ALLEGATO 2

Sintesi degli adempimenti in carico ad ASUR in conseguenza della diretta applicazione, a far data dal 25 maggio 2018, del nuovo Regolamento Europeo sulla privacy.

In appresso si rappresentano in modo schematico gli adempimenti cui deve far fronte ASUR per effetto delle norme europee, distinguendo ambiti di intervento ed obblighi.

Ambiti di attività aziendali correlati ai nuovi obblighi europei in materia di privacy

Il Regolamento europeo, infatti, detta obblighi di carattere:

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

Di seguito si riporta il dettaglio specifico degli adempimenti per ciascuno dei ***macro-obblighi*** sopra menzionati:

A. Obblighi di carattere strategico ed organizzativo

Adempimento	*Riferimento normativo*	*Area o Servizio competente per l'adempimento*
In capo al "Titolare del trattamento dei dati" è posto l'obbligo di adottare **misure tecniche ed organizzative, anche certificate**, che siano concretamente e sempre **dimostrabili** (principio dell'*accountability*) Formalmente, il Regolamento UE pone direttamente a carico del "Titolare" numerosi adempimenti tecnici, che in realtà dovranno essere tradotti e gestiti a livello aziendale dai Servizi dell'Area Informativa; su tutti, si segnalano: *a)* L'adozione del *Registro delle tività di trattamento* *b)* L'adozione delle *Misure di sicurezza dei dati* *c)* La *Valutazione di impatto sulla privacy*	**Regolamento UE (art. 24 e seg.)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	Il Titolare del trattamento dei dati. Azienda Sanitaria Unica Regionale delle Marche Egli risponde civilmente e penalmente del mancato adeguamento, con onere a suo carico di provare che il danno non gli è imputabile (art. 82 e seguenti del Reg. UE)

Obbligo di adottare misure tecniche ed organizzative per garantire i nuovi principi di **"privacy by design"** e **"privacy by default"** nell'intero ambito aziendale *(Cioè in tutte le operazioni di trattamento dati, sia nella progettazione, che nella impostazione predefinita)*	**Regolamento UE (art. 25)** **Guida applicativa del Garante (pagina n. 24)** **Guida giuridica "Italia Oggi" (pagina n. 27 e seguenti)**	**Direttore Generale** *Avvalendosi dell'Area Servizi Informativi e del DPO*
Obbligo di stipulare i nuovi **"Patti di contitolarità"** (serve accordo contrattuale per c.d. "Joint Controller")	**Regolamento UE (art. 26 e seg.)** **Guida applicativa del Garante (pagina n. 20)** **Guida giuridica "Italia Oggi" (pagina n. 46 e seguenti)**	**Direttore Generale** avvalendosi del *Data Protection Officer*
Obbligo di notifica al Garante delle **violazioni dei dati personali** nei casi previsti dal Regolamento UE (c.d. **"Data Breach"**)	**Regolamento UE (art. 33)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 39 e seguenti)**	**Direzione Aziendale** avvalendosi del *Data Protection Officer*
Obbligo di documentare le violazioni dei dati personali (c.d. **"Registro delle violazioni privacy"**)	**Regolamento UE (art. 33)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 39 e seguenti)**	**Direzione Aziendale** avvalendosi del *Data Protection Officer*
Obbligo, in capo al Titolare (tramite il *Data Protection Officer*) di effettuare la **"Consultazione preventiva"**	**Regolamento UE (art.36)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	**Direzione Aziendale** avvalendosi del *Data Protection Officer*
Obbligo, in capo al Titolare, di designare il **"Responsabile della Protezione dei dati"**, c.d. *"Data Protection Officer"*	**Regolamento UE (art. 37, 38 e 39)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 20 / 22 – 63 / 67 e 116 / 135)**	**Direttore Generale**

