SviluppoToscana S.p.A.

DISPOSIZIONE DELL'AMMINISTRATORE UNICO

N. 40 DEL 03 OTTOBRE 2018

OGGETTO: Regolamento (UE) 2016/679 "*Regolamento Generale sulla Protezione dei Dati" (GDPR)* -Adozione delle indicazioni operative per la formulazione di linee guida in materia di protezione dati personali al fine di garantire la compliance dei trattamenti ai sensi del regolamento (ue) 2016/679 - GDPR - individuazione delle persone autorizzate al trattamento dei dati personali per Sviluppo Toscana S.p.A.

SviluppoToscana S.p.A.

L'AMMINISTRATORE UNICO

VISTA la Legge Regionale n.28/2008 istitutiva di Sviluppo Toscana S.p.A.;

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)»* (di seguito *anche regolamento europeo*), 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 (*c.d. 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 in sigla "DPO" in omogeneità con il GDPR) "*(…) quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (...)*";

VISTA la D.G.R. 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:

- informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento europeo, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali;
- sorvegliare l'osservanza del regolamento europeo, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali nonché delle politiche del titolare del trattamento in materia, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Reg.(UE) 2016/679;
- definire un piano di azioni per la piena applicazione del regolamento europeo e della normativa di riferimento, avvalendosi delle competenti strutture dell'Ente, in relazione ai trattamenti di cui sono responsabili;
- provvedere alla tenuta del Registro dei trattamenti.

DATO ATTO che la citata Delibera n. 325/2018 prevede la possibilità che il Consiglio regionale, gli Enti e le Agenzie regionale possano avvalersi della facoltà prevista dall'art. 37, par. 3, del GDPR, procedendo alla nomina condivisa di uno stesso DPO;

VISTA la Disposizione dell'Amministratore Unico di Sviluppo Toscana S.p.A. n. 15 del 04/05/2018, con la quale si è proceduto alla nomina condivisa del DPO individuato dalla Regione Toscana nella figura del Dott. Giancarlo Galardi con Delibera di Giunta n. 325/2018, incaricando il Dott. Giancarlo Galardi delle funzioni di cui all'art. 37 del Reg. (UE) n. 679/2016;

PRESO ATTO delle indicazioni prodotte dal DPO, allegate al presente atto di cui costituiscono parte integrante e sostanziale, in merito a:

- indicazioni operative per la redazione di linee guida per il registro dei trattamenti (**Allegato 1**);
- indicazioni operative per la redazione di linee guida per l'organizzazione dell'ente per la compliance al GDPR (**Allegato 2**);
- indicazioni operative per la redazione di linee guida per il processo di Data Breach (**Allegato 3**);

- indicazioni operative per redazione di linee guida per la valutazione di impatto del rischio (DPIA) (**Allegato 4**).

RITENUTO CHE:

- si debba accompagnare tutto il processo di adozione del GDPR con adeguati interventi di informazione, comunicazione e formazione continua atti a modificare i comportamenti e introdurre una nuova cultura e un modo di agire consapevole delle responsabilità di una corretta gestione dei dati, in quanto essi rappresentano un valore economico e sociale delle persone e delle organizzazioni;
- i principi fondamentali del regolamento europeo (GDPR) richiamati in precedenza (*accountability, privacy by design, privacy by default*, separazione delle responsabilità) innestino all'interno della struttura organizzativa 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;
- sia specifico compito di Sviluppo Toscana S.p.A., attraverso le proprie strutture, favorire e promuovere la diffusione della conoscenza in tema di sicurezza e protezione dei dati personali, attraverso processi di informazione e comunicazione;
- sia un valore aggiunto condividere in una forte logica di sistema le soluzioni in tema di protezione dei dati personali, con la Regione e gli altri enti e agenzie regionali;
- si debba procedere attraverso una pianificazione certa alla traduzione delle "*indicazioni*" in linee guida operative e in interventi organizzati nell'ambito delle responsabilità, competenze tecniche e amministrative delle strutture di Sviluppo Toscana S.p.A. preposte;
- per la pianificazione di cui sopra occorra attivare uno specifico ruolo per l'analisi e la reingegnerizzazione dei processi di lavoro anche in ottica di protezione dei dati personali;
- la traduzione delle indicazioni in linee guida operative, l'attuazione delle eventuali modifiche organizzative e al rispetto dei tempi debbano essere pianificate e costantemente monitorate dal DPO tenuto a darne comunicazione periodica al titolare;
- al processo di attuazione del GDPR debba essere assicurato un adeguato supporto legale.

