Sistema Socio Sanitario
Ospedale Maggiore
Regione Lombardia
ASST Crema

STRUTTURA: SC AFFARI GENERALI E LEGALI

Dirigente Responsabile: Nolli Elena

Responsabile del procedimento: Nolli Elena

Responsabile dell'istruttoria: Nolli Elena

DELIBERAZIONE N. 1044 DEL 30/12/2025

OGGETTO: APPROVAZIONE DEL REGOLAMENTO SUL MODELLO ORGANIZZATIVO PRIVACY (MOP) DELL'ASST DI CREMA.

IL DIRETTORE GENERALE - ALESSANDRO COMINELLI

ASSISTITO DA:

IL DIRETTORE AMMINISTRATIVO: GIUSEPPE FERRARI

IL DIRETTORE SANITARIO: ALESSANDRO MALINGHER

IL DIRETTORE SOCIOSANITARIO: CAROLINA MAFFEZZONI

Firmato digitalmente ai sensi della normativa vigente da: Direttore Generale, Direttore Amministrativo, Direttore Sanitario, Direttore Sociosanitario

IL DIRETTORE GENERALE

Richiamate:

La LR 30/12/2009 n. 33 "Testo unico delle leggi regionali in materia di sanità";

La DGR n. X/4496 del 10/12/2015 con la quale è stata disposta la costituzione dell'Azienda Socio-Sanitaria Territoriale (ASST) di Crema;

La DGR n. XII/1626 del 21/12/2023 di nomina del dott. Alessandro Cominelli quale Direttore Generale della ASST di Crema;

Rilevato che il Responsabile del procedimento riferisce quanto segue:

RICHIAMATI:

- il decreto legislativo 30.06.2003 n.196 "Codice in materia di protezione dei dati personali";
- il Regolamento Europeo 2016/679(GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati;
- il decreto legislativo 10.08.2018 n.101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR";

DATO ATTO che con deliberazione n. 520/2019 è stato adottato il Regolamento aziendale per l'attuazione del Regolamento UE n.679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali dell'ASST di Crema;

DATO ATTO altresì che con deliberazione n.782 del 29/12/2021 è stata approvata la procedura operativa per la gestione della violazione dei dati personali – data breach;

RICHIAMATA la deliberazione aziendale n.748 del 19/10/2023 con la quale è stato affidato il servizio di DPO e le attività finalizzate alla compliance alla normativa europea sulla protezione dei dati personali alla società LTA S.r.l. nella persona del dott. Luigi Recupero;

RILEVATA, anche in esito a interlocuzioni con il DPO aziendale, la necessità di adeguare l'assetto organizzativo interno dell'ASST di Crema finalizzato ad una migliore gestione della privacy e del trattamento dei dati personali, oltre che ad allineare le previsioni ed i compiti dei soggetti coinvolti nell'attuazione del GDPR ai contenuti della normativa comunitaria;

RITENUTO, pertanto, opportuno procedere all'approvazione del Regolamento sul Modello Organizzativo Privacy (MOP) in sostituzione del precedente regolamento aziendale in materia, come da documento allegato quale parte integrante e sostanziale al presente provvedimento;

RITENUTO altresì di disporre la più ampia diffusione del Regolamento sul Modello Organizzativo Privacy (MOP), mediante pubblicazione sul sito internet aziendale, nonché attraverso ogni altra idonea modalità di conoscenza formativa e informativa;

DATO ATTO che il presente provvedimento viene adottato su proposta di Nolli Elena, Direttore della SC AFFARI GENERALI E LEGALI, quale Responsabile del procedimento che in tale veste ne attesta la regolarità tecnica e la legittimità;

DATO ATTO che il presente provvedimento non comporta oneri a carico del bilancio aziendale;

ACQUISITO il parere del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio-Sanitario, per quanto di competenza, così come previsto dall'art. 3 del Decreto Legislativo 30/12/1992, n. 502 e successive modificazioni;

DELIBERA

per le motivazioni di cui in premessa che qui si intendono integralmente trascritte:

