Domande Frequenti sul GDPR e sui relativi servizi di LepidaScpA

Aggiornato al 03.08.2018

(Rev. 14.03.2019)

Vengono di seguito riportate alcune domande frequenti pervenute, nell'ambito delle attività di supporto agli Enti negli adempimenti derivanti dal GDPR, a Lepida con le relative risposte.
Si precisa che le risposte fornite indicano una versione della risposta che viene aggiornata nei casi in cui la risposta viene modificata in virtù di maggiori dettagli, precisazioni e approfondimenti.

Q1: Dovendo iniziare il censimento dei trattamenti del Comune, è sorto un dubbio preliminare sulla qualificazione del concessionario di servizi (ad es. ICA per riscossione tributi o tesoriere). E' corretto definirlo responsabile del trattamento o questa definizione si addice soltanto agli appaltatori?

Lepida (A1 V1)
E' necessario acquisire informazioni al riguardo al fine di poter fornire una risposta.
In via generale non v'è coincidenza necessaria tra fornitori e responsabili. Questo perché anche un ente pubblico potrebbe essere responsabile del trattamento di un altro ente (ad esempio per alcuni servizi).
Pertanto, bisogna in effetti verificare il grado di autonomia di tale soggetto, la sua natura giuridica, il contratto/convenzione che disciplina i rapporti tra le parti.

Q2: Quali sono i documenti che verranno forniti da Lepida, da utilizzare da parte dell'Ente come template, nell'ambito del proprio servizio

Lepida (A2 V1) Lepida fornirà i seguenti documenti:

- Designazione incaricati
- Designazione responsabile trattamento
- Modello organizzativo;
- Disciplinare utenti;
- Fac-simile di informativa.

Tutti i documenti dovranno poi essere adeguati, tra le altre cose, alla realtà organizzativa specifica di ciascun ente.

Q3: Il sistema RecordER permette anche la produzione di autorizzazione o designazione?

Lepida (A3 V1) Il sistema permette la produzione, secondo modelli definiti, di:

- Autorizzazione al trattamento per gli incaricati
- Designazione dei Responsabili del trattamento per i soggetti esterni

Si precisa che La conformazione del registro (ovvero, RecordER) è incompatibile con la designazione degli amministratori di sistema: infatti nella designazione devono essere indicati i sistemi amministrati e i privilegi assegnati. Dato che non è previsto l'inventario di sistemi, base dati, software complessi ecc. fare la designazione a mezzo del registro è esercizio inutile. Inoltre, il Responsabile della protezione dei dati personali sarà designato nel modello organizzativo che è documento di cui verrà fornito un fac-simile

---

Q4: quali tipologie di ruoli prevede il sistema RecordER?

Lepida (A4 V1) Il sistema prevede le seguenti tipologie di ruolI:

- Titolare del trattamento
- Contitolare del trattamento
- Responsabile della protezione dei dati
- Destinatario di comunicazione dei dati
- Incaricato del trattamento
- Responsabile del trattamento
- Soggetto delegato
- Amministratore di sistema

Q5: quali categorie statiche prevede il sistema RecordER?

Lepida (A5 V1) Il sistema prevede le seguenti categorie:

- Categorie di interessati
    - Amministratori locali
    - Destinatari dell'atto/provvedimento/contratto
    - Dipendenti
    - Richiedenti
    - Altro (+ campo libero da compilare)
- Categorie di dati personali
    - Dati identificativi della persona: Cognome, Nome
    - Dati identificativi della persona: data di nascita, luogo di nascita, codice fiscale

    - Dati identificativi della persona: residenza, domicilio
    - Dati identificativi della persona: telefono, email, PEC
    - Dati identificativi della persona: stato civile, relazioni di parentela
    - Dati identificativi della persona: immagini
    - Dati identificativi digitali: Credenziali di accesso ai servizi online (Federa, SPID, ecc.)
    - Dati identificativi digitali: Identificativi online (dati di connessione, indirizzo Ip, ecc..)
    - Dati relativi alla vita personale (abitudini di vita, situazione familiare, attività lavorativa)
- Categorie di dati particolari
    - Appartenenza sindacale
    - Biometrici
    - Convinzioni religiose o filosofiche
    - Genetici
    - Geolocalizzazione
    - Giudiziari
    - Opinioni politiche
    - Orientamento sessuale
    - Vita sessuale
    - Origine razziale o etnica
    - Salute
- Termini per la cancellazione
    - Termine delle finalità per le quali il dato è stato raccolto
    - Campo libero in cui specificare termine effettivo

Si fa presente che gli Enti pubblici non chiedono, per normativa, un consenso all'interessato.

