AZIENDA SANITARIA PROVINCIALE

U.O. UFFICIO DEL D.P.O.
via G. di Vittorio n. 51
97100 Ragusa

Data Protection Officer
Dott.ssa Giovanna Di Stefano
Telefono:
0932 600.739
EMAIL:
dpo@asp.rg.it

Sig.ra Angela Consuelo Leontini
Telefono:
0932 600.788
EMAIL:
consueloangela.leontini@asp.rg.it

WEB
www.asp.rg.it

Al Direttore Generale

SEDE

OGGETTO: **Relazione Tecnica sugli adempimenti in carico all'A.S.P. di Ragusa relativi all'applicazione del Regolamento Europeo 2016/679 (GDPR): stato dell'arte e azioni da intraprendere.**

Premessa di carattere metodologico

La presente relazione è volta a rappresentare, in modo schematico e per quanto possibile sintetico, gli adempimenti posti a carico dell'Azienda per quanto in oggetto specificato.

Di seguito, si dà conto degli adempimenti realizzati e di quelli da implementare e/o intraprendere.

Ambiti di attività aziendali correlati ai nuovi obblighi europei

In base allo studio effettuato dalla scrivente, risultano al momento, **quattro tipologie di adempimenti** e quindi quattro macro- ambiti di attività aziendali ad essi correlati.

Il Regolamento europeo, infatti, detta obblighi di carattere:

- **strategico ed organizzativo**
- **giuridico-documentale**
- **tecnologico ed informatico**
- **comunicativo**

Obblighi di carattere strategico-organizzativo

Adempimento	Riferimento normativo	Area/Serv. competente
In capo al "Titolare del trattamento dei dati" è posto l'obbligo dia attuare politiche adeguate in materia di protezione dei dati, con l'adozione di **misure tecniche ed organizzative** che siano concretamente e sempre dimostrabili (principio dell'*accontability*) Formalmente il regolamento pone direttamente a carico del "Titolare" numerosi adempimenti tecnici, che in realtà dovranno essere tradotti e gestiti a livello aziendale dal Servizio Informatico (vedasi successivo punto….) Fra tutti, si segnalano:	Reg.UE artt. 24 e segg. Guida applicativa del Garante (pagg. n.24/29)	Il Titolare del trattamento dei dati è il Direttore Generale dell'Azienda
-adozione del *Registro delle attività di trattamento* elettronico e relativa implementazione;		
- adozione delle *Misure di sicurezza dei dati*		avvalendosi del Serv. Informatico
-Valutazione di impatto sulla privacy (VIP)		avvalendosi del Serv. Informatico
- obbligo di adottare misure tecniche ed organizzative adeguate per garantire i principi di **"privacy by design" e " privacy by default"** nell'intero ambito aziendale		avvalendosi del Serv. Informatico
Obbligo di stipulare i nuovi **"Patti di contitolarità"**	Reg.ue artt. 26 e segg. Guida applicativa Garante (pag. n.20)	avvalendosi del *Data Protection Officer*

Obbligo di notifica al Garante (per il tramite del *Data Protection Officer)* delle **violazioni dei dati personali** (c.d. **Data Breach)**	Reg. ue art. 33 Guida applicativa Garante (pagg n.24/29)	Direttore Generale avvalendosi del *Data Protection Officer*
Obbligo di documentare le violazioni dei dati personali (c.d. "*Registro delle violazioni privacy*")	Reg. ue art. 33 Guida applicativa Garante (pagg n.24/29)	Direttore Generale avvalendosi del *Data Protection Officer*
Obbligo di effettuare la **"Consultazione preventiva"**	Reg. ue art. 36 Guida applicativa Garante (pagg n.24/29)	Direttore Generale avvalendosi del *Data Protection Officer*
Obbligo di designare il **"Responsabile della Protezione dei dati"** c.d. "*Data Protection Officer*"	Reg. ue artt. 37-38 e 39 Guida applicativa Garante (pagg n.24/29	Direttore Generale
Obbligo di garantire la **formazione** sul nuovo Regolamento europeo a favore dei soggetti "designati /autorizzati" e quindi di tutti i dipendenti	Reg. ue artt. 39 e segg. Guida applicativa Garante (pag. 20 e segg.)	Direttore Generale avvalendosi del *Data Protection Officer* e dell'u.o.s. Formazione
Acquisizione **certificazione** ed adesione a **codici di condotta**	Reg. ue artt.40/43 Guida applicativa Garante (pagg. 20/23)	Direttore Generale avvalendosi del *Data Protection Officer*

