RegioneLombardia

DECRETO N. 144 Del 16/10/2018

Identificativo Atto n. 6517

PRESIDENZA

Oggetto

DEFINIZIONE ASSETTO ORGANIZZATIVO DELLA GIUNTA REGIONALE IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

L'atto si compone di _____ pagine

di cui _____ pagine di allegati

parte integrante

RegioneLombardia

IL PRESIDENTE

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, di seguito GDPR, che contempla nelle definizioni di cui all'art.4 numero 7) la figura del "*titolare*" come: "la persona fisica, o giuridica, o l'autorità pubblica … omissis…che determina le finalità e i mezzi del trattamento" nonché le modalità e le misure di sicurezza;

RICHIAMATI

Il D. Lgs. N. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali";

La DGR n. X/7837 del 12 febbraio 2018 "Approvazione della policy regionale "Regole per il governo e applicazione dei principi di privacy by design e by default ai trattamenti di dati personali di titolarità di Regione Lombardia";

il D.Lgs.10 agosto 2018 n.101 " Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 della protezione dei dati)"

il D.Lgs.165/2001 " Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche"

La L.R.20/2008 " Testo unico delle leggi regionali in materia di organizzazione e personale"

RILEVATO altresì che, alla luce dell'entrata in vigore della nuova normativa europea, l'assetto organizzativo della Giunta Regionale, costruito e definito ai sensi degli artt. 28, 29 e 30 del D.Lgs.196/2003 deve essere obbligatoriamente rivisto e adeguato;

DATO ATTO che titolare del trattamento resta confermato Regione Lombardia nella persona del suo legale rappresentante il Presidente;

CONSIDERATO che dal 2006 ad oggi la Giunta Regionale ha definito e formalizzato con diversi provvedimenti organizzativi e decreti del Segretario Generale un'architettura organizzativa che prevedeva l'individuazione e la designazione di tutti i Direttori Centrali, Generali e responsabili di Area quali responsabili interni del trattamento con la definizione dei compiti e delle istruzioni loro impartiti da parte

del titolare;

DATO ATTO altresì che, con decreto del Segretario Generale n. 6805/2010, venivano individuati i suddetti soggetti quali responsabili interni ai sensi dell'art. 29 del D.lgs.196/2003 e agli stessi veniva attribuito il potere di individuare e nominare i dirigenti delegati che trattano dati sensibili e giudiziari;

CONSIDERATO che la nuova normativa (GDPR 2016/679), oltre a confermare la figura del titolare, prevede la figura del responsabile solo e unicamente nell'accezione di responsabile cosiddetto "esterno", quale soggetto incaricato a trattare i dati personali per conto del titolare del trattamento, come si evince da quanto previsto:

dall'art.4, numero 8): Definizione: "responsabile del trattamento",

dall'art. 26: Contitolari del trattamento

dall'art. 28: Responsabile del trattamento

dall'art. 82, comma 4): Diritto al risarcimento e responsabilità

oltre che dai diversi punti del considerando del GDPR, e dalle indicazioni dell'Autorità Garante per la protezione dei dati personali, che confermano l'esistenza della figura del responsabile quale soggetto esterno che tratta i dati per conto del titolare, prevedendo tutte le misure organizzative e tecniche per un corretto trattamento;

RITENUTO necessario, alla luce delle predette considerazioni, rivedere con il presente provvedimento l'organizzazione interna della Giunta Regionale, attestando nelle figure dei Direttori Centrali, Direttori Generali della Giunta e dei due Direttori di Area di Funzione Specialistica della Presidenza oltre al Direttore Sistema Controlli Prevenzione Corruzione Trasparenza e Privacy il ruolo di soggetti che esercitano le funzioni di titolare del trattamento dei dati personali in qualità di soggetti "*delegati*" che agiscono in nome e per conto del titolare, svolgendo una serie di compiti che dovranno essere sottoscritti dagli stessi per accettazione, secondo specifiche istruzioni;

RITENUTO altresì che i suddetti soggetti "delegati" (Direttori Centrali e Generali, i Direttori di Area di Funzione Specialistica della Presidenza e il Direttore Sistema Controlli Prevenzione Corruzione e Trasparenza, Privacy) possano attribuire la delega ai dirigenti per le funzioni di cui all'allegato 1;

PRECISATO che le figure dei soggetti delegati sono indicate nell'**allegato 1 "Funzioni del titolare",** che forma parte integrante e sostanziale del presente atto;

PRECISATO altresì che le nuove e principali funzioni in capo al titolare previste dall'applicazione del Regolamento Europeo da esercitare dai delegati sono:

Tenuta del registro dei trattamenti (art.30)

Privacy by design e default (art.25)

Valutazione impatto protezione dei dati (art.35)

Comunicazione violazione dei dati personali art. 33 e 34 (data breach)

Consultazione preventiva (art.36)

Definizione dei casi di contitolarità del trattamento (art.26)

PRECISATO altresì che per l'esercizio delle predette funzioni con particolare riferimento all'analisi della sicurezza dei dati, i soggetti delegati saranno supportati da soggetti con specifiche competenze tecniche/tecnologiche;

