Deliberazione della Giunta Regionale 22 dicembre 2022, n. 1-6294

Integrazione delle istruzione operative di cui alla D.G.R N. 1 -7574 del 28.9.2018 per l'individuazione dei soggetti autorizzati al trattamento dei dati personali negli Uffici di comunicazione della Giunta regionale e agli esperti di supporto al Presidente della Giunta regionale di cui agli artt. 13 e 15 della L.R. 23/2008.

A relazione del Presidente Cirio:

Premesso che:

- il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- il 25 maggio 2018 è il Regolamento è diventato direttamente applicabile a tutti gli Stati membri il 25 maggio 2018;
- l'evoluzione della normativa in esame, di matrice europea, ha portato un profondo cambiamento della normativa nazionale; il d.Lgs. 196/2003 è stato profondamente innovato dal d.Lgs. 101/2018 che ha introdotto diversi articoli tra cui l'art. 2-quaterdecies relativo all'attribuzione di funzioni e compiti a soggetti designati, che prevede che il titolare del trattamento possa disporre, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità;
- è compito del titolare individuare le modalità più opportune per autorizzare le persone che operano sotto la propria autorità diretta al trattamento dei dati personali.

Dato atto che la Giunta regionale avvalendosi dei delegati al trattamento dati relativamente al personale di riferimento (Dirigenti per il personale incardinato presso i Settori regionali, Direttori relativamente al personale in Staff) ha effettuato le assegnazioni dei trattamenti di dati personali, mediante una procedura prevista all'interno del Registro dei trattamenti tramite l'applicativo Data Protection Manager (DPM).

Richiamata la D.G.R. n. 1 -7574 del 28.9.2018 recante "Adempimenti in attuazione al Regolamento UE 2016/679. Designazione degli incaricati e istruzioni operative. Disposizioni procedurali in materia di incidenti di sicurezza e di violazione di dati personali (Data Breach), adozione del relativo registro e modello di informativa.

Ritenuto opportuno, alla luce di quanto sopra riportato, integrare le istruzioni operative della deliberazione su indicata, dando indicazioni ai responsabili degli Uffici di comunicazione affinché procedano con l'assegnazione dei trattamenti, con apposita lettera di autorizzazione al trattamento di dati personali, a tutti i dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa di cui all'art. 13 della l.r. 23/2008 nonché al Capo di Gabinetto della Presidenza della Giunta regionale che provvede in merito agli incaricati di supporto al Presidente della Giunta regionale di cui all'art. 15 della l.r. 23/2008.

Considerato che il titolare del trattamento ha l'obbligo di formare gli addetti autorizzati al trattamento dei dati e di fornire apposite istruzioni comuni, al fine di omogeneizzare i comportamenti.

Ritenuto pertanto opportuno predisporre uno schema tipo di lettera allegato alla presente deliberazione (Allegato 1) contenente, a mero titolo esemplificativo e non esaustivo, alcuni esempi di trattamento che possono interessare i dipendenti degli uffici di comunicazione e le relative istruzioni operative che dovrà essere compilato a cura dei responsabili degli Uffici di comunicazione e del Capo di Gabinetto sulla base dei trattamenti assegnati ai singoli collaboratori.

Attestata l'assenza degli effetti diretti ed indiretti, del presente provvedimento, sulla situazione economico-finanziaria e sul patrimonio regionale, ai sensi della D.G.R. 1-4046 del 17 ottobre 2016, come modificata dalla D.G.R. 1-3361 del 14 giugno 2021.

Attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. n. 1-4046 del 17.10.2016 "Approvazione della "Disciplina del sistema dei controlli interni" parziale revoca della D.G.R. 8-29910 del 13.4.2000, come modificata dalla D.G.R. 1-3361del 14 giugno 2021.

Visto il Regolamento generale sulla protezione dei dati 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;

visto il Decreto Legislativo 10 agosto 2018, n. 101;

vista la Legge regionale 28 luglio 2008, n. 23;

vista la D.G.R. n. 1-6847 del 18.5.2018;

vista la D.G.R. n. 1-192 del 9.8.2019;

vista la D.G.R. n 10-5171 del 14.06.2022.