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;
- il GDPR riguarda tutte le misure di sicurezza per la protezione dei dati personali ha potenzialmente potere di impatto su tutti i contratti di fornitura di servizi e che tali contratti debbono essere rivisti inserendo specifiche norme per essere rispettosi del nuovo Regolamento.

RITENUTO per quanto sopra di dover procedere ad una revisione dell'organizzazione privacy di Sviluppo Toscana S.p.A., per adeguarla a quanto previsto dal Regolamento Europeo, individuando le persone autorizzate al trattamento dei dati personali come segue;

RITENUTO in primo luogo di:

a) di delegare l'esercizio delle proprie competenze in materia di protezione dei dati personali ai Responsabili ed ai dipendenti alle Funzioni/ASA presso le quali si svolgono i trattamenti e, dove possibile, con la responsabilità del procedimento amministrativo;

b) stabilire che i trattamenti di dati personali afferenti a ciascuna Funzioni/ASA siano censiti nella procedura informatizzata "Registro trattamenti – Trattamenti Dati Personali", che deve sempre essere esaustiva di tutti i trattamenti effettuati ed aggiornata in tempo reale;

c) di autorizzare i dipendenti assegnati alle strutture dei Responsabile di ASA/Funzione ed 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;

d) istruire le persone autorizzate sulle modalità del trattamento come riportato nell'Allegato 5;

e) stabilire 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 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:

a) individuare come Amministratori di sistema, ai sensi del Provvedimenti Garante del 27/11/2008 e del 25/06/2009, i dipendenti 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) per effettuare trattamenti di dati personali e altre figure, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi, equiparabili ai primi dal punto di vista dei rischi relativi alla protezione dei dati personali, 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;

b) stabilire che nello svolgimento dei compiti loro assegnati, gli amministratori di sistema si attengono alle regole tecniche, previste nel disciplinare tecnico (**Allegato 6**);

c) 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 coinvolto nelle attività di gestione e debba sovraintendere e controllare che vengono seguite tutte le misure atte a garantire la sicurezza dei sistemi, delle reti e degli accessi;

d) fornire al responsabile della Sicurezza IT la collaborazione di adeguate risorse e competenze per lo svolgimento del proprio ruolo;

e) stabilire che l'elenco degli amministratori di sistema con i nominativi e gli ambiti di operatività in funzione dei profili autorizzativi assegnati, deve essere aggiornato a cura dal Responsabile della sicurezza IT (Security IT Manager), previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità, dei soggetti, tramite l'apposita procedura informatizzata "*Registro trattamenti – Trattamenti Dati Personali*", che integra e completa l'individuazione del titolare degli amministratori di sistema e pertanto deve sempre essere esaustiva di tutti i trattamenti effettuati ed aggiornata in tempo reale;

f) di stabilire che il Responsabile della Sicurezza IT debba indicare, monitorare e controllare il "*sistema IT*" nel suo complesso ponendo in capo alle strutture di gestione la responsabilità diretta delle azioni e della collaborazione che debbono fornire attraverso la messa a disposizione al Responsabile della sicurezza IT stesso, di tutte le informazioni e gli strumenti idonei al fine che possa svolgere i suoi compiti di monitoraggio e controllo generali e con particolare riferimento agli obblighi derivanti dal GDPR di rilevazione e comunicazione al Garante Nazionale, per il tramite del DPO, di eventi di violazione dei dati personali (*Data Protection Breach*).