Obblighi di carattere giuridico-documentale

Adempimento	Riferimento normativo	Area/Serv. competente
Predisposizione del nuovo modello aziendale di **Informativa** che ottemperi alle previsioni europee	Reg. ue artt.13 e 14 Guida applicativa Garante (pagg.8 e segg.)	Direttore Generale avvalendosi del *Data Protection Officer*
Predisposizione di *Informative stratificate e differenziate*	Reg. ue art.5, par.1, lett.a). e Provvedimento Garante n.55 del 7 marzo 2019	Direttore Generale avvalendosi del *Data Protection Officer*
Diritto di accesso: armonizzazione delle procedure e della modulistica in materia di *accesso civico*, di *accesso generalizzato* e di *accesso documentale* con i principi e le nuove prescrizioni di matrice europea	Reg.ue art.15 Guida applicativa Garante (pag.15)	Resp. della Trasparenza e della Prevenzione della Corruzione previa intesa con il *Data Protection Officer*
Nomina per l'intero ambito aziendale dei *Delegati al trattamento dei dati personali* in ottemperanza alle nuove previsioni europee: predisposizione modulistica e trasmissione delle nomine con le istruzioni operative disposizioni	Reg.ue artt.29 e D.lgs. n.101/2008 art. 2-*quaterdecies* Guida applicativa Garante (pagg.20 e segg.)	Direttore Generale avvalendosi del *Data Protection Officer*
Predisposizione della modulistica e delle linee procedurali per la nomina dei **Responsabili esterni del trattamento dei dati** in ottemperanza alle nuove previsioni	Reg.ue artt.28 e segg. Guida applicativa Garante (pagg.20 e segg.)	Direttore Generale avvalendosi del *Data Protection Officer* e con il supporto, per l'ambito di relativa competenza delle strutture aziendali: Serv. Tecnico, Serv. Provveditorato e Affari Generali

Adozione, con atto deliberativo, di un "**Regolamento aziendale privacy**" che dia evidenza complessiva della policy aziendale adottata in materia al fine di ottemperare alle nuove previsioni europee	Principi generali dell'ordinamento giuridico nella P.A. Linee generali di carattere organizzativo, riconducibili al "Titolare" che si desumono dal Regolamento UE (artt.24/43)	Direttore Generale avvalendosi del *Data Protection Officer*
Predisposizione di modulistica, linee guida, procedure, disposizioni operative, registri e policy necessari a rendere operative le indicazioni di legge e del "**Regolamento aziendale privacy**"	Linee generali di carattere organizzativo, riconducibili al "Titolare" che si desumono dal Regolamento UE (artt.24/43) Regolamento aziendale privacy art. 16	Direttore Generale avvalendosi del *Data Protection Officer*

Obblighi di carattere tecnologico ed informatico

Adempimento	Riferimento normativo	Area/Serv. competente
Misure tecnologiche per **adeguare i sistemi informativi ai nuovi principi europei** in materia di: - *profilazione automatizzata* *-pseudonimizzazione* *-diritto all'oblio* *-minimizzazione dei dati* *- limitazione del trattamento.*	Reg.ue (artt.12 e segg) Guida applicativa Garante (pagg. 12 e segg.)	Serv. Informatico
Misure tecnologiche per garantire la protezione dei dati sia nella progettazione che nella impostazione predefinita **(privacy by design e by default)**	Reg.ue (artt.25 e segg.) Guida applicativa Garante (pag. 24)	Serv. Informatico
Predisposizione **Registro** elettronico **delle attività di trattamento**	Reg.ue art. 30 Guida applicativa Garante (pagg. 26 e segg.)	Serv. Informatico consultandosi con il *Data Protection Officer*
Predisposizione delle **Misure di sicurezza informatica dei dati** con l'adozione di un **Documento Analisi e Valutazione Rischi (DAVR)**	Reg.ue artt. 32 e segg.) Guida applicativa Garante (pagg. 27 e segg.) Regolamento aziendale privacy ar.t31	Serv. Informatico con la collaborazione del *Data Protection Officer*
Valutazione d'Impatto Privacy (VIP) c.d. *"Data Protection Impact Assessment"*	Reg.ue artt. 35 e segg. Guida applicativa Garante (pagg. 25 e segg.)	Serv. Informatico consultandosi con il *Data Protection Officer*
Predisposizione del **"Registro delle violazioni dei dati personali"**	Reg.ue artt.30/33 Guida applicativa Garante (pagg.24/29)	Serv. Informatico consultandosi con il *Data Protection Officer*

Predisposizione delle **Misure tecniche ed informatiche** per garantire che (l'eventuale) **trasferimento in Paesi terzi fuori dall'U.E.** avvenga nel rispetto delle nuove norme europee	Reg.ue artt.44 e segg. Guida applicativa Garante (pagg.30 e segg.)	Serv. Informatico

Obblighi di carattere comunicativo

Adempimento	Riferimento normativo	Area/Serv. competente
Aggiornamento del sito web aziendale con l'inserimento della nuova documentazione e di tutta la modulistica necessaria ad ottemperare alle norme europee	Principi generali dell'ordinamento giuridico della P.A. Linee generali di carattere organizzativo, riconducibili al "Titolare" che si desumono dal Regolamento UE (artt.24/43)	Ufficio Comunicazione U.R.P. e Stampa consultandosi con il *Data Protection Officer*
Formazione al personale dipendente	Reg.ue art.39 Guida applicativa Garante (pagg.24/29)	U.O.S. Formazione
Nomina dei **"Responsabili del trattamento dei dati"**	Reg.ue art.28 e segg. Guida applicativa Garante (pagg. 24/29)	Strutture interessate alle nomine in virtù di **gare ed appalti, di servizi, forniture e convenzioni con enti esterni**

Il *Data Protection Officer*
Dr.ssa Giovanna Di Stefano