

Sistema Socio Sanitario



Regione  
Lombardia

ASST Ovest Milanese

# **REGOLAMENTO AZIENDALE IN MATERIA DI PRIVACY**

**Aggiornamento 2018**

## **Indice**

### **1. DEFINIZIONI PRINCIPALI**

---

**pag. 3**

#### **1.1 CATEGORIE DI DATI**

- 1.1.1 Dato personale*
- 1.1.2 Dati relativi alla salute*
- 1.1.3 Dati genetici*
- 1.1.4 Dati biometrici*
- 1.1.5 Trattamento*

#### **1.2 RUOLI E FIGURE**

- 1.2.1 Titolare del trattamento*
- 1.2.2 Soggetti autorizzati al trattamento*
- 1.2.3 Responsabile del trattamento (esterno)*
- 1.2.4 Responsabile del trattamento (interno)*
- 1.2.5 Amministratore di Sistema*
- 1.2.6 Responsabile Protezione Dati – RPD (Data Protection Officer – DPO)*
- 1.2.7 Gruppo di lavoro aziendale in materia di privacy*
- 1.2.8 Gruppo di valutazione delle violazioni*

### **2. INFORMAZIONI E TRASPARENZA**

---

**pag. 6**

#### **2.1 INFORMATIVA**

#### **2.2 DIRITTI DELL'INTERESSATO**

### **3. REGISTRO DEI TRATTAMENTI**

---

**pag. 6**

### **4. SICUREZZA DEI DATI PERSONALI**

---

**pag. 7**

#### **4.1 MISURE ORGANIZZATIVE**

- 4.1.1 Esattezza dei dati*
- 4.1.2 Scanner*
- 4.1.3 Archivi cartacei*
- 4.1.4 Spedizione di documenti a mezzo posta*
- 4.1.5 Utilizzo del fax*
- 4.1.6 Sportelli*
- 4.1.7 Luoghi di cura*
- 4.1.8 Colloqui*
- 4.1.9 Telefoni*
- 4.1.10 Consegna referti*
- 4.1.11 Comunicazione a terzi*

#### **4.2 VIOLAZIONE DEI DATI – DATA BREACH**

### **5. VIDEOSORVEGLIANZA**

---

**pag. 10**

### **ALLEGATI**

---

**pag. 11**

- Allegato 1 – autorizzazione dipendenti*
- Allegato 2 – autorizzazione studenti e volontari*
- Allegato 3 – autorizzazione operatori centro antiviolenza*
- Allegato 4 – nomina Responsabile (esterno)*
- Allegato 5 – nomina Responsabile (esterno) e Amministratore di sistema*
- Allegato 6 – nomina Responsabile (interno)*
- Allegato 7 – nomina Amministratore di sistema*
- Allegato 8 – nomina Amministratore di sistema - referente*

## **1. DEFINIZIONI PRINCIPALI**

### **1.1 CATEGORIE DI DATI**

**1.1.1 "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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

**1.1.2 "Dati relativi alla salute"** – dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

**1.1.3 "Dati genetici"** – dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

**1.1.4 "Dati biometrici"** – dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

**1.1.5 "Trattamento"** – qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

### **1.2 RUOLI E FIGURE**

**1.2.1 "Titolare del trattamento"** – 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 (Reg UE 2017/679 art. 4).

Pertanto Titolare del trattamento di tutti i dati personali è l'ASST Ovest Milanese, nella persona del Rappresentante Legale (Direttore Generale).

**1.2.2 "Soggetti autorizzati al trattamento"** – sono le persone fisiche autorizzate e designate in forma scritta a compiere le operazioni di trattamento dal Titolare e/o dal Responsabile. Pur non essendo prevista in modo specifico la figura dell'"incaricato", nel Regolamento UE 2016/679, si parla comunque di "persone autorizzate" al trattamento dei dati.

I soggetti autorizzati al trattamento dei dati all'interno dell'ASST Ovest Milanese sono tutti i dipendenti che quotidianamente gestiscono i dati, sia su supporto cartaceo che su supporto informatico (medici, infermieri, tecnici, ausiliari, amministrativi etc).

Sono altresì autorizzati al trattamento i soggetti (studenti, tirocinanti, volontari ecc.) che, pur essendo esterni ai ruoli aziendali, sono integrati nel contesto organizzativo per le attività loro affidate e accedono ai dati personali di cui l'Azienda è titolare.

Gli autorizzati ricevono un atto di autorizzazione al trattamento con le istruzioni necessarie (allegati 1,2,3) per lo svolgimento della propria attività: in tali istruzioni si concretizza la "diretta autorità" del Titolare e del Responsabile, sui cui grava, pertanto, l'obbligo di vigilare l'operato degli autorizzati stessi.

Per i dipendenti autorizzati, la nomina è consultabile e scaricabile, tramite login con le credenziali personali, nell'applicativo "Data Protection Manager", disponibile nel portale aziendale, previa comunicazione via mail.

**1.2.3 "Responsabile del trattamento" (esterno)** – viene definito dal Reg. UE 2016/679 come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (Reg UE 2017/679 art. 4 c. 1 punto 8).

Il ruolo e la funzione del Responsabile sono definite all'art. 28 del Reg UE 2016/679. Tale disciplina si rivolge a tutti coloro che effettuano operazioni di trattamento sulle banche dati e/o applicativi aziendali per conto e nell'interesse dell'Azienda per finalità connesse all'esercizio delle funzioni istituzionali, sulla base di accordi giuridici. Sono soggetti esterni specificatamente designati con un atto di nomina (allegato 4) correlato all'accordo/contratto/convenzione.

Gli uffici che gestiscono i rapporti con soggetti nominati "Responsabili esterni" ne tengono un elenco aggiornato a disposizione del Responsabile della Protezione dei Dati e del Titolare.

La nomina può contenere l'incarico di Amministratore di Sistema (allegato 5) di cui al provvedimento del Garante del 27 novembre 2008, aggiornato al 25 giugno 2009.

Il soggetto Responsabile del trattamento dovrà individuare all'interno della sua organizzazione chi ha le competenze per svolgere la funzione di Amministratore di sistema (v. punto 1.2.5 del presente Regolamento).

Il Responsabile del trattamento può ricorrere ad un sub responsabile nelle modalità indicate dall'art. 28 c. 2 del Regolamento UE.

**1.2.4 "Responsabile del trattamento" (interno)** – Tenuto conto della complessità e della eterogeneità organizzativa dell'ASST è opportuno che alcune funzioni del Titolare siano distribuite a coloro che vengono individuati Responsabili interni, scelti tra le figure dirigenziali, di seguito indicate:

- i Direttori di Unità Operativa complessa (UOC) dell'area clinica, amministrativa e tecnica;
- i Responsabili di Unità Operativa Semplice Dipartimentale (UOSD) dell'area clinica, amministrativa e tecnica;
- i Responsabili di Unità Operativa Semplice di Staff (UOS di Staff);
- i Responsabili di specifiche funzioni assegnate agli staff della Direzione strategica;
- il Responsabile del Centro di Fisiologia Sportiva

La designazione di Responsabile interno è legata al conferimento dell'incarico di responsabilità della struttura o funzione e comporta lo svolgimento di attività di supporto al Titolare nel controllo, nella supervisione e nell'attuazione delle istruzioni e delle policy aziendali.

Al Responsabile (cd. interno) vengono delegate (allegato 6) anche le funzioni di nomina per autorizzare al trattamento (allegato 2) i soggetti esterni all'organizzazione (studenti, tirocinanti, volontari ecc.) che accedono ai dati personali di cui l'ASST è Titolare.

Inoltre i Responsabili interni possono integrare le istruzioni già date dal Titolare laddove necessario.

La nomina a Responsabile del trattamento è consultabile e scaricabile, tramite login con le credenziali personali, nell'applicativo "Data Protection Manager", disponibile nel portale aziendale, previa comunicazione.

Il Responsabile interno informa il Titolare e il DPO nel caso in cui si renda necessario un nuovo trattamento di dati, così da poter effettuare la Valutazione d'impatto (art. 35 del Reg. UE 2016/679) prima di procedere al trattamento. Il Responsabile interno è coinvolto nel procedimento di valutazione del data breach, secondo le modalità indicate nel Regolamento aziendale relativo alla violazione dei dati – data breach (Del. 201 del 31/05/2018).

### **1.2.5 "Amministratore di Sistema"**

La figura dell'Amministratore di sistema è prevista nel provvedimento del Garante del 27 novembre 2008 il quale segnala ai titolari dei trattamenti dei dati, effettuati con strumenti elettronici, la particolare criticità del ruolo degli amministratori di sistema, richiamando l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di "amministratore di sistema", "amministratori di base di dati" o "amministratore di rete", laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso anche fortuito a dati personali.

Nell'ASST Ovest Milanese sono Incaricati (allegato 7) della funzione di Amministratore di sistema gli operatori dei Sistemi Informativi Aziendali con funzioni tecniche, ad esclusione del personale amministrativo.

Il Titolare può nominare (allegato 8) un referente del SIA "Amministratore di sistema" per tutte le attività che attengono ai sistemi informatici e delegarlo all'individuazione di ogni specifico ambito di competenza di ciascun operatore SIA, che agisce nella funzione di Amministratore di Sistema.

Il Titolare può delegare lo stesso referente alla verifica e al controllo dell'operato degli Amministratori di Sistema, tenendone l'elenco aggiornato.

### **1.2.6 "Responsabile Protezione Dati" – RPD (Data Protection Officer – DPO)**

In ASST Ovest Milanese il Responsabile della Protezione dei Dati è nominato con Delibera del Direttore Generale ed il nominativo è comunicato al Garante per la Protezione dei Dati Personali, mediante la piattaforma in uso.

Le sue funzioni, previste dagli artt. 37-38-39 del Reg UE 2016/679, riguardano principalmente l'informazione e la consulenza al Titolare del trattamento, ai Responsabili del trattamento, nonché ai dipendenti che eseguono il trattamento oltre alla sorveglianza sull'osservanza del Regolamento UE (e delle altre disposizioni normative), comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

Il DPO cura la stesura e l'aggiornamento dei modelli e della documentazione relativa all'ambito "privacy" nei processi aziendali, in collaborazione con i componenti del Gruppo di lavoro privacy e/o con i Responsabili interni del trattamento interessati.

### **1.2.7 "Gruppo di lavoro aziendale in materia di privacy"**

Il gruppo di lavoro è composto dalle figure aziendali che rappresentano le funzioni trasversali necessarie agli adempimenti normativi privacy ed è costituito con Deliberazione del Direttore Generale.

### **1.2.8 "Gruppo di valutazione delle violazioni"**

Il gruppo di valutazione è sempre composto dal Titolare (che può delegare anche uno dei Direttori della Direzione strategica), dal DPO, da un rappresentante del SIA, dal Responsabile della Sicurezza delle Informazioni e opera in caso di segnalazione di un possibile Data Breach, di cui al punto 4.2 del presente Regolamento.

Di volta in volta vi partecipa anche il Responsabile del trattamento ex art 28 (Reg. UE 2016/679) e/o il Responsabile (interno) delegato dal Titolare che ha rilevato o segnalato la violazione dei dati. Il gruppo è integrato dalla presenza del Responsabile della comunicazione in caso si debba attivare la procedura di cui all'art. 34 del Regolamento UE 2016/679 (comunicazione della violazione dei dati personali all'interessato).

## **2. INFORMAZIONI E TRASPARENZA**

### **2.1 INFORMATIVA**

L'ASST Ovest Milanese fornisce agli interessati tutte le informazioni di cui agli articoli 13 e 14 del Regolamento UE 2016/679 tramite modelli, codificati dalla UOC Qualità e Accreditamento, in forma concisa e trasparente, con un linguaggio semplice e chiaro, redatti seguendo le indicazioni delle norme di cui sopra.

Le informative, declinate in forma generale e in forma più specifica per alcune attività, sono pubblicate nella sezione "privacy" del sito istituzionale, nell'intranet aziendale e nei punti di informazione dell'ASST. Quelle di carattere generale sono anche affisse nei punti di maggior frequentazione dell'utenza.

### **2.2 DIRITTI DELL'INTERESSATO**

L'interessato può esercitare il diritto di accesso, di rettifica, di limitazione del trattamento, di opposizione al trattamento, di revoca del consenso, nonché della cancellazione e della portabilità del dato, laddove è possibile, valutata la natura del documento che contiene i dati. Per l'esercizio di tali diritti l'utente può utilizzare l'apposito modulo scaricabile dal sito o reperibile presso l'Ufficio Relazioni col Pubblico (URP). Sono responsabili del procedimento i Responsabili del trattamento interni individuati nell'ambito di questo provvedimento, supportati, qualora necessario, dall'ufficio privacy.

L'interessato può proporre reclamo all'Autorità del Garante.

## **3. REGISTRO DEI TRATTAMENTI**

Il Titolare tiene il Registro delle attività di trattamento, di cui all'articolo 30 del Regolamento UE 2016/679.

Il Registro è compilato e aggiornato in collaborazione con i membri del Gruppo di lavoro aziendale, coordinato dal Responsabile della Protezione dei Dati.

Per ogni attività di trattamento, il Registro contiene una serie di informazioni, tra cui:

- a) il nome e i dati di contatto del Titolare del trattamento e del Responsabile della Protezione dei Dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e) una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il Registro è gestito con l'aiuto del software "Data Protection Manager" che rielabora le informazioni introdotte anche per produrre la DPIA (Valutazione d'Impatto sulla Protezione dei Dati – art 35 Reg UE 2016/679), nonché le lettere di nomina dei Responsabili interni e dei dipendenti autorizzati al trattamento di tutta l'Azienda.

Tutti i soggetti autorizzati al trattamento, prendono visione delle proprie nomine e deleghe e delle informazioni contenute nel Registro, accedendo con login all'applicativo, dal portale aziendale.

## **4. SICUREZZA DEI DATI PERSONALI**

### **4.1 MISURE ORGANIZZATIVE**

Partendo dal presupposto che i dati possono essere utilizzati solo da coloro che sono stati espressamente autorizzati al trattamento, vengono elencate una serie di misure organizzative a cui devono attenersi tutti gli operatori.

Le indicazioni seguenti non riguardano il tema della sicurezza informatica, le cui policy sono previste da altro regolamento aziendale, ma sono istruzioni e indicazioni sui comportamenti corretti da tenere, per lo svolgimento delle attività amministrative e cliniche al fine di contenere il rischio di episodi di violazioni alla riservatezza.

#### **4.1.1 Esattezza dati**

Occorre prestare la massima attenzione alla digitazione ed alla scrittura manuale di dati identificativi, facendo il possibile per evitare errori di battitura o di scrittura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo.

#### **4.1.2 Scanner**

Gli autorizzati che utilizzano lo scanner devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile al fine di evitare confusione di dati.

Nel caso di apparecchi condivisi fra diversi uffici, occorre prestare attenzione affinché il documento digitalizzato venga inviato alla cartella gestita da autorizzati al trattamento.

In caso di errore di selezione del destinatario è necessario chiedere al collega l'immediata cancellazione del documento inviato.

#### **4.1.3 Archivi cartacei**

In ASST sono presenti numerosi archivi cartacei.

I documenti o gli atti che contengono dati personali devono essere contenuti in armadi, schedari e contenitori ad accesso controllato, muniti di serratura o riposti in locali con porta dotata di serratura.

Le copie delle chiavi devono essere in numero minimo, per garantire l'accesso solo agli autorizzati al trattamento.

Le chiavi devono essere custodite con diligenza e non in prossimità dell'armadio o del locale.

Inoltre le persone autorizzate:

- contribuiscono a garantire e perfezionare le misure di accesso ai locali e le misure di sicurezza contro il rischio di intrusione (il primo livello di protezione di qualunque sistema è quello fisico: una porta e/o un contenitore chiuso può in molti casi non costituire una protezione sufficiente, ma pone, se non altro, un primo ostacolo e richiede comunque uno sforzo volontario non banale per la sua rimozione);
- accedono ai dati che siano strettamente necessari all'esercizio delle proprie funzioni e competenze;
- custodiscono gli atti e i documenti durante il trattamento e li restituiscono o li ricollocano nel posto dal quale li avevano prelevati, al termine delle operazioni;
- prestano attenzione a non lasciare pratiche e fascicoli in gestione incustoditi sulla scrivania, soprattutto se contenenti dati personali;
- nell'ipotesi di stampante usata da più persone, prestano attenzione a non lasciare incustodite le stampe contenenti dati personali;

È necessario, prima di gettare la documentazione nel cestino della carta, provvedere a renderne non comprensibile il contenuto, anche utilizzando apparati distruggi documenti o altri più banali accorgimenti come ad esempio lo strappo dei documenti, la separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli, etc.

#### **4.1.4 Spedizione di documenti a mezzo posta**

La documentazione contenente dati personali movimentata con posta interna deve essere trasferita in busta chiusa, in modo da assicurare la protezione della riservatezza sia del documento che dei dati contenuti.

Per dare garanzia della non apertura della busta e della integrità del contenuto sarebbe opportuno che i lembi della busta fossero siglati.

#### **4.1.5 Utilizzo del fax**

Il Fax è un mezzo obsoleto di trasmissione di dati e documenti, perché non è garantita la consegna direttamente al destinatario dei documenti che vengono inviati.

Nei casi in cui non sia possibile trasmettere i dati con altri strumenti (applicativi, mail, pec, raccomandata, busta chiusa a mano) è consentito l'utilizzo del fax, nel rispetto di alcune misure di sicurezza:

- in calce ai fax trasmessi dall'ASST Ovest Milanese, sia all'interno che all'esterno, deve essere posta la seguente dicitura:

*Il contenuto del presente fax ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con divieto di diffusione.*

*Se il fax e i suoi allegati sono stati ricevuti per errore da persona diversa dal destinatario siete pregati di distruggere tutto quanto ricevuto e di informare il mittente ai numeri telefonici indicati.*

- prima di inviare un fax, l'operatore inviante deve avvisare della spedizione e quindi accertarsi che il destinatario sia nella condizione di poter ritirare rapidamente il documento stampato;

- l'apparecchio che riceve il documento deve essere allocato in un locale non aperto al pubblico, al quale possono accedere solo gli autorizzati al trattamento dei dati trasmessi;

- le comunicazioni ricevute via fax non devono essere lasciate incustodite e visibili a terzi ed immediatamente prese in carico dall'autorizzato

#### **4.1.6 Sportelli**

Per garantire la riservatezza dei colloqui, presso gli sportelli o gli ambulatori devono essere previsti appositi spazi, segnalati con una riga gialla oltre i quali gli utenti possano attendere il proprio turno.

I nomi dei pazienti in attesa di una prestazione o di documentazione (ad esempio delle analisi cliniche) non devono essere divulgati ad alta voce. Si suggerisce l'attribuzione un codice alfanumerico al momento della prenotazione o accettazione.

#### **4.1.7 Luoghi di cura**

Nei reparti dove si possono visitare i degenti solo attraverso vetrature devono essere adottati accorgimenti, anche provvisori (ad esempio mediante paraventi), che delimitino la visibilità dell'interessato durante l'orario di visita ai soli familiari e conoscenti.



Il personale sanitario deve evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dall'organizzazione dello spazio dei locali o dalle modalità utilizzate.

Non devono essere affisse liste di pazienti ricoverati o in attesa di prestazione in locali aperti al pubblico, con o senza la descrizione della patologia sofferta.

Non devono essere resi visibili ad estranei documenti sulle condizioni cliniche del malato (ad esempio lasciando le cartelle cliniche vicino al letto di degenza).

#### **4.1.8 Colloqui**

È doveroso adottare idonee cautele in relazione allo svolgimento di colloqui (ad esempio in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

Gli operatori ricevono cittadini e utenti, rimanendo sempre presenti nel proprio ufficio o luogo di lavoro, avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi, ad esempio rivoltando le cartelle o evitando di riportare sul frontespizio delle stesse, dati ed informazioni che permettano a terzi estranei di percepire l'identità dei soggetti interessati dal trattamento.

#### **4.1.9 Telefoni**

È assolutamente necessario non fornire per mezzo telefono dati ed informazioni di carattere sanitario o di natura comunque riservata qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione ad ottenere i dati richiesti del soggetto chiamante.

Si consiglia, qualora si nutrano dubbi sull'identità di chi è dall'altra parte dell'apparecchio, di richiedere il nome e qualità dell'interlocutore al fine di richiamarlo successivamente dopo aver ottenuto certezze sulla identità.

#### **4.1.10 Consegna referti**

I referti diagnostici, le cartelle cliniche, i risultati delle analisi e i certificati rilasciati dagli organismi sanitari possono essere consegnati in busta chiusa anche a persone diverse dai diretti interessati purché munite di delega scritta.

#### **4.1.11 Comunicazioni a terzi**

Le informazioni ai familiari e conoscenti possono essere fornite solo su espressa indicazione del paziente, come indicato nelle informative, se cosciente e capace.

Il personale autorizzato deve accertare l'identità dei terzi legittimati a ricevere le informazioni, avvalendosi anche di elementi desunti dall'interessato.

Occorre rispettare l'eventuale richiesta della persona assistita a non rendere note a terzi la propria presenza in ASST o le informazioni sulle sue condizioni di salute.

### **4.2 VIOLAZIONE DI DATI – DATA BREACH**

Il Titolare, nel valutare l'adeguato livello di sicurezza, tiene conto in special modo dei rischi presentati dai trattamenti, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Si rimanda per questo ambito al Regolamento aziendale in materia di violazione dei dati – data breach, approvato con la Deliberazione n. 201 del 31 maggio 2018 e pubblicato sul sito internet nella sezione “Privacy”, anche per le modalità di notifica all’Autorità di controllo e di comunicazione all’interessato.

## **5. VIDEOSORVEGLIANZA**

L’installazione di impianti di videosorveglianza nei locali dell’Azienda è ammessa solo dopo attenta valutazione sulla proporzionalità tra lo strumento impiegato e gli scopi perseguiti, e quando altre misure possibili siano realmente insufficienti o inattuabili, nel rispetto del Provvedimento del Garante in materia di videosorveglianza del 8 aprile 2010.

In ASST le valutazioni relative all’installazione di apparecchiature di videosorveglianza vengono effettuate da un team composto dal Responsabile della Protezione dei Dati, dal Direttore dell’UOC Tecnico Patrimoniale, dal Direttore dell’UOC Gestione Risorse Umane e dal Responsabile interno di riferimento per le strutture coinvolte in questa tipologia di trattamento dei dati.

Nel trattamento dei dati effettuato tramite impianti di videosorveglianza, sono rispettati i seguenti principi:

- la raccolta e l’uso delle immagini sono consentiti solo se necessari allo svolgimento di funzioni istituzionali e per il perseguimento di finalità di pertinenza dell’Azienda;
- i sistemi di videosorveglianza possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non possono essere utilizzati dati anonimi;
- l’attività di videosorveglianza è effettuata nel rispetto del cd. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione, e nelle varie fasi del trattamento (sono trattati solo dati pertinenti e non eccedenti rispetto alle finalità perseguite);
- i cittadini che transitano nelle aree sorvegliate sono informati della rilevazione dei dati mediante affissione di specifico cartello secondo il modello proposto dal Garante; i cartelli sono visibili in ogni condizione di illuminazione ambientale (anche di notte) e informano se le immagini sono solo visionate o anche registrate e se vi è un collegamento diretto con le forze di polizia;
- in caso di registrazione, il periodo di conservazione delle immagini è limitato al periodo sufficiente per consentire la messa in atto di tutte le azioni di tutela necessarie al fine di rendere più efficace l’azione di prevenzione e di contrasto agli atti di natura penale.
- al momento dell’installazione della telecamera viene attentamente valutato dove collocare le apparecchiature e la tipologia (fisse o mobili);
- l’installazione degli impianti è concordata con le Rappresentanze Sindacali.

Il Titolare designa per iscritto tutte le persone fisiche, autorizzate al trattamento, ad accedere ai locali dove sono situate le postazioni di controllo e ad utilizzare gli impianti e, nei casi in cui sia indispensabile, per gli scopi perseguiti, a visionare le immagini

Quando il Titolare si avvale di collaborazioni esterne, il soggetto che, sulla base di un contratto, si occupa di gestire e mantenere gli impianti, viene nominato Responsabile esterno (v. art. 1.2.3 del presente Regolamento); tale soggetto autorizza specificatamente le persone che trattano i dati nelle diverse modalità (visione, registrazione, copia, cancellazione, etc).

Al Sig./Alla Sig.ra  
(Nome Cognome)  
(Unità Operativa)

IN LUOGO

### **Oggetto: Autorizzazione al trattamento di dati personali e istruzioni operative**

Con la presente Le comunico che, per le funzioni a Lei attribuite, è autorizzato al trattamento dei dati personali (comprese le categorie particolari) relativi a:

- (nome trattamento)
- (nome trattamento)

Per consentirLe di operare in modo corretto è necessario che si attenga alle seguenti informazioni di carattere generale.

Dovrà operare garantendo la massima riservatezza delle informazioni di cui viene in possesso, considerando tutti i dati personali coperti da riservatezza, non potendo divulgare a terzi le informazioni di cui ha conoscenza anche successivamente all'incarico svolto.

I dati dovranno essere trattati in modo lecito e secondo correttezza e quindi solo in funzione delle attività che Le vengono assegnate, nei limiti delle finalità istituzionali dell'ASST. Pertanto l'accesso ai dati è consentito quando la conoscenza è strettamente necessaria allo svolgimento delle attività.

I dati dovranno essere custoditi e controllati in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

Per una completa informazione circa i comportamenti da tenere Lei è invitato a visionare i regolamenti aziendali vigenti riguardanti le misure di sicurezza tecniche ed organizzative e a rispettare le disposizioni ivi contenute.

L'ASST si è dotata del Registro dei trattamenti, accessibile dal portale applicativi aziendali, per informazioni integrative sui trattamenti per i quali Lei è autorizzato.

In ogni caso Lei è tenuto al rispetto delle specifiche ed ulteriori istruzioni fornite dal Responsabile, delegato dal Titolare, individuato in ASST nel Direttore di UOC, nel Responsabile di UOSD, nel Responsabile di UOS di Staff, nonché nel Responsabile di specifiche funzioni assegnate agli Staff della Direzione Strategica.

Le segnalo in sintesi le principali istruzioni operative, già contenute nella descrizione delle misure di sicurezza dei Regolamenti aziendali.

#### 1) TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone estranee al trattamento.
- I documenti contenenti dati personali devono essere conservati in contenitori o locali muniti di serratura.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie e tavoli di lavoro e i documenti che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- Devono essere distrutte le copie di stampa che per il particolare contenuto di riservatezza, non si prestano al riuso per bozze.

#### 2) TRATTAMENTI CON STRUMENTI ELETTRONICI

Gli autorizzati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- Le password devono essere mantenute riservate.
- Username e password non devono mai essere condivise tra più soggetti. Nel caso in cui altri utenti debbano poter accedere ai dati è necessario richiedere credenziali aggiuntive.
- Le password sono sostituite periodicamente in base alle istruzioni contenute nel Regolamento aziendale per l'utilizzo dei Sistemi Informativi Aziendali.
- Non devono essere lasciate incustodite le postazioni di lavoro durante una sessione di trattamento senza avere preventivamente bloccato il PC o disconnesso l'utenza (premere contemporaneamente i tasti CTRL + ALT + CANC e selezionare l'opzione "blocca computer" o "Disconnetti").

Cordiali saluti

Legnano, *(data)*

**Titolare del trattamento**  
**Il Direttore Generale**

Al Sig./Alla Sig.ra  
(Nome Cognome)

IN LUOGO

### **Oggetto: Autorizzazione al trattamento di dati personali e istruzioni operative**

Con la presente Le comunico che, è autorizzato al trattamento dei dati personali (comprese le categorie particolari) per le funzioni a Lei attribuite nell'ambito dell'accordo assunto tra l'ASST e il Suo Ente di provenienza (attività di tirocinio, alternanza scuola-lavoro, volontariato).

Per lo svolgimento della Sua attività, è stato abilitato all'uso dei seguenti applicativi:

- (nome applicativo)
- (nome applicativo)
- oppure
- (NESSUN APPLICATIVO)

e all'accesso alle seguenti informazioni:

- (nome banca dati)
- (archivi)
- (notizie acquisite in reparto/uffici)

Per consentirLe di operare in modo corretto è necessario che si attenga alle seguenti indicazioni di carattere generale.

Dovrà infatti operare garantendo la massima riservatezza delle informazioni di cui viene in possesso, considerando tutti i dati personali coperti da segretezza, non potendo divulgare a terzi le informazioni di cui viene a conoscenza anche successivamente all'incarico svolto.

I dati dovranno essere trattati in modo lecito e secondo correttezza e quindi solo in funzione delle attività che Le vengono assegnate, nei limiti delle finalità istituzionali dell'ASST. Pertanto l'accesso ai dati è consentito quando la conoscenza è strettamente necessaria allo svolgimento delle attività. I dati dovranno essere custoditi e controllati in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

Lei è tenuto al rispetto delle istruzioni fornite dal Responsabile, delegato dal Titolare, anche per il tramite del Suo Tutor, qualora presente.

Le segnalo in sintesi le principali istruzioni operative, già contenute nella descrizione delle misure di sicurezza dei Regolamenti aziendali.

### 3) TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento.
- I documenti contenenti dati personali devono essere conservati in contenitori o locali muniti di serratura.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie e tavoli di lavoro e i documenti che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- Devono essere distrutte le copie di stampa che per il particolare contenuto di riservatezza, non si prestano al riutilizzo per bozze.

### 4) TRATTAMENTI CON STRUMENTI ELETTRONICI

- Gli incaricati devono utilizzare e gestire le proprie credenziali di autenticazione con diligenza.
- Le password devono essere mantenute riservate. Username e password non devono mai essere condivise tra più soggetti. Nel caso in cui altri utenti debbano poter accedere ai dati è necessario richiedere credenziali aggiuntive.
- Le password sono sostituite periodicamente in base alle istruzioni contenute nel Regolamento aziendale per l'utilizzo dei Sistemi Informativi Aziendali.
- Non devono essere lasciate incustodite le postazioni di lavoro durante una sessione di trattamento senza avere preventivamente bloccato il PC o disconnesso l'utenza (premere contemporaneamente i tasti CTRL + ALT + CANC e selezionare l'opzione "blocca computer" o "Disconnetti").