Q6: L'art. 32 del GDPR recita "Tenendo conto dello stato dell'arte e dei costi di attuazione...". Siccome si dice che il GDPR non preveda che gli enti non possano sostenere i costi per applicarne le misure prescritte come va interpretata questa la summenzionata dicitura?

Lepida (A6 V1) Sulla scorta del principio dell'accountability, il GDPR impone al Titolare di valutare i rischi afferenti ai trattamenti effettuati, commisurando le misure tecniche ed organizzative al livello di rischio rilevato. Ciò significa che l'Ente adotterà tutte le misure di sicurezza adeguate a "trattare" il rischio. La norma prevede anche i criteri che consentono di determinare l'adeguatezza delle misure applicate: tra gli altri, lo stato dell'arte (le misure di sicurezza che erano adeguate diversi anni fa non lo sono attualmente), i costi di attuazione di misure di sicurezza commisurate al livello del rischio , anche con riferimento alla natura del

trattamento (che per un ospedale ha teoricamente rischi maggiori rispetto ai trattamenti di un Comune).

Q7: Vanno inseriti nel Registro dei Trattamenti quelli riguardanti imprese/aziende/persone giuridiche, laddove essi comprendano anche i dati personali dei titolari delle stesse (anche solo nome e cognome delle persone fisiche)?

Lepida (A7 V1) Il GDPR definisce all'art. 4 n. 1) il concetto di dato personale:
1) «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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Pertanto, ricadono nell'ambito della normativa, anche i dati del nome e cognome del legale rappresentante di una società.

Q8: Ai fini della compilazione del Registro e dell'Informativa, tra i "Destinatari esterni" è necessaria l'indicazione specifica della denominazione dei soggetti ai quali i dati saranno comunicati (es. Tribunale, ANAC, società x, società y...) o è sufficiente l'indicazione della categoria di appartenenza dei soggetti stessi (es. "soggetti pubblici" o "società")?

Lepida (A8 V1) E' necessario indicare i nominativi dei soggetti destinatari nel Registro selezionandoli da un elenco predisposto da Lepida sulla base di indicazioni dal GDL della Comunità Tematica. Il Registro prevede anche, obbligatoriamente, l'indicazione della norma di legge o regolamento legittimante la comunicazione di dati personali ai soggetti indicati. L'Elenco dei soggetti non viene incluso nell'informativa.

Q9: L'essere rappresentante legale di enti/associazioni con orientamento sessuale o religioso determina un trattamento di categorie di dati personali?

Lepida (A9 V1) Dipende dal contesto in cui il trattamento è effettuato. Occorre specificare il caso specifico in considerazione.

Q10: E' da inserire come "Trattamento" nel Registro quello che contiene il nome e cognome del progettista o RUP di elaborati tecnici ?

Lepida (A10 V1) Il nome e cognome del progettista o RUP è un dato personale, tuttavia nel registro devono essere censiti ed inseriti i trattamento e non il dato di per sé. Pertanto, per individuare il trattamento deve essere individuata la finalità per cui tale dato è trattato.

Q11: Il trattamento di dati di persone decedute (es. cause di morte) è da includere nel registro dei trattamenti?

Lepida (A11 V1) Il GDPR non si applica ai dati delle persone decedute, occorre verificare l'evoluzione della normativa nazionale al riguardo.

Q12: Un cittadino chiede l'accesso ai suoi dati personali in modo generico, sulla base dell'informativa che prevede il diritto agli interessati di chiedere all'Ente l'accesso ai dati personali l'accesso ai dati personali, la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (art. 15 ss. Regolamento UE 2016/679). Come si deve comportare l'Ente?

Lepida (A12 V1) Come indicato dal Considerando n. 63 del GDPR, l'Ente, in ragione del fatto che tratta una notevole quantità di dati, è legittimato a richiedere all'interessato di precisare le informazioni e le attività di trattamento cui si riferisce la sua richiesta.

Q13: Un cittadino comunica all'Ente di dare il consenso al trattamento dei propri dati personali solo ed esclusivamente per ricevere comunicazioni o eventuali news, ma comunica anche di non dare il consenso per trattare i suoi dati personali ai fini statistici e/o la cessione a terzi. Come si deve comportare l'Ente?

Lepida (A13 V1) Gli Enti pubblici effettuano trattamenti di dati personali al fine di dare attuazione alle proprie attività istituzionali. Non devono, nè sono legittimati dalla norma, richiedere il consenso al trattamento dei dati personali. Inoltre, gli Enti non possono "cedere a terzi" i dati personali relativi ai trattamenti di cui sono Titolari. Sono ammissibili le operazioni di comunicazione e diffusione previste da norma di legge o di regolamento.

Q14: Sarebbe opportuno stipulare una polizza assicurativa che copra l'ente dai rischi derivanti da incidenti di sicurezza e violazione della privacy?

Lepida (A14 V1) Gli incidenti di sicurezza e le violazioni in materia di protezione dei dati personali sono eventi suscettibili di causare sanzioni e risarcimenti economici, anche di rilevante entità. Quindi si ritiene sia una scelta opportuna quella di stipulare una polizza assicurativa.

Q15: Nel caso di un fornitore software che eroga servizi di assistenza e manutenzione al software con interventi ascrivibili alle attività di amministratore di sistema effettuate direttamente sulla banca dati presso l'Ente anche con collegamento da remoto senza effettuare operazioni di trattamento dei dati per le finalità per cui sono raccolti, il fornitore va comunque nominato responsabile esterno con i template di cui alla mail in calce o va solo nominato amministratore di sistema?

Lepida (A15 V1) La nomina ad amministratore di sistema è conferibile ad una persona fisica. Nel contratto di fornitura il fornitore deve essere designato responsabile del trattamento. A tal punto l'Ente può scegliere se demandare al fornitore gli oneri di designazione degli amministratori, di tenuta dell'elenco e di verifica delle attività degli stessi, oppure procedere esso stesso alla designazione degli amministratori, previa attestazione da parte della società fornitrice, delle competenze del soggetto da nominare in materia di sicurezza informatica

---

Q16: Nel caso di un fornitore software di licenza e fornitore partner di servizi di assistenza e manutenzione al software con interventi ascrivibili alle attività di amministratore di sistema: se un fornitore eroga solo la licenza, ed un'azienda partner i servizi di cui sopra, gli stessi servizi non vengono contrattualizzati e fatturati dal partner, bensì dall'azienda principale, chi deve essere nominato responsabile? Il primo, il secondo o entrambi?

Lepida (A16 V1) A prescindere dalla formalizzazione contrattuale, deve essere designato responsabile del trattamento chi effettua materialmente il trattamento. Pertanto, la società deve essere designata responsabile del trattamento. A tal punto l'Ente può scegliere se demandare al fornitore gli oneri di designazione degli amministratori, di tenuta dell'elenco e di verifica delle attività degli stessi, oppure procedere esso stesso alla designazione degli amministratori, previa attestazione da parte della società fornitrice, delle competenze del soggetto da nominare in materia di sicurezza informatica.

Q17: Videosorveglianza

1) Quali sono gli adempimenti in caso di eventi che prevedano l'installazione di telecamere con sistemi che fanno uso di tecnologie in grado di rilevare dati biometrici, di individuare determinati eventi o comportamenti o di riconoscere automaticamente una persona sulla base delle immagini riprese (sensori per il rilevamento della folla, videocamere per il rilevamento termico e possibile riconoscimento facciale, ecc.)?

2) Che caratteristiche devono avere i cartelli informativi nelle aree di transito dei cittadini (grandezza, illuminazione, posizione, eventuali icone...)?

3) Se la raccolta di questi dati (che avviene nel corso di un evento del Comune e su territorio comunale) è effettuata con l'utilizzo di tecnologia di un fornitore esterno: è il Comune che deve adempiere agli obblighi previsti? Oppure occorre nominare responsabile esterno il fornitore, che dovrà adempiere? Vale lo stesso se il dato è raccolto in forma aggregata?