Tutto quanto premesso e considerato, la Giunta regionale, a voti unanimi resi nelle forme di legge;

delibera

1. di integrare le istruzioni operative di cui alla D.G.R n. 1 -7574 del 28.9.2018 (Adempimenti in attuazione al Regolamento UE 2016/679. Designazione degli incaricati e istruzioni operative. Disposizioni procedurali in materia di incidenti di sicurezza e di violazione di dati personali (Data Breach), adozione del relativo registro e modello di informativa), dando indicazioni ai responsabili degli Uffici di comunicazione affinché procedano con l'assegnazione dei trattamenti, con apposita lettera di autorizzazione al trattamento di dati personali, a tutti i dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa di cui all'art. 13 della l.r. 23/2008;

2. di dare atto che si provvede all'assegnazione dei trattamenti al Capo di Gabinetto della Presidenza della Giunta regionale con apposita lettera di autorizzazione al trattamento di dati personali, a cura del Presidente della Giunta regionale;

3. di dare atto che si provvede all'assegnazione dei trattamenti agli esperti di supporto al Presidente della Giunta regionale di cui all'art. 15, comma 3, della l.r. 23/2008 con apposita lettera di autorizzazione al trattamento di dati personali, a cura del Presidente della Giunta regionale ;
4. di approvare lo schema tipo di lettera allegato alla presente deliberazione (Allegato 1) per farne parte integrante e sostanziale, e le relative istruzioni operative da compilarsi a cura dei responsabili degli Uffici di comunicazione o del sottoscrittore del contratto di collaborazione sulla base dei trattamenti assegnati;
5. di dare atto che restano invariate le restanti disposizioni procedurali di cui agli allegati 2 e 3 della D.G.R n. 1 -7574 del 28.9.2018;
6. di dare atto che il presente provvedimento non comporta oneri per il bilancio regionale.

La presente deliberazione sarà pubblicata sul Bollettino Ufficiale della Regione Piemonte ai sensi dell'articolo 61 dello Statuto e dell'articolo 5 della legge regionale 12 ottobre 2010, n. 22.

(omissis)

Allegato

Allegato 1.

SCHEMA DI LETTERA

Oggetto: Attribuzione delle funzioni di autorizzato al trattamento di dati personali e istruzioni operative

La S.V._____è individuata quale autorizzato al trattamento di dati relativi alle seguenti attività:

(*Elenco proposto a titolo esemplificativo e non esaustivo)*

- ARCHIVIO DIGITALE (ARCHIVIO GENERALE DELLA GIUNTA) e gestione della documentazione cartacea. Piattaforma di gestione documentale comprensiva del modulo protocollo, dello smistamento, della classificazione e fascicolazione dei documenti elettronici (Archivio corrente). La finalità è quella di Garantire la gestione dell'archivio corrente

- Attività relative al conferimento di incarichi e alla sottoscrizione di contratti, convenzioni - Gestione di: 1) contratti di collaborazione; 2) contratti di servizio; 3) convenzioni con Enti pubblici. Il trattamento riguarda dati personali dei titolari dei contratti o - nel caso di Enti pubblici, di istituzioni o di imprese – dati riferiti ai legali rappresentanti necessari alla stipula dei contratti o delle convenzioni**;**

- Attività relative alla predisposizione delle risposte ad interrogazioni e interpellanze degli organi politici della Regione. Gestione e monitoraggio delle interrogazioni al Consiglio regionale, question time, interrogazioni a risposta immediata , ordini del giorno e mozioni;

- Nomine e designazioni in enti e istituzioni varie – Gestione dei dati riferiti a soggetti candidati e, successivamente nominati o designati, da parte della Regione in Aziende sanitarie, in enti e agenzie regionali, in altri enti vigilati e controllati dalla Regione stessa.

ISTRUZIONI OPERATIVE PER L'ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Al fine di facilitare comportamenti corretti, è innanzitutto necessario condividere il significato di alcuni termini connessi al trattamento dei dati personali. Di seguito un breve glossario di quelli più utili:

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 on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

dati particolari: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Nell'ambito dell'attività lavorativa deve assicurarsi che i dati personali siano:

a. **trattati** in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b. **raccolti** per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c. **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d. **esatti** e, se necessario, **aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e. **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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f. **elaborati** in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

Chiunque abbia accesso, nel ruolo di dipendente dell'Ufficio di Comunicazione/Incarico di supporto al Presidente della Giunta regionale, a banche dati cartacee e informatiche gestite dalla Struttura di appartenenza, nell'ambito dello svolgimento delle proprie mansioni, deve eseguire tutte le operazioni di trattamento di dati personali**,** necessarie e opportune al corretto adempimento delle sue mansioni, nel rispetto del principio di liceità del trattamento.

I trattamenti dei dati effettuati attraverso l'utilizzo di sistemi, applicazioni e strumenti informatici dell'Ente devono rispettare quanto indicato nella D.G.R. 2-5456 del 3 agosto 2022 "*Disciplinare per l'utilizzo dei sistemi informatici".*

Custodia degli strumenti di lavoro

Gli strumenti di lavoro messi a disposizione dalla Regione sono finalizzati all'uso professionale e destinati all'adempimento delle mansioni assegnate. È responsabilità dei singoli assegnatari custodirli in modo appropriato e diligente al fine di evitare, per quanto possibile, il furto, l'appropriazione o anche solo l'utilizzo da parte di terzi non autorizzati. In caso di furto e/o smarrimento è compito dell'utente assegnatario dell'attrezzatura presentare denuncia all'autorità giudiziaria. Copia della denuncia presentata dovrà essere inoltrata al proprio referente SIRe Asset ed è necessario informare, contestualmente, i Settori coinvolti nella gestione delle attrezzature. In caso di furto di smartphone/sim è necessario inoltrare copia della denuncia al competente Ufficio Area TLC Mobili.

