PIANO OPERATIVO PER APPLICAZIONE DI ALCUNI ADEMPIMENTI PREVISTI DAL REGOLAMENTO EUROPEO (UE) 2016/679 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

REV.	DATA	PREDISPOSIZIONE	APPROVAZIONE
00	30/6/2020	UOC Affari Generali _____	Direttore Amministrativo _____

NORMATIVA DI RIFERIMENTO

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).

Decreto legislativo 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 sulla protezione dei dati).

Linee guida metodologiche di Azienda Zero

PREMESSA

Con nota 16336 del 17 dicembre 2018 Azienda Zero trasmetteva alle aziende sanitarie ed ospedaliere della Regione del Veneto le seguenti "Linee Guida metodologie e documentali in materia di protezione dei dati personali" affinchè nel sistema sanitario regionale fossero posti in essere in maniera omogenea gli gli adempimenti previsti dalla normativa europea in materia di protezione di privacy.

A seguire pertanto ogni Azienda Sanitaria si è attivata per ridefinire:

1. *Revisione e monitoraggio dell'apparato giuridico e documentale*
2. *Implementazione del Registro elettronico delle attività di trattamento*
3. *Adozione della procedura "Garanzia esercizio dei diritti degli interessati sul trattamento del dato personale"*
4. *Adozione della procedura "Valutazione degli incidenti di sicurezza e gestione delle eventuali violazioni*
5. *Applicazione delle Linee guida "Gestione del Risk Assessment e del Data Protection Impact Assessment"*
6. *Applicazione delle Linee guida "Principio di Privacy by Design e Privacy by Default" (Data Breach)"*

In tutti i documenti inviati da Azienda Zero si stabilisce espressamente quanto segue:

" (...) Ogniqualvolta, a seguito di specifico riferimento normativo, sia indicato quale soggetto il "Titolare del trattamento" si faccia riferimento, per lo svolgimento dei diversi adempimenti, al soggetto e/o alla struttura aziendale individuata dal Titolare del trattamento ratione materiae ed in base all'organizzazione dettata dall'Atto Aziendale, così come riportato nella tabella di cui al paragrafo 5 "Ruoli e Responsabilità"; tabella che dovrà essere quindi completata, da ciascuna Azienda, tenendo conto del proprio, peculiare assetto organizzativo, nonché delle eventuali deliberazioni aziendali già assunte in materia di "privacy europea" per far fronte agli obblighi di cui al G.D.P.R. Ciò detto, al fine di applicare efficacemente le presenti procedure e linee guida, ciascuna Azienda, nel caso in cui non lo avesse già fatto, ***individuerà preliminarmente le strutture aziendali che dovranno concorrere all'attuazione degli adempimenti oggetto del presente documento****, in ragione della natura degli adempimenti medesimi (a titolo esemplificativo e non esaustivo: verranno distinti gli obblighi di carattere giuridico da quelli di carattere tecnologico ed informatico, piuttosto che da quelli afferenti all'area statistica, di internal auditing o di controllo di gestione, etc...) (....)"*

PIANO OPERATIVO AZIENDALE

Nella definizione del proprio sistema aziendale privacy l'AULSS 6 Euganea procedeva ad individuare il Referente Aziendale Privacy, nella figura del Direttore dell'UOC Affari Generali, istituiva l'Ufficio Privacy e assegnava alla medesima struttura le funzioni in materia di implementazione, gestione, adeguamento del sistema. Definiva inoltre un'Unità Funzionale Privacy ovvero un gruppo multidisciplinare trasversale aziendale composto da RPD, da un professionista dell'UOS Sistemi Informativi, da un professionista dell'UOC Direzione Medica e dal Responsabile URP con il compito di supportare l'UOC Affari Generali e il RPD nella definizione di valutazioni particolarmente complesse in materia di trattamento dei dati personali e per supportare il Referente Privacy nell'attuazione degli adempimenti previsti dalla nuova normativa europea.
Venivano identificati, secondo quanto previsto dalla norma, i Delegati del trattamento affidando tale incarico ai Direttori di Unità Operativa Complessa, di Unità Operativa Semplice a valenza Dipartimentale, di Unità Operativa Semplice in staff alle direzioni aziendali, OC /UOS / UOS di staff quali Delegati del trattamento ai quali sono state assegnate responsabilità e compiti in materia di trattamento dei dati personali tra i quali la nomina e la formazione degli autorizzati al trattamento.
Veniva nominato il Responsabile Protezione Dati collocato all'interno dell'UOC Affari Generali, con garantendo comunque ambiti di autonomia per l'espletamento delle sue funzioni e correlandolo funzionalmente all'Unità Privacy e all'attività dell'Ufficio Privacy.

