REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679

luglio 2020

INDICE

CAPO I: DISPOSIZIONI GENERALI

Oggetto e campo di applicazione

a. Il presente Regolamento ha per oggetto le misure organizzative per l'attuazione della protezione dei dati personali di Interessati interni ed esterni all'Ente, trattati dall'Ente in qualità di Titolare del trattamento ai sensi dell'art.4 comma 7 del Regolamento UE 2016/679 ("GDPR"), nel rispetto della normativa vigente
b. Il presente Regolamento sostituisce i precedenti Regolamenti in materia di protezione dei dati personali (se approvati)

Definizioni

a. Il presente Regolamento adotta le definizioni di cui all'art.4 del GDPR e all'art. 2-quaterdecies del D.Lgs. 196/2003 nonché le seguenti ulteriori definizioni
b. "Figura Apicale": responsabile organizzativo di vertice di Area Settore Ufficio
c. Altre eventuali definizioni utili, es. nomi degli uffici citati nel resto del Regolamento

CAPO II: ORGANIZZAZIONE DELLA PROTEZIONE DEI DATI PERSONALI

Ruoli

a. L'organizzazione che attua nell'Ente la protezione dei dati personali è formata dalle persone fisiche e giuridiche che rivestono i seguenti ruoli: il Titolare del trattamento; il Comitato per la protezione dei dati personali; i Responsabili interni del trattamento ; i Responsabili esterni del trattamento; gli Amministratori di Sistema; gli Incaricati; gli eventuali Contitolari; il Responsabile della Protezione dei dati personali ("RPD").
b. Il Comitato per la protezione dei dati personali ("Comitato") segnala al Titolare eventuali carenze o necessità di aggiornamento relative alla copertura dei ruoli.

Titolare del trattamento

a. Ai sensi dell'art.4 comma 7 GDPR, il Titolare è la persona giuridica dell'Ente, rappresentato dal Sindaco, legale rappresentante pro tempore.
b. Il Titolare del trattamento determina le finalità e i mezzi del trattamento di dati personali; i compiti e le responsabilità del Titolare sono definite dall'art. 24 del GDPR.

Comitato per la protezione dei dati personali

a. E' istituito il Comitato per la protezione dei dati personali ("Comitato"), con compiti di coordinamento e controllo generali sull'attuazione del presente Regolamento.
b. La composizione del Comitato è definita ed aggiornata secondo necessità da un atto del Sindaco, includendo almeno il Segretario Generale dell'Ente, i Responsabili interni e l'Amministratore di Sistema principale.
c. Nell'ambito del Comitato, il Sindaco sceglie un Coordinatore, con compiti operativi di organizzazione delle attività del Comitato e può nominare un proprio Delegato, definendone i compiti; Coordinatore e Delegato possono coincidere.
d. Il Comitato predispone le procedure, i modelli ed ogni altro strumento necessario all'attuazione del presente Regolamento.
e. Il Comitato mantiene ed aggiorna un archivio documentale ("archivio") contenente il Registro delle attività di trattamento, gli atti di nomina dei Responsabili, la Procedura ed il Registro delle violazioni ed ogni altro documento utile a dimostrare l'attuazione del presente Regolamento e in generale dell'adeguatezza dell'Ente al GDPR, rendendolo disponibile in caso di controlli da parte del Garante o del RPD.

f. Il Comitato coordina e cura le comunicazioni dell'Ente con il Garante, con il RPD e con gli Interessati.
g. Il Comitato è responsabile della gestione delle segnalazioni delle violazioni dei dati personali.
h. Il Comitato si riunisce almeno semestralmente per verificare l'attuazione del presente Regolamento e programmare nuove attività per la risoluzione dei problemi emersi e migliorare l'adeguatezza dell'Ente al GDPR, da sottoporre al Titolare.
i. Le riunioni del Comitato sono convocate dal Coordinatore e presiedute dal Sindaco o dal suo Delegato.
j. Le attività del Comitato sono sottoposte ai controlli amministrativi dell'Ente.