1) di approvare il modello organizzativo privacy così come definito nel "Regolamento sul Modello Organizzativo in materia di Protezione dei dati personali (MOP) dell'Azienda Socio Sanitaria Territoriale di Crema" allegato al presente provvedimento quale parte integrante e sostanziale;
2) di stabilire l'entrata in vigore della regolamentazione allegata a decorrere dalla data di adozione del presente provvedimento deliberativo e la revoca, dalla stessa data, della disciplina aziendale prevista nella medesima materia;
3) di disporre la più ampia diffusione del Regolamento sul Modello Organizzativo Privacy (MOP), così come indicato in premessa;
4) di dare atto che dal presente provvedimento non derivano oneri a carico dell'ASST di Crema;
5) di trasmettere al Collegio Sindacale il presente provvedimento ai sensi dell'art. 3 ter D.Lgs. n. 502/1992 e s.m.i. e art. 12, comma 14, L.R. n. 33/2009 come modificata dalla L.R. n. 23/2015 e s.m.i.;
6) di dare atto che il presente provvedimento è immediatamente esecutivo, in quanto non soggetto a controllo della Giunta Regionale, ai sensi dell'art. 17, comma 6, della L.R. n. 33/2009 e s.m.i. e verrà pubblicato all'Albo pretorio on line sul sito istituzionale dell'Azienda ai sensi dell'art. 32 della Legge n. 69/2009.

IL DIRETTORE GENERALE

ATTESTAZIONE DI REGOLARITA' TECNICA

Il Responsabile del Procedimento attesta la regolarità tecnica e la legittimità della proposta sopra riportata

Data, 24/12/2025

Il Direttore di SC AFFARI GENERALI E LEGALI

Nolli Elena

(firma elettronica apposta ai sensi del D.Lgs. n. 82/2005 e s.m.i.)

REGOLAMENTO SUL MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (MOP) DELL'AZIENDA SOCIO SANITARIA TERRITORIALE DI CREMA

SOMMARIO

CAPO I – DISPOSIZIONI GENERALI

Art. 1 - Oggetto

Il presente Regolamento sul Modello Organizzativo in materia di Protezione dati personali (MOP) disciplina l'assetto di *governance* e le disposizioni procedimentali per l'adeguamento della Azienda Socio Sanitaria Territoriale di CREMA (di seguito, per brevità, anche solo "ASST CREMA") al Regolamento Generale Protezione Dati UE del 27 aprile 2016 n. 679 (RGPD[1]) ed al D. Lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali" o "Codice Privacy") e successive modifiche ed integrazioni.

Art. 2 - Definizioni

Ai fini del presente Regolamento[2] si intende per:

RGPD/GDPR: Regolamento Generale Protezione Dati Personali e la loro libera circolazione UE/679/2016 o General Data Protection Regulation (GDPR);

Codice privacy: "*Codice in materia di protezione dei dati personali*", D. Lgs. n. 196 del 30 giugno 2003 e successive modifiche ed integrazioni;

Titolare del trattamento o Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

RPD/DPO: Responsabile Protezione Dati personali o Data Protection Officer;

Responsabile al trattamento dei dati personali: la persona fisica espressamente designata che opera sotto l'autorità dell'Ente (che agisce in qualità di Titolare o di Responsabile esterno del trattamento) nell'ambito del proprio assetto organizzativo con specifici compiti e funzioni;

Responsabile esterno del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

Interessato: la persona fisica a cui si riferiscono i dati personali;

Incaricato/Autorizzato: il soggetto (persona fisica) che effettua materialmente le operazioni di trattamento sui dati personali;

[1] Come presente sul sito del Garante Privacy.
[2] Si tengono in considerazione le definizioni di cui all'art. 4 del GDPR.

Violazione dei dati personali (*Data Breach*): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Garante Privacy: l'autorità di controllo pubblica istituita dallo Stato Italiano; nello specifico, l'Autorità Garante per la Protezione dei Dati Personali.

