REGIONE TOSCANA

UFFICI REGIONALI GIUNTA REGIONALE

ESTRATTO DAL VERBALE DELLA SEDUTA DEL 04-06-2018 *(punto N 7)*

Delibera *N 585* *del 04-06-2018*

Proponente
VITTORIO BUGLI
DIREZIONE ORGANIZZAZIONE E SISTEMI INFORMATIVI

Pubblicita'/Pubblicazione Atto soggetto a pubblicazione su Banca Dati (PBD)
Dirigente Responsabile Giancarlo GALARDI
Estensore Giancarlo GALARDI
Oggetto
Regolamento (UE) 2016/679 "Regolamento Generale sulla Protezione dei Dati" (GDPR) - Indicazioni alle strutture regionali per la formulazione di linee guida in materia di protezione dati al fine di garantire la compliance dei trattamenti al GDPR.

Presenti

ENRICO ROSSI	VITTORIO BUGLI	STEFANO CIUOFFO
FEDERICA FRATONI	CRISTINA GRIECO	MARCO REMASCHI
MONICA BARNI		

Assenti

VINCENZO CECCARELLI	STEFANIA SACCARDI

ALLEGATI N°4

ALLEGATI

Denominazion	*Pubblicazione*	*Tipo di trasmissione*	*Riferimento*
1	Si	Cartaceo+Digitale	allegato 1
2	Si	Cartaceo+Digitale	allegato 2
3	Si	Cartaceo+Digitale	allegato 3
4	Si	Cartaceo+Digitale	allegato 4

LA GIUNTA REGIONALE

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, <<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 - GDPR), in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018;

Richiamato in particolare l'articolo 5 del GDPR , che al par 1 enuncia i principi applicabili al trattamento dei dati personali e al par 2 pone in capo al titolare il principio di responsabilizzazione (cd accountability) , in base al quale lo stesso deve assicurare, ed essere in grado di comprovare, il rispetto di tali principi;

Dato atto che la responsabilizzazione del titolare si realizza anche mediante:
- la concreta adozione, sia al momento della determinazione dei mezzi del trattamento che all'atto del trattamento stesso, di misure tecniche e organizzative adeguate ed efficaci, che tengano conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché del rischio per i diritti e le libertà delle persone fisiche (privacy by design)
- l'adozione di misure tecniche ed organizzative adeguate che garantiscano che siano trattati soltanto i dati personali necessari per ogni finalità di trattamento (privacy by default)
- l'individuazione di un Responsabile della Protezione dei dati (DPO) che, tra le altre funzioni, dà indicazioni e vigila sulla corretta osservanza del GDPR all'interno dell'organizzazione del titolare;

Richiamato l'art. 37, par. 1, lett. a) del succitato Regolamento, che prevede l'obbligo per il titolare del trattamento di nominare il Responsabile della Protezione dei Dati, nel seguito indicato con la sigla DPO in omogeneità con il DGPR <<quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, [...]>>;

Vista la DGR n. 208 del 9 marzo 1998 l'ente "Regione Toscana – Giunta regionale" è stato individuato quale titolare dei trattamenti di dati personali effettuati nei dipartimenti (oggi Direzione generale della Giunta/Direzioni regionali) e uffici della Regione Toscana, con esclusione dell'ambito di competenza del Consiglio regionale;

Vista la DGR n. 325/2018 con la quale si è proceduto a nominare il DPO per la Regione Toscana - Giunta regionale, affidandogli, tra gli altri, i seguenti compiti e funzioni:
- definire un piano di azioni per la piena applicazione del regolamento europeo e della normativa di riferimento per la Giunta regionale, avvalendosi delle competenti strutture delle Direzioni, in relazione ai trattamenti di cui sono responsabili
- provvedere alla tenuta del Registro dei trattamenti della Giunta regionale;

Vista la DGR 319/2014 <<Direttiva per l'attuazione del D.Lgs 196/2003 "Codice in materia di protezione dei dati personali">>, nella quale, tra le altre cose, si disponeva in merito all'attribuzione dei compiti e delle responsabilità dei soggetti che in Regione Toscana trattano i dati personali;