Responsabili interni del trattamento

a. Il Titolare nomina per iscritto i Responsabili interni del trattamento ex art.4 comma 8 del GDPR ("Responsabili interni), indicandone l'ambito di attività in termini di processi o gruppi di procedimenti che trattano i dati – in coerenza con la descrizione adottata per il Registro delle attività di trattamento ex art.30 del GDPR - oppure di unità organizzative in cui si svolgono tali trattamenti.
b. Se l'ambito coincide con una intera unità organizzativa, il Responsabile interno è la Figura Apicale dell'unità organizzativa stessa, salvo diversa valutazione del Titolare, motivata nell'atto di nomina.
c. I compiti del Responsabile interno sono definiti dall'art. 28 del GDPR. Ai sensi del comma 2 del medesimo articolo, se il Responsabile è autorizzato a stipulare contratti con enti terzi che tratteranno dati personali per conto dell'Ente, il Responsabile è anche autorizzato in via generale dal Titolare alla loro nomina a Responsabili esterni del trattamento.
d. Il Comitato per la protezione dei dati personali predispone modelli per la nomina dei Responsabili Interni e segnala al Titolare le necessità di aggiornamento delle nomine conseguenti a riorganizzazioni dell'Ente, esternalizzazioni o internalizzazioni di attività e sostituzioni di figure apicali.
e. Nel caso in cui la struttura organizzativa preveda centri di responsabilità elementari (es., uffici o unità organizzative) per alcuni trattamenti omogenei, previo parare del Comitato, è possibile nominare formalmente -con atto analogo a quello che individua i Responsabili interni del trattamento- la figura del subresponsabile, definendo in modo univoco all'interno dell'atto di nomina il livello di responsabilità rispetto alla protezione dei dati personali e il rapporto con il Responsabile del trattamento suo superiore gerarchico.
f. Resta fatta salva la facoltà del Titolare o del Responsabile del trattamento di nominare, ai sensi degli artt. 4, comma 10°, Regolamento UE 2016/679; 2-quaterdecies, D.Lgs 101/2018) i soggetti "*autorizzati e designati al trattamento di dati personali*" (addetti al trattamento). Siffatti soggetti dovranno:
    - Effettuare direttamente ed integralmente l'attività di trattamento dati personali, in relazione a tutte le banche dati e qualsivoglia dato, nessuno escluso, afferente il Settore assegnato.
    - Tenere, curare ed aggiornare, in riferimento alle attività del Settore assegnato, un "*Registro dei trattamenti*" nel quale indicare le caratteristiche, le modalità e le finalità dei medesimi trattamenti, i mezzi utilizzati e, se possibile, una descrizione delle misure di sicurezza adottate.
    - Segnalare al Titolare ed al Responsabile del trattamento situazioni di rischio e/o criticità in ordine alla sicurezza dei dati trattati con particolare riferimento ai rischi di perdita, distruzione, modifica, divulgazione non autorizzata, di accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati.
    - Mettere a disposizione del Titolare e del Responsabile del Trattamento tutte le informazioni/documenti necessari al fine di dimostrare l'osservanza della normativa vigente, acconsentendo all'effettuazione di verifiche/controlli e ispezioni.

- Supportare il Titolare ed il Responsabile del Trattamento nel garantire i diritti degli interessati contemplati dalla normativa europea (es. diritto alla portabilità dei dati, diritto di rettifica e/o cancellazione dei dati, diritto alla limitazione del trattamento, etc.).
- Supportare il Titolare ed il Responsabile del Trattamento in ordine all'obbligo di formazione del personale dipendente autorizzato al trattamento dei dati prescritto dalla normativa europea.
- Supportare il Titolare ed il Responsabile del Trattamento nelle attività di analisi della natura, contesto e finalità dei trattamenti effettuati ai fini dell'adozione delle relative misure di sicurezza, tecniche ed organizzative, nonché nella predisposizione di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure adottate al fine di garantire la protezione dei dati trattati.
- Supportare il Titolare ed il Responsabile del Trattamento in ordine alle attività di analisi/valutazione dei rischi inerenti ai trattamenti effettuati, alla realizzazione di misure di sicurezza per limitare tali rischi (es. cifratura e/o pseudonimizzazione), alla riprogettazione del sistema informativo e, in caso di riscontro di rischi elevati per la protezione dei dati, alla valutazione di impatto prescritta dalla normativa in questione.
- Comunicare immediatamente qualsiasi anomalia al trattamento dati al Responsabile del Trattamento del proprio settore, oltre che al RPD.