Art. 3 - Presupposti di liceità del trattamento

1. Ai sensi di quanto previsto dal Regolamento europeo 679/2016 ogni trattamento deve trovare fondamento in un'idonea base giuridica.
2. I trattamenti di dati personali sono effettuati da ASST CREMA sulla base dei presupposti di liceità indicati nel Regolamento europeo agli articoli 6 (rubricato "Liceità del trattamento") e 9 (rubricato "Trattamento di categorie particolari di dati personali") e che di volta in volta devono essere utilizzati al fine di rendere tali trattamenti legittimi.

CAPO II – MODELLO ORGANIZZATIVO

Art. 4 - Titolare del trattamento

1. ASST CREMA, rappresentata, ai fini previsti dal GDPR, dal Direttore Generale, è il Titolare del trattamento dei dati personali (d'ora in poi anche solo "Titolare") raccolti anche in banche dati, digitali o cartacee.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR:
   - liceità, correttezza e trasparenza;
   - limitazione della finalità e minimizzazione dei dati;
   - esattezza;
   - limitazione della conservazione;
   - integrità e riservatezza.
3. Il Titolare mette in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare che il trattamento di dati personali è effettuato in modo conforme al GDPR. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati, per agevolare l'esercizio dei diritti dell'Interessato stabiliti dagli articoli 15-22 del GDPR e tutte le comunicazioni e informazioni occorrenti per il loro esercizio.
4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio mediante analisi della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
5. Il Titolare provvede a:

a) nominare il Data Protection Officer (d'ora in poi anche solo "DPO");

b) nominare i Responsabili interni al trattamento dei dati nelle persone dei Dirigenti apicali delle singole Strutture in cui si articola l'organizzazione dell'Ente, quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati personali effettuati dall'Ente e preposti al trattamento dei dati contenuti nelle banche dati di competenza delle

articolazioni organizzative cui sono preposti;

c) assegnare distinti compiti a specifiche Strutture, in ragione delle peculiari competenze alle medesime attribuite dal POAS, al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento dell'Ente al GDPR;

d) definire gli indirizzi per l'attribuzione di specifiche competenze all'Ufficio di supporto al Data Protection Officer (d'ora in poi anche "Ufficio Privacy"), anche con riguardo alla funzione di raccordo e di collaborazione con il Garante per la Protezione dei Dati Personali (d'ora in poi anche solo "Garante Privacy"), al fine di supportare l'attività del DPO nel rapporto con le Strutture organizzative dell'Ente e fornire a queste ultime le necessarie indicazioni in materia di protezione dati sui trattamenti sviluppati dalle stesse.

6. Il Titolare è Contitolare del trattamento, ai sensi dell'art. 26 del GDPR, nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata a ASST CREMA da enti ed organismi statali o regionali, allorché due o più Titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.
7. ASST CREMA favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto sia qualora agisca in qualità di Titolare del trattamento che di Responsabile esterno del trattamento.

Art. 5 - Data Protection Officer (DPO)

1. Il Data Protection Officer è scelto tra il personale dipendente di ASST CREMA ovvero è individuato nella figura unica di un professionista o di una società nel rispetto delle prescrizioni recate dal Codice degli appalti in materia di contratti di servizio. In entrambi i casi, il soggetto deve possedere i requisiti specificati dagli artt. 37 e 38 del GDPR.
2. Il DPO è incaricato dei seguenti compiti:

a) informare e fornire consulenza all'ASST (in qualità di Titolare o di Responsabile esterno del trattamento), nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati personali;

b) fungere da supporto alle Strutture competenti sulle richieste di accesso per tutti gli aspetti relativi alla protezione dei dati personali ai sensi del GDPR;

c) fornire, se richiesto, un parere in merito alla Valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;

d) rendere una consulenza idonea, scritta od orale, anche nell'individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati; cooperare con il Garante Privacy e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione inerente al trattamento di dati personali;

e) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati personali, ferme restando le responsabilità dell'Ente (in qualità di Titolare o di Responsabile

esterno del trattamento). Fanno parte di questi compiti: la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti dell'Ente (in qualità di Titolare o di Responsabile esterno del trattamento);

f) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dall'Ente (in qualità di Titolare o di Responsabile esterno del trattamento);

g) altri compiti e funzioni a condizione che l'Ente (in qualità di Titolare o di Responsabile esterno del trattamento) si assicuri che non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

