# AGENDA

- ❖ Il ruolo del medico competente e la salvaguardia del dipendente
- ❖ Le recenti pronunce del Garante
- ❖ Protezione degli archivi e dei sistemi IT, trasmissione dei dati
- ❖ Digitalizzazione dei processi e delle attività di trattamento
- ❖ Sistemi innovativi per il trattamento dei dati sanitari sul luogo di lavoro

- La tutela dei **dati personali del dipendente** è da sempre un elemento importante della normativa di settore. Perché questa attenzione particolare?

- Per molti aspetti il dipendente è visto come **un interessato "vulnerabile"**, un soggetto che per la sproporzione nei rapporti di forza fra Datore di Lavoro e Lavoratore può vedere limitati i suoi diritti fondamentali e invasa la sfera personale

- Facciamo un esempio: se il datore di lavoro, in fase di assunzione, fosse libero di richiedere un "consenso" al lavoratore per avere pieno accesso alle informazioni sul suo stato di salute, quanti candidati rifiuterebbero?

Il focus del Garante per la Protezione dei Dati Personali sul ruolo del Medico Competente:

- Una barriera alle interferenze del Datore di Lavoro su aspetti delicati della vita personale del dipendente (lo stato di salute)
- Un soggetto indipendente a tutela di possibili abusi
- L'unico legittimato a trattare in piena autonomia e competenza tecnica i dati personali di natura sanitaria

# AGENDA

- Il ruolo del medico competente e la salvaguardia del dipendente
- Le recenti pronunce del Garante
- Protezione degli archivi e dei sistemi IT, trasmissione dei dati
- Digitalizzazione dei processi e delle attività di trattamento
- Sistemi innovativi per il trattamento dei dati sanitari sul luogo di lavoro

COVID-19
CORONAVIRUS
E PROTEZIONE
DEI DATI

COVID-19
CORONAVIRUS
E PROTEZIONE
DEI DATI

## Protezione dei dati

**Il ruolo del "*medico competente*" in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale**

## Documento di indirizzo

**Vaccinazione nei luoghi di lavoro: indicazioni generali per il trattamento dei dati personali**

# Il medico competente

- La **funzione di medico competente è espressione di un interesse pubblico** (tutela del lavoratore e della collettività), individuato e disciplinato dalla legge e, in quanto tale, sottratta alla sfera di competenza del datore di lavoro e ai relativi poteri.

- Nello svolgimento di tali compiti che la legge gli attribuisce in via esclusiva, in particolare l'attività di sorveglianza sanitaria e la tenuta delle cartelle sanitarie e di rischio dei singoli lavoratori, il medico competente è, per legge, **l'unico legittimato a trattare in piena autonomia e competenza tecnica i dati personali di natura sanitaria** indispensabili per lo svolgimento della funzione di protezione della salute e sicurezza dei luoghi di lavoro, non potendo informazioni relative, ad esempio, alla diagnosi o all'anamnesi familiare del lavoratore essere in alcun modo trattate dal datore di lavoro, se non nella misura del mero giudizio di idoneità alla mansione specifica e delle eventuali prescrizioni che il professionista fissa come condizioni di lavoro (arg. art. 25, comma 1, lett. i) che prevede che il medico "comuni[chi] al datore di lavoro […] i risultati anonimi collettivi della sorveglianza sanitaria").

# Il medico competente

- Sebbene gli accertamenti volti a verificare l'idoneità alla "mansione specifica" del dipendente siano obbligatori per legge e siano svolti "a spese" e "a cura" del datore di lavoro (artt. 39, comma 5 e 41, comma 4 d.lgs. n. 81/2008, cit.), **essi devono essere posti in essere esclusivamente per il tramite del medico competente**.

- Il quadro normativo stabilisce, quindi, anche le modalità di impiego dei mezzi e delle risorse strumentali all'attività posta in essere dal medico competente e dei conseguenti trattamenti, facendo ricadere sul datore di lavoro i costi della relativa funzione (sul piano economico ma, in alcuni casi e per alcuni profili, sul piano organizzativo), **senza che ciò si traduca**, tuttavia, **nella titolarità** dello specifico trattamento di dati personali posto in essere dal medico.