Responsabili esterni del trattamento

a. I soggetti esterni che trattano dati personali per conto del Titolare sulla base di un contratto sono nominati Responsabili esterni del trattamento ("Responsabili esterni") dal Titolare o da un Responsabile interno autorizzato dal Titolare.
b. La nomina è parte del contratto col soggetto esterno oppure può avvenire con atto separato, secondo i modelli predisposti dal Comitato.
c. Con riferimento al contratto, la nomina specifica almeno le categorie di interessati e di dati personali trattati, i principali trattamenti effettuati, i doveri del Responsabile verso il Titolare, le modalità di controllo dell'operato del Responsabile e le modalità di riconsegna dei dati al termine del contratto, nel rispetto dell'art.28 del GDPR.
d. La nomina specifica altresì le modalità con cui il fornitore può ricorrere a sub fornitori nel trattamento ex art.28 comma 2 del GDPR, con particolare attenzione ai trattamenti svolti fuori del territorio dell'Unione Europea, ai sensi del Capo V del GDPR
e. Il Comitato predispone modelli per la nomina dei Responsabili esterni, ne verifica la concreta applicazione da parte del Titolare e dei Responsabili interni, segnalando al Titolare eventuali difformità o mancate nomine.

Amministratori di Sistema

a. Per garantire un livello di sicurezza dei dati personali adeguato al rischio ai sensi dell'art. 32 del GPDR, il Titolare ricorre ad uno o più Amministratori di Sistema, i cui compiti sono definiti dal Provvedimento del Garante della Protezione dei Dati Personali ("Garante") del 27 novembre 2008 e seguenti.
b. Il Titolare nomina per iscritto gli Amministratori di Sistema, l'ambito di responsabilità nell'atto di nomina in termini di servizi e sistemi informatici gestiti.
c. Gli Amministratori di Sistema possono essere persone fisiche e giuridiche, interne o esterne all'Ente.
d. Tra gli Amministratori di Sistema nominati, il Titolare ne identifica uno principale, che coordina e controlla l'operatività degli altri; di preferenza, l'Amministratore di Sistema principale è scelto all'interno dell'Ente o presso un altro Ente pubblico convenzionato.
e. Il Comitato predispone modelli per la nomina degli Amministratori di Sistema, verifica che le nomine corrispondano alle reali responsabilità operative dei medesimi, segnalando al Titolare eventuali difformità o mancate nomine.

Incaricati

a. Sono considerati "Incaricati" le persone fisiche che hanno accesso ai dati personali di cui è Titolare l'Ente ed agiscono sotto l'autorità del Titolare o di uno dei Responsabili ex art. 29 del GDPR.

b. Gli Incaricati sono assegnati ad una unità organizzativa dell'Ente; l'assegnazione li autorizza a svolgere i trattamenti necessari ai procedimenti svolti nell'unità, coerentemente con l'inquadramento e le mansioni assegnate.
c. Il Titolare provvede ad istruire l'Incaricato attraverso il Responsabile interno dell'unità organizzativa cui l'Incaricato è assegnato, secondo le indicazioni del Comitato ed in collaborazione con l'Ufficio Gestione del Personale.
d. Il Comitato verifica periodicamente l'efficacia delle istruzioni impartite agli Incaricati, segnalando al Titolare ed ai Responsabili interni eventuali necessità di aggiornamento della formazione.

Contitolari

a. Se necessario, l'Ente stipula per iscritto accordi di Contitolarità con altri Enti, pubblici e privati, ai sensi dell'art. 26 del GDPR.
b. Le Convenzioni con altri Enti per lo svolgimento congiunto di attività valgono come accordi di Contitolarità, se contengono le informazioni richieste dall'art.26 del GDPR
c. Il Comitato predispone gli accordi di Contitolarità ad integrazione delle Convenzioni in essere o da stipulare e ne controlla l'applicazione.

Responsabile della Protezione dei Dati personali

a. Il Responsabile della Protezione dei Dati personali (RPD) è nominato per iscritto dal Titolare; la nomina è comunicata al Garante con le modalità previste dal Garante stesso.
b. Le modalità di selezione del RPD e i suoi compiti sono definiti dagli artt. 37, 38 e 39 del GPDR.
c. Il Comitato collabora col RPD nelle sue attività di sorveglianza e cura l'attuazione dei miglioramenti da esso proposti.