3. La figura del DPO è incompatibile con chi determina le finalità o i mezzi del trattamento e con il ruolo di fornitore dell'Ente, tranne nel caso in cui l'attività di fornitura sia da considerarsi quale ausilio e supporto allo svolgimento delle attività in capo al DPO medesimo. In particolare, risultano incompatibili con la figura del DPO i seguenti ruoli:

- il Responsabile per la Prevenzione della Corruzione e per la Trasparenza;
- il Responsabile esterno del Trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

4. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. ASST CREMA (in qualità di Titolare o di Responsabile esterno del trattamento) fornisce al DPO le risorse necessarie per assolvere ai compiti attribuiti e per accedere ai dati personali ed ai trattamenti posti in essere.

In particolare, al DPO sono assicurati:

- il supporto attivo per lo svolgimento dei compiti da parte dei Responsabili di cui all'art. 6 del presente Regolamento e degli altri organi di natura amministrativa e politica, anche considerando l'attuazione delle attività necessarie per la protezione dei dati nell'ambito della programmazione operativa e di bilancio;
- la collaborazione continua da parte dell'Ufficio Privacy aziendale;
- l'accesso alle articolazioni funzionali dell'Ente per fornire il supporto, le informazioni e gli *input* essenziali.

5. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti e non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione riguardante la normativa sulla protezione dei dati personali. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente all'Ente (in qualità di Titolare o di Responsabile esterno del trattamento). Nel caso in cui siano rilevate dal DPO o siano sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, questo è tenuto a manifestare le proprie osservazioni e i propri rilievi comunicandoli all'Ente (in qualità di Titolare o di Responsabile esterno del trattamento).

Art. 6 – Responsabili al trattamento dei dati

1. Il Titolare nomina i Dirigenti apicali delle Strutture in cui si articola l'organizzazione dell'Ente quali Responsabili al trattamento dei dati personali relativamente ai trattamenti effettuati dall'articolazione organizzativa di competenza. Ciascun Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.
2. Il Titolare, nell'atto di nomina, indica gli specifici ambiti di attività o l'elenco dei trattamenti di dati personali cui i singoli Responsabili sono preposti.
3. Ai Responsabili sono attribuiti i seguenti compiti:
   a) verificare la legittimità dei trattamenti di dati personali effettuati dalla Struttura di riferimento;
   b) disporre l'attuazione dei provvedimenti emessi dal Garante Privacy;
   c) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
   d) individuare i soggetti Incaricati al trattamento per la Struttura organizzativa di competenza e attribuire loro specifici compiti e attività di protezione dei dati;
   e) individuare ed incaricare i Referenti Protezione Dati di cui all'art. 7 del presente Regolamento per la propria Struttura organizzativa;
   f) individuare il personale della propria articolazione organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
   g) adottare soluzioni di privacy "*by design* e *by default*", ovvero di protezione dei dati fin dalla progettazione e per impostazione predefinita, prevedendo, già dall'origine e in considerazione del contesto complessivo ove il trattamento si colloca e dei rischi stimati, un paradigma di trattamento e misure di protezione prefissate;
   h) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e aggiornare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura organizzativa;
   i) individuare i Responsabili esterni del trattamento ex art. 28 del GDPR e proporre la nomina al Titolare, con il supporto dell'Ufficio Privacy, nonché conservare/aggiornare i Registri delle attività di trattamento dei dati personali previsti dall'art. 30 del GDPR;
   j) programmare, ove ritenuto opportuno ed in accordo con il DPO, un calendario di audit da svolgere con i Responsabili esterni del trattamento nominati ai sensi dell'art. 28 del GDPR. I Responsabili esterni verranno individuati tramite meccanismi di rotazione ovvero a campione;
   k) adottare, se necessario, specifici disciplinari tecnici di settore, anche congiuntamente con altri Responsabili e/o Responsabili esterni del trattamento, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla specifica area di competenza;

l) fornire riscontro alle richieste dell'Interessato per i trattamenti di dati di competenza della propria Struttura organizzativa;
m) rilevare e comunicare i casi di violazione dei dati personali (*Data Breach*) nell'ambito organizzativo di riferimento.

