

Traccia n. 1

Oggetto: Servizio web a mezzo di piattaforma per l'espletamento delle procedure selettive. Analisi dei Rischi e rilascio parere ai sensi dell'art. 39 Regolamento UE 2016/679 in merito alla necessità, in capo al Titolare del trattamento, di condurre una Valutazione di Impatto (D.P.I.A.).

1. Con la presente comunicazione, si procede ad una "Analisi dei rischi", condotta alla luce delle indicazioni contenute nel Manuale RPD – Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del regolamento generale sulla protezione dei dati dell'Unione Europea (luglio 2019), di cui si comunica l'esito.
2. I rischi oggetto di valutazione non si limitano ai rischi per la sicurezza intesa in senso stretto – cioè alla probabilità e all'impatto di una violazione dei dati – bensì anche ai **rischi per i diritti e le libertà degli interessati (e di altre persone fisiche)** posti dal trattamento. Gli **elementi che compongono la valutazione del rischio** sono stati:
 - ❖ il bene (vulnerabilità e controlli),
 - ❖ la minaccia (profilo dell'agente responsabile della minaccia, probabilità della minaccia)
 - ❖ l'impatto.

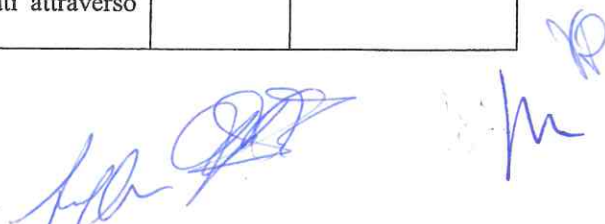
Premesso che una corretta valutazione del rischio prevede quattro fasi:

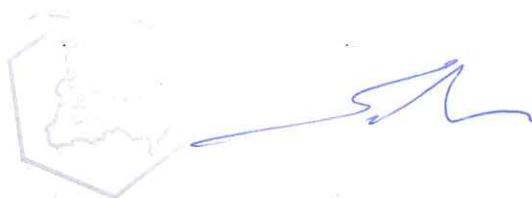
- a) Definizione del trattamento e del relativo contesto
- b) Comprensione e valutazione dell'impatto sulle persone
- c) Definizione di eventuali minacce e valutazione della loro probabilità (probabilità del verificarsi delle minacce)
- d) Valutazione del rischio (attraverso l'associazione di probabilità del verificarsi di minacce e impatto).

Considerato che gli elementi di cui si è a conoscenza sono i seguenti:

- il gestionale di che trattasi è fornito da un soggetto esterno, su piattaforma web, e si interfaccia con altro gestionale già in uso presso la ASL di Pescara; l'accesso avviene previo rilascio di credenziali di autenticazione.
- Il personale che accede al gestionale è inquadrato in ruoli e procedure aziendali; i dati viaggiano su canali sicuri (protocolli di trasmissione https), ma sono in chiaro; il trattamento ha luogo esclusivamente presso i locali della ASL di Pescara; i dati trattati appartengono anche a categorie particolari (art. 9 GDPR) e a condanne penali e reati (art. 10 GDPR).
- Ai dipendenti non è consentito l'utilizzo di dispositivi personali né il trasferimento e/o la memorizzazione dei dati personali al di fuori del perimetro della ASL di Pescara.
- Il numero di persone che utilizza il gestionale – pur in assenza della figura di un Amministratore di Sistema - è definito; gli accessi al gestionale non sono registrati; non si ha evidenza della designazione del Fornitore in qualità di Responsabile/Contitolare del trattamento/autonomo titolare; il personale ha seguito corsi di formazione di base sulla protezione dei dati; non si ha evidenza di report che attestino il rispetto delle specifiche relative alle modalità di conservazione e/o distruzione dei dati.
- La ASL di Pescara non ha subito attacchi cibernetici ma ha rilevato diverse violazioni dei dati personali (data breach) nel corso del presente anno; il numero delle persone fisiche oggetto di trattamento attraverso il gestionale in questione è considerato, nel complesso, relativamente alto.
- In materia di sicurezza applicata al trattamento di che trattasi esistono migliori pratiche.
- Non si hanno evidenze di notifiche e/o reclami relativamente alla sicurezza dei sistemi IT utilizzati.