Lepida (A17 V1) L'entrata in vigore del nuovo regolamento europeo ha avuto un impatto significativo anche nella regolamentazione delle tecnologie "biometriche". Il trattamento di dati biometrici è ora direttamente disciplinato dall'art 9 del GDPR, il quale dispone che "*È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica*…." . Tale generico divieto è contemperato di diverse eccezioni elencate nel medesimo articolo. Quella pertinente al caso di specie -si assume che il sistema di videosorveglianza sia installato per finalità di pubblica sicurezza- è quella indicata alla lettera g) dell'art. 9, ovvero "*g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*;".
Pertanto, preventivamente all'implementazione di un siffatto sistema deve essere valutata la proporzionalità della finalità perseguita rispetto allo strumento utilizzato, prevedere adeguate e specifiche misure di sicurezza.
Ai sensi del Considerando 91 e dell'art. 35 del GDPR non sussistono dubbi in ordine al fatto che si renda necessario esperire una valutazione d'impatto e, nel caso in cui il rischio presenti indici elevati nonostante le misure implementate, la consultazione preventiva all'Autorità Garante. Nella fase di progettazione del sistema sicuramente assumono preminente rilievo le indicazioni contenute nel Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014 del Garante per la protezione dei dati personali e il Parere 3/2012- WP193 sugli sviluppi nelle tecnologie biometriche adottato il 27 aprile 2012 al Gruppo Artl 29 dei Garanti europei. In ordine alla cartellonistica, nel Provvedimento in materia di videosorveglianza dell'8 aprile 2010 il Garante aveva ribadito l'opportunità di installare appositi cartelli informativi per segnalare la presenza di sistemi di videosorveglianza. In allegato al provvedimento stesso erano proposti alcuni fac-simili.
Il titolare del trattamento è sempre l'Ente. La presenza di un fornitore esterno non sposta l'ago delle responsabilità. In ogni caso, il Comune deve procedere con la designazione del

fornitore a responsabile del trattamento, ivi fornendo compiti ed oneri, compresi quelli di stampo tecnologico.

Q18: Nel caso di un sito di progetto europeo, il cui dominio è intestato all'Ente, sviluppato da un partner, ma aggiornato da tutti i partner: chi è il titolare del trattamento dei dati? Ci sono contitolari?

Lepida (A18 V1) Dipende dalle modalità di gestione del sito. Qualora il sito contiene dei dati personali occorre capire come è stata regolamentata la gestione della redazione. Il gestore del sito, qualora sia il partner sviluppatore del medesimo, potrebbe configurarsi come responsabile di trattamento.
L'intestazione del dominio non è elemento dirimente la questione. Nel caso di un progetto europeo è certamente configurabile la contitolarità dei partner, anche se è tutt'altro che scontata. Dovrà essere sottoposta al DPO la fattispecie specifica.

Q19: L'Ente intende realizzare un filmato in occasione di un evento e una mostra fotografica (aperta al pubblico) che illustrano quanto si è fatto negli anni.
Come ci si deve comportare per le immagini delle persone (alcune deboli) che compariranno nel filmato e nella mostra fotografica?
Nel caso in cui l'Ente è in possesso di autorizzazione di parte delle persone interessate (o dei loro familiari) all'utilizzo di tali immagini per occasioni del genere, ma per tutti (ad esempio vecchie fotografie per cui non si ha nessuna autorizzazione), come ci si deve comportare?

Lepida (A18 V1) Pubblicare immagini di eventi istituzionali significa procedere alla pubblicazione di dati personali. Ciò deve essere previsto da norma di legge o di regolamento. L'uso di immagini su supporto fotografico o video al fine di comunicazione e diffusione è, quindi soggetto ad un duplice "regime normativo", quello relativo alla protezione del diritto d'autore e, come già indicato, quello inerente la normativa in materia di protezione dei dati personali.
Devono poi essere oggetto di considerazione ulteriori elementi, tra cui il

- Soggetto ripreso
- Il luogo in cui si svolge la manifestazione
- Lo scopo perseguito con la diffusione

Nel caso in cui sia accertata la sussistenza di una norma di legge o regolamento che legittima la pubblicazione, l'operatore dovrà considerare la seguente casistica:

Immagine di un luogo pubblico o di un avvenimento, in cui una o più persone siano riconoscibili.	Sono pubblicabili senza consenso e autorizzazione le immagini del luogo pubblico o dell'evento, nelle quali alcune persone possono essere incidentalmente riconoscibili.
Le immagini di persone comuni che si trovano in luogo pubblico o ad un evento, ma che sono isolati dal contesto.	Si tratta a tutti gli effetti di ritratti e sono pubblicabili solo con l'autorizzazione ed il consenso dei soggetti ripresi. E' ritratto quando il soggetto ripreso è portante nell'economia dell'immagine, tanto che la sua esclusione dalla foto significherebbe eliminare la foto.
Immagini di personaggi comuni ripresi in luogo pubblico o ad un evento, isolati dal contesto, ma il cui volto non sia riconoscibile	L'immagine è pubblicabile anche senza autorizzazione e consenso perché la persona non è riconoscibile.
Immagini di persone comuni pubblicate con finalità esclusivamente culturali e/o didattiche.	Pubblicabili senza autorizzazione e consenso.
Immagini di personaggi noti e che ricoprono determinati uffici pubblici che partecipano alle manifestazioni/eventi della Società	Sono pubblicabili senza autorizzazione e consenso.
Immagini di minori ripresi durante una manifestazione o evento istituzionale.	Non pubblicabile se non con l'autorizzazione e il consenso dei genitori.
Foto di minori sulle quali si sia provveduto a rendere non riconoscibile il volto	Pubblicabile senza autorizzazione e consenso