RITENUTO pertanto di approvare l'**allegato 2 e 2bis** contenenti l'indicazione dei compiti e le istruzioni impartite ai delegati quali parti integranti e sostanziali del presente atto;

RITENUTO inoltre che i compiti e le istruzioni impartiti ai Direttori in qualità di delegati debbano essere riferiti ai trattamenti di competenza avendo quale punto di riferimento il Registro dei trattamenti previsto dall'art. 30 del Regolamento Europeo in materia di protezione dei dati personali;

RITENUTO inoltre che i Direttori delegati debbano essere necessariamente supportati nello svolgimento di tutti gli adempimenti privacy dai Dirigenti e dai funzionari individuati quali referenti privacy di Direzione che agiscono al fine di sensibilizzare e intercettare tutte le esigenze e gli adempimenti privacy di competenza della Direzione;

PRECISATO che tutti i predetti adempimenti sono da condividere con la Struttura del privacy Officer e con il supporto e la consulenza del Data Protection Officer;

RITENUTO inoltre, a completamento della definizione del modello organizzativo della Giunta regionale, di procedere alla definizione della figura dell'operatore incaricato al trattamento ai sensi dell'art. 24, comma 1) del GDPR ;

RITENUTO pertanto di individuare tutti i dipendenti della Giunta regionale che trattano dati personali come operatori incaricati autorizzati al trattamento secondo il modello funzionale esistente, e prevedendo i relativi compiti e le istruzioni di cui all'**allegato 3**, che forma parte integrante e sostanziale del presente atto;

VALUTATO opportuno definire in modo più capillare il ruolo dell'operatore incaricato autorizzato che tratta particolari categorie di dati personali prevedendo, da parte dei soggetti delegati, la facoltà di designare con atto scritto i singoli incaricati attribuendo in capo agli stessi compiti e istruzioni specifici (come previsto negli **allegati 3 e 4**);

DATO ATTO che la nomina dell'operatore incaricato che tratta dati sensibili, giudiziari, biometrici e genetici di cui all'**allegato 4**, che forma parte integrante e sostanziale del presente atto deve essere formalizzata da parte del Direttore o dal dirigente di UO/Struttura e validata dal Direttore secondo modelli che verranno appositamente definiti con il supporto del Privacy Officer e del D.P.O.;

DATO ATTO altresì che debbano essere previste delle determinazioni in merito al trattamento dei dati personali e agli attori coinvolti all'interno dell'Organismo Pagatore Regionale (OPR) così come previsto dall'**allegato 5** che forma parte integrante e sostanziale del presente atto;

RITENUTO inoltre che debba essere obbligatoriamente fornita a tutti i dipendenti regionali neo assunti l'informativa sul trattamento dati da parte del titolare ai sensi dell'art.13 del GDPR e che la stessa debba essere pubblicata sull'intranet aziendale;

D E C R E T A

Di approvare per le motivazioni indicate in premessa il modello organizzativo della Giunta Regionale compliant al Regolamento in materia di protezione dei dati personali UE 2016/679 così definito:

di individuare le funzioni esercitate dal titolare del trattamento così come esplicitate **nell'allegato 1 "Funzioni del titolare"** parte integrante e sostanziale del presente atto, che specifica altresì le figure dei soggetti "delegati" all'esercizio di tali funzioni;

di individuare e designare i Direttori Centrali, Generali della Giunta regionale, i due Direttori di Area di Funzione Specialistica della Presidenza oltre al Direttore Sistema Controlli Prevenzione Corruzione Trasparenza Privacy quali soggetti che esercitano le funzioni di titolare come soggetti "delegati "da parte del titolare, attribuendo agli stessi i compiti e le istruzioni di cui **allegato 2**), parte integrante e

sostanziale del presente atto, che dovranno essere obbligatoriamente firmati per accettazione dagli stessi;

di prevedere che i suddetti soggetti "delegati" (Direttori Centrali e Generali , i Direttori di Area di Funzione Specialistica della Presidenza e il Direttore Sistema Controlli Prevenzione Corruzione e Trasparenza Privacy, possano attribuire la delega ai dirigenti per le funzioni di cui all'**allegato 1** e secondo i compiti e istruzioni di cui all'**allegato 2 bis**;

di prevedere per l'esercizio delle funzioni di cui all'allegato 1, con particolare riferimento all'analisi della sicurezza dei dati, che i soggetti delegati saranno supportati da soggetti con specifiche competenze tecniche/tecnologiche;

di assegnare agli stessi Direttori delegati i compiti e le istruzioni per i trattamenti di competenza così come previsto dal Registro dei trattamenti di cui all'art. 30 del GDPR;

di prevedere che i Direttori delegati debbano essere necessariamente supportati nello svolgimento e nel rispetto di tutti gli adempimenti privacy dai Dirigenti e funzionari individuati quali referenti privacy di Direzione che agiscono al fine di sensibilizzare e intercettare tutte le esigenze, adempimenti privacy di competenza della Direzione;

di prevedere che tutti i predetti adempimenti debbano essere condivisi con la Struttura del Privacy Officer e il supporto e la consulenza del Data Protection Officer;

di demandare alla Struttura del Privacy Officer la proposta di definizione di clausole tipo e di modelli tipo per la designazione dei responsabili;