Valutazione complessiva dell'impatto		
A. Risorse di rete e tecnologiche (hardware e software), barrare le risposte affermative: <ul style="list-style-type: none"> ○ vi sono parti del trattamento svolte attraverso Internet ○ è possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per es., riguardo a certi utenti o gruppi di utenti)? 	Probabilità del verificarsi di minacce	
	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">Livello</td> <td style="width: 50%;">Punteggio</td> </tr> </table>	Livello
Livello	Punteggio	





<ul style="list-style-type: none">○ il sistema di trattamento dati personali è interconnesso a un altro sistema o servizio interno della ASL di Pescara o un servizio IT interno o esterno alla ASL di Pescara?○ è facile per i soggetti non autorizzati accedere all'ambiente di trattamento dati?○ il sistema di trattamento dati personali è progettato, implementato o mantenuto senza seguire le migliori pratiche del settore?		
B. Processi/procedure connessi al trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?○ L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno della ASL di Pescara è definito in modo incerto o insufficiente?○ Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?○ Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro della ASL di Pescara?○ Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?		
C. Soggetti e persone coinvolti nel trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?○ Vi sono parti del trattamento svolte da un soggetto terzo designato Responsabile del trattamento?○ Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?○ Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?○ I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?		
D. Settore di attività e scala del trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ La ASL di Pescara è passibile di attacchi cibernetici?○ La ASL di Pescara ha subito attacchi cybernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?○ Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?○ Il trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?○ Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività della ASL di Pescara che non siano state implementate in misura adeguata?		

n.b.

- Qualora le sottovoci della griglia non siano prese in considerazione negli "elementi di cui si è a conoscenza" essi non vanno conteggiati ma possono essere utilizzati come spunto di riflessione nell'individuazione delle "misure di contenimento dei rischi".

- Nella colonna "Livello" vanno conteggiate le voci ritenute pertinenti per la valutazione del caso in questione; ad es. se nel riquadro "A. Risorse di rete e tecnologiche (hardware e software), barrare le risposte affermative" son pertinenti tre voci va riportato il numero totale: 3

Nella colonna "Punteggio" attenersi alle indicazioni sotto riportate (cfr. paragrafo "Probabilità del verificarsi di minacce (1)")

**Probabilità del verificarsi di minacce (1)**

Area di valutazione	Numero di risposte affermative	Livello	Punteggio
A. Risorse di rete e tecnologiche (hardware e software)	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
B. Processi/procedure connessi al trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
C. Soggetti e persone coinvolti nel trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
D. Settore di attività e scala del trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3

Probabilità del verificarsi di minacce (2)

Somma dei punteggi	Livello di probabilità del verificarsi di minacce
4 - 5	Basso
6 - 8	Medio
9 - 12	Alto

VALUTAZIONE DELL'IMPATTO		
Riservatezza	Integrità	Disponibilità

Nella griglia di cui sopra riportare a quale voce/i l'impatto va ad incidere.

Valutazione del rischio complessivo

PROBABILITA'	LIVELLO DI IMPATTO		
	Basso	Medio	Alto/Molto alto
Bassa			
Media			
Alta			

Legenda

Rischio basso ■ rischio medio ■ rischio elevato ■

Pertanto il rischio è da classificare come

Livello impatto	di	Descrizione
Basso		Piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, irritazione, ecc.)
Medio		Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)
Alto		Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato della salute, ecc.)
Molto Alto		Conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)

In caso di violazione dei dati si pronosticano le seguenti possibili conseguenze significative, che si elencano:

perdita della riservatezza (specificare in dettaglio):

.....

perdita della integrità del dato (specificare in dettaglio):

.....

perdita della disponibilità (specificare in dettaglio):

.....

Indicare le misure di contenimento dei rischi, relativamente alle singole aree di valutazione:

A. Risorse di rete e tecnologiche (hardware e software):

1

.....

2

.....

3

.....

[Handwritten signature]



B. Processi/procedure connessi al trattamento

1
.....
.....

2
.....
.....

3
.....
.....

C. Soggetti e persone coinvolti nel trattamento

1
.....
.....

2
.....
.....

3
.....
.....