Obbligo, in capo al Titolare, di garantire la **formazione** sul nuovo Regolamento UE a favore degli "autorizzati" al trattamento dei dati (quindi di tutti i dipendenti)	**Regolamento UE (art. 39 e seg.)** **Guida applicativa del Garante (pagine n. 20 e seguenti)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	Direzione Aziendale avvalendosi del *Data Protection Officer* e del *Servizio aziendale responsabile della formazione*
Acquisizione **certificazione** ed **adesione a codici di condotta**	**Regolamento UE (articoli 40 / 43)** **Guida applicativa del Garante (pagine n. 20 / 23)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	Direzione Aziendale avvalendosi del *Data Protection Officer*

B. Obblighi di carattere documentale

Adempimento	***Riferimento normativo***	***Area o Servizio competente per l'adempimento***
Predisposizione del nuovo modello aziendale di **Informativa**, che ottemperi alle previsioni europee *N.B. nella nuova Informativa vanno inseriti anche i "dati di contatto" del Data Protection Officer*	**Regolamento UE (art. 13 e 14)** **Guida applicativa del Garante (pagina n. 8 e seguenti)** **Guida giuridica "Italia Oggi" (pagina n. 55 e seguenti)**	***Data Protection Officer***
Predisposizione del nuovo modello aziendale di **consenso al trattamento dei dati**, che ottemperi alle previsioni europee	**Regolamento UE (art. 7 e seg.)** **Guida applicativa del Garante (pagine n. 4 / 7)** **Guida giuridica "Italia Oggi" (pagina n. 60 e seguenti)**	***Data Protection Officer***
In progress integrazione del regolamento con le appendici regolamentari contenenti tutta la normativa di settore concernente la Privacy. (Per sostituire il dossier Privacy) (ad esempio): ✓ *Dossier Sanitario Elettronico* ✓ *Fascicolo Sanitario Elettronico* ✓ *Regolamento aziendale sulla videosorveglianza* ✓ *Regolamento sull'utilizzo dei mezzi informatici e telematici dell'Azienda*	**Principi generali dell'ordinamento giuridico nella PA** **Linee generali, di carattere organizzativo, riconducibili al "Titolare", che si desumono dal Regolamento UE (art. 24 / 43)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	***Area Dipartimentale Affari Generali e Contenzioso avvalendosi delle Strutture aziendali competenti alla elaborazione dei documenti e regolamenti***

C. Obblighi di carattere tecnologico ed informatico

Adempimento	*Riferimento normativo*	*Area o Servizio competente per l'adempimento*
Misure tecnologiche per **adeguare i sistemi informatici ai nuovi principi europei** in materia di: ✓ *Profilazione automatizzata* ✓ *Pseudonomizzazione* ✓ *Diritto all'Oblio* ✓ *Minimizzazione dei dati* ✓ *Limitazione del trattamento*	**Regolamento UE (art. 12 e seg.)** **Guida applicativa del Garante (pagina n. 12 e seguenti)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	**Area Dipartimentale Servizi Informativi**
Misure tecnologiche per garantire il nuovo **diritto alla portabilità dei dati** (fra diversi *Service Provider*) **in formato interoperabile** *(queste misure si applicano esclusivamente ai trattamenti effettuati "con mezzi automatizzati")*	**Regolamento UE (art. 20, 22 e 23)** **Guida applicativa del Garante (pagine n. 18 e 19)** **Guida giuridica "Italia Oggi" (pagina n. 99 e seguenti)**	**Area Dipartimentale Servizi Informativi**
Misure tecnologiche per garantire la protezione dei dati sia nella progettazione, che nella impostazione predefinita **(privacy by design e by default)**	**Regolamento UE (art. 25 e seg.)** **Guida applicativa del Garante (pagina n. 24)** **Guida giuridica "Italia Oggi" (pagina n. 27 e seguenti)**	**Area Dipartimentale Servizi Informativi**
Predisposizione del Registro delle attività di trattamento	**Regolamento UE (art. 30)** **Guida applicativa del Garante (pagine n. 26 e seg.)** **Guida giuridica "Italia Oggi" (pagina n. 28 e seguenti**	**Data Protection Officer** **Con il supporto dell' Area Dipartimentale Servizi Informativi**
Predisposizione delle **Misure di sicurezza informatica dei dati** con la riedizione del ***Documento Programmatico della Sicurezza***	**Regolamento UE (art. 32 e seg.)** **Guida applicativa del Garante (pagina n. 27 e seg.)** **Guida giuridica "Italia Oggi" (pagina n. 31 e seguenti)**	**Area Dipartimentale Servizi Informativi unitamente al DPO per i profili di competenza**