Con il presente piano operativo l'Azienda, individuando le strutture aziendali che si occuperanno dell'attuazione degli adempimenti previsti dal dettato normativo e precisando ruoli e ambiti di competenza, potrà procedere a recepire ed adottare tutto l'apparato documentale nell'ambito del sistema aziendale privacy

Di seguito, ottemperando alle indicazioni di Azienda Zero e sulla base delle funzioni attribuite dall'Atto Aziendale alle diverse strutture dell'Azienda, si stabilisce il seguente affidamento delle competenze in materia di privacy e di protezione del dato, per ciascuno dei sei adempimenti sopra citati secondo le linee metodologiche indicate dall'Ente di Governance:

1) Revisione e monitoraggio della modulistica aziendale (adempimenti di carattere giuridico-legale e amministrativo)

Responsabilità diretta *(Titolarità)*	**Struttura aziendale competente per gli adempimenti** *(Preposto)*	**Altre strutture aziendali a supporto del preposto** *(Collaboratori)*	**Responsabile Protezione Dati** *(Supervisore)*
Titolare del trattamento (AULSS 6 Euganea)	UOC Affari Generali	Tutte le strutture aziendali coinvolte dal Preposto in ragione di diversi adempimenti di carattere giuridico e documentale	Soggetto nominato con delibera n. 177 del 28.2.2019

Compiti assegnati all' UOC Affari Generali

- ✓ Promuove, anche sulla base delle indicazioni di Azienda Zero, le azioni utili a garantire nell'ambito aziendale l'assolvimento dei molteplici obblighi previsti dalla legislazione vigente in materia, sia nazionale che europea;
- ✓ Fornisce supporto alle strutture dell'Azienda sugli aspetti di carattere giuridico relativi all'applicazione della privacy europea;
- ✓ Adegua l'apparato documentale aziendale alle indicazioni di Azienda Zero (vedasi le modulistiche di cui alla nota 17.12.2018 prot. 16336, nonché il materiale inviato con nota del 13.07.2018 prot. 9132), tenendo conto dei precetti di cui al GDPR e delle recenti novità di cui al D.lgs. 101 del 2018 recante misure nazionali di adeguamento al Regolamento Europeo;
- ✓ predispone e aggiornare il Regolamento aziendale privacy attuativo del GDPR, curando in ogni caso la comunicazione della nuova modulistica a tutte le strutture aziendali interessate, al fine di darne massima pubblicità e diffusione
- ✓ predispone gli atti deliberativi in materia d'intesa con la Direzione Strategica;
- ✓ cura la pubblicazione e gli aggiornamenti della relativa documentazione nella sezione dedicata alla *"Sistema Privacy Aziendale"* presente sul sito web aziendale e nella sezione dedicata presente nell'intranet aziendale.

2) Implementazione del Registro elettronico delle attività di trattamento

Responsabilità diretta *(Responsabile)*	**Struttura aziendale competente per gli adempimenti** *(Preposto)*	**Altre strutture aziendali a supporto del preposto** *(Collaboratori)*	**Responsabile Protezione Dati** *(Supervisore)*
Titolare del trattamento (AULSS 6 Euganea)	UOS Sistemi Informativi con la collaborazione dell'UOC Affari Generali (Ufficio Privacy)	Tutte le UU.OO.CC. e le UU.OO.SS.DD e le strutture di staff coinvolte in ragione di diversi adempimenti di carattere giuridico o informatico (delibera n. 583 del 4.7.2018)	Soggetto nominato con delibera n. 177 del 28.2.2019

