Allegato 1

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

Ai sensi della deliberazione della Giunta regionale n. 1-6847 del 18 maggio 2018 ha individuato tutti i dipendenti della Regione Piemonte, nonché tutti i soggetti dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa, come incaricati del trattamento dei dati effettuato nello svolgimento delle proprie funzioni.

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, il dipendente 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 della Direzione/Settore/Struttura speciale/Struttura flessibile/ Ufficio di Comunicazione, 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.

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 ed 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. E' indispensabile segnalare prontamente alla struttura competente il danneggiamento, lo smarrimento o il furto di tali strumenti (si segnala la DGR 2-12269 del 5 ottobre 2009 "*Disciplinare per l'utilizzo di personal computer, dispositivi elettronici aziendali, posta elettronica e internet*").

E' altresì doveroso salvaguardare l'integrità 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.

In particolare è vietato memorizzare sui dischi interni delle postazioni di lavoro o dei dispositivi mobili documenti/report (nei vari formati 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, cambiando regolarmente i codici.

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.

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 contenenti dati personali, ed 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) 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);
- sia al referente privacy di Direzione.

Ai dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa, di cui all’art. 13 della l.r. 23/2008, comportano i medesimi obblighi.

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 informazion~~;~~
- 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).