E' altresì doveroso salvaguardare la riservatezza, l'integrità, la disponibilità e la sicurezza dei dati e dei documenti trattati o comunque accessibili attraverso gli strumenti di cui sopra, prestando la massima attenzione per le informazioni a carattere riservato e particolare.

I dischi interni delle postazioni di lavoro, gli eventuali dispositivi di memorizzazione locali o in disponibilità personale come hard disk portatili, chiavette usb, Network Attached Storage ad uso esclusivo oppure lo spazio di archiviazione disponibile sui dispositivi mobili (smartphone, tablet, etc...), non devono ospitare dati di interesse quali documenti/report (in qualsiasi formato essi siano es. ODT, WORD, ODS, EXCEL, ODP, POWER-POINT, PDF, JPG, etc...) contenenti dati personali e/o particolari afferenti alle attività di trattamento svolte.

Dispositivi mobili

Particolare attenzione va posta verso i dispositivi mobili, per loro natura estremamente vulnerabili, che sono veri e propri punti di accesso al Sistema Informativo; è fondamentale proteggerne l'accesso mediante gli strumenti messi a disposizione dal loro sistema operativo(riconoscimento biometrico, pin, password, etc...) cambiando regolarmente i relativi codici di accesso.

Memorizzazione dei dati

Gli incaricati del trattamento devono sempre utilizzare, per la memorizzazione, gli appositi share messi a disposizione da Regione (abilitati ai soli incaricati necessari) o i relativi database previsti dal progetto. In caso di necessità (anche solo temporanea) di mantenere per i fini di lavorazione una copia delle informazioni off-line (sul disco interno delle postazioni di lavoro), la copia locale deve essere cifrata (es. tramite funzioni di cifratura delle applicazioni) ed eliminata al termine della lavorazione.

Le cartelle di rete, siano esse condivise o personali, ospitano esclusivamente contenuti professionali e sono quotidianamente oggetto di backup.

E' buona regola la periodica pulizia degli spazi di memorizzazione delle unità di rete, dell'hard-disk della propria postazione di lavoro e della casella di posta, con cancellazione di file ed e-mail obsoleti e inutili o contenenti dati personali, evitando la duplicazione dei dati memorizzati. La medesima attenzione dovrà essere riservata ai documenti cartacei contenenti dati personali che, per quanto possibile, non devono essere lasciati sulla scrivania, ma riposti, quando non utilizzati e comunque al termine dell'attività lavorativa, negli appositi archivi correnti come da misure di sicurezza.

Comportamento in caso di violazione della sicurezza

La “violazione” è definita all’art. 4 par. 12 GDPR come *“la violazione di sicurezza che comporta accidentalmente in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati”* (data breach).

Non appena viene a conoscenza di una violazione di dati personali, al momento del verificarsi del fatto o della sua scoperta, il dipendente deve attivare apposita procedura di segnalazione, che prevede l’immediata comunicazione scritta e inviata con posta elettronica:

- sia al delegato al trattamento dati (Direttore per i dipendenti in staff; Dirigente per i dipendenti nei Settori/Strutture temporanee o di progetto) ~~e~~ o, in sua assenza, al Vicario quando individuato (indirizzando la segnalazione sia alla casella di posta elettronica personale del Direttore o Dirigente di riferimento sia a quella di Direzione/Settore/Struttura, se esistente) e, per conoscenza, all’Assessore di riferimento;

- sia al referente privacy di Direzione.

Esempi, a puro titolo esemplificativo, di eventi che possono comportare un *data breach*:

- pubblicazione dell’atto nella sua interezza senza omissione di dati personali/particolari;

- inoltro di messaggi contenenti dati personali/particolari a soggetti non interessati al trattamento;

- abbandono della postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, disattivare le procedure sulla risorsa informatica utilizzata, ecc..) e vi è evidenza che terzi abbiano avuto accesso alle informazioni~~;~~

- perdita della chiave di decriptazione di dati crittografati in modo sicuro(*se l’unica copia a disposizione)* ;

- cancellazione dei dati in modo accidentale o da parte di soggetti non autorizzati (senza possibilità di recupero);

- *data exfiltration* (copia o trasferimento non autorizzati di dati);

- *ransomware/malware*;

- distruzione accidentale di uno spazio di memorizzazione;

- smarrimento, furto di PC o server;

- smarrimento, furto di dispositivo mobile (smartphone, USB KEY, CD/DVD HD, etc.);

- smarrimento, furto o distruzione accidentale di documenti o aggregazioni documentali negli archivi cartacei (correnti o di deposito).