D. Settore di attività e scala del trattamento

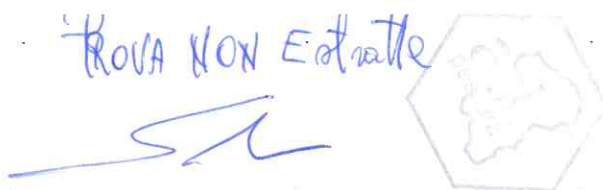
1
.....
.....

2
.....
.....

3
.....
.....

[Handwritten signatures]

ROVA NON Estratte



Traccia n. 2

Oggetto: Percorso Diagnostico Terapeutico Assistenziale (DPTA) del Diabete di tipo 1, di tipo 2 e Gestazionale. Analisi dei Rischi e rilascio parere ai sensi dell'art. 39 Regolamento UE 2016/679 in merito alla necessità, in capo al Titolare del trattamento, di condurre una Valutazione di Impatto (D.P.I.A.).

1. Con la presente comunicazione, si procede ad una "Analisi dei rischi", condotta alla luce delle indicazioni contenute nel Manuale RPD – Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del regolamento generale sulla protezione dei dati dell'Unione Europea (luglio 2019), di cui si comunica l'esito.
2. I rischi oggetto di valutazione non si limitano ai rischi per la sicurezza intesa in senso stretto – cioè alla probabilità e all'impatto di una violazione dei dati – bensì anche ai **rischi per i diritti e le libertà degli interessati (e di altre persone fisiche)** posti dal trattamento. **Gli elementi che compongono la valutazione del rischio sono stati:**
 - ❖ il bene (vulnerabilità e controlli),
 - ❖ la minaccia (profilo dell'agente responsabile della minaccia, probabilità della minaccia)
 - ❖ l'impatto.

Premesso che una corretta valutazione del rischio prevede quattro fasi:

- a) Definizione del trattamento e del relativo contesto
- b) Comprensione e valutazione dell'impatto sulle persone
- c) Definizione di eventuali minacce e valutazione della loro probabilità (probabilità del verificarsi delle minacce)
- d) Valutazione del rischio (attraverso l'associazione di probabilità del verificarsi di minacce e impatto).

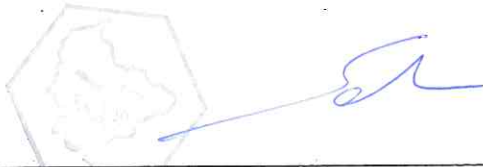
Considerato che gli elementi di cui si è a conoscenza sono i seguenti:

- Il gestionale di che trattasi è fornito da un soggetto esterno, su piattaforma web, e si interfaccia con altro gestionale già in uso presso la ASL di Pescara; l'accesso avviene previo rilascio di credenziali di autenticazione.
- Il personale che accede al gestionale è inquadrato in ruoli e procedure aziendali; i dati viaggiano su canali sicuri (protocolli di trasmissione https), ma sono in chiaro; il trattamento ha luogo esclusivamente presso i locali della ASL di Pescara; i dati trattati appartengono anche a categorie particolari.
- Il numero di persone che utilizza il gestionale – pur in assenza della figura di un amministratore di Sistema - è definito; non si ha evidenza della designazione del Fornitore in qualità di Responsabile/Contitolare del trattamento/autonomo titolare; il personale ha seguito corsi di formazione di base sulla protezione dei dati; non si ha evidenza di report che attestino il rispetto delle specifiche relative alle modalità di conservazione e/o distruzione dei dati.
- La ASL di Pescara non ha subito attacchi cibernetici ma ha rilevato diverse violazioni dei dati (data breach) nel corso del presente anno; il numero delle persone fisiche oggetto di trattamento attraverso il gestionale in questione è considerato, nel complesso, relativamente alto.
- Ai dipendenti non è consentito l'utilizzo di dispositivi personali né il trasferimento e/o la memorizzazione dei dati personali al di fuori del perimetro della ASL di Pescara.
- In materia di sicurezza applicata al trattamento attraverso un sistema di video sorveglianza esistono migliori pratiche.
- Il numero di persone oggetto di trattamento, su base giornaliera, non è da ritenersi consistente.
- Si hanno evidenze di notifiche e/o reclami relativamente alla sicurezza dei sistemi IT utilizzati.