4. Per i trattamenti dei dati personali che coinvolgono più Strutture in modo trasversale, laddove applicabile vige il criterio della prevalenza, secondo il quale la Struttura che ha competenza principale nel trattamento dei dati personali coordina le attività delle altre Strutture coinvolte.

Art. 7 - Referenti Protezione Dati

1. Il Referente Protezione Dati è nominato dal Dirigente apicale di Struttura (quale Responsabile al trattamento dati ai sensi dell'art. 6 del presente Regolamento) ed è incaricato della generale attività di supporto al Responsabile nello svolgimento e nello sviluppo dei compiti di responsabilità al medesimo attribuiti dal Titolare. Nel compimento delle proprie attività il Referente è funzionalmente coordinato dall'Ufficio Privacy.
2. I compiti di supporto affidati al Referente riguardano:
a) l'individuazione dei rapporti intercorrenti con soggetti terzi in materia di trattamento e protezione dei dati personali;
b) l'analisi della progettazione delle misure di trattamento dei dati da predisporre preventivamente all'avvio di nuove attività/progetti/servizi;
c) la comunicazione delle modifiche intervenute nei trattamenti di competenza della propria Struttura organizzativa;
d) la gestione delle richieste dell'Interessato per i dati personali trattati dalla Struttura organizzativa preposta, con il supporto dell'Ufficio Privacy;
e) la proposizione/revisione dell'informativa all'Interessato;
f) l'aggiornamento e l'adeguamento dei contenuti della modulistica di competenza della propria Struttura organizzativa alla normativa in materia di protezione dati personali;
g) la formalizzazione e l'aggiornamento degli incarichi agli Incaricati al trattamento e la verifica e il supporto alla loro attività;
h) gli adempimenti correlati con la rilevazione dei casi di violazione dei dati personali (*Data Breach*).

Art. 8 - Responsabile esterno del trattamento

1. Il Responsabile esterno del trattamento è il soggetto, pubblico o privato, che tratta dati personali, anche particolari, per conto del Titolare, e che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei dati dell'Interessato. Tale soggetto assume il ruolo di Responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR. Ai sensi dell'art. 6 del presente Regolamento, la formalizzazione di detto ruolo avviene mediante atto giuridico redatto in forma scritta da parte del Titolare, su proposta dei Responsabili interni del trattamento dei dati per gli ambiti gestionali di propria competenza.
2. I rapporti tra il Titolare ed i Responsabili esterni sono disciplinati dagli atti di cui al comma 1 del presente articolo, i quali specificano la finalità perseguita, la tipologia dei dati, la categoria degli Interessati, la durata del trattamento, gli obblighi e i diritti del Responsabile esterno del trattamento

e le modalità di trattamento. Tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante Privacy oppure dalla Commissione Europea.
3. Il Responsabile esterno del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa ed ai compiti affidatigli dal Titolare.
4. Qualora l'Ente proceda alla nomina di Responsabili esterni dovrà prevedere, in sede di contratto di servizio, che questi ultimi sviluppino il Registro dei trattamenti coordinandosi con ASST CREMA.

Art. 9 – Incaricati/Autorizzati al trattamento

1. I Responsabili di cui all'art. 6, individuano, nell'ambito della propria responsabilità e con il supporto dei Referenti Protezione Dati di rispettiva assegnazione, gli Incaricati/Autorizzati al trattamento quali persone ammesse a compiere operazioni sui dati personali.
2. Nell'atto di individuazione, i Responsabili indicano, per ciascun Incaricato/Autorizzato, gli ambiti di attività e/o l'elenco dei trattamenti di dati personali di competenza.