CONSIDERATO che il tema della protezione dei dati personali e il GDPR deve coprire tutta la gestione del dato in tutte le sue forme e non solo in quella digitale, ritiene inoltre di:

- stabilire che la struttura competente in materia di archivio e protocollo contribuisca alla determinazione: delle misure di sicurezza degli archivi cartacei a tutti i livelli dalla gestione corrente a quella di archivio storico, della emanazione di indicazioni di comportamenti dei dipendenti nel trattamento di documenti cartacei contenenti dati personali, nella gestione della comunicazioni in entrata e uscita attraverso il protocollo digitale e non;

- stabilire che la struttura competente in Archivio e Protocollo collabori strettamente con il Responsabile della sicurezza IT nella rilevazione e comunicazione di eventi di violazione dei dati personali (*Data Protection Breach*) che avvengano su documenti cartacei o in forma mista cartacei e digitali.

CONSIDERATO, altresì, che si deve 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 personali da soggetti esterni alla organizzazione di Sviluppo Toscana S.p.A.

DATO ATTO che per lo svolgimento delle attività di Security IT Manager è individuata la persona del Sig. Romolo Manfredini, nominato con Disposizione dell'Amministratore n. 37 del 01/10/2018;

RITENUTO indispensabile, alla luce del GDPR e alle indicazioni redatte dal DPO, nominato con Determina n. 15 del 04/05/2018, e fatte proprie da Sviluppo Toscana S.p.A. con il presente atto, procedere alla:

- rilevazione dello stato dell'arte;
- alla formulazione di una analisi di distanza dello stato dell'arte rispetto all'atteso (*Gap-Analisys*);
- definizione di un piano di lavoro che in tempi rapidi consenta a Sviluppo Toscana S.p.A. la piena attuazione del Regolamento Europeo (DGPR) e delle sue evoluzioni.

D I S P O N E

in qualità di titolare del trattamento dei dati:

1) di approvare le indicazioni prodotte dal DPO, di cui agli Allegati da 1 a 4, parti integranti e sostanziali del presente atto;

2) di delegare l'esercizio delle proprie competenze in materia di protezione dei dati personali ai Responsabili di ASA/Funzione delle strutture presso le quali si svolgono i trattamenti ed ai dipendente loro rispettivamente assegnati, stabilendo che nel decreto di conferimento dell'incarico dirigenziale, sia richiamato espressamente l'atto che prevede la delega e che i trattamenti di dati personali afferenti di ciascun dirigente delegato siano essere appositamente censiti nella procedura informatizzata "*Registro trattamenti – Trattamenti Dati Personali*", 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;

3) di autorizzare i dipendenti assegnati alle strutture dei Responsabili di ASA/Funzione ed 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 5, stabilendo inoltre 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, che integra e completa l'autorizzazione del titolare e legittima le persone autorizzate al trattamento dei dati personali e che pertanto deve sempre essere esaustivo ed aggiornato in tempo reale;

4) di individuare come Amministratori di sistema, ai sensi del Provvedimento del Garante del 27/11/2008, modificato dal Provvedimento del 25/06/2009, i dipendenti 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) per effettuare trattamenti di dati personali e altre figure, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi, equiparabili ai primi dal punto di vista dei rischi relativi alla protezione dei dati personali, 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 stabilire che, nello svolgimento dei compiti loro assegnati, gli amministratori di sistema si attengono alle regole tecniche, previste nel disciplinare tecnico (Allegato 6) e che l'elenco degli amministratori di sistema con i nominativi e gli ambiti di operatività in funzione dei profili autorizzativi assegnati deve essere aggiornato a cura del Responsabile della sicurezza IT, previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità dei soggetti, tramite l'apposita procedura informatizzata "*Registro trattamenti – Trattamenti Dati Personali*", che integra e completa l'individuazione del titolare degli amministratori di sistema e che pertanto deve sempre essere esaustiva di tutti i trattamenti effettuati ed aggiornata in tempo reale;

6) di individuare la figura incaricata dello svolgimento delle attività di Security IT Manager nella persona del Sig. Romolo Manfredini, nominato con Disposizione dell'Amministratore n.37 del 01/10/2018;

7) di impegnarsi, con successivo atto, a:

   a) aggiornare i compiti del responsabile dell'archivio e protocollo ai fini della Protezione dei dati;

   b) pianificare e mettere in atto interventi di informazione e formazione a tutto il personale intesi a favorire una migliore consapevolezza, acquisire conoscenze e competenze in tema di protezione dei dati con particolare riferimento alla valutazione di impatto sui rischi (DPIA) previsti dal GDPR, attraverso incontri seminariali, interventi di aula, attraverso formazione a distanza (FAD e specifici laboratori);

   c) effettuare la rilevazione, in collaborazione con tutte le strutture di Sviluppo Toscana S.p.A., di tutti i contratti che hanno una rilevanza in termini di Protezione dei Dati e procedere con la consulenza della struttura del DPO, ad un loro eventuale adeguamento;

8) di impegnarsi, altresì, ad effettuare, con la consulenza della struttura DPO, e la piena e fattiva collaborazione di tutte le funzioni Sviluppo Toscana S.p.A.:

   a) la rilevazione dello stato dell'arte del sistema dei processi e del relativo impatto sul tema della Protezione dei dati;
   b) l'analisi delle carenze al fine del pieno rispetto del GDPR e sua evoluzione;
   c) la produzione, sulla base di tale rilevazione e della conseguente analisi, di un piano di lavoro che preveda la riduzione delle eventuali carenze, ponendo specifici obiettivi di adeguamento e la relativa indicazione dei tempi, degli atti e delle risorse necessarie;

9) impegna la Direzione Organizzazione e Sistemi Informativi della Regione Toscana a rendere operativo per l'Agenzia il nuovo registro dei trattamenti;

10) di impegnarsi con le strutture coinvolte, di concerto con il DPO, a tradurre le indicazioni in linee guida operative e a pianificare i relativi interventi organizzativi;

11) di impegnarsi ad attivare l'analisi e la re-ingegnerizzazione dei processi di lavoro, di concerto con il Responsabile della prevenzione della corruzione e della trasparenza;

12) di impegnarsi

    a) a dare supporto al DPO nella messa in atto di strumenti e azioni idonei a garantire l'adeguato livello di conoscenza dell'azione regionale, compresa l'attivazione di una struttura di *front end* sui temi del GDPR quale indispensabile collaborazione con la struttura dell'ufficio del DPO

    b) ad avviare in collaborazione con il DPO azioni di informazione e comunicazione atti a diffondere la conoscenza del regolamento sulla protezione dei dati personali e la condivisione di buone prassi, nel sistema pubblico regionale, come azione atta a favorire l'efficienza, l'efficacia, l'uniformità dei comportamenti verso la società toscana e la economicità, delle soluzioni;

13) di impegnare il DPO:

    - a fornire indicazioni sull'aggiornamento dei contratti di fornitura di servizi e sulla nomina del "*Responsabile del Trattamento*" da mettere in atto dai Responsabili di ASA/Funzione, laddove applicabili;
    - nel monitoraggio della pianificazione di tutto il processo di adeguamento al GDPR garantendo l'eventuale supporto di consulenza, e dandone comunicazione periodica al titolare;

14) di impegnare il DPO nel monitoraggio della pianificazione di tutto il processo di adeguamento al GDPR garantendo l'eventuale supporto di consulenza, e dandone comunicazione periodica al titolare;

15) di trasmettere il presente atto alla Regione Toscana–Direzione Organizzazione e Sistemi informativi.

Il presente atto è soggetto a pubblicità sulla rete internet ai sensi del D.Lgs. n. 33/2013 ed è pertanto pubblicato sul sito istituzionale di Sviluppo Toscana S.p.A. all'indirizzo www.sviluppo.toscana.it nella sezione *"Società trasparente"*.

L'AMMINISTRATORE UNICO

Dott. Orazio Figura