggiornare "misure tecniche e organizzative" per assicurare e, soprattutto, "poter dimostrare", che il trattamento dei dati sia effettuato conformemente alla disciplina del regolamento stesso. Il titolare definisce tali "misure tecniche e organizzative" sin dalla fase di progettazione dei trattamenti, per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
- ✓ "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 per soddisfare i requisiti del regolamento e tutelare i diritti degli interessati. La pseudonimizzazione è il trattamento dei dati personali in modo tale che gli stessi dati **"non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive" conservate separatamente**.
- ✓ applica misure adeguate "per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari" per ogni specifica finalità del trattamento.

IL RESPONSABILE DEL TRATTAMENTO (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento**). È necessario predisporre un atto con cui il titolare (Il Sindaco, quale Legale rappresentante dell'Ente Comune oppure con atto organizzativo della Giunta Comunale) designa i responsabili del trattamento dei dati, un "contratto", o altro "atto giuridico" conforme al diritto dell'Unione o nazionale, e deve essere "stipulato in forma scritta, anche in formato elettronico". Tale contratto

vincola il responsabile al titolare del trattamento, definisce **durata, natura e finalità del trattamento, regolamenta il tipo di dati personali e le categorie di interessati, fissa obblighi e diritti del titolare del trattamento**.
Questa figura verrà a coincidere prevalentemente con i **Responsabili di Area**, che già in passato, con il precedente codice, venivano indicati come incaricati del trattamento; nel nuovo regolamento europeo non è più presente questa distinzione fra responsabile ed incaricato, essendo definito solo il ruolo di chi materialmente gestisce e tratta concretamente il dato e ne è quindi **Responsabile.**
Quando i **dati vengono gestiti con autonomia ed operatività per l'intero settore**, può essere attribuito il ruolo di responsabile del trattamento a prescindere dalla responsabilità del servizio; si tratta quindi di una responsabilità collegata al corretto trattamento del dato personale.

Se il responsabile del trattamento ricorre ad altra figura per il trattamento del dato deve darne comunicazione al titolare, questo avviene quando nell'ufficio del Responsabile è presente altro personale al quale il predetto può affidare la gestione di specifici dati" Il *responsabile del trattamento non ricorre a un altro responsabile senza previa* ***autorizzazione scritta, specifica o generale, del titolare del trattamento****. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche" (*Art. 28 comma 2 reg. UE)**.** Questi sono i
Sub-responsabili del trattamento
Il nuovo regolamento UE 679/2016 consente la designazione di "sub-responsabili", per specifiche attività di trattamento, applicando i medesimi obblighi contrattuali che vincolano il responsabile principale al titolare; con contratto o altro atto giuridico devono essere imposti al sub responsabile gli stessi obblighi, in materia di protezione dei dati, già contenuti nel contratto tra il titolare e il responsabile principale. Per nominare dei sub-responsabili, il responsabile del trattamento necessita della autorizzazione scritta rilasciata dal titolare. L'autorizzazione potrebbe essere "specifica", quindi riferita alla singola nomina, ovvero "generale" e permettere al responsabile la designazione in autonomia dei sub-responsabili. Nel caso l'autorizzazione sia di tipo generale, il responsabile dovrà informare il titolare ogni qualvolta sostituisca o aggiunga sub-responsabili. Il titolare potrà opporsi a tali modifiche.
Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile principale conserva nei confronti del titolare l'intera responsabilità circa l'adempimento.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO). Il responsabile della protezione dei dati può essere un dipendente, oppure un soggetto esterno ed "assolvere i suoi compiti in base a un contratto di servizi"; deve poter adempiere alle proprie funzioni e compiti in maniera indipendente. Ne consegue che il responsabile per la protezione dei dati, nell'esecuzione dei compiti attribuitigli, **non deve ricevere istruzioni sull'approccio da seguire nel caso specifico** e non deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
Il responsabile per la protezione dei dati "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". L'articolo 37, comma 7 del Regolamento UE impone al titolare del trattamento o al responsabile:

- di pubblicare i "**dati di contatto**" del RPD nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente;
- di comunicarli al **Garante della privacy**.

non è invece necessario **pubblicare** anche il **nominativo** del RPD.

I Registri

L'articolo 30 del regolamento UE 679/2016 sulla protezione dei dati personali disciplina **due "registri" da tenere in forma scritta, anche con modalità elettronica**.

Hanno finalità di ricognizione delle varie operazioni svolte: compresa la formazione, la programmazione, analisi dei rischi, consentendo di evidenziare la corretta gestione del trattamento dati: è la documentazione che deve essere esibita all'autorità nel caso di controllo.

Il primo registro è tenuto dal titolare del trattamento ed è il "registro delle attività di trattamento svolte sotto la propria responsabilità". Tale registro deve riportare tutte le seguenti informazioni:

- 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;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- se applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale (ipotesi prevista, in particolare, negli uffici anagrafici degli enti locali per gli stranieri extra UE) e, per i trasferimenti di cui al comma 2 dell'articolo 49 del Regolamento UE, la documentazione delle garanzie adeguate;
- se possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il secondo registro, è tenuto dal responsabile del trattamento e riguarda "tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento".

Il registro deve contenere:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare per conto del quale il responsabile agisce, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo e dell'organizzazione e, nel caso dei trasferimenti di cui al comma 2 dell'articolo 49 del regolamento UE, la documentazione comprovante le garanzie;
- una descrizione generale delle "misure di sicurezza tecniche e organizzative" previste dall'articolo 32 del regolamento UE.

Il registro, la cui tenuta è obbligatoria, deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto.

Dal 25 maggio 2018, tutti i **titolari dovranno notificare al Garante** della privacy le **violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma solo se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati "senza ingiustificato ritardo".

Definizioni

Per **"dato personale**" si intende 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.
Per «**trattamento**» si intende 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.

Valutazione d'impatto sulla protezione dei dati.

Per i dati il cui trattamento comporta particolare criticità, individuati dall'art. 35 del regolamento UE nei seguenti casi:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 (si tratta di dati sensibili: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), o dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

l'analisi dei rischi deve prevedere quanto segue

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) 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 al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

riportando le informazioni nel registro o nei registri del trattamento dati.

Modello di informativa

Deve essere adeguato al nuovo regolamento europeo. Per i trattamenti effettuati dal Comune, nell'ambito delle finalità istituzionali, non è richiesto il consenso.

Attività di formazione

Tutti i dipendenti che svolgono attività di trattamento dati devono per legge essere formati e seguire corsi di formazione. Si prevedono a tal fine diverse modalità: corsi esterni, circolari informative, nel cui contesto si inserisce anche la presente corsi on line. Si segnalano i webinar in materia di privacy, presenti sul sito dell'Ifel al seguente indirizzo https://www.fondazioneifel.it/formazione-ifel-20 : corso registrato del 03 maggio e del 09 maggio, ciascuno della durata di un'ora e mezza, che potranno essere visionati negli orari più opportuni in relazione all'esigenze del lavoro. Si informa che un altro corso avrà luogo il 25 maggio dalle ore 12, anche di questo potrà essere visionata la registrazione in differita.

22/05/2018

Il Segretario Generale
Dott.ssa Antonella Patrizia Nostro
(Firmata digitalmente)