CAPO III: STRUMENTI PER LA PROTEZIONE DEI DATI PERSONALI

Registro del trattamento

a. Il Titolare tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità, i cui contenuti sono definiti dall'art. 30 del GDPR ("Registro del Titolare")
b. Il Comitato definisce il formato del Registro e ne cura la redazione.
c. Il Registro è approvato con atto del Sindaco o delibera di giunta; l'atto di approvazione è pubblicato secondo i termini di legge senza però allegare il contenuto del Registro; analogamente, in caso di richiesta di accesso al Registro, l'eventuale accettazione è subordinata ad un parere del Comitato per la protezione dei dati personali, in quanto la conoscenza delle misure tecniche ed organizzative in atto potrebbe indirettamente pregiudicare la protezione dei dati personali detenuti dell'Ente, con un danno nei confronti degli interessati.
d. Il Registro è custodito nell'Archivio del Comitato
e. Almeno una volta all'anno, il Comitato verifica il contenuto del Registro e, se necessario, ne cura l'aggiornamento sottoponendo la nuova versione all'approvazione.
f. Per le attività di trattamento per le quali l'Ente è stato nominato Responsabile da altri Enti per effetto di una Convenzione o di un altro accordo, viene tenuto un Registri distinto ("Registro del Responsabile") con modalità analoghe a quelle del Registro del Titolare; la sua approvazione può essere delegata dal Titolare alla Figura Apicale dell'unità organizzativa primariamente incaricata delle attività.

Valutazione del rischio

a. E' compito del Titolare del trattamento effettuare, prima di procedere ad un trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35 del GDPR). Lo stesso articolo prevede l'obbligatorietà di tale valutazione per alcune casistiche di trattamenti.

b. In coerenza con il principio di adeguatezza e per una maggiore consapevolezza dei potenziali rischi, il Titolare e i Responsabili del trattamento effettuano una prima valutazione d'impatto su tutti i trattamenti di propria competenza, in cui siano gestiti dati non solo identificativi; nel caso in cui emergano da questa prima valutazione elevati rischi per i diritti e le libertà delle persone fisiche, si procede ad una valutazione d'impatto più approfondita, contenente quanto previsto dal comma 7 dell'art. 35 del GDPR. Tali valutazioni sono effettuate in base a criteri metodologici validati dal Responsabile della Protezione dei dati e approvati dal Titolare, sentito il Comitato.
c. La valutazione d'impatto, al pari dei registri delle attività di trattamento, è approvata con atto del Sindaco o delibera di giunta, è custodita nell'Archivio del Comitato e l'allegato all'atto di approvazione non è pubblicato, in quanto la sua conoscenza potrebbe indirettamente pregiudicare la protezione dei dati personali detenuti dell'Ente, con un danno nei confronti degli interessati; i Responsabili del trattamento procedono ad un riesame almeno annuale della valutazione d'impatto, anche in funzione degli interventi messi in atto.

Sicurezza Informatica

a. L'Amministratore di Sistema principale è responsabile della sicurezza informatica dell'Ente, coordinando le attività di esperti interni ed esterni
b. L'Amministratore di Sistema principale cura annualmente una Relazione illustrativa dello stato di attuazione delle protezioni attuate e pianificate e le conseguenti necessità di aggiornamento di sistemi e procedure; la Relazione è presentata al Comitato.
c. La sicurezza informatica è verificata con audit specialistici svolti da un ente esterno, con periodicità e modalità definite nella Relazione.

Sicurezza fisica

a. Per i trattamenti di propria competenza, ogni Figura Apicale è responsabile della protezione fisica dei dati personali trattati durante l'orario di lavoro, nei colloqui con l'utenza e nella produzione e circolazione delle stampe; verifica l'attuazione delle istruzioni da parte dei propri Incaricati; segnala al Comitato eventuali migliorie da apportare a strutture, strumenti e procedure
b. In caso di non adeguatezza della situazione rilevata, il Comitato propone al Titolare le migliorie da apportare a strutture, strumenti e procedure affinché l'accesso fisico ai locali in cui si svolgono i trattamenti, gli archivi, le sale server e in generale gli uffici siano resi adeguati ad una efficace gestione dei dati personali, anche quando i locali non sono presidiati dal personale.
c. Il Responsabile del protocollo informatico e dei flussi documentali è responsabile dell'accesso ai documenti custoditi negli archivi centrali dell'Ente.

Videosorveglianza

a. Il Regolamento della disciplina della videosorveglianza regola l'accesso ai dati personali raccolti dai sistemi di videosorveglianza dell'Ente, se presenti.

