Valutazione d'impatto sulla protezione dei dati - DPIA

Attività di trattamento **Gestione del rapporto contrattuale di lavoro, registrazione delle presenze**
Soggetti interessati Dipendenti

Titolare del trattamento	Rappresentante Legale
Centro Medico Ascione S.R.L. **Via Napoli, 35/37 – Torre del Greco (NA)** **P.IVA 03983920632**	**ASCIONE ANDREA**

Redatta in collaborazione con il Responsabile della Protezione dei Dati

Rev. 1 del 07/01/2020 – pagine totali 14

Sommario

Nozione di valutazione d'impatto

Il Data Protection Impact Assessment (DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Si tratta di una valutazione preliminare eseguita dal Titolare del trattamento dei dati relativamente agli impatti di un trattamento laddove dovessero essere violate le misure di protezione.
Il DPIA va inquadrato come uno strumento essenziale e fondamentale al fine di dar corso al nuovo approccio alla protezione dei dati personali richiamato dal regolamento europeo e fortemente basato sul principio della accountability.

Quadro normativo

- REGOLAMENTO 2016/679/UE: Articoli 35 e 36
- Considerando C84, C89, C90, C91, C92, C93, C94, C95
- WP248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679
- provvedimento Garante n. 467 dell'11.10.2018 – G.U. 269 del 19.11.2018

Motivi della valutazione d'impatto

L'attività di trattamento oggetto della presente valutazione d'impatto – DPIA considerati la natura, l'oggetto, il contesto e le finalità del trattamento, potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche secondo i criteri di cui all'art.35, c. 3 del GDPR 2016/679.
Il trattamento ricade nelle seguenti due categorie per le quali si rende necessario lo sviluppo di un processo di valutazione di impatto in base alle indicazioni della linea guida WP248:

- dati sensibili o dati aventi carattere altamente personale
- dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati può causare squilibrio di potere tra il titolare del trattamento e gli interessati, che potrebbero non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.

E' inoltre compresa nell'elenco di trattamenti soggetti al requisito di una valutazione d'impatto redatto dall'Autorità di controllo nazionale (Garante per la Privacy – provvedimento 467/18 - allegato 1- punto 6. "Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)).

Metodo di conduzione della DPIA

Scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battuta comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA.
Il presente documento comprende, principalmente:

- una descrizione sistematica del trattamento previsto e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati.

In ossequio al principio del *data protection by design* il Titolare del Trattamento ha consultato il Responsabile della Protezione dei Dati circa:

- se condurre o meno la presente DPIA
- se condurre la DPIA con risorse interne o esternalizzandola
- quale metodologia adottare per la conduzione della stessa
- quali salvaguardie applicare per attenuare i rischi per i diritti e gli interessi delle persone interessate

Il Responsabile della Protezione dei Dati si è espresso favorevolmente sulla correttezza della conduzione della DPIA e sulla conformità alle normative vigenti delle conclusioni raggiunte.

Valutazione preliminare

FASE 1 - Descrizione del trattamento

Soggetti interessati

Dipendenti della Società

Finalità del trattamento

I dati personali oggetto della presente analisi sono trattati nell'ambito della normale attività svolta dalla scrivente organizzazione per la gestione del rapporto lavorativo con i dipendenti

Descrizione del trattamento e flussi informativi

Il trattamento riguarda attività correlate alla gestione delle presenze del personale.

Dati oggetto del trattamento

Dati anagrafici, dati sensibili anche biometrici

Modalita' di trattamento

Con ausilio di strumenti elettronici

Operazioni eseguite

Raccolta, registrazione conservazione estrazione, consultazione, utilizzo, raffronto, limitazione, cancellazione, distruzione.

Conservazione dei dati trattati

I dati sono conservati in archivi elettronici

Processi aziendali coinvolti nel trattamento

Il trattamento viene svolto nel comparto amministrazione

FASE 2 - Valutazione della conformita'

Modalita' di raccolta dei dati
Raccolta diretta presso l'interessato e/o acquisizione da altri soggetti.

Soggetti che hanno accesso ai dati
Titolare del trattamento e incaricati del trattamento opportunamente individuati
Nello svolgimento delle proprie funzioni istituzionali l'Azienda potrebbe comunicare anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.

Modalita'di trasferimento dei dati a soggetti terzi
In formato elettronico o cartaceo.

Modalita' di aggiornamento e eliminazione dei dati
E' previsto l'aggiornamento periodico delle banche dati aziendali , in particolare per quanto riguarda i dati sensibili, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi.
I dati informatici non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.
I documenti cartacei riportanti dati non più occorrenti vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili.
I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti.

Motivazione legittima per il trattamento (anche per categorie speciali di dati)/base giuridica del trattamento
Consenso; adempimento di obblighi precontrattuali e contrattuali; obblighi di legge cui è soggetto il titolare del trattamento; interessi vitali della persona interessata.

Modalità di offerta di informativa agli interessati e di raccolta del consenso
Su modulistica predisposta a livello aziendale: precedentemente alla raccolta dei dati;

Utilizzo per nuove/diverse finalità di dati personali già raccolti
Non è previsto

Modalità di verifica della accuratezza dei dati personali raccolti e trattati
Verifiche documentali;

Asset model a sostegno dei trattamenti
Hardware, software, archivi, reti e piattaforme aziendali.

Periodo massimo di conservazione dei dati
I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di rapporti di lavoro.