# Il medico competente

- Lo stesso Regolamento considera in via autonoma i trattamenti necessari per le finalità di “medicina del lavoro” (art. 9 lett. h) del Regolamento), nel quale ambito è riconducibile la funzione del medico competente prevista dall’ordinamento nazionale, che devono essere effettuati **“sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell’Unione o degli stati membri […]”** (art. 9, par. 3 del Regolamento; cfr. anche art. 2-sexies, comma 2, lett. u) del Codice “compiti di igiene e sicurezza sui luoghi di lavoro”). Tali trattamenti sono infatti disciplinati in maniera distinta rispetto a quelli posti in essere dal datore di lavoro e necessari per assolvere i propri obblighi normativi in materia di “salute e sicurezza sul lavoro” (art. 9, lett. b) e 88 del Regolamento).

- Stante la titolarità del trattamento dei dati del medico competente (artt. 4, n. 7 e 24 del Regolamento), essendo questo l’unico legittimato a trattare i dati sanitari dei lavoratori per le finalità indicate dalla legge di settore, **gli eventuali flussi di dati personali tra il datore di lavoro e il medico competente devono intendersi quali “comunicazioni” di dati personali** (cfr. la definizione contenuta all’art. 2-ter, par. 4, lett. a) del Codice), i cui presupposti sono rinvenibili nel richiamato quadro normativo di settore.

# Il medico competente e l'emergenza SARS-CoV-2

- Fin dalle prime settimane dell'emergenza, alla luce del quadro normativo di settore e di quello progressivamente delineatosi, tenuto conto dei principi di protezione dei dati e di quelle disposizioni più specifiche che, nell'ordinamento nazionale, tutelano la dignità e la sfera privata degli interessati sul luogo di lavoro (es. art.113 del Codice), il Garante **ha sottolineato la funzione di garanzia del medico competente nel trattamento dei dati dei lavoratori** (cfr., FAQ relative al trattamento dei dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria- doc. web n. 9337010, spec. FAQ nn. 4, 7 e 8 e, da ultimo, FAQ sul "Trattamento di dati relativi alla vaccinazione anti Covid-19 nel contesto lavorativo", doc. web n. 9543615)

- I compiti che la disciplina di settore assegna tradizionalmente al medico competente nella tutela della salute e sicurezza delle attività lavorative, assumono, nell'evoluzione del quadro normativo nazionale legato all'emergenza, la funzione di **"misure di prevenzione di carattere generale"** (cfr. FAQ n. 4, cit.) da attuare, in ogni caso, nel rispetto della disciplina di settore in materia di sicurezza sul lavoro, dei principi di protezione dei dati personali, dei citati protocolli di sicurezza e delle indicazioni del Ministero della Salute (cfr. sul punto, circolare del Ministero della Salute del 29 aprile 2020, n. 0014915).

# Il medico competente e l'emergenza SARS-CoV-2

- collabora con il datore di lavoro e con il servizio di prevenzione e protezione, anzitutto, nella valutazione dei rischi, nell'individuazione, attuazione e perfezionamento delle misure e nell'osservanza dei protocolli anti-contagio, nell'informazione e formazione dei lavoratori sul rischio di contagio da SARS-CoV-2 (arg. art. 25 del citato D.lgs. 81/2008 e s.m.i.), **nell'esame dei rischi riguardanti gruppi di lavoratori maggiormente esposti al contagio** (es. operatori sanitari, forze dell'ordine) o in particolari situazioni di "fragilità" legata a fattori quali l'età anagrafica o a situazioni di pregressa morbilità

- In tale contesto, inoltre, è particolarmente utile il coinvolgimento del medico competente nella precoce identificazione dei **contatti in ambito lavorativo** (c.d. contact tracing) e nel loro isolamento in ragione della collaborazione qualificata che può fornire ai medici di medicina generale e ai dipartimenti di prevenzione per la corretta gestione e presa in carico del lavoratore con sintomatologia sospetta