di individuare quali operatori incaricati autorizzati al trattamento ai sensi dell'art.24, comma 1) tutti i dipendenti della Giunta regionale che trattano dati personali e agiscono in nome e per conto del titolare secondo un modello funzionale, impartendo agli stessi i compiti e le istruzioni di cui all'**allegato 3**), che forma parte integrante e sostanziale del presente atto;

di prevedere da parte del Direttore o dei Dirigenti di UO/Struttura con la validazione del Direttore, la nomina degli incaricati che trattano particolari categorie di dati personali (sensibili, giudiziari, biometrici e genetici), impartendo

agli stessi più capillari istruzioni come specificato nell'**allegato 4,** che forma parte integrante e sostanziale del presente atto e secondo modelli che verranno appositamente definiti con il supporto del Privacy Officer sentito il parere del D.P.O.;

di prevedere le determinazioni in materia del trattamento dei dati personali e degli attori coinvolti all'interno dell'Organismo Pagatore Regionale (OPR) così come previsto dall'**allegato *5*** che forma parte integrante e sostanziale del presente atto;

di prevedere a carico dell'Area di Funzione Specialistica Organizzazione, personale, patrimonio e sistema informativo in collaborazione con il Privacy Officer e sentito il DPO, la definizione del modello di informativa ai sensi dell'art.13 del GDPR, da fornire a tutti i dipendenti regionali neoassunti e da pubblicare sulla sezione intranet aziendale. Sarà cura di ciascun Direttore darne diffusione a tutti gli incaricati della Direzione di competenza;

di disporre la pubblicazione del presente atto e dei suoi allegati sulla intranet aziendale nella Sezione dedicata: "Privacy".

IL PRESIDENTE

ATTILIO FONTANA

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge

ALLEGATO 1

Funzioni del titolare

Il titolare del trattamento cosi come si evince dal combinato disposto dell'art. 4, numero 7 e dell'art. 24 del Regolamento Europeo(GDPR) è il soggetto che definisce le finalità, i mezzi, le modalità e le misure di sicurezza del trattamento. Titolare è Regione Lombardia nella persona del suo legale rappresentante il Presidente.

Il titolare esercita le sue funzioni tramite i seguenti soggetti delegati:

- Direttori Centrali
- Direttori Generali
- Direttori Area Funzione specialistica della Presidenza Organizzazione, personale, patrimonio e sistema informativo e Programmazione e Relazioni Esterne
- Presidenza-Direttore Sistema dei Controlli Prevenzione Corruzione Trasparenza e Privacy

che, nell'ambito delle Direzioni/Aree cui sono preposti, assicurano il rispetto di tutti gli obblighi previsti dal regolamento GDPR e dalla normativa nazionale posti in capo al titolare del trattamento.

I soggetti indicati in qualità di delegati dal titolare sono tenuti a rispettare i compiti e le istruzioni di cui all' allegato 2 "Compiti e istruzioni per i Delegati" e ad esercitare inoltre le seguenti funzioni per conto del titolare:

a) stipulare i contratti/incarichi /convenzioni di cui all'art. 28, comma 3, del Regolamento (GDPR), per disciplinare il rapporto con il responsabile del trattamento come previsto nell'allegato 2 sopra citato laddove tale funzione non venga delegata ai Dirigenti;
b) notificare al Garante della protezione dei dati personali le violazioni dei dati personali (Data breach) e comunicare la violazione agli interessati, nei tempi e con le modalità previste dagli articoli 33 e 34 del Regolamento con il supporto del DPO e del Gruppo di lavoro che verrà costituito per tale adempimento ;
c) nominare un dirigente in qualità di "referente privacy" a supporto all'esercizio delle funzioni di titolare del trattamento e alle attività di gestione degli adempimenti connessi alla protezione dei dati nonché come punto di contatto con il RPD;
d) validare con il supporto dei dirigenti competenti per funzione e materia trattata la Privacy By Design (art.25) e la valutazione dell'impatto sulla protezione dei dati di cui all'art. 35 del Regolamento;
e) adottare misure appropriate al fine di garantire l'esercizio dei diritti di coloro i cui dati personali sono oggetto di trattamento previsti agli articoli da 15 a 18 e da 20 a 22 del regolamento;
f) aggiornare il Registro dei trattamenti (art.30 del Regolamento)

g) fornire a tutti gli operatori incaricati i compiti e le istruzioni di cui all'allegato 3 al fine di rispettare in modo puntuale il corretto trattamento dei dati ;
h) consultare preventivamente l'Autorità Garante per la Protezione dei dati personali per i casi critici di Valutazione di Impatto privacy (art.36 comma 1);
i) designare le figure degli Amministratori di Sistema ai sensi del decreto 4171/2018.
j) verificare la corretta predisposizione delle informative e curarne il costante aggiornamento;
k) determinare ai sensi dell'art.26 i casi di contitolarità tramite accordi interni fra i titolari ;
l) designare ove necessario gli operatori incaricati autorizzati che trattano particolari categorie di dati personali (sensibili, e giudiziari, biometrici e genetici) come previsto dall'allegato 4 "Compiti e istruzioni per gli incaricati autorizzati al trattamento che trattano particolari categorie di dati personali (sensibili, giudiziari, biometrici e genetici)"