Art. 10 - Ufficio Data Protection Officer (Ufficio Privacy)

1. L'Ufficio aziendale di supporto al Data Protection Officer ha il compito di supportare il DPO nel rapporto con tutte le Strutture organizzative in materia di adeguamento al GDPR. L'Ufficio Privacy collabora con il DPO nella definizione della proposta di Modello Organizzativo in materia di Protezione dati personali (MOP); si relaziona con le Strutture organizzative dell'Ente fornendo linee operative per l'implementazione del medesimo modello prevedendo anche una gestione digitalizzata dei procedimenti, dei processi e delle attività dell'Ente per la corretta e tempestiva applicazione del GDPR.
2. All'Ufficio Privacy compete l'individuazione di modalità e procedure operative volte alla:
   a) trasmissione dei pareri richiesti dalle Strutture organizzative dell'Ente al DPO;
   b) individuazione, contrattualizzazione e nomina dei Responsabili esterni del trattamento da parte del Titolare secondo le modalità di cui all'art. 8;
   c) adozione di soluzioni di privacy *by design e by default*;
   d) gestione e conservazione del Registro delle attività di trattamento (in qualità di Titolare del trattamento);
   e) gestione dell'analisi del rischio e Valutazione di impatto (DPIA);
   f) gestione degli episodi di violazione di dati personali (*Data Breach*);
   g) coordinamento funzionale dei Referenti Protezione Dati;
   h) rilevazione del personale individuato dai Responsabili al trattamento, nell'ambito delle Strutture organizzative dirette, da sottoporre ad attività formativa in materia di protezione dei dati;
   i) ricezione e risposta alle richieste degli Interessati inviate direttamente all'Ufficio Privacy;
   j) presentazione dell'informativa all'Interessato;
   k) comunicazione delle modifiche intervenute nei trattamenti di competenza della propria Struttura organizzativa.

CAPO III – SICUREZZA E PROTEZIONE DEI DATI

Art. 11 - Sicurezza del trattamento

1. Il Titolare del trattamento e tutti i soggetti aventi i ruoli descritti al Capo II del presente Regolamento mettono in atto, per i distinti profili di responsabilità e di azione, misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre, i sistemi di autenticazione, autorizzazione, rilevazione di intrusione, sorveglianza; di protezione (antivirus; firewall; antintrusione); sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
2. La conformità del trattamento dei dati al GDPR è dimostrata attraverso l'adozione delle misure di sicurezza adeguate oppure con l'adesione a codici di condotta approvati ovvero a meccanismi di certificazione approvati.
3. ASST CREMA, attraverso i ruoli individuati nel presente Regolamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbiano accesso a dati personali.
4. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati particolari (ex sensibili) per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi adottati ai sensi del D. Lgs. 196/2003 nella versione antecedente alle modifiche apportate dal D. Lgs. 101/2018.

Art. 12 - Registro del Titolare del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente in qualità di Titolare reca almeno le seguenti informazioni, come previsto dall'art. 30, par. 1, del GDPR:
   a) il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento e del Data Protection Officer (DPO);
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un Paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è conservato dall'Ufficio Privacy per conto del Titolare del trattamento.

Art. 13 - Registro del Responsabile esterno del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente in qualità di Responsabile esterno del trattamento contiene almeno le seguenti informazioni, come previsto dall'art. 30, par. 2, del GDPR:
   a) il nome e i dati di contatto del Responsabile esterno o dei Responsabili esterni del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile

esterno del trattamento, del Rappresentante del Titolare del trattamento o del Responsabile esterno del trattamento e del DPO;
b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
c) l'eventuale trasferimento di dati personali verso un paese terzo od un'organizzazione internazionale;
d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

2. Il Registro è conservato dal Responsabile al trattamento ai sensi dell'art. 6 del presente Regolamento ed inviato periodicamente in copia all'Ufficio Privacy.

Art. 14 - Valutazione d'impatto sulla protezione dei dati (DPIA)

1. Il Titolare, prima di effettuare il trattamento, deve attuare una Valutazione d'impatto (DPIA) quando il trattamento medesimo, considerati la natura, l'oggetto, il contesto e le finalità dello stesso, nonché l'eventuale utilizzo di nuove tecnologie, presenta un rischio elevato per i diritti e le libertà delle persone fisiche.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione, come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35 del GDPR.
3. La DPIA non è necessaria nei casi seguenti:
a) se il trattamento non presenta un rischio elevato per i diritti e le libertà delle persone fisiche;
b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso, si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subìto modifiche;
d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta;
e) se i trattamenti sono già stati oggetto di verifica preliminare da parte del Garante Privacy o del DPO e che proseguono con le stesse modalità oggetto di tale verifica.

Art. 15 - Violazione dei dati personali (*Data Breach*)

1. La violazione dei dati personali (*Data Breach*) è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente.
2. L'Ente deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.
3. Il Titolare del trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante Privacy a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle

persone fisiche. La notifica della violazione viene effettuata tramite utilizzo del form dell'apposita piattaforma raggiungibile dal sito dell'Autorità Garante. Se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve darne comunicazione a tutti gli Interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto. Il Titolare del trattamento, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali secondo le modalità individuate dall'Ufficio Privacy. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.
4. Il Responsabile esterno del trattamento che viene a conoscenza di un'eventuale violazione è tenuto a informare tempestivamente il Titolare in modo che quest'ultimo possa attivarsi secondo quanto disposto dalla normativa.
5. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.
6. Per quanto non espressamente previsto si rimanda alla procedura operativa aziendale per la gestione della violazione dei dati personali – data breach.

Art. 16 - Diritti degli interessati

1. L'interessato, cioè la persona fisica a cui si riferiscono i dati personali trattati da ASST CREMA, è la figura posta al centro del GDPR con riferimento soprattutto ai diritti ed alle libertà fondamentali.
2. ASST CREMA, dopo aver adottato tutte le misure appropriate per fornire all'interessato le informazioni cui agli artt. 13 e 14 GDPR e le comunicazioni di cui agli artt. 15-22 GDPR e all'art. 34 GDPR, deve agevolare l'esercizio dei diritti di cui al Capo III del GDPR da parte dell'interessato.
3. Il Titolare del trattamento, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta dell'interessato, deve fornire allo stesso adeguato riscontro. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. In ogni caso, il Titolare del trattamento deve informare l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato.
4. Il Responsabile esterno del trattamento che riceve una richiesta di esercizio dei diritti da parte di un interessato è tenuto a informare tempestivamente il Titolare in modo che quest'ultimo possa attivarsi secondo quanto disposto dalla normativa.
5. Il Titolare del trattamento documenta tutte le richieste e i riscontri forniti agli interessati in modo tale da dimostrare la corretta gestione delle pratiche nel rispetto della normativa (in particolare nel rispetto del principio di *accountability* stabilito dal GDPR).

CAPO IV – ORGANIZZAZIONE INTERNA

Art. 17 - Struttura competente in materia di ICT

1. La Struttura competente in materia di ICT è la Struttura che in ambito di protezione dati fornisce il contributo nella valutazione degli aspetti tecnologici relativamente all'impatto di questi sulle attività di trattamento di dati personali, fatte salve le eventuali specifiche competenze attribuite alla medesima Struttura dal Titolare.

2. La Struttura, in particolare, svolge i seguenti compiti:
   a) realizzazione di una apposita base di dati contenente le caratteristiche dell'infrastruttura tecnologica *hardware* e *software* utilizzata dall'Ente per le attività di trattamento di dati, secondo modalità sviluppate di comune accordo con l'Ufficio Privacy;
   b) sviluppo degli aspetti tecnologici inerenti l'analisi del rischio (ai sensi dell'art. 32 GDPR) e della Valutazione di impatto (ai sensi dell'art. 35 GDPR) attraverso criteri e modelli concordati con l'Ufficio Privacy;
   c) supporto alle Strutture organizzative nel caso di istanze degli Interessati che richiedano valutazioni di natura tecnologica relative agli strumenti di trattamento dati utilizzati dal Titolare;
   d) predisposizione della procedura interna di segnalazione *Data Breach,* secondo modalità sviluppate di comune accordo con l'Ufficio Privacy nel caso di una violazione che abbia avuto ad oggetto sistemi tecnologici del Titolare del Trattamento o dei Responsabili esterni del Trattamento nel rispetto di quanto previsto all'art. 15 del presente Regolamento.

Art. 18 - Rinvio

1. Per tutto quanto non espressamente disciplinato, si applicano le disposizioni del GDPR e tutte le norme vigenti in materia.