# Il medico competente e l'emergenza SARS-CoV-2

- Nell'ambito della valutazione dei rischi e della sorveglia sanitaria (artt. 25, 39, comma 5, e 41, comma 4, d.lgs. n. 81/2008), il medico competente in qualità di professionista sanitario potrà suggerire l'adozione di eventuali mezzi diagnostici, qualora ritenuti utili al fine del contenimento della diffusione del virus e della salute dei lavoratori, ponderando la necessità, "in funzione della valutazione del rischio" e delle "condizioni di salute" dei lavoratori, di sottoporre i lavoratori a ulteriori indagini diagnostiche, che possono consistere anche in **"esami clinici e biologici"**(art. 41, commi 2 e 4 d.lgs. 81/2008) o test sierologici, nel rispetto delle disposizioni generali **che vietano al datore di lavoro di trattare informazioni relative alla diagnosi del lavoratore o di effettuare direttamente esami diagnostici sui dipendenti**

# Dati personali inerenti la vaccinazione dei dipendenti

- Il datore di lavoro **non può acquisire**, neanche con il consenso del dipendente o tramite il medico compente, **i nominativi del personale vaccinato o la copia delle certificazioni vaccinali** (cfr. FAQ 1 e 2 sul "Trattamento di dati relativi alla vaccinazione anti Covid-19 nel contesto lavorativo", doc. web n. 9543615). Ciò anche per l'impossibilità di considerare il consenso dei dipendenti, una valida condizione di liceità per il trattamento dei dati personali in ambito lavorativo

- Il tema del trattamento dei dati relativi alla vaccinazione può allo stato **essere inquadrato nell'ambito della verifica dell'idoneità alla mansione specifica**, che consente quindi al medico competente (e solo a lui), nella sua funzione di raccordo tra il sistema sanitario nazionale/locale e lo specifico contesto lavorativo e nel rispetto delle indicazioni fornite dalle autorità sanitarie, anche in merito all'efficacia e all'affidabilità medico-scientifica della somministrazione dei vaccini, **di emettere giudizi di idoneità parziale e/o inidoneità temporanee per i lavoratori non vaccinati** (salvo che il rischio non possa essere ridotto con misure di protezione e/o organizzative alternative e di eguale efficacia).

# Il medico competente dipendente da una struttura

- Le strutture sanitarie dispongono, per legge, di un proprio servizio di medicina del lavoro, che eroga le proprie prestazioni sia nei confronti di persone fisiche che di aziende e amministrazioni convenzionate. Tale servizio infatti può erogare le prestazioni di sorveglianza sanitaria in favore di datori di lavoro pubblici o privati (ai sensi dell'art. 39, comma 1 lett. a) d.lgs. n. 81/2008). **In tal caso, la struttura sanitaria, in qualità di titolare del trattamento, impiega, proprio personale "autorizzato" per i trattamenti di dati personali dei lavoratori dipendenti delle imprese o degli enti convenzionati.**

- È necessario tuttavia evidenziare il diverso caso in cui la struttura sanitaria pubblica, in qualità di datore di lavoro, dovendo assolvere agli obblighi in materia di igiene e sicurezza **nei confronti dei lavoratori alle proprie dipendenze**, si avvalga invece della facoltà, prevista dalla legge, di impiegare, a tal fine, personale dipendente in possesso dei requisiti stabiliti dalla legge (artt. 18, comma 1, lett. a) e 39 del d.lgs. n. 81/2008). Il medico competente, così individuato, dovrà svolgere i propri compiti, nei limiti stabiliti e alle condizioni dettate dalla disciplina di settore e dalla disciplina di protezione dei dati personali, con le risorse fornite dall'azienda.

# AGENDA

- Il ruolo del medico competente e la salvaguardia del dipendente
- Le recenti pronunce del Garante
- Protezione degli archivi e dei sistemi IT, trasmissione dei dati
- Digitalizzazione dei processi e delle attività di trattamento
- Sistemi innovativi per il trattamento dei dati sanitari sul luogo di lavoro

# Principali adempimenti del medico competente

- **Istituzione del registro delle attività di trattamento**: con riferimento all'obbligo di tenere un registro delle attività di trattamento svolte dal titolare sotto la propria responsabilità (art. 30, par. 1 Regolamento), il medico competente dovrà istituire e tenere un proprio registro, distinto da quello del datore di lavoro che gli ha conferito l'incarico (anche nel caso in cui sia un dipendente che svolge il ruolo di medico competente per il proprio datore di lavoro), considerando che tratta in maniera non occasionale categorie particolari di dati relativi allo stato di salute.