Per le funzioni di cui al **punto A)** viene precisato che Il responsabile esterno del trattamento è tenuto, in caso di modifiche, implementazioni di nuovi servizi o regole afferenti a piattaforme tecnologiche, ad informare, condividere con il titolare (nella figura del delegato) del trattamento, tutti gli aspetti che abbiano impatto sul trattamento dati ed è tenuto prima di procedere a qualsiasi validazione e produzione di tali implementazioni a ottenere l'autorizzazione all'avvio di tali modifiche. Il responsabile pertanto ne risponde direttamente nel caso non venissero attivate tali procedure di condivisione con il titolare (nella figura del delegato)

I compiti e le istruzioni di cui alle predette funzioni dei direttori delegati sono evidenziati nell'allegato 2.

Il Direttore delegato può facoltativamente attribuire la delega ai dirigenti competenti per materia su tutte le seguenti funzioni :

1.verificare la corretta predisposizione delle informative e curarne il costante aggiornamento;
2.designare ove necessario gli operatori incaricati autorizzati che trattano particolari categorie di dati personali (sensibili, e giudiziari, biometrici e genetici) come previsto dall'allegato 4 "Compiti e istruzioni per gli incaricati autorizzati al trattamento che trattano particolari categorie di dati personali (sensibili, giudiziari, biometrici e genetici)";
3.determinare ai sensi dell'art.26 i casi di contitolarità tramite accordi interni fra i titolari e dopo avere informato il direttore delegato:
4.Predisporre la Privacy By Design (art.25) e la valutazione dell'impatto sulla protezione dei dati di cui all'art. 35 del Regolamento secondo le modalità di cui alla dgr 7837/2018 e decreto 8384/2018;
5.stipulare i contratti/incarichi /convenzioni di cui all'art. 28, comma 3, del Regolamento (GDPR), per disciplinare il rapporto con il responsabile del trattamento come previsto nell'allegato 2 sopra citato laddove tale funzione non venga mantenuta dai Direttori;

Non possono essere delegate dal Direttore le funzioni di cui alle lettere b) c) d) f) h) i) ;

I compiti e le istruzioni di cui alle predette funzioni dei dirigenti sono evidenziati nell'allegato 2 bis.

ALLEGATO 2

Direttori Centrali, Generali, Direttori Area Funzione Specialistica della Presidenza Organizzazione, personale, patrimonio e sistema informativo e Programmazione e Relazioni Esterne e Direttore Sistema Controlli Prevenzione Corruzione Trasparenza e Privacy - Delegati dal titolare –

Compiti e istruzioni

In attuazione a quanto previsto dagli artt. 4 e 24 comma 1 del Regolamento (UE) 2016/679 e in continuità con quanto previsto dal D.Lgs.196/2003 e il D.Lgs.101/2018, si impartiscono ai direttori delegati i compiti e le istruzioni di seguito individuati:

- Trattare i dati personali esclusivamente per lo svolgimento di finalità istituzionali nei limiti stabiliti dalla legge, dallo Statuto e dai regolamenti;
- Trattare i dati personali solamente quando le finalità perseguite nel singolo caso non possono essere realizzate mediante l'utilizzo di dati anonimi e con modalità che permettano di identificare "l'interessato" solo in caso di necessità;
- Trattare i dati personali in modo lecito e secondo correttezza nonché per scopi determinati, espliciti e legittimi;
- Verificare periodicamente l'esattezza, la pertinenza, la completezza, la non eccedenza dei dati trattati rispetto alle finalità perseguite nei singoli casi e provvedere, quando necessario, a segnalare al Privacy Officer eventuali anomalie;
- Disporre o proporre al Privacy Officer , in conseguenza della verifica di cui al punto precedente, le modifiche necessarie a rendere il trattamento dei dati conforme alla normativa vigente;
- Confrontarsi e raccordarsi con il Privacy Officer nel caso di istituzione di un nuovo trattamento di dati;
- Adottare anche in relazione al progresso tecnico e se del caso, d'intesa eventualmente con altri soggetti delegati, misure di sicurezza idonee ad evitare rischi di distruzione o danneggiamento o perdita anche accidentale dei dati nonché pericoli di accesso non autorizzato o di trattamento non consentito o non conforme alla legge o al regolamento o alla finalità della raccolta;
- Collaborare in sinergia con i Dirigenti di UO/Struttura che trattano dati sensibili e giudiziari nella predisposizione degli aggiornamenti del Regolamento per il trattamento dei dati sensibili e giudiziari coinvolgendo il DPO e il Privacy Officer;

- Proporre e/o predisporre – anche di intesa con altri soggetti eventualmente delegati - ogni soluzione organizzativa, logistica tecnica o procedurale affinché sia assicurato agli "interessati" l'esercizio dei diritti di cui agli artt. da 15 a 22 del GDPR;
- Adottare modalità operative necessarie conformi alla norma a rendere all'"interessato" o alla persona presso la quale i dati personali sono raccolti, l'informativa di cui all'art. 13 del Regolamento UE 2016/679;
- Garantire e informare gli incaricati sulla legittimità e correttezza della comunicazione e della diffusione dei dati ad altri soggetti pubblici e privati nel rispetto delle normative di settore e delle relative finalità istituzionali, tenendo conto che i dati idonei a rivelare lo stato di salute non possono essere diffusi;