Protezione fin dalla progettazione (by design) e per impostazione predefinita (by default)

a. Il Titolare e i Responsabili del trattamento, coerentemente con i principi del GDPR, privilegiano soluzioni organizzative che minimizzino già in fase progettuale ("by design") la presenza di dati personali gestiti e il conseguente rischio che all'interno dei trattamenti vi siano loro violazioni.
b. Le azioni previste (dematerializzazione dei processi, riorganizzazione delle competenze, scelta di fornitori qualificati, ecc.) sono preventivamente comunicate al Comitato per una valutazione dell'impatto e dell'ordine di priorità dell'eventuale investimento necessario.
c. Il Titolare e i Responsabili del trattamento, coerentemente con i principi del GDPR, garantiscono che siano trattati per impostazione predefinita ("by default") solo i dati personali necessari a specifici trattamenti, privilegiando sempre la supervisione e validazione da parte di persone fisiche.
d. Eventuali trattamenti per i quali un Responsabile del trattamento ritenga opportuna una impostazione predefinita devono essere preventivamente comunicati al Comitato affinchè, visti i rischi intrinseci in tali trattamenti, sia effettata una preventiva valutazione dell'impatto.

CAPO IV: RELAZIONI CON GLI INTERESSATI

Informative e consensi

a. Il Comitato predispone modelli di Informative conformi agli artt. 13 e 14 del GDPR e ne verifica l'adozione.
b. Partendo dai modelli, i Responsabili interni Soggetti designati predispongono le Informative specifiche per i diversi trattamenti di loro competenza, in coerenza con le informazioni contenute nel Registro dei trattamenti, ne curano la pubblicazione sul sito istituzionale ed il richiamo – anche in forma abbreviata – nella modulistica.
c. Con la collaborazione dell'Amministratore di Sistema principale, il Comitato predispone l'Informativa relativa ai trattamenti svolti dal sito istituzionale e la Cookie Policy e ne curano la pubblicazione.
d. Il Comitato verifica la facile reperibilità delle Informative da parte degli utenti sul sito e nella modulistica.
e. Il consenso deve essere raccolto separatamente per ogni differente finalità del trattamento, distinguendo tra i consensi necessari allo svolgimento del servizio richiesto all'Ente e quelli facoltativi.
f. Se il consenso è raccolto attraverso una procedura informatica, la sua registrazione e conservazione è a cura dell'Amministratore di Sistema; se raccolto su modulo cartaceo, la sua conservazione è a cura dell'unità organizzativa responsabile del servizio.

Comunicazioni e contatti

a. Il Comitato cura una sezione del sito istituzionale dedicata alla protezione dei dati personali, richiamata nella prima pagina del sito.
b. Nella sezione sono presenti i rimandi alle Informative ed ad altri documenti reputati utili alla comprensione da parte degli utenti delle modalità di protezione dei dati personali attuate dall'Ente
c. Nella sezione sono presenti i riferimenti di contatto cui gli Interessati possono rivolgersi.

CAPO V: GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Segnalazioni interne

a. Il personale dell'Ente che viene a conoscenza di possibili violazioni di dati personali è tenuto a metterne tempestivamente a conoscenza il proprio responsabile diretto o la Figura Apicale dell'unità organizzativa in cui lavora o, in caso di sua indisponibilità, una qualunque Figura Apicale dell'Ente.
b. La segnalazione può avvenire in forma scritta o verbale e deve contenere ogni dettaglio utile alla sua tempestiva e corretta valutazione da parte del Comitato, tra cui il luogo e data del fatto, una breve descrizione dell'accaduto, le categorie di dati personali e di interessati verosimilmente coinvolti, le modalità con cui si è venuti a conoscenza del fatto, altre persone presenti.

Valutazione, notifiche e comunicazioni agli Interessati

a. Il Comitato è responsabile della valutazione delle segnalazioni e dell'esecuzione delle azioni conseguenti, ivi comprese le eventuali notifiche al Garante e comunicazioni agli Interessati ai sensi dell'art. 33 e 34 del GDPR, nel rispetto dei tempi dettati dai medesimi articoli.
b. Il Comitato si dota di una procedura di gestione, che definisce le modalità di valutazione, la suddivisione di responsabilità ed attività, le deleghe in caso di assenza, le modalità di rendicontazione delle attività svolte.

Registro delle violazioni

a. Ai fini dell'art. 33 comma 5 GDPR, il Comitato predispone, compila e custodisce nel proprio Archivio un Registro delle violazioni dei dati personali, attraverso cui documentare le attività svolte in seguito alle segnalazioni
b. Il Registro è messo a disposizione del RPD.