- **Informativa agli interessati (art. 14 del Regolamento)**: per quanto attiene agli obblighi informativi nei confronti degli interessati, si evidenzia che, di regola, il medico competente riceve i dati anagrafici dei lavoratori dal datore di lavoro (a seguito del conferimento dell'incarico ovvero in caso di nuove assunzioni di personale) così come ogni utile aggiornamento o rettifica dei dati. Di conseguenza, il medico competente potrà fornire le informazioni di cui ai paragrafi 1 e 2 dell'art. 14 al momento della prima comunicazione all'interessato

# Principali adempimenti del medico competente

- **Sicurezza dei dati personali:** In relazione all'obbligo di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento), il medico competente dovrà identificare e adottare tali misure in proprio, fermo restando che potrà avvalersi della cooperazione e del supporto, anche economico, del datore di lavoro

- **Nomina del Responsabile della protezione dei dati**: il Garante ha recentemente chiarito che il singolo professionista sanitario che operi in regime di libera professione a titolo individuale, non è tenuto alla designazione del responsabile della protezione dei dati (RPD) con riferimento allo svolgimento della propria attività

# Un focus sul Data Breach

**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.

## Qual è l'impatto di un Data Breach?

Una violazione […] può comportare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata (Considerando 85 del Regolamento UE 2016/679).

- **Violazione di confidenzialità**
- **Violazione di disponibilità**
- **Violazione di integrità**

Il Titolare ha a disposizione 72 ore dal momento in cui viene a conoscenza del Data Breach, per segnalarlo al Garante.

## Deve essere segnalato?

Il potenziale data breach deve essere prontamente analizzato ed **eventualmente segnalato** all'Autorità Garante entro 72 ore! Ancora una volta è necessaria un'analisi di rischio

# Un focus sul Data Breach


## *Qual è la probabilità di un Data Breach in ambito sanitario?*

Negli ultimi anni, i *Data Breach* nell'ambito del settore sanitario sono aumentati esponenzialmente.

Le minacce sono legate prevalentemente a:
- Assenza di misure di sicurezza fisica dei supporti (PC, tablet, etc.)
- Vulnerabilità informatiche
- Errori umani

Le possibili conseguenze di un *Data Breach*:
- Impatto per gli interessati
- Danni reputazionali
- Sanzioni delle Autorità
- Costi

**Tricase, furto nel poliambulatorio. L'appello: ridateci i pc con i dati 2300 pazienti cardiopatici**

6 Marzo 2019 - 14:38 Redazione Cronaca 0 2.634

BUSINESS INSIDER

**Last year healthcare had more cybersecurity breaches than any other industry — and it will likely intensify**

Zoë LaRock Apr. 15, 2019, 11:38 AM

**Data breach, record di furti di dati sensibili nel settore sanitario**

18 Febbraio 2019 Italia

La sanità è uno dei settori più bersagliati dai pirati della Rete. Utilizzati software dannosi per realizzare estorsioni via internet, 17 le strutture hackerate in Italia

**Attacchi gravi**
- Osp. S. Andrea (Rm)

**Attacchi dimostrativi**
- Azienda Sanitaria Provinciale (RC)
- Sistema Informativo Veterinario Ministero della salute (Rm)
- Federazione Italiana Medici Medicina Generale (Pi)
- Azienda sanitaria locale Ciriè, Chivasso e Ivrea (To)
- Portale Cure Primarie Ulss 21 Legnago (Vr)
- Istituto di Ricovero e Cura a Carattere Scientifico (An)
- Sistema Sanitario Sardegna Ospedale Brotzu (Ca)
- Asl (Ri)
- Asl (Vt)
- Osp. S. Giovanni (Rm)
- Istituto superiore di sanità (Rm)
- Agenzia nazionale per i servizi sanitari regionali (Rm)
- Difarma (distribuzione farmaceutica in Sardegna)
- Federsanità
- Asst Lariana (Co)
- Asl (Cs)

# Un focus sul Data Breach

- Bloccare i PC quando ci allontaniamo anche temporaneamente
- Non applicare post-it con password dei pc in prossimità degli stessi
- Non lasciare incustoditi documenti cartacei
- Distruggere accuratamente i documenti cartacei contenenti dati personali prima di buttarli via
- Rivolgere particolare attenzione all'uso di stampanti e fotocopiatrici condivise
- Rivolgere particolare attenzione all'uso del fax
- Mantenere chiusi a chiave gli armadi
- Mantenere chiuse le stanze
- Non condividere le proprie password
- Rivolgere particolare attenzione nell'invio di email contenenti dati personali
- Non divulgare informazioni mediante strumenti di messaggistica istantanea
- Attenzione alle email!