Si impartiscono, inoltre, ai direttori delegati i seguenti specifici compiti ed istruzioni:

Specifici compiti previsti dal Regolamento UE 2016/679:

- Trattare i dati pseudoanomizzati secondo le regole di cui all'art. 4 numero 5) del GDPR secondo misure tecniche e organizzative che garantiscano che le informazioni relative a dati personali non siano attribuibili a una persona fisica identificata o identificabile;
- Trattare tutti i dati riferiti alle banche dati e i trattamenti di competenza facendo riferimento al Registro dei trattamenti di cui all'art.30 del GDPR;
- Aggiornare il Registro trattamenti (art.30) con cadenza trimestrale, con l'obbligo per i referenti privacy di Direzione di verificare tutti i trattamenti in collaborazione con il Privacy Officer;
- Conservare i dati in una forma che consenta l'identificazione dell'"interessato" per un periodo non superiore a quello occorrente agli scopi per i quali gli stessi sono stati raccolti e trattati e definire il tempo di conservazione dei dati come previsto da norma di legge o necessario al perseguimento di finalità istituzionale;
- Rispettare tutte le disposizioni previste dalla dgr 7837/2018 e successive modifiche relativa ai principi di Privacy by design e default attivando il processo definito all'interno della dgr e dell'art.25 del GDPR per tutti i trattamenti rientranti in tale ambito;
- Rispettare tutte le disposizioni previste dal decreto n. 8384/2018 e s.m.i. "Metodologia Data Impact Assessment" per tutti i trattamenti che presentano un rischio per la libertà e la dignità dell'interessato e che ricadono nell'ambito della check list per cui risulta obbligatorio effettuare un'analisi dei rischi;

- Richiedere la consultazione preventiva all'Autorità Garante ai sensi dell'art. 36 del GDPR nei casi in cui il trattamento presenti un rischio elevato in assenza di misure adeguate adottate dal titolare;
- Coordinare le operazioni affidate agli incaricati appartenenti alla struttura o organizzazione di riferimento e vigilare sull'operato degli stessi;
- Collaborare con il Privacy Officer all'attuazione di tutti gli adempimenti in materia che comportino il trattamento di dati sensibili, giudiziari, biometrici e genetici;
- Garantire l'accesso ai dati personali dell'interessato di cui agli artt. da 15 a 22 del GDPR anche con il supporto dei dirigenti competenti per materia;
- Nominare ove necessario con atto scritto, gli operatori incaricati autorizzati al trattamento che trattano particolari categorie di dati personali (sensibili, giudiziari, biometrici e genetici) che sono previsti nella scheda competenze del Dirigente di UO/Struttura di riferimento, impartendo loro specifici compiti e istruzioni, come previsto dagli allegati 3 e 4;
- Individuare e designare in nome e per conto del titolare ai sensi dell'art. 28 del GDPR i soggetti Responsabili, verificando che gli stessi presentino le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato;
- Garantire nell'ambito dell'attività di controllo e audit da parte del titolare, del DPO prevista con cadenza annuale, la presenza del personale convolto nei trattamenti e l'esistenza della documentazione necessaria a supporto dell'audit;
- Attuare le prescrizioni del Garante per la protezione dei dati personali ed evadere, in collaborazione con "DPO" e "Privacy Officer", le richieste di chiarimenti da parte dell'autorità di controllo su specifici trattamenti;
- Provvedere con atto scritto alla nomina degli Amministratori di Sistema da individuarsi nelle figure apicali, come da decreto n. 4171/2018 e così come previsto dal provvedimento del Garante del 27 novembre 2008 e procedere alla vigilanza e al controllo sull'operato degli stessi al fine di redigere, con il supporto del Privacy Officer e DPO, con cadenza annuale, l'elenco aggiornato degli ADS;
- Provvedere ad avvisare tempestivamente tramite nota scritta il DPO, il Privacy Officer, il titolare e il Gruppo di lavoro costituito con apposita dgr eventuali casi di violazioni dei dati personali di cui all'art.33 e seguenti del GDPR per la tempestiva notificazione all'autorità entro le 72 ore;
- Definire, ai sensi dell'art.32 e nel rispetto del principio di accountability, le misure di sicurezza adeguate e idonee da adottare per singoli trattamenti;
- Tracciare con il supporto del dirigente delegato tramite apposita reportistica tutti i progetti tecnologici/informatici e cartacei che comportano il trattamento di dati e darne informazione al Privacy Officer e al DPO;
- Prevedere i casi di contitolarità di cui all'art.26 del Regolamento Europeo;

- verificare la corretta predisposizione delle informative e curarne il costante aggiornamento;, comunicandone ogni variazione al Privacy Officer.

I soggetti "DELEGATI "del trattamento dei dati personali devono provvedere all'espletamento di tutte le suddette operazioni, necessarie ad assicurare in ogni momento la corretta applicazione della normativa vigente in materia di protezione dei dati personali .