Compiti assegnati all'UOS Sistemi Informativi e all'UOC Affari Generali

- ✓ L'UOS Sistemi Informativi provvede al censimento aziendale dei trattamenti dati personali (lato titolare / lato responsabile), per la definizione dei Registri delle attività di trattamento, sulla base di "schema tipo" fornito da Azienda Zero, coinvolgendo le strutture complesse aziendali (UOC / UOS / strutture di staff), avvalendosi della collaborazione dell'UOC Affari Generali;
- ✓ L'UOS Sistemi Informativi acquisisce un applicativo informatico per la gestione del registro e lo rende attivo con le funzionalità necessarie (collegamenti con ulteriori applicativi che lo collegano all'anagrafica aziendale e alla struttura organizzativa derivante dall'atto aziendale per mantenere gli aggiornamenti organizzativi aziendali)
- ✓ L'UOS Sistemi Informativi inserisce i trattamenti dati personali censiti nell'applicativo aziendale dedicato del quale assume la funzione di "Amministratore di Sistema", con la collaborazione dell'UOC Affari Generali che abilita alla medesima funzione;
- ✓ L'UOS Sistemi Informativi produce distinti documenti di evidenza (Registro attività di trattamento – Lato titolare / Registro attività di trattamento – Lato Responsabile), generati dall'applicativo aziendale, da esibire in occasione di verifica interna (a cura del Responsabile della Protezione dei dati - RPD) e/o di verifica esterna (a cura dell'Autorità Nazionale) come previsto dalla normativa vigente;
- ✓ L'UOS Sistemi Informativi, con la collaborazione dell'UOC Affari Generali, provvede all'aggiornamento annuale dell'applicativo e pertanto all'aggiornamento dei Registri sopraindicati ovvero qualora intervengano dei cambiamenti organizzativi di processo e/o l'acquisizione di nuovi software per l'implementazione di ulteriori attività che contemplino il trattamento di dati personali;
- ✓ L'UOS Sistemi Informativi, rimane a disposizione di Azienda Zero per fornire il contenuto dell'intero censimento ai fini di ottemperare agli sviluppi di carattere tecnologico ed organizzativo che riterrà di porre in essere nell'ambito della rete regionale di cui fanno parte tutte le aziende sanitarie ed ospedaliere del Veneto;
- ✓ L'UOC Affari Generali comunica alle strutture che hanno già predisposto il censimento delle attività di trattamento dati personali le modalità per effettuare l'aggiornamento annuale dei dati dei Registri posti in essere;
- ✓ Le strutture aziendali (UOC / UOS / Strutture di staff) producono i documenti e/o le comunicazioni per l'aggiornamento annuale dei dati secondo le indicazioni fornite dall'UOC Affari Generali
- ✓ L'UOS Sistemi Informativi con la collaborazione dell'UOC Affari Generali cura l'aggiornamento dei Registri mediante le funzioni di utilizzo dell'applicativo dedicato aziendale;
- ✓ L'UOS Sistemi Informativi garantisce la sicurezza informatica delle componenti utilizzate nella fruizione del software utilizzato per l'implementazione del Registro dei Trattamenti, dall'impiego di credenziali individuali e qualificate, alla tracciatura di tutte le attività svolte, alla sicurezza dei collegamenti tra pc e servizio in cloud, alla corretta policy di backup e restore da adottarsi;
- ✓ L'UOS Sistemi Informativi cura la compilazione dei Registri per le informazioni relative agli asset informatici coinvolti e alle misure di sicurezza relative alla parte IT applicate nei trattamenti individuati ed elencati nei registri stessi.

3) Procedura per esercizio dei diritti degli interessati sul trattamento dato personale

Responsabilità diretta *(Responsabile)*	**Struttura aziendale competente per gli adempimenti** *(Preposto)*	**Altre strutture aziendali a supporto del preposto** *(Collaboratori)*	**Responsabile Protezione Dati** *(Supervisore)*
Titolare del trattamento (AULSS 6 Euganea)	Delegato al trattamento (UOC – UOS – UOS in staff, cui si riferisce l'istanza del cittadino) con il supporto della UOC Affari Generali	Tutte le strutture aziendali coinvolte, volta per volta, in base all'istanza del cittadino	Soggetto nominato con delibera n. 177 del 28.2.2019

Compiti assegnati all' UOC Affari Generali:

✓ predispone la procedura aziendale "Garanzia dei diritti degli interessati", secondo quanto indicato nelle Linee Guida metodologiche licenziate da Azienda Zero; cura la distribuzione del documento a tutte le strutture aziendali per la gestione delle istanze degli interessati; revisiona il documento ad ogni aggiornamento normativo;

✓ pubblica sul sito internet aziendale, nella sezione "Sistema Privacy Aziendale" la modulistica prevista dalla procedura per la presentazione dell'istanza di esercizio dei diritti;

✓ fornisce il necessario supporto di carattere giuridico e normativo alla struttura aziendale (UOC – UOS – UOS in staff) che prende in carico l'istanza presentata dall'interessato. L'UOC Affari Generali si avvale della consulenza dell'RPD per la valutazione di eventuali violazioni sul trattamento del dato personale da notificare all'Autorità;

✓ gestisce l'archivio delle istanze relative alla procedura aziendale.