Considerato che il Regolamento (UE) 2016/679, oltre ad indurre nel titolare una sostanziale revisione delle proprie "privacy policies", dovuta in particolar modo all'applicazione del principio di responsabilizzazione, innova sia il glossario sia i ruoli privacy e le connesse responsabilità all'interno dell'organizzazione del titolare e innesta all'interno della struttura organizzative nuove responsabilità sulla protezione dei dati senza creare ulteriori figure, ritenendo che il dato, per il suo valore economico sociale ed organizzativo, sia una risorsa assegnata alla responsabilità dell'azione dirigenziale alla stregua di quelle finanziarie ed umane;

Ritenuto per quanto sopra di procedere ad un adeguamento dell'organizzazione privacy in Regione Toscana, delegando l'esercizio delle proprie competenze in materia di protezione dei dati ai dirigenti responsabili delle strutture presso le quali si svolgono i trattamenti, per mantenere coerenza con le responsabilità derivanti dalla l.r. 1/2009 e, dove possibile, con la responsabilità del procedimento amministrativo;

Ritenuto altresì che i trattamenti di dati afferenti a ciascun dirigente delegato debbano essere appositamente censiti nella procedura informatizzata "Registro trattamenti – Trattamenti Dati", che integra e completa la delega di funzioni e che pertanto deve sempre essere esaustiva di tutti i trattamenti effettuati ed aggiornata in tempo reale;

Ritenuto di autorizzare i dipendenti assegnati alle strutture dei dirigenti delegati e i soggetti che vi operano ad altro titolo, che agiscono sotto la loro autorità, al trattamento dei dati personali, nel rispetto del principio di minimizzazione dei dati, istruendo le persone autorizzate sulle modalità del trattamento come riportato nell'allegato 1), parte integrante e sostanziale del presente atto, stabilendo che l'ambito di operatività di ciascun autorizzato (tipi di dati personali trattati, operazioni di trattamento eseguibili, banche dati/archivi acceduti...) deve essere appositamente censito nella procedura informatizzata "Registro trattamenti – Trattamenti Dati Personali" a cura del dirigente delegato. Tale censimento integra e completa l'autorizzazione del titolare e legittima le persone autorizzate al trattamento dei dati personali e pertanto deve essere sempre esaustivo ed aggiornato in tempo reale;

Ritenuto inoltre di confermare come Amministratori di sistema, ai sensi dei Provvedimenti del Garante del 27/11/2008 e del 25/06/2009, i dipendenti individuati con provvedimento dirigenziale che svolgono le funzioni di gestione e manutenzione di un impianto di elaborazione o di sue componenti (quali ad esempio gli amministratori di dominio e di server) nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, specificando che non vi sono ricompresi coloro che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software , per es. per scopi di manutenzione a seguito di guasti o malfunzionamenti;

Preso atto della necessità di individuare una nuova figura di "Security IT Manager" (responsabile della sicurezza delle infrastrutture tecnologiche) che secondo il principio di divisione delle responsabilità non possa essere coinvolta nelle attività di gestione con il compito di sovraintendere e controllare che vengono eseguite tutte le misure atte a garantire la sicurezza dei sistemi, delle reti e degli accessi;

Considerato che ogni responsabile del contratto dovrà procedere laddove necessario alla individuazione del responsabile dei trattamenti nei modi e nelle forme previsti all'art. 28 dal GDPR, qualora sia prevista la gestione di dati o di sistemi da soggetti esterni alla organizzazione della Giunta Regionale ;

Preso atto delle prime indicazioni prodotte dal DPO, allegate al presente atto, in merito a:
. Indicazioni per la redazione di linee guida per il registro dei trattamenti (allegato 2)
. Indicazioni per la redazione di linee guida per il processo di Data Breach (allegato 3)
. Indicazioni per redazione di linee guida per la valutazione di impatto del rischio (DPIA) (allegato 4);

Ritenuto che si debba procedere attraverso una pianificazione certa alla traduzione delle indicazioni di cui agli allegati 2), 3) e 4), parti integranti e sostanziali del presente atto, in linee guida operative e in interventi organizzati nell'ambito delle responsabilità, competenze tecniche e amministrative delle Direzioni e delle strutture dirigenziali preposte, partendo dalla rilevazione dell'attuale stato dell'arte(Gap-Analisys) per

giungere alla definizione di un piano di lavoro che in tempi rapidi consenta alla Regione Toscana la piena attuazione del regolamento europeo (GDPR) e delle sue evoluzioni;

Visto il parere favorevole del Comitato di Direzione formulato nella seduta del 31.05.2018;

A VOTI UNANIMI:

DELIBERA

1)di procedere ad un adeguamento dell'organizzazione privacy in Regione Toscana, delegando l'esercizio delle proprie competenze in materia di protezione dei dati ai dirigenti responsabili delle strutture presso le quali si svolgono i trattamenti, per mantenere coerenza con le responsabilità derivanti dalla l.r. 1/2009 e, dove possibile, con la responsabilità del procedimento amministrativo, stabilendo che i trattamenti di dati afferenti a ciascun dirigente delegato debbano essere appositamente censiti nella procedura informatizzata "Registro trattamenti – Trattamenti Dati", che integra e completa la delega di funzioni;
2)di prendere atto della esistenza del Registro dei trattamenti conforme al GDPR e di dare mandato alle strutture competenti di mantenerlo costantemente aggiornato in tempo reale;
3)di autorizzare i dipendenti assegnati alle strutture dei dirigenti delegati e i soggetti che vi operano ad altro titolo, che agiscono sotto la loro autorità, al trattamento dei dati personali, nel rispetto del principio di minimizzazione dei dati, istruendo le persone autorizzate sulle modalità del trattamento come riportato nell'allegato 1), parte integrante e sostanziale del presente atto, stabilendo che l'ambito di operatività di ciascun autorizzato (tipi di dati personali trattati, operazioni di trattamento eseguibili, banche dati/archivi acceduti...) deve essere appositamente censito nella procedura informatizzata "Registro trattamenti – Trattamenti Dati Personali" a cura del dirigente delegato. Tale censimento integra e completa l'autorizzazione del titolare e legittima le persone autorizzate al trattamento dei dati personali;
4)di confermare come Amministratori di sistema, ai sensi dei provvedimenti del Garante del 27/11/2008 e del 25/06/2009, i dipendenti individuati con provvedimento dirigenziale che svolgono le funzioni di gestione e manutenzione di un impianto di elaborazione o di sue componenti (quali ad esempio gli amministratori di dominio e di server) nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, specificando che non vi sono ricompresi coloro che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software , per es. per scopi di manutenzione a seguito di guasti o malfunzionamenti;
5)di dare mandato alla Direzione Organizzazione e Sistemi informativi di individuare ed assegnare ad un dipendente della Direzione Organizzazione e Sistemi Informativi, dotato delle necessarie competenze professionali, i compiti di responsabile della Sicurezza IT (security IT manager);
6)di stabilire che ogni responsabile del contratto dovrà procedere, laddove necessario, alla individuazione del responsabile dei trattamenti nei modi e nelle forme previsti all'art. 28 dal GDPR, qualora sia prevista la gestione di dati o di sistemi da soggetti esterni alla organizzazione della Giunta Regionale ;
7)di prendere atto delle indicazioni operative prodotte dal DPO, di cui agli allegati 2, 3 e 4, parti integranti e sostanziali del presente atto, e di dare mandato alla Direzione Organizzazione e Sistemi informativi di redigere, con la consulenza della struttura DPO e la piena e fattiva collaborazione delle altre Direzioni, sulla base delle indicazioni operative in allegato, specifiche linee guida; nonchè di redigere, entro il 30 luglio 2018, un primo piano di attività per un progressivo adeguamento dell'organizzazione regionale al GDPR.

Il presente atto è pubblicato sulla banca dati degli atti amministrativi della Giunta regionale ai sensi
dell’articolo 18 della l.r. 23/2007.

SEGRETERIA DELLA GIUNTA

IL DIRETTORE GENERALE

ANTONIO DAVIDE BARRETTA

Il Dirigente responsabile
Giancarlo Galardi

Il Direttore
Carla Donati