# AGENDA

- Il ruolo del medico competente e la salvaguardia del dipendente
- Le recenti pronunce del Garante
- Protezione degli archivi e dei sistemi IT, trasmissione dei dati
- Digitalizzazione dei processi e delle attività di trattamento
- Sistemi innovativi per il trattamento dei dati sanitari sul luogo di lavoro

# Accountability e approccio risk-based all'interno del GDPR

Per ***data protection by default*** si intende l'insieme delle regole di progettazione del trattamento che circoscrivono e limitano l'utilizzo dei dati personali per impostazione predefinita, sia nelle finalità sia nel tempo di *retention* (ad esempio, l'utilizzo dei dati personali strettamente necessari alla finalità del trattamento, la limitazione del trattamento alle sole finalità per le quali è stata fornita informativa e, ove necessario, raccolti i consensi, la limitazione del periodo di *retention* dei dati).

Per ***data protection by design*** si intende l'insieme delle regole di progettazione del trattamento che consentono nativamente il rispetto dei principi del Regolamento senza la necessità di interventi successivi (ad esempio, progettare un sistema con il livello di misure di sicurezza tecnico-organizzative adeguate al rischio potenziale del trattamento, oppure progettare un sistema che preveda la possibilità di estrarre un formato standard per garantire la portabilità dei dati personali).

Fin dalla fase di progettazione del trattamento:

01 LIMITAZIONE DELLA FINALITÀ DEL TRATTAMENTO

02 MINIMIZZAZIONE DEI DATI TRATTATI

03 MINIMIZZAZIONE DELLE OPERAZIONI DI TRATTAMENTO

04 LIMITAZIONE DELLA CONSERVAZIONE


Fin dalla fase di progettazione del trattamento:

01 DEFINIZIONE DELL'INTERO CICLO DI VITA DEL DATO

02 TRASPARENZA NEI CONFRONTI DELL'INTERESSATO

03 CORRETTEZZA DEI DATI

04 GARANTIRE L'ESERCIZIO DEI DIRITTI

05 SECURITY BY DESIGN

# Accountability e approccio risk-based all'interno del GDPR

## Come garantire la Data Protection By Design e By Default?

Lo sviluppo di adeguati sistemi IT, la digitalizzazione e l'abbandono del cartaceo consentono di soddisfare il principio della protezione dei dati fin dalla progettazione e della protezione dei dati di default (*Data Protection by Design e by Default*) e, nello specifico, di:

- Circoscrivere e limitare l'utilizzo dei dati personali, mediante:
  - L'applicazione di coni di visibilità specifici per mansione
- Consentire nativamente il rispetto dei principi del Regolamento e in particolare:
  - L'applicazione di misure di sicurezza tecniche adeguate al rischio
  - Il controllo sull'intero ciclo di vita del dato (dalla creazione alla cancellazione)
  - L'utilizzo di interfacce con l'interessato per agevolare gli obblighi informativi del Titolare
  - L'utilizzo di modalità automatizzate per consentire l'esercizio dei diritti da parte dell'interessato


# AGENDA

- Il ruolo del medico competente e la salvaguardia del dipendente
- Le recenti pronunce del Garante
- Protezione degli archivi e dei sistemi IT, trasmissione dei dati
- Digitalizzazione dei processi e delle attività di trattamento
- Sistemi innovativi per il trattamento dei dati sanitari sul luogo di lavoro

# Wearable devices sul luogo di lavoro

- Sensori precisi e poco costosi
- Archiviazione e trasmissione dei dati
- Elaborazione in tempo reale delle informazioni

Sviluppo di un mercato potenzialmente molto attraente

# Wearable devices sul luogo di lavoro

- I primi casi d'uso prevedono il «monitoraggio» dello stato di salute di dipendenti in remoto
- Le finalità del trattamento sono prevalentemente di sicurezza

RISCHI!!!

# GRAZIE PER L'ATTENZIONE