Si allega procedura operativa correlata (**allegato 1)**

4) Procedura per la valutazione degli incidenti di sicurezza e gestione delle eventuali violazioni (Data Breach)

Responsabilità diretta *(Responsabile)*	**Struttura aziendale competente per gli adempimenti** *(Preposto)*	**Altre strutture aziendali a supporto del preposto** *(Collaboratori)*	**Responsabile Protezione Dati** *(Supervisore)*
Titolare del trattamento (AULSS 6 Euganea)	**Delegato al trattamento dati** (*struttura ove si è verificato il così detto "incidente di sicurezza") avvia Istruttoria sull'incidente di sicurezza e valutazione di 1° istanza con supporto UOC Affari Generali* ↓ ***Unità Funzionale Privacy*** *Valutazione di 2° istanza e relaziona al Titolare del Trattamento* ↓ ***Direttore Generale*** *Decisione finale per la notifica al Garante*	Tutte le aree aziendali coinvolte volta per volta in base al processo in esame	Soggetto nominato con delibera n. 177 del 28.2.2019

<u>Compiti assegnati all' UOS Sistemi Informativi e all'UOC Affari Generali</u>:

- ✓ predispongono di concerto la procedura aziendale "Valutazione degli incidenti di sicurezza e di violazione sui dati personali", secondo quanto indicato nelle Linee Guida metodologiche licenziate da Azienda Zero;
- ✓ L'UOC Affari Generali cura la distribuzione del documento a tutte le strutture aziendali per la rilevazione della violazione del dato interna e/o esterna da parte degli interessati; revisiona il documento ad ogni aggiornamento normativo;
- ✓ l'UOC Affari Generali fornisce il necessario supporto di carattere giuridico e normativo alla struttura aziendale (UOC – UOS – UOS in staff) che rileva l'incidente di sicurezza e la violazione sui dati personali unitamente all'Unità Funzionale Privacy aziendale.

Compiti assegnati al Delegato del trattamento dei dati della struttura interessata:

✓ attenendosi alla procedura aziendale rileva la segnalazione relativa all'incidente di sicurezza e a avvia l'istruttoria di 1° istanza per la valutazione di violazione di dati personali chiedendo la collaborazione dell'UOC Affari Generali e il supporto dell'Unità Funzionale Privacy;

✓ L'Unità Funzionale Privacy, che opererà quale organismo di 2° istanza, in posizione di indipendenza e terzietà di giudizio, potrà confermare la conclusione del Valutatore di 1° istanza, oppure formulare una conclusione diversa da quella del Valutatore di 2° istanza.

✓ L'Unità Funzionale Privacy darà quindi comunicazione, sull'esito della propria valutazione, sia al Delegato che al Direttore Generale.

✓ Nel solo caso in cui la segnalazione sull'insorgenza dell'incidente di sicurezza provenga dall'esterno dell'azienda (ad esempio da una istanza o da un reclamo di un cittadino) il Delegato del trattamento dei dati, qualunque sia l'esito della valutazione sull'incidente di sicurezza, concorderà con l'Unità Funzionale Privacy e con la Direzione Generale il tenore della risposta da fornire al cittadino / utente autore della segnalazione sul presunto data breach;

✓ Nel solo caso in cui la valutazione finale dell'Unità Funzionale Privacy "sancisca la conclusione di cui alla lettera "c" dell'art. 33 del GDPR (c'è stata violazione dei dati che presenta un effettivo e comprovato rischio per i diritti e le libertà delle persone fisiche), il Titolare del trattamento dei dati (Direzione Generale) provvederà alla notifica al Garante e agli interessati (nei casi di cui all'art. 34 del GDPR), secondo le modalità previste dalla procedura;

✓ Le risultanze istruttorie di ogni incidente sono, in ogni caso, inserite nel "Registro delle violazioni sui trattamenti dei dati personali" aziendale;

Si allega procedura operativa **(allegato 2)**

5) Linee Guida per la gestione del Risk Assessment e del Data Protection Impact Assessment (DPIA)

Responsabilità diretta *(Responsabile)*	**Struttura aziendale competente per gli adempimenti** *(Preposto)*	**Altre strutture aziendali a supporto del preposto** *(Collaboratori)*	**Responsabile Protezione Dati** *(Supervisore)*
Titolare del trattamento (AULSS 6 Euganea)	UOS Sistemi Informativi con supporto UOC Affari Generali	Tutte le strutture aziendali coinvolte chiamate a concorrere all'adempimento di cui si tratta	Soggetto nominato con delibera n. 177 del 28.2.2019