Valutazione complessiva dell'impatto				
A. Risorse di rete e tecnologiche (hardware e software), barrare le risposte affermative: <ul style="list-style-type: none"> ○ vi sono parti del trattamento svolte attraverso Internet ○ è possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per es., riguardo a certi utenti o gruppi di utenti)? 	Probabilità del verificarsi di minacce			
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Livello</td> <td style="width: 50%; text-align: center;">Punteggio</td> </tr> <tr> <td style="height: 40px;"></td> <td style="height: 40px;"></td> </tr> </table>	Livello	Punteggio	
Livello	Punteggio			

1





<ul style="list-style-type: none">○ il sistema di trattamento dati personali è interconnesso a un altro sistema o servizio interno della ASL di Pescara o un servizio IT interno o esterno alla ASL di Pescara?○ è facile per i soggetti non autorizzati accedere all'ambiente di trattamento dati?○ il sistema di trattamento dati personali è progettato, implementato o mantenuto senza seguire le migliori pratiche del settore?		
B. Processi/procedure connessi al trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?○ L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno della ASL di Pescara è definito in modo incerto o insufficiente?○ Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?○ Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro della ASL di Pescara?○ Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?		
C. Soggetti e persone coinvolti nel trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?○ Vi sono parti del trattamento svolte da un soggetto terzo designato Responsabile del trattamento?○ Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?○ Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?○ I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?		
D. Settore di attività e scala del trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ La ASL di Pescara è passibile di attacchi cibernetici?○ La ASL di Pescara ha subito attacchi cybernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?○ Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?○ Il trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?○ Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività della ASL di Pescara che non siano state implementate in misura adeguata?		

n.b.

- Qualora le sottovoci della griglia non siano prese in considerazione negli "elementi di cui si è a conoscenza" essi non vanno conteggiati ma possono essere utilizzati come spunto di riflessione nell'individuazione delle "misure di contenimento dei rischi".

- Nella colonna "Livello" vanno conteggiate le voci ritenute pertinenti per la valutazione del caso in questione; ad es. se nel riquadro "A. Risorse di rete e tecnologiche (hardware e software), barrare le risposte affermative" son pertinenti tre voci va riportato il numero totale: 3

Nella colonna "Punteggio" attenersi alle indicazioni sotto riportate (cfr. paragrafo "Probabilità del verificarsi di minacce (1)")



Probabilità del verificarsi di minacce (1)

Area di valutazione	Numero di risposte affermative	Livello	Punteggio
A. Risorse di rete e tecnologiche (hardware e software)	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
B. Processi/procedure connessi al trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
C. Soggetti e persone coinvolti nel trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
D. Settore di attività e scala del trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3

Probabilità del verificarsi di minacce (2)

Somma dei punteggi	Livello di probabilità del verificarsi di minacce
4 - 5	Basso
6 - 8	Medio
9 - 12	Alto

VALUTAZIONE DELL'IMPATTO		
Riservatezza	Integrità	Disponibilità

Nella griglia di cui sopra riportare a quale/i voce/i l'impatto va ad incidere.

Valutazione del rischio complessivo

PROBABILITA'	LIVELLO DI IMPATTO		
	Basso	Medio	Alto/Molto alto
Bassa			
Media			
Alta			

Legenda

Rischio basso ■ rischio medio ■ rischio elevato ■

Pertanto il rischio è da classificare come



Livello di impatto	Descrizione
Basso	Piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, irritazione, ecc.)
Medio	Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)
Alto	Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato della salute, ecc.)
Molto Alto	Conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)

In caso di violazione dei dati si pronosticano le seguenti possibili conseguenze significative, che si elencano:

perdita della riservatezza (specificare in dettaglio):

.....

perdita della integrità del dato (specificare in dettaglio):

.....

perdita della disponibilità (specificare in dettaglio):

.....

Indicare le misure di contenimento dei rischi, relativamente alle singole aree di valutazione:

A. Risorse di rete e tecnologiche (hardware e software):

1

.....

2

.....

3

.....

[Handwritten signature]



B. Processi/procedure connessi al trattamento

1

.....
.....

2

.....
.....

3

.....
.....

C. Soggetti e persone coinvolti nel trattamento

1

.....
.....

2

.....
.....

3

.....
.....