Il titolare dei dati, nella persona del Presidente della Giunta delega i succitati compiti e istruzioni in capo al Direttore che firma per accettazione

Il Direttore

Firma per accettazione

ALLEGATO 2 BIS

Dirigenti delegati dai Direttori Centrali, Generali, Direttori Area Funzione Specialistica della Presidenza Organizzazione, personale, patrimonio e sistema informativo e Programmazione e Relazioni Esterne e Direttore Sistema Controlli Prevenzione Corruzione Trasparenza Privacy

Compiti e istruzioni

In attuazione a quanto previsto dagli artt. 4 e 24 comma 1 del Regolamento (UE) 2016/679 e in continuità con quanto previsto dal D.Lgs.196/2003 e il D.Lgs.101/2018 si impartiscono ai dirigenti delegati dai direttori i compiti e le istruzioni di seguito elencati:

- Trattare i dati personali esclusivamente per lo svolgimento di finalità istituzionali nei limiti stabiliti dalla legge, dallo Statuto e dai regolamenti;
- Trattare i dati personali solamente quando le finalità perseguite nel singolo caso non possono essere realizzate mediante l'utilizzo di dati anonimi e con modalità che permettano di identificare "l'interessato" solo in caso di necessità;
- Trattare i dati personali in modo lecito e secondo correttezza nonché per scopi determinati, espliciti e legittimi;
- Verificare periodicamente l'esattezza, la pertinenza, la completezza, la non eccedenza dei dati trattati rispetto alle finalità perseguite nei singoli casi e provvedere, quando necessario a segnalare al Privacy Officer eventuali anomalie;
- Disporre o proporre al Privacy Officer , in conseguenza della verifica di cui al punto precedente, le modifiche necessarie a rendere il trattamento dei dati conforme alla normativa vigente;
- Confrontarsi e raccordarsi con il Privacy Officer nel caso di istituzione di un nuovo trattamento di dati;
- Adottare anche in relazione al progresso tecnico e se del caso, d'intesa eventualmente con altri soggetti delegati, misure di sicurezza idonee ad evitare rischi di distruzione o danneggiamento o perdita anche accidentale dei dati nonché pericoli di accesso non autorizzato o di trattamento non consentito o non conforme alla legge o al regolamento o alla finalità della raccolta;
- Adottare modalità operative necessarie a rendere all' "interessato" o alla persona presso la quale i dati personali sono raccolti, l'informativa di cui all'art. 13 del Regolamento UE 2016/679;

Specifici compiti previsti dal Regolamento UE 2016/679:

- Trattare i dati pseudoanomizzati secondo le regole di cui all'art. 4 numero 5) del GDPR secondo misure tecniche e organizzative che garantiscano che le informazioni relative a dati personali non siano attribuibili a una persona fisica identificata o identificabile;
- Trattare tutti i dati riferiti alle banche dati e i trattamenti di competenza facendo riferimento al Registro dei trattamenti di cui all'art.30 del GDPR;
- Conservare i dati in una forma che consenta l'identificazione dell'"interessato" per un periodo non superiore a quello occorrente agli scopi per i quali gli stessi sono stati raccolti e trattati e definire il tempo di conservazione dei dati come previsto da norma di legge o necessario al perseguimento di finalità istituzionale;
- Rispettare tutte le disposizioni previste dalla dgr 7837/2018 e successive modifiche relativa ai principi di Privacy by design e default attivando il processo definito all'interno della dgr e dell'art.25 del GDPR per tutti i trattamenti rientranti in tale ambito;
- Rispettare tutte le disposizioni previste dal decreto n. 8384/2018 e s.m.i. "Metodologia Data Impact Assessment" per tutti i trattamenti che presentano un rischio per la libertà e la dignità dell'interessato e che ricadono nell'ambito della check list per cui risulta obbligatorio effettuare un'analisi dei rischi;
- Nominare facoltativamente con atto scritto, gli incaricati autorizzati al trattamento che trattano particolari categorie di dati personali (sensibili, giudiziari, biometrici e genetici) che sono previsti nella scheda competenze del Dirigente di UO/Struttura di riferimento, impartendo loro specifici compiti e istruzioni, come previsto dagli allegati 3 e 4;
- Validare con il supporto del Privacy Officer il modello di informativa idonea e adeguata da inserire nel singolo incarico/servizio/ bando;
- Individuare e designare in nome e per conto del titolare ai sensi dell'art. 28 del GDPR i soggetti Responsabili, verificando che gli stessi presentino le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato;
- Definire, ai sensi dell'art.32 e nel rispetto del principio di accountability, le misure di sicurezza adeguate e idonee da adottare per i singoli trattamenti;
- Tracciare con la validazione del Direttore, tramite apposita reportistica tutti i progetti tecnologici/informatici e cartacei che comportano il trattamento di dati e darne informazione al Privacy Officer .
- Prevedere i casi di contitolarità di cui all'art.26 del Regolamento Europeo;

Allegato 3

Operatori Incaricati del trattamento dei dati personali di titolarità di Regione Lombardia – Giunta Regionale – art. 4 GDPR

Compiti ed istruzioni

In ottemperanza a quanto previsto dal D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e all'art. 4, numero10) del Regolamento UE 2016/679 e al fine di assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dell'"interessato", ciascun soggetto "autorizzato al trattamento da parte del titolare"- definito pertanto incaricato al trattamento- è tenuto ad effettuare i trattamenti di dati personali di titolarità di Regione Lombardia - Giunta regionale in osservanza delle istruzioni di carattere generale di seguito riportate e di ogni eventuale ulteriore indicazione espressa, facendo riferimento ai compiti ed istruzioni impartiti al Direttore delegato di cui all'allegato 2:

- trattare i dati personali esclusivamente per lo svolgimento di finalità istituzionali, nei limiti stabiliti dalla legge, dal Garante, dallo Statuto e dai regolamenti;
- trattare i dati personali solamente quando le finalità perseguite nel singolo caso non possono essere realizzate mediante l'utilizzo di dati anonimi o con modalità che permettano di identificare l'"interessato" solo in caso di necessità o con le modalità di pseudonimizzazione di cui all'art.4 numero 5);
- trattare i dati personali in modo lecito e secondo correttezza, per scopi determinati, espliciti e legittimi;
- verificare periodicamente l'esattezza, la pertinenza, la completezza, la non eccedenza dei dati trattati rispetto alle finalità perseguite nei singoli casi;
- conservare i dati in modo da non renderli accessibili a persone non autorizzate, in una forma che consenta l'identificazione dell' "interessato" per un periodo non superiore a quello occorrente agli scopi per i quali i dati sono stati raccolti e trattati e verificare il rispetto del tempo di conservazione secondo quanto indicato/previsto nel Registro dei trattamenti;
- comunicare preventivamente al "Direttore in qualità di delegato dal titolare" gli eventuali nuovi trattamenti da iniziare;
- trattare i dati sensibili e giudiziari contenuti in elenchi, registri o banche dati tenuti con l'ausilio di strumenti elettronici, con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerata la natura e il numero dei dati trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli "interessati" solo in caso di necessità (per gli incaricati che trattano particolari categorie di dati personali sono previste, se ritenuto necessario ed opportuno, nomine ad hoc tra gli incaricati);
- collaborare nella predisposizione degli aggiornamenti del Regolamento per il trattamento dei dati sensibili e giudiziari e di ogni altro atto regionale in materia di privacy;
- collaborare, con il supporto del dirigente competente e del referente privacy, all'aggiornamento del Registro dei trattamenti di cui all'art.30 del GDPR;

- proporre al Direttore delegato ogni soluzione organizzativa, logistica, tecnica e procedurale affinché sia assicurato agli "interessati" l'esercizio dei diritti di cui agli artt. da 15 a 22 del Regolamento UE 2016/679;
- adottare le modalità operative necessarie a rendere all'"interessato" o alla persona presso la quale i dati personali sono raccolti, l'informativa di cui all'art. 13 del Regolamento UE 2016/679 secondo il modello validato dal titolare del trattamento;
- garantire la legittimità e correttezza della comunicazione e della diffusione dei dati ad altri soggetti, pubblici o privati, tenendo conto che i dati idonei a rivelare lo stato di salute non possono essere diffusi e tenendo conto che la comunicazione interna ed esterna viene consentita solo laddove la norma di legge o Regolamento o la finalità istituzionale lo consenta e lo renda legittimo;
- evadere tempestivamente e correttamente le richieste degli "interessati" di cui agli artt.15-22 del Regolamento UE 2016/679 tramite il dirigente di riferimento o il direttore delegato;
- collaborare con i soggetti legittimati a svolgere ispezioni, controlli e verifiche;
- non lasciare incustoditi il proprio ufficio e i propri strumenti di lavoro senza aver preventivamente adottato tecniche e misure idonee a impedire l'accesso ai dati personali da parte di persone non autorizzate;
- utilizzare, gestire e custodire le proprie credenziali di autenticazione e autorizzazione, la posta elettronica, Internet e Intranet, le strumentazioni informatiche - compresi i supporti rimovibili - e ogni strumento di lavoro con modalità idonee a garantire la protezione dei dati personali degli "interessati", nel rispetto delle esigenze d'ufficio;
- collaborare con il Privacy Officer su tutti gli adempimenti di competenza che riguardino la corretta applicazione della privacy by design di cui all'art. 25 e della dgr 7837/2018;
- collaborare con il DPO e Privacy Officer su tutti gli adempimenti di competenza che riguardino la corretta applicazione della metodologia della Impact Assessment (DPIA) di cui all'art.35 del GDPR e del decreto 8384/2018, per una corretta effettuazione dell'analisi dei rischi;
- collaborare e informare il direttore delegato, il DPO nei casi di violazione dei dati personali di cui agli artt.33 e 34 per la corretta applicazione del data breach, per attivare in modo adeguato il processo di comunicazione all'autorità di controllo entro le 72 ore.

Le presenti istruzioni rivestono carattere generale e sono suscettibili di essere integrate, specificate e aggiornate dal "titolare" del trattamento dei dati, nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali.