Compiti assegnati a UOS Sistemi Informativi con la collaborazione dell'UOC Affari Generali:

✓ gestisce l'adempimento di cui si tratta sulla base delle indicazioni contenute nelle Linee Guida metodologiche licenziate da Azienda Zero, utilizzando a tale scopo l'apposita funzionalità dell'applicazione utilizzata per la gestione del Registro delle attività dei trattamenti;

✓ Adotta le scelte tecnologiche, statistiche ed informatiche opportune a realizzare questo adempimento;

✓ predispone apposita procedura aziendale relativa al Data Protection Impact Assessment ("PIA) per ogni nuovo trattamento automatizzato avvalendosi della consulenza dell'RPD.

Si allegano linee guida **(allegato 3)**

6) Linee guida per l'applicazione del principio di Privacy by Design e Privacy by Default

Responsabilità diretta *(Responsabile)*	**Struttura aziendale competente per gli adempimenti** *(Preposto)*	**Altre strutture aziendali a supporto del preposto** *(Collaboratori)*	**Responsabile Protezione Dati** *(Supervisore)*
Titolare del trattamento (AULSS 6 Euganea)	UOS Sistemi Informativi con supporto Unità Funzionale Privacy	I Delegati del trattamento dati coinvolti volta per volta in base al processo in esame	Soggetto nominato con delibera n. 177 del 28.2.2019

<u>Compiti assegnati alla UOS Sistemi Informativi con il supporto dell'Unità Funzionale Privacy</u>

✓ gestisce, tenendo conto dei principi esposti nelle Linee Guida metodologiche di Azienda Zero, l'adempimento di cui si tratta anche fornendo le apposite indicazioni tecniche e tecnologiche a tutte le Ditte esterne che attivano collaborazioni e nuovi processi per la gestione di hardware e software, anche utilizzando a tale scopo l'apposita funzionalità dell'applicazione per la gestione del Registro delle attività dei trattamenti

✓ Adottare, secondo un piano strategico di medio-lungo termine, le scelte tecnologiche e informatiche necessarie per realizzare questo adempimento;

✓ Proporre, se ritenuto necessario, un regolamento aziendale che disciplini in modo più dettagliato e specifico la procedure aziendali volte a realizzare concretamente l'adempimento

Si allegano linee guida **(allegato 4)**

Tempi di realizzazione del piano sopraindicato

Si riporta il diagramma di Gant per la pianificazione delle attività descritte dal piano operativo:

DIAGRAMMA DI GANT PIANO OPERATIVO SISTEMA ADEGUAMENTO PRIVACY AZIENDALE

Piano operativo adeguamento sistema privacy aziendale	**anno 2019**	**1° trimestre 2020**	**2° trimestre 2020**	**3° trimestre 2020**	**4° trimestre 2020**
revisione e monitoraggio apparato giuridico e documentale					
mappatura della modulistica aziendale esistente		covid-19	covid-19		
avvio adeguamento della modulistica con incontri info-formativi strutture aziendali		covid-19	covid-19		
avvio stesura del Regolamento privacy aziendale con collaborazione dell'Unità Funzionale Privacy		covid-19	covid-19		
registro attività di trattamento		covid-19	covid-19		
acquisizione e messa in opera dell'applicativo con allineamento alle banche dati aziendali		covid-19	covid-19		
popolamento del registro con trattamenti dichiarati al 28.5.2018		covid-19	covid-19		
aggiornamento del registro agli attuali trattamenti con incontri info-formativi programmati con UOC/UOSD/UOS di staff		covid-19	covid-19		
adozione e pubblicazione **procedura per esercizio diritti interessato sui trattamenti dati personali**					
adozione e pubblicazione **procedura per violazioni Data Breach**					
recepimento e messa in atto delle **procedura per gestione del Risk Assessment e del Data Protection Impact Assessment (DPIA)**					
recepimento e messa in atto delle **linee guida per l'applicazione dei principio della Privacy by design e by default**					

Verifica della messa in opera degli adeguamenti del piano sopraindicato

Si rinvia ad un piano di audit annuale a cura dell'RPD aziendale per la verifica della messa in opera degli adeguamenti descritti e pianificati nel Piano Operativo descritto a seguito del quale sarà realizzata relazione annuale al Titolare del trattamento.