D. Settore di attività e scala del trattamento

1

.....
.....

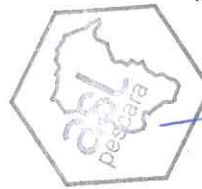
2

.....
.....

3

.....
.....

[Handwritten signatures and initials]



KROVA Non Entrate
Sh

Traccia n. 3

Oggetto: Servizio di video sorveglianza. Analisi dei Rischi e rilascio parere ai sensi dell'art. 39 Regolamento UE 2016/679 in merito alla necessità, in capo al Titolare del trattamento, di condurre una Valutazione di Impatto (D.P.I.A.).

1. Con la presente comunicazione, si procede ad una "Analisi dei rischi", condotta alla luce delle indicazioni contenute nel Manuale RPD – Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del regolamento generale sulla protezione dei dati dell'Unione Europea (luglio 2019), di cui si comunica l'esito.
2. I rischi oggetto di valutazione non si limitano ai rischi per la sicurezza intesa in senso stretto – cioè alla probabilità e all'impatto di una violazione dei dati – bensì anche ai **rischi per i diritti e le libertà degli interessati (e di altre persone fisiche)** posti dal trattamento. **Gli elementi che compongono la valutazione del rischio sono stati:**

- ❖ il bene (vulnerabilità e controlli),
- ❖ la minaccia (profilo dell'agente responsabile della minaccia, probabilità della minaccia)
- ❖ l'impatto.

Premesso che una corretta valutazione del rischio prevede quattro fasi:

- a) Definizione del trattamento e del relativo contesto
- b) Comprensione e valutazione dell'impatto sulle persone
- c) Definizione di eventuali minacce e valutazione della loro probabilità (probabilità del verificarsi delle minacce)
- d) Valutazione del rischio (attraverso l'associazione di probabilità del verificarsi di minacce e impatto).

Considerato che gli elementi di cui si è a conoscenza sono i seguenti:

- Il gestionale di che trattasi è fornito da un soggetto esterno, su piattaforma web, con possibilità di interfacciamento con il gestionale dei controlli degli accessi già in uso presso la ASL di Pescara; l'accesso avviene previo rilascio di credenziali di autenticazione.
- Il personale che accede al gestionale è inquadrato in ruoli e procedure aziendali; i dati viaggiano su canali sicuri (protocolli di trasmissione https), ma sono in chiaro; non è presente un canale di trasmissione delle immagini dedicato, ma il trasferimento avviene attraverso la LAN aziendale; il trattamento ha luogo esclusivamente presso i locali della ASL di Pescara; i dati trattati appartengono anche a categorie particolari.
- Il numero di persone che utilizza il gestionale è definito; il Fornitore è stato designato in qualità di Responsabile; il personale ha seguito corsi di formazione di base sulla protezione dei dati; non si ha evidenza di report che attestino il rispetto delle specifiche relative alle modalità di conservazione e/o distruzione dei dati; non si ha, altresì, evidenza se il principio di minimizzazione sia applicato alle riprese video.
- Il numero di persone riprese, su base giornaliera, è da ritenersi consistente.
- La ASL di Pescara non ha subito attacchi cibernetici ma ha rilevato diverse violazioni dei dati (data breach) nel corso del presente anno; il numero delle persone fisiche oggetto di trattamento attraverso il gestionale in questione è considerato, nel complesso, relativamente alto.
- Alcune telecamere sono installate all'interno degli uffici per riprendere l'attività svolta dai lavoratori, al fine di tutelarne la sicurezza (camere sterili, ecc.)
- In materia di sicurezza applicata al trattamento attraverso un sistema di video sorveglianza esistono migliori pratiche.
- Non si hanno evidenze di notifiche e/o reclami relativamente alla sicurezza dei sistemi IT utilizzati.
- Ai dipendenti non è consentito l'utilizzo di dispositivi personali né il trasferimento e/o la memorizzazione dei dati personali al di fuori del perimetro della ASL di Pescara.