Immagini di persone comuni di cui sia pubblicato solo un particolare, ma il cui volto non sia riconoscibile.	L'immagine è pubblicabile purché il volto non sia riconoscibile.

Q19: Si chiede un chiarimento circa l'invito di Lepida agli Enti di precisare nelle informative che le richieste degli interessati per l'esercizio dei propri diritti debbano pervenire ad un apposito ufficio dell'Ente e non al DPO.

Lepida (A19 V1) La previsione di cui all'art. 38 del GDPR regala all'interessato un approccio diretto, immediato e funzionale alla propria istanza, riconoscendo nel DPO, in tema di protezione dei dati personali, primario riferimento per il cittadino. A tal fine, si rammenta che, ai fini del riscontro a tali istanze, la norma prevede tempistiche ristrette. La ricezione di istanze da parte di Lepida che svolge il Servizio di DPO per molti Enti non è misura organizzativa che consente di soddisfare le richieste dei cittadini nelle tempistiche imposte normativamente. Ciò perché il DPO non ha disponibilità delle banche dati (né deve averla) e, senza l'apporto della struttura che, per l'appunto, detiene i dati personali di cui all'istanza dell'interessato, non gli è certamente possibile esaudire le richieste dei cittadini. Peraltro, le stesse richieste giungono prive di tutti i riferimenti necessari ad identificare l'Ente destinatario della richiesta.
Pertanto, la corretta gestione delle suddette istanze impone l'implementazione di una misura differente: ovverosia il veicolamento delle istanze su canali propri dell'Ente che, senza indugio, interessa il DPO della questione posta.

Q20: Considerando l'obbligo di comunicare agli interessati nell'informativa l'eventuale trasferimento dei dati personali all'estero e che altresì si dovrebbe inserire nella designazione di responsabili esterni la precisazione che "L'Ente non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea", si chiede come si deve comportare nel caso di utilizzo di Google suite da parte dell'Ente.

Lepida (A20 V1) Occorre verificare il contratto stipulato con Google ed eventuali adeguamenti apportati dalla medesime alla luce del GDPR. Qualora i dati siano fuori dall'Unione Europea si tratta di un trasferimento all'estero.

Q21: L'Ente utilizza i servizi di Google LLC che ha il ruolo di responsabile del trattamento dei dati. Si chiede:

1) Se siano disponibili documentazioni riguardo il tema del trasferimento dei dati fuori dall'Unione Europea;
2) Nel caso di utilizzo degli strumenti di Google suite, da parte degli utenti dell'Ente, per la gestione di informazioni personali (es. inserimento nel calendario personale aziendale di impegni privati contenenti dati particolari), che tipo di documentazione e informative devono essere forniti agli utenti per chiarire il ruolo di Google e dell'Ente nel trattamento dei dati.
3) Nel caso in cui l'utente configuri sul proprio dispositivo mobile personale la propria utenza fornita dall'Ente quest'ultimo, in qualità di amministratore della Google Suite, è in grado di sapere quali applicazioni vengono installate e quindi risalire a informazioni che possono essere delicate. Come bisogna comportarsi?

Lepida (A21 V1)

1) Occorre verificare il contratto stipulato con Google ed eventuali adeguamenti apportati dalla medesime alla luce del GDPR.
   Si suggerisce di leggere:
   https://services.google.com/fh/files/misc/googlecloud_gdpr_whitepaper_english_618.pdf
   https://services.google.com/fh/files/misc/googlecloud_gpdr_1pager_618.pdf
   https://cloud.google.com/security/gdpr/
2) Gli strumenti IT dell'Ente devono essere utilizzati solo per scopi istituzionali e nel rispetto del disciplinare ICT dell'Ente
3) Gli strumenti messi a disposizione dell'Ente devono essere utilizzati attraverso i dispositivi forniti dall'Ente e solo per finalità istituzionali. Nel caso di Smart Working e BYOD occorre prevedere un regolamento apposito.