Valutazione d'impatto sulla protezione dei dati c.d. *"Data Protection Impact Assessment"*	**Regolamento UE (art. 35 e seg.)** **Guida applicativa del Garante (pagina n. 25 e seg.)** **Guida giuridica "Italia Oggi" (pagina n. 36 e seguenti)**	**Area Dipartimentale Servizi Informativi unitamente al DPO per i profili di competenza**
Predisposizione del **"Registro delle violazioni nel trattamento dei dati personali"**	**Regolamento UE (art.30 / 33)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 39 e seguenti)**	**Area Dipartimentale Servizi Informativi consultandosi con il Data Protection Officer**
Predisposizione delle **Misure tecniche ed informatiche** per garantire che (l'eventuale) **trasferimento in Paesi Terzi fuori dell'Unione Europea dei dati personali** avvenga nel rispetto delle nuove norme europee	**Regolamento UE (art. 44 e seg.)** **Guida applicativa del Garante (pagine n. 30 e seg.)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	**Area Dipartimentale Servizi Informativi**

D. Obblighi di carattere comunicativo

Adempimento	*Riferimento normativo*	*Area o Servizio competente per l'adempimento*
Aggiornamento del sito web aziendale con l'inserimento della nuova documentazione e di tutta la nuova modulistica necessaria ad ottemperare alle norme europee	**Principi generali dell'ordinamento giuridico nella PA** **Linee generali, di carattere organizzativo, riconducibili al "Titolare", che si desumono dal Regolamento UE (art. 24 / 43)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	**Area Formazione e Comunicazione** *consultandosi con il Data Protection Officer*
Formazione a favore del personale dipendente, così da ottemperare alle previsioni europee	**Regolamento UE (art. 39)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	**Area Formazione e Comunicazione**
Nomina dei **Responsabili "esterni"** del trattamento dei dati	**Regolamento UE (art. 28 e seg.)** **Guida applicativa del Garante (pagine n. 24 / 29)** **Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)**	**Secondo quanto stabilito nel Regolamento aziendale organizzativo Privacy**

Inserimento di **clausole sulle misure di sicurezza nel trasferimento dei dati** all'interno del ***Disciplinare degli appalti pubblici***, che prevedono un flusso di dati da Pubblica Amministrazione a impresa aggiudicataria del servizio (e viceversa)	Regolamento UE (art. 28 / 32 e seg.) Guida applicativa del Garante (pagine n. 24 / 29) Guida giuridica "Italia Oggi" (pagina n. 34 in particolare)	**Secondo quanto stabilito nel Regolamento aziendale organizzativo Privacy**

Sanzioni previste dal Regolamento UE per la violazione degli obblighi indicati

N. progr.	*Adempimento*	*Entità sanzione*
1	Registro trattamenti	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
2	Documento valutazione dei rischi	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
3	Documento di valutazione di impatto privacy	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
4	Procedura Data Breach	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
5	Accordo con contitolari	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
6	Contratto di responsabile esterno	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
7	Contratto con sub-responsabili	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
8	Nomine dipendenti e collaboratori	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
9	Corsi per gli autorizzati *(dipendenti dell'azienda)*	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
10	Informativa	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
11	Raccolta consensi, salvo esonero	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
12	Nomina Data Protection Officer	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
13	Trasferimenti dati all'estero	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
14	Certificazione	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo