

Sanitaservice ASL BT s.r.l.

con sede in Via Fornaci n. 201 – 76123 Andria BT www.sanitaserviceaslbat.it e-mail:

segreteria@sanitaserviceaslbat.it.

ORGANIGRAMMA ESPLICATIVO

1. INTRODUZIONE

La formalizzazione di un organigramma esplicativo pertinente ed adeguato è certamente uno degli strumenti che il titolare del trattamento Sanitaservice Asl Bt s.r.l. può validamente utilizzare per dimostrare, in un'ottica di accountability, di aver adottato misure tecniche ed organizzative adeguate a norma dell'art. 24 del Regolamento UE 2016/679.

Sicuramente la realizzazione di quello che potremmo definire come "organigramma" rientra all'interno di quella lunga lista di accountability che ciascuna azienda oggi è chiamata a rispettare al fine di gestire in modo corretto e tempestivo le problematiche legate alla tutela e protezione del dato.

2. SCOPO

Il regolamento in materia di protezione dei dati personali UE n. 2016/679 spiega il principio di *"accountability"* ossia di responsabilizzazione dei soggetti che pongono in essere attività di trattamento di dati personali. A tale riguardo, l'art. 24 del Regolamento UE 2016/679 prevede che il titolare del trattamento adotti misure tecniche ed organizzative adeguate ed efficaci al fine di garantire che il trattamento dei dati personali abbia luogo in conformità alle leggi sulla protezione dei dati applicabili.

Per questo motivo la società Sanitaservice Asl Bt s.r.l. ha ritenuto necessario adottare il presente organigramma al fine di specificare i ruoli e le responsabilità attribuite ad ogni soggetto coinvolto nel trattamento di dati personali. In particolare, lo scopo del presente documento è quello di elencare le figure interne ed eventualmente esterne che trattano dati personali e specialmente elencare i compiti, le funzioni e le responsabilità, che sono ad esso attribuiti

3. DEFINIZIONI

Amministratore di sistema (ADS): professionista che generalmente in ambito informatico, gestisce e manutiene un impianto di elaborazione o di sue componenti ad esempio, gestore delle password, amministratore di database e di reti;
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Data breach (Violazione dei dati personali): 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;
Data Protection Officer o Responsabile dei dati personali (DPO-RDP): professionista generalmente appartenente all'organico della società, che il titolare nomina al fine di avere al suo interno un punto di riferimento, esperto di privacy e di facilitare l'osservanza della predetta materia;
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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Dati genetici: i 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;
Dati biometrici: i 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;

Dati relativi alla salute: i 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;
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
Informativa: documento o insieme di informazioni contenente le informazioni che il titolare deve fornire all'interessato per chiarire se quest'ultimo è obbligato o meno a rilasciare i dati personali;
Interessato: persona fisica a cui si riferiscono i dati;
Misure di sicurezza: complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione;
Responsabile 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;
Soggetto autorizzato: la persona fisica, espressamente designata e specificatamente istruita, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali;
Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
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, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
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;

4. RUOLI E RESPONSABILITÀ

L'organigramma di cui si è dotata l'organizzazione si articola su diversi livelli, riconoscendo poteri e relative responsabilità in capo a diversi soggetti:

- **IL TITOLARE DEL TRATTAMENTO:** è il soggetto che determina le finalità e i mezzi del trattamento dei dati personali. Il Titolare del trattamento è la società Sanitaservice Asl Bt s.r.l. che riveste tale funzione e sulla quale, conseguentemente, incombono tutti gli obblighi e le responsabilità che la legge nazionale ed europea impone. Primo fra tutti, l'obbligo di mettere in atto, riesaminare ed aggiornare le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è da essa effettuato conformemente al Regolamento Ue 2016/679 e al D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018.

- **IL RESPONSABILE DEL TRATTAMENTO DATI:** è il soggetto (persona fisica o giuridica) che tratta i dati personali per conto del titolare del trattamento Sanitaservice Asl Bt s.r.l. in base alle sue istruzioni. Due sono le condizioni per qualificare un soggetto come responsabile: deve essere un soggetto distinto dal titolare, e deve elaborare dati per conto del titolare. Il titolare del trattamento risponde della gestione effettuata dai responsabili nominati, dovendo ricorrere per tale ruolo a soggetti che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento UE 2016/679.

Generalmente vengono individuati quali responsabili del trattamento dati personali all'interno dell'organizzazione i seguenti soggetti: Consulenti del lavoro 1, Consulente fiscale, software gestionali ecc. ecc. Sanitaservice Asl Bt s.r.l. redige e aggiorna costantemente l'elenco di censimento dei responsabili del trattamento dati personali attraverso il documento denominato "*GDPR - censimento responsabili del trattamento dati*".

Si evidenzia che i g riferimento alla gestione dei servizi di Ausiliariato/Pulizia, di Emergenza Urgenza, Logistica e Accoglienza, Supporto ai Sistemi Informativi, la Sanitaservice ASL BT s.r.l. svolge tale ruolo in qualità di responsabile del trattamento dati ex articolo 28 del Regolamento UE 2016/679, in quanto tratta dati personali "per conto" del titolare del trattamento Asl Bat.

- **IL DATA PROTECTION OFFICER:** è il soggetto designato internamente o esternamente dal titolare del trattamento che ha la funzione di affiancare il titolare/responsabile del trattamento affinché conservi i dati e gestisca i rischi seguendo i princìpi e le indicazioni del Regolamento europeo. Il responsabile della protezione dati è quindi un consulente tecnico e legale, con potere esecutivo. Infatti, il suo ruolo è doppio, perché non solo consiglia e sorveglia, ma funge anche da tramite fra l'organizzazione e l'autorità. I suoi compiti sono indicati in maniera puntuale nel Regolamento UE 2016/679 all'articolo 39 e sono essenzialmente tre: informare, sorvegliare e cooperare.

- **L'AMMINISTRATORE DI SISTEMA:** è il soggetto esterno o interno all'organizzazione chiamato, in ambito informatico, alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, facendo però rientrare in essa anche le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. L'amministratore di sistema è un ruolo operativo, essenziale per la sicurezza dei sistemi informatici e telematici e delle banche dati, e quindi con specifiche competenze tecniche, al quale è affidato il compito della gestione di tali sistemi, oltre al compito di vigilare sull'utilizzo dei sistemi. L'amministratore di sistema è il soggetto principale con riferimento alle problematiche dei data breach.

- **IL REFERENTE PRIVACY AZIENDALE** è il soggetto interno designato direttamente e formalmente dal Titolare *(cfr. gdpr- nomina referente privacy aziendale)* che, nello svolgimento delle proprie funzioni e nei limiti dei poteri attribuiti, è deputato alla gestione dei seguenti ambiti:
  - controllo del rispetto delle istruzioni in materia di trattamento di dati personali a carico dei dipendenti aziendali;
  - far sottoscrivere le informative verso gli interessati;
  - supportare le funzioni dell'azienda nelle nomine verso autorizzati e responsabili esterni del trattamento;

[1] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9080970

- predisporre il registro dei trattamenti privacy ex articolo 30 del Regolamento UE 2016/679, sia in qualità di titolare del trattamento che di responsabile e curarne il relativo aggiornamento;
- supportare le funzioni dell'azienda nell'applicazione di specifici provvedimenti emessi dal Garante;
- essere membro del Team che gestisce eventuali violazioni di dati personali "Data Breach";
- partecipare a riunioni ogniqualvolta si introduca all'interno dell'azienda una nuova tecnologia o debbano essere attuate campagne o operazioni che riguardino il trattamento dei dati personali;
- partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'azienda che impattano sulla riservatezza dei dipendenti;
- conservare l'archivio della documentazione richiesta dal Regolamento UE 2016/679;
- mettere in atto le disposizioni richieste in materia di protezione dei dati;
- relazionare sullo stato di avanzamento ed eventuali problematiche;
- predisporre e tenere sotto controllo il piano delle attività previste;
- pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul Regolamento UE 2016/679);
- tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'audit;
- tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi;
- informare e comunicare di ogni questione relativa alla protezione dei dati personali il titolare del trattamento;
- collaborare attivamente con l'amministratore di sistema;

❖ **SOGGETTI DESIGNATI AL TRATTAMENTO**

L'art. 2-quaterdecies del D.lgs. 196/03 recita: "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*". A questo scopo, il comma 2 dello stesso articolo prevede che il titolare o il responsabile del trattamento individuino le modalità più opportune per autorizzare al trattamento le persone che operano sotto la propria autorità diretta.

Il soggetto designato al trattamento dei dati personali è quindi una persona fisica e non giuridica. Solitamente è "interno" alla struttura organizzativa, quale dipendente o collaboratore del titolare del trattamento.

L'organizzazione può redigere delle deleghe/nomine (con compiti o funzioni specifiche) singole o per tipologie di designati, delimitando l'ambito del trattamento al quale si è autorizzati, consentendo, di dare seguito agli adempimenti organizzativi interni alla struttura del titolare del trattamento.

I compiti del soggetto designato sono ad esempio:

- individuare gli autorizzati al trattamento;
- fornire istruzioni operative;
- attuare gli obblighi di formazione;
- predisporre la notificazione del data breach;

- garantire l'esercizio dei diritti dell'interessato e collaborare con l'autorità garante per l'attuazione delle prescrizioni;

Si tratta di un ruolo intermedi tra il titolare del trattamento e i soggetti autorizzati. Peraltro, la individuazione del "soggetto designato" non è di per sé obbligatoria, ma è tanto più opportuna in strutture di media o grande dimensione.

All'interno dell'organizzazione Sanitaservice ASL BT viene individuato, attraverso formale atto, quale soggetto designato ex articolo 2-quaterdecies del D.lgs. 196/03 l'amministratore unico della società.

❖ **SOGGETTI AUTORIZZATI AL TRATTAMENTO (ex incaricati al trattamento)**

La figura del soggetto autorizzato al trattamento è definibile come la persona fisica autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile. Tale figura è espressamente prevista da norma (dall'art. 29 del Regolamento UE 2016/679) e viene formalmente nominata tramite apposite lettere d'incarico e nomina.

I soggetti autorizzati della Sanitaservice Asl Bt s.r.l. sono coloro i quali, facenti parte dell'organico, provvedono materialmente al trattamento dei dati personali sotto la supervisione del titolare del trattamento. Sanitaservice Asl Bt s.r.l., inoltre, cura l'aggiornamento costante dei propri soggetti autorizzati mediante corsi di formazione ed aggiornamento sulla protezione dei dati personali.

Le suddette nomine, al fine di soddisfare il criterio sancito anche dall'art. 29 del Regolamento UE 2016/679 secondo cui non si possa avere accesso a dati personali e quindi non si possa trattarli se non adeguatamente istruiti, dovranno contenere specifiche indicazione in relazione a:

- tipologie di attività di trattamento svolte per ciascuna unità organizzativa di riferimento;
- tipologia di applicativi utilizzati per le attività di trattamento;
- regole di comportamento e di trattamento dei dati personali;

❖ **COORDINATORE/RESPONSABILE DI PROCEDURA:**

All'interno dell'organizzazione sono state previste due specifiche figure denominate coordinatore/responsabile di procedura. Detti soggetti designati all'interno della procedura, gestiscono e sovraintendono la stessa procedura curandone ogni aspetto, quale: tempistiche di risposta, coinvolgimento di soggetti esterni, registrazione eventi su appositi registri, riscontri al richiedente, e disporre documentazione ecc. ecc.

Le uniche due procedure ove è presente il coordinatore/responsabile sono:

- Procedura operativa per l'esercizio dei diritti degli interessati;
- Procedura operativa per la gestione della violazione della sicurezza dei dati personali "data breach".

Andria, _____

IL TITOLARE DEL TRATTAMENTO

Sanitaservice ASL BT s.r.l.

_____