ALLEGATO 4

Operatori Incaricati autorizzati al trattamento che trattano particolari categorie di dati personali (sensibili, giudiziari, biometrici e genetici)

Compiti e istruzioni

I Direttori /Dirigenti di UO/struttura, in qualità di Delegati del trattamento da parte del titolare possono facoltativamente nominare con atto scritto, i dipendenti che trattano dati sensibili, giudiziari, biometrici e genetici.

I soggetti "incaricati" sono tenuti quindi a seguire i seguenti compiti ed istruzioni:

- Aggiornare l'elenco delle banche dati –informatizzate e non- relative ai dati sensibili, giudiziari**,** biometrici e genetici costituite nell'ambito della propria struttura organizzativa o delle quali abbiano comunque la responsabilità trasmettendo quanto richiesto al "titolare";
- Collaborare per quanto di competenza -anche tramite il supporto del Privacy Officer e del DPO -all'aggiornamento del Registro dei trattamenti (art. 30 del GDPR);
- Aggiornare periodicamente l'elenco dei trattamenti dei dati sensibili, giudiziari, biometrici e genetici e, con il supporto del Privacy Officer, provvedere alle modifiche del Regolamento per il trattamento dei dati sensibili e giudiziari per le banche dati di competenza;
- Trattare i dati sensibili, giudiziari, biometrici e genetici solo ove indispensabili per lo svolgimento di attività istituzionali che non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa e autorizzato da un'espressa disposizione di legge o regolamentare o da un provvedimento del Garante che specifichino i dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite;
- Conformare il trattamento dei dati sensibili, giudiziari, biometrici e genetici secondo le modalità volte a prevenire violazioni dei diritti delle libertà fondamentali e delle dignità dell'interessato e secondo quanto previsto dal relativo Regolamento Regionale.
- Non trattare i dati sensibili, giudiziari, biometrici e genetici nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato.
- Conservare i dati idonei a rivelare lo stato di salute e la vita sessuale separatamente da ogni altro dato personale e trattarli secondo quanto previsto dalla normativa anche quando sono tenuti in elenchi registri o banche dati senza l'ausilio di strumenti elettronici.

I compiti di cui al presente allegato devono essere sempre coordinati con i compiti di cui all'allegato 3
Il modello di nomina ad incaricato verrà formalizzato con il supporto del Privacy Officer sentito il parere del D.P.O.;

ALLEGATO 5

Ruolo del Dirigente della Struttura Organizzativa dell'organismo pagatore (OPR)di Regione Lombardia rispetto al trattamento dati.

Rispetto alle determinazioni relative al ruolo del Dirigente della Struttura Organizzativa di OPR all'interno della Giunta Regionale definite con l' allegato C) della dgr n. X/3839 del 14.07. 2015 "XII Provvedimento organizzativo del 2015" come previsto dal presente decreto che prevede il ruolo dei Direttori quali delegati al trattamento dei dati del titolare e considerato che la struttura organizzativa dell'Organismo Pagatore Regionale (OPR) risulta a seguito dei cambiamenti organizzativi intervenuti collocata all'interno della Direzione Centrale Bilancio e Finanza, si prevede quanto segue :

1. l'Organismo Pagatore Regionale (OPR), quale soggetto autonomo e indipendente previsto e disciplinato dal Reg. (UE) 1306/13 e dal Reg. Del. (UE) 907/14, per l'erogazione di aiuti dei fondi unionali FEAGA e FEASR e individuato ai sensi del DM 162/2015 art. 3, quale titolare del trattamento dei dati del Fascicolo Aziendale dell'Agricoltore, istituito con DPR 503/99, risulta "Titolare" del trattamento dei dati pur se collocato all'interno di Regione;
2. viene altresì prevista una *contitolarità* da parte di Regione in quanto la struttura organizzativa dell'OPR è collocata, attualmente, all'interno della Direzione Centrale Bilancio e Finanza; la contitolarità di Regione si riferisce alla gestione delle attività istruttorie e delle misure di sicurezza e gestione congiunta dei diversi adempimenti in materia di trattamento dei dati personali;
3. la previsione delle contitolarità dell'OPR e di Regione determina l'individuazione del delegato del trattamento nella figura del Dirigente dell'OPR per tutti gli adempimenti conseguenti;
4. gli adempimenti previsti in materia di trattamento dati riferiti ad OPR (Registro trattamenti, nomina Amministratori di sistema, nomine incaricati, modulistica, DPIA e Privacy By Design, ed eventuali altri adempimenti previsti dal GDPR) saranno gestiti da Regione quale contitolare del trattamento;
5. la struttura organizzativa dell'OPR provvederà a declinare con atti successivi le determinazioni conseguenti al presente provvedimento;
6. le determinazioni che precedono prescindono dalla specifica allocazione dell'OPR all'interno della Regione, ora incardinato nell'ambito della Direzione Centrale Bilancio e Finanza.

Tutti gli aspetti previsti dalla contitolarità verranno definiti all'interno di uno specifico accordo che verrà sottoscritto dai due titolari ai sensi dell'art.26 del Regolamento UE 2016/679 nelle figure dei delegati come previsto dall'allegato 1, 2 e 2 bis