Cordiali saluti

Legnano, *(data)*

Il Responsabile del trattamento, delegato dal Titolare

---

Per presa visione, l'autorizzato

---

Al Sig./Alla Sig.ra  
(Nome Cognome)

IN LUOGO

**Oggetto: Autorizzazione al trattamento di dati personali e istruzioni operative**

Con la presente Le comunico che è autorizzato al trattamento dei dati personali (comprese le categorie particolari di dati), per le attività che Lei svolge in ASST nell'ambito delle attività definite nel "protocollo d'intesa per la promozione di strategie condivise finalizzate alla prevenzione e al contrasto del fenomeno della violenza nei confronti delle donne" del 28/11/2013 aggiornato il 14/7/2016.

Considerato che lo svolgimento della Sua attività, svolta presso l'Azienda, comporta l'acquisizione e la conoscenza di informazioni contenenti dati personali (comprese le categorie particolari di dati) di specifiche categorie di Pazienti, Le vengono fornite indicazioni operative atte a consentirLe il corretto operare nel rispetto alle disposizioni del Reg. UE 2016/679.

Dovrà pertanto garantire la massima riservatezza dei dati personali di cui viene a conoscenza, non potendo divulgare le informazioni acquisite, a terzi che non siano gli operatori autorizzati dell'ASST o della rete di cui ai protocolli sopracitati, anche al termine del Suo incarico, se non per obbligo di legge.

La comunicazione dei dati e delle informazioni dovrà pertanto avvenire secondo le modalità operative del contesto organizzativo dell'Azienda, mantenendo un ambito limitato e necessario di contatti con gli operatori. I dati dovranno essere trattati in modo lecito e secondo correttezza e quindi solo in funzione delle attività che svolge, nei limiti delle finalità istituzionali dell'ASST. Pertanto l'accesso ai dati è consentito in quanto strettamente necessaria allo svolgimento delle attività.

I dati, nelle varie forme di trattamento, dovranno essere anche custoditi e controllati in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

In ogni caso Lei è tenuto al rispetto di tutte Le eventuali ulteriori specifiche indicazioni fornite dal Responsabile, delegato dal Titolare.

Distinti saluti

Legnano, (data)

Titolare del trattamento  
Il Direttore Generale

---

Per presa visione, l'autorizzato

---

Legnano,

**Spett.**

Oggetto: nomina di responsabile del trattamento

Con la presente, ai sensi dell'art. 28 del Reg UE 2016/679, comunico la nomina a Responsabile del trattamento, in capo al rappresentante legale di codesta società, per gli adempimenti di cui al contratto sottoscritto.

La presente nomina comporta il trattamento di dati personali, comprese le categorie di dati particolari, di cui l'ASST è Titolare, nell'ambito circoscritto per l'esecuzione del contratto.

Pertanto la nomina è condizionata nella durata e nei contenuti, dall'esistenza del contratto in essere tra le parti e il trattamento è consentito e limitato al solo fine di dare attuazione agli adempimenti contrattuali.

All'atto di cessazione del contratto il Responsabile dovrà rendere al Titolare i dati personali, comprese le categorie di dati particolari, oggetto di trattamento, e provvedere a eliminare dal proprio sistema informativo e dagli archivi cartacei i medesimi dati o copie degli stessi, dandone conferma allo stesso Titolare.

Inoltre il Responsabile del trattamento non può comunicare, diffondere e trasferire i dati a soggetti terzi né, tantomeno, a Paesi terzi senza l'autorizzazione del Titolare e in ogni caso in conformità alle disposizioni del Regolamento UE 2016/679.

In nessun caso il Responsabile acquisisce la proprietà intellettuale dei dati e delle informazioni trattate nell'ambito dello svolgimento del contratto.

L'incarico comporta altresì lo svolgimento delle seguenti attività:

a) adottare le misure tecniche ed organizzative, in osservanza dell'art. 32 del Regolamento UE 2016/679, attenendosi anche alle ulteriori disposizioni del Titolare, in tema di sicurezza. Quindi, tra le altre misure, adottare tutti i provvedimenti necessari per evitare la perdita o la distruzione, anche solo accidentale, dei dati personali trattati, gli accessi non autorizzati, i trattamenti non consentiti o non conformi alle finalità del contratto.

b) rendere disponibili al titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Reg. UE, consentendo eventuali controlli dello stesso titolare (art 28 c. 3 lett h).

c) eseguire la valutazione di impatto sulla protezione dei dati di cui all'art. 35 del Reg UE ed eventualmente la consultazione preventiva di cui all'art. 36.



d) redigere il Registro dei trattamenti di cui all'art. 30 del Reg. UE 2016/679.

e) individuare per iscritto i soggetti incaricati e definire le attività operative degli stessi, per lo svolgimento delle mansioni loro affidate garantendo un corretto, lecito e sicuro trattamento dei dati nell'ambito del sistema informatico oltre che l'impegno alla riservatezza degli stessi incaricati.

e) collaborare con il Titolare per l'attuazione delle prescrizioni impartite dal Garante;

f) comunicare, senza ingiustificato ritardo, al Titolare qualsiasi situazione di cui sia venuta a conoscenza, nell'espletamento delle attività di esecuzione del contratto, che possa configurare una violazione dei dati, ai sensi dell' art 33 del Reg. 2016/679.

Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento solo con autorizzazione scritta del titolare ai sensi dell'art. 28 c. 2 del Reg UE 2016/679 e affidarne l'incarico nel rispetto delle disposizioni del c. 4 dello stesso art. 28.

Il Responsabile, qualora possibile, aderirà ai codici di condotta o alle certificazioni di cui agli artt. 40 e 42 del Reg UE 2016/679.

Si fa presente che Titolare e Responsabile del Trattamento sono corresponsabili degli eventuali danni subiti dagli interessati nelle modalità indicate agli artt. 28 c.10, 82 e 83 del Reg. UE 2016/679.

Con i migliori saluti

Il Direttore generale

.....

Per presa visione e accettazione

Il Legale Rappresentante della Società, quale Responsabile esterno del trattamento

.....

Legnano,

**Spett.**

Oggetto: nomina di responsabile del trattamento e degli amministratori di sistema.

Con la presente, ai sensi dell'art. 28 del Reg UE 2016/679, comunico la nomina a Responsabile del trattamento, in capo al rappresentante legale di codesta società, per gli adempimenti di cui al contratto sottoscritto.

La presente nomina comporta il trattamento di dati personali, comprese le categorie di dati particolari, di cui l'ASST è Titolare, nell'ambito circoscritto per l'esecuzione del contratto.

Pertanto la nomina è condizionata nella durata e nei contenuti, dall'esistenza del contratto in essere tra le parti e il trattamento è consentito e limitato al solo fine di dare attuazione agli adempimenti contrattuali.

All'atto di cessazione del contratto il Responsabile dovrà rendere al Titolare i dati personali, comprese le categorie di dati particolari, oggetto di trattamento, e provvedere a eliminare dal proprio sistema informativo e dagli archivi cartacei i medesimi dati o copie degli stessi, dandone conferma allo stesso Titolare.

Inoltre il Responsabile del trattamento non può comunicare, diffondere e trasferire i dati a soggetti terzi né, tantomeno, a Paesi terzi senza l'autorizzazione del Titolare e in ogni caso in conformità alle disposizioni del Regolamento UE 2016/679.

In nessun caso il Responsabile acquisisce la proprietà intellettuale dei dati e delle informazioni trattate nell'ambito dello svolgimento del contratto.

L'incarico comporta altresì lo svolgimento delle seguenti attività:

a) adottare le misure tecniche ed organizzative, in osservanza dell'art. 32 del Regolamento UE 2016/679, attenendosi anche alle ulteriori disposizioni del Titolare, in tema di sicurezza. Quindi, tra le altre misure, adottare tutti i provvedimenti necessari per evitare la perdita o la distruzione, anche solo accidentale, dei dati personali trattati, gli accessi non autorizzati, i trattamenti non consentiti o non conformi alle finalità del contratto.

b) rendere disponibili al titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Reg. UE, consentendo eventuali controlli dello stesso titolare (art 28 c. 3 lett h).

c) eseguire la valutazione di impatto sulla protezione dei dati di cui all'art. 35 del Reg UE ed eventualmente la consultazione preventiva di cui all'art. 36.

d) redigere il Registro dei trattamenti di cui all'art. 30 del Reg. UE 2016/679.

e) individuare per iscritto i soggetti incaricati e definire le attività operative degli stessi, per lo svolgimento delle mansioni loro affidate garantendo un corretto, lecito e sicuro trattamento dei dati nell'ambito del sistema informatico oltre che l'impegno alla riservatezza degli stessi incaricati.

e) collaborare con il Titolare per l'attuazione delle prescrizioni impartite dal Garante;

f) comunicare, senza ingiustificato ritardo, al Titolare qualsiasi situazione di cui sia venuta a conoscenza, nell'espletamento delle attività di esecuzione del contratto, che possa configurare una violazione dei dati, ai sensi dell' art 33 del Reg. 2016/679.

Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento solo con autorizzazione scritta del titolare ai sensi dell'art. 28 c. 2 del Reg UE 2016/679 e affidarne l'incarico nel rispetto delle disposizioni del c. 4 dello stesso art. 28.

Il Responsabile, qualora possibile, aderirà ai codici di condotta o alle certificazioni di cui agli artt. 40 e 42 del Reg UE 2016/679.

Si fa presente che Titolare e Responsabile del Trattamento sono corresponsabili degli eventuali danni subiti dagli interessati nelle modalità indicate agli artt. 28 c.10, 82 e 83 del Reg. UE 2016/679.

Con riferimento allo svolgimento delle attività attinenti la funzione di Amministratore di sistema, si indicano le seguenti attività di cui al provvedimento del Garante del 27/11/08 aggiornato al 25/6/09:

- individuare, nell'ambito della propria organizzazione, la o le persone (dipendenti o collaboratori) munite dei necessari requisiti di esperienza, capacità ed affidabilità, cui attribuire, rispetto al sistema informatico aziendale del Titolare, le mansioni di amministratore di sistema definendone gli ambiti di operatività, in conformità al provvedimento 27 novembre 2008 (aggiornato al 2009) del Garante per la protezione dei dati personali;
- conservare, aggiornare e mettere a disposizione del Titolare, l'elenco con i dati (nome, cognome, funzione) degli amministratori;
- predisporre ed attuare un idoneo sistema di controllo periodico sull'operato dei propri amministratori, in particolare per la registrazione degli accessi logici, fornendo tutte le informazioni al Titolare sulla correttezza dell'attività di queste persone rispetto alle misure di sicurezza adottate ed alle mansioni attribuite.

Con i migliori saluti

Il Direttore generale

.....

Per presa visione e accettazione

Il Legale Rappresentante della Società, quale Responsabile esterno del trattamento

.....

Al Dott./Alla Dott.ssa  
(Nome Cognome)  
(Unità Operativa)

IN LUOGO

### **Oggetto: Nomina a Responsabile del trattamento dei dati**

In base al Reg UE 2016/679, in qualità di rappresentante legale dell'ASST Ovest Milanese, Titolare del Trattamento dei dati, a seguito dell'incarico di Direttore/Responsabile della struttura (*tipo e nome struttura*) da Lei assunto in attuazione del POAS 2017, Le affido l'incarico di Responsabile dei seguenti trattamenti:

(nome trattamento)

(nome trattamento)

secondo quanto contenuto nel Registro delle attività di trattamento (ex Art. 30 del Reg. UE 2016/679), accessibile dal portale applicativi aziendali.

Per Regolamento aziendale, il Titolare designa Responsabili del trattamento, tutti coloro che ricoprono incarichi di Direttore di Unità Operativa Complessa, di Responsabile di Unità Operativa Semplice Dipartimentale, di Responsabile di Unità Operativa Semplice di Staff della Direzione Strategica, nonché di Responsabile delle specifiche funzioni assegnate agli Staff della Direzione Strategica, con la delega delle funzioni in seguito elencate.

L'incarico conferitoLe si riferisce ai trattamenti di tutti i dati (comprese le categorie particolari di dati) che attengono alle attività rese ai pazienti e agli utenti ed effettuate nell'ambito della struttura da Lei diretta.

Tale funzione ha durata per tutto il periodo di assunzione del Suo incarico ed è da considerarsi confermata con il rinnovo dell'incarico stesso a seguito di valutazione positiva, quando prevista.

La nomina a Responsabile del trattamento è consultabile e scaricabile, tramite login con le credenziali personali, nell'applicativo "Data Protection Manager", disponibile nel portale aziendale, previa comunicazione.

Il Responsabile è pertanto tenuto a:

1. accertarsi che il trattamento dei dati nell'ambito della propria UOC/UOSD/UOS/funzione di staff sia preceduto da una corretta informazione all'utente, avvalendosi dei modelli e delle procedure predisposti dall'azienda;
2. provvedere, su richiesta dell'interessato, ad aggiornare e/o modificare, i dati dello stesso, laddove possibile, nell'ambito della sua capacità organizzativa;
3. segnalare al Titolare del trattamento eventuali reclami da parte di terzi e informare di qualunque fatto che possa compromettere la sicurezza dei dati;
4. garantire il rispetto della normativa in materia di tutela dei dati personali, anche sotto il profilo delle misure di sicurezza, attenendosi alle misure tecniche ed organizzative previste dai regolamenti aziendali;
5. accertarsi che le persone siano autorizzate agli accessi ai dati effettivamente necessari allo svolgimento delle attività nel proprio ambito organizzativo e che cessino di esserlo nel caso in cui non sia più necessario;
6. accertarsi che le persone autorizzate a trattare i dati nel Suo ambito organizzativo operino in conformità alle istruzioni ricevute dal Titolare e alle misure tecniche ed organizzative adottate in azienda. A tal proposito Lei è delegato a conferire più specifiche istruzioni se

- necessarie e a fornirle anche ai soggetti esterni autorizzati ai trattamenti (ad es. personale volontario, studenti ecc.);
7. comunicare immediatamente al Titolare del trattamento gli eventuali nuovi trattamenti da intraprendere;
  8. collaborare con il Titolare per tutti gli adempimenti attribuiti a quest'ultimo nel Regolamento UE, compresa la redazione del Registro dei trattamenti (quando coinvolto dal Titolare e dal Responsabile della Protezione dei Dati) e la valutazione d'impatto per le attività di trattamento di sua competenza;
  9. collaborare con il Titolare e il Responsabile della Protezione dei Dati aziendale per tutte le necessità, in particolare per le segnalazioni di Data Breach, nell'ambito del gruppo di valutazione previsto nel Regolamento di cui alla delibera n. 201 del 31-5-2018, nonché per evadere tempestivamente eventuali richieste di informazioni dal parte dell'Autorità Garante e dare immediata esecuzione alle indicazioni della stessa Autorità.

Cordiali saluti

Legnano, *(data)*

**Il Direttore generale  
Titolare del Trattamento**

Al Sig./Alla Sig.ra  
(Nome Cognome)  
(Unità Operativa)

IN LUOGO

**Oggetto: Nomina ad "Amministratore del sistema"**

Il provvedimento del Garante per la protezione dei dati personali "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema**" del 27 novembre 2008, aggiornato al 25 giugno 2009, definisce le caratteristiche e i compiti dell' Amministratore di sistema, che svolge attività particolarmente qualificate nell'ambito degli apparati di rete e per la sicurezza delle informazioni.

Pertanto, tenuto conto delle competenze tecniche, delle mansioni svolte e della sua assegnazione presso la UO Servizi Informativi Aziendali, con la presente viene nominato "**Amministratore di sistema**", nell'ambito di operatività delle sue funzioni, meglio descritte di seguito:

.....  
.....  
.....

Si fa presente che il Provvedimento di cui sopra, obbliga l'Azienda alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza dei trattamenti dei dati eseguiti, alle misure organizzative, tecniche e di sicurezza.

Inoltre i suoi estremi identificativi e le funzioni correlate sono comunicate al Garante in caso di accertamenti e ai soggetti indicati al punto 4.3 del Provvedimento qualora si ravvisino le condizioni.

Cordiali saluti

Legnano, (data)

**Il Direttore generale  
Titolare del Trattamento**

Al Sig./Alla Sig.ra  
(Nome Cognome)  
**Sistemi Informativi Aziendali**

IN LUOGO

**Oggetto: Nomina ad "Amministratore del sistema" - Referente**

Il provvedimento del Garante per la protezione dei dati personali "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema**" del 27 novembre 2008, aggiornato al 25 giugno 2009, definisce le caratteristiche e i compiti dell' Amministratore di sistema, che svolge attività particolarmente qualificate nell'ambito degli apparati di rete e per la sicurezza delle informazioni.

Pertanto, tenuto conto delle competenze tecniche, delle mansioni svolte e del Suo ruolo nell'ambito della UO Servizi Informativi Aziendali, con la presente viene nominato "**Amministratore di sistema**", per tutte le attività e le funzioni che attengono ai sistemi informatici.

Oltre a tutte le attività attinenti la funzione di Amministratore di sistema, indicate nel provvedimento del Garante del 27/11/08 aggiornato al 25/6/09, le sono assegnate in particolare le seguenti funzioni:

- individuare, nell'ambito della propria struttura, gli operatori con competenze tecniche munite dei necessari requisiti di esperienza, capacità ed affidabilità, cui attribuire le più specifiche mansioni di amministratore di sistema definendone gli ambiti di operatività, in conformità al provvedimento 27 novembre 2008 (aggiornato al 2009) del Garante per la protezione dei dati personali;
- conservare, aggiornare e mettere a disposizione del Titolare, l'elenco con i dati (nome, cognome, funzione) degli amministratori, secondo le modalità stabilite al punto 4.3 del Provvedimento del Garante di cui sopra;
- predisporre ed attuare un idoneo sistema di controllo periodico (almeno annuale) sull'operato degli amministratori, in particolare per la registrazione degli accessi logici, fornendo tutte le informazioni al Titolare e al Responsabile della Protezione dei Dati, sulla correttezza dell'attività di queste persone rispetto alle misure di sicurezza adottate ed alle mansioni attribuite;
- tenere aggiornato il Regolamento aziendale sull'utilizzo dei sistemi informatici per gli operatori.

Cordiali saluti

Legnano, (data)

**Titolare del trattamento  
Il Direttore Generale**