Valutazione complessiva dell'impatto		
A. Risorse di rete e tecnologiche (hardware e software), barrare le risposte affermative: <input type="radio"/> vi sono parti del trattamento svolte attraverso Internet	Probabilità del verificarsi di minacce	
	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">Livello</td> <td style="width: 50%;">Punteggio</td> </tr> </table>	Livello
Livello	Punteggio	

[Handwritten signatures]

[Handwritten mark]



<ul style="list-style-type: none">○ è possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per es., riguardo a certi utenti o gruppi di utenti)?○ il sistema di trattamento dati personali è interconnesso a un altro sistema o servizio interno della ASL di Pescara o un servizio IT interno o esterno alla ASL di Pescara?○ è facile per i soggetti non autorizzati accedere all'ambiente di trattamento dati?○ il sistema di trattamento dati personali è progettato, implementato o mantenuto senza seguire le migliori pratiche del settore?		
B. Processi/procedure connessi al trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?○ L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno della ASL di Pescara è definito in modo incerto o insufficiente?○ Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?○ Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro della ASL di Pescara?○ Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?		
C. Soggetti e persone coinvolti nel trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?○ Vi sono parti del trattamento svolte da un soggetto terzo designato Responsabile del trattamento?○ Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?○ Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?○ I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?		
D. Settore di attività e scala del trattamento, barrare le risposte affermative: <ul style="list-style-type: none">○ La ASL di Pescara è passibile di attacchi cibernetici?○ La ASL di Pescara ha subito attacchi cibernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?○ Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?○ Il trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?○ Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività della ASL di Pescara che non siano state implementate in misura adeguata?		

n.b.

- Qualora le sottovoci della griglia non siano prese in considerazione negli "elementi di cui si è a conoscenza" essi non vanno conteggiati ma possono essere utilizzati come spunto di riflessione nell'individuazione delle "misure di contenimento dei rischi".

- Nella colonna "Livello" vanno conteggiate le voci ritenute pertinenti per la valutazione del caso in questione; ad es. se nel riquadro "A. Risorse di rete e tecnologiche (hardware e software), barrare le risposte affermative" son pertinenti tre voci va riportato il numero totale: 3

Nella colonna "Punteggio" attenersi alle indicazioni sotto riportate (cfr. paragrafo "Probabilità del verificarsi di minacce (1)")



Handwritten signature

Probabilità del verificarsi di minacce (1)

Area di valutazione	Numero di risposte affermative	Livello	Punteggio
A. Risorse di rete e tecnologiche (hardware e software)	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
B. Processi/procedure connessi al trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
C. Soggetti e persone coinvolti nel trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3
D. Settore di attività e scala del trattamento	0 - 1	Basso	1
	2 - 3	Medio	2
	4 - 5	Alto	3

Probabilità del verificarsi di minacce (2)

Somma dei punteggi	Livello di probabilità del verificarsi di minacce
4 - 5	Basso
6 - 8	Medio
9 - 12	Alto

VALUTAZIONE DELL'IMPATTO		
Riservatezza	Integrità	Disponibilità

Nella griglia di cui sopra riportare a quale/i voce/i l'impatto va ad incidere.

Valutazione del rischio complessivo

PROBABILITA' MINACCE	LIVELLO DI IMPATTO		
	Basso	Medio	Alto/Molto alto
Bassa			
Media			
Alta			

Legenda

Rischio basso ■ rischio medio ■ rischio elevato ■■

Pertanto il rischio è da classificare come

Handwritten signatures and initials



Livello impatto	di	Descrizione
Basso		Piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, irritazione, ecc.)
Medio		Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)
Alto		Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato della salute, ecc.)
Molto Alto		Conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)

In caso di violazione dei dati si pronosticano le seguenti possibili conseguenze significative, che si elencano:

perdita della riservatezza (specificare in dettaglio):

.....
.....

perdita della integrità del dato (specificare in dettaglio):

.....
.....

perdita della disponibilità (specificare in dettaglio):

.....
.....

Indicare le misure di contenimento dei rischi, relativamente alle singole aree di valutazione:

A. Risorse di rete e tecnologiche (hardware e software):

1

.....
.....

2

.....
.....

3

.....
.....



B. Processi/procedure connessi al trattamento

1

.....
.....

2

.....
.....

3

.....
.....

C. Soggetti e persone coinvolti nel trattamento

1

.....
.....

2

.....
.....

3

.....
.....

D. Settore di attività e scala del trattamento

1

.....
.....

2

.....
.....

3

.....
.....