Misure di sicurezza a garanzia della riservatezza dei dati / per prevenire trattamenti di dati personali non autorizzati o illegittimi
organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative
fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti

logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione; CRITTOGRAFIA; ANONIMIZZAZIONE .

Trasferimento di dati personali in un paese non facente parte dell'unione europea

Non è previsto

Diritti degli interessati

L'interessato ha diritto di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento; può inoltre opporsi al trattamento ed esercitare il diritto alla portabilità dei dati forniti e trattati in via automatizzata, con il consenso dell'interessato o sulla base di contratto stipulato fra le parti. I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
È diritto dell'interessato proporre reclamo avverso il trattamento dei dati operato dall'Azienda alla competente Autorità di Controllo (Garante per la protezione dei dati personali), ovvero ricorso dinanzi all'Autorità Giudiziaria.

Il trattamento rispetta

- i principi di liceità, correttezza e trasparenza
- il principio di limitazione della finalità
- il principio di minimizzazione dei dati
- il principio di esattezza dei dati
- il principio di limitazione della conservazione dei dati
- il diritto di informazione
- il diritto di accesso ai dati
- il diritto di portabilità
- il diritto di rettifica
- il diritto di cancellazione (diritto all'oblio)
- il diritto di limitazione del trattamento
- il diritto di opposizione al trattamento

FASE 3 - CONDURRE LA DPIA?

Le risultanze della valutazione preliminare dianzi condotta non paiono evidenziare la sussistenza di rischi g r a v i aventi particolare impatto su diritti e libertà delle persone i cui dati sono oggetto di trattamento. Alla luce di tali considerazioni, si ritiene che eventuali rischi possano ritenersi sostanzialmente nel complesso **accettabili.**
In ogni caso, siccome il trattamento prevede l'uso di nuove tecnologie, l'Azienda - anche in considerazione della rilevante delicatezza dei dati trattati - ritiene comunque utile la conduzione di attività di miglior approfondimento della valutazione in questione.

Quindi, la tabella seguente illustra i principali rischi afferenti alla protezione dei dati, che si ritengono identificabili in fase di valutazione preliminare, correlati ad eventi relativi al contesto in cui si opera o relativi agli strumenti, oppure a comportamenti degli operatori:

Descrizione del rischio
Danneggiamento/ perdita/distruzione non autorizzata dati personali
Accesso non autorizzato dati personali
Trattamento non autorizzato (comprensivo di modifica, divulgazione……)
Trattamento non conforme alla finalità della raccolta o illecito

Esecuzione DPIA

Fase 1 - Informazioni integrative per analisi del rischio

(in aggiunta a quanto già esposto in sede di valutazione preliminare, cui si rimanda)

Tecnologie utilizzate

Per il trattamento dei dati vengono integrati n° 3 rilevatori di presenze capaci di rilevare l'impronta digitale; quest'ultima – tuttavia – non viene associata direttamente ad un dato anagrafico .

Coinvolgimento di altre strutture

L'iniziativa di trattamento non coinvolge altre strutture.

Modifiche alle modalità di trattamento dei dati

I dati personali, afferenti all'interessato, già presenti in un esistente data base, verranno interconnessi con i dati registrati dalle predette apparecchiature. L'interconnessione avviene su una sola postazione informatica, protetta da doppia chiave di accesso, munita di sistema di crittografia , firewall, antivirus e salvataggio dei dati.

Modifiche alle procedure di trattamento dei dati

Il trattamento introduce nuove modalità e procedure di raccolta dei dati, che tuttavia saranno rese trasparenti agli interessati.

Il trattamento introdurrà nuove procedure sicure di accesso ai dati e stringenti modalità di consultazione.

Il trattamento non introdurrà nuove o modificate modalità di conservazione dei dati, che possano essere non chiare o prolungate oltremodo.

Esenzioni dalla applicazione delle disposizioni del regolamento

L'attività di trattamento non esula dall'ambito delle disposizioni legislative dell'unione europea, non è svolto da una persona fisica esclusivamente per fini personali e familiari e non è svolta da autorità pubbliche al fine di prevenzione, indagine, individuazione e perseguimento di reati o al fine di applicare pene.

Fase 2 - Valutazione del rischio

a) metodologia di valutazione

L'analisi del rischio è un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione su uno o più asset aziendali ben precisi. Serve inoltre a giustificare le contromisure, a valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto e in grado di rispondere in tempo alle minacce. Tale analisi ha come obiettivo minimizzare la probabilità di accadimento dei rischi e gli impatti che possibili violazioni dei dati personali potrebbero comportare agli individui, come di seguito esemplificativamente sintetizzati:

Rischi: distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati personali.

Impatto:

- da violazione della sicurezza fisica
- da violazione dei dati di identificazione o attinenti l'identità personale
- materiale (perdite finanziarie o al patrimonio)
- morale o biologico (turbamento per la diffusione di una notizia riservata, compromissione di uno stato salute, evento lesivo di diritti umani o integrità della persona)
- sociale (conseguenze di tipo discriminatorio, perdite di autonomia)

La DPIA si basa su un'analisi dei rischi centrata su
- rischi derivanti da contenuto intrinseco del trattamento
- rischi derivanti da possibili violazioni di sicurezza

in relazione ai possibili controlli applicabili, ricavando, così, un **indice di rischio "normalizzato"** rispetto al contesto aziendale.

Il rischio normalizzato RN viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f(P, C, V)$$

dove:

P = probabilità (stima della probabilità di accadimento degli eventi che causano la perdita, violazione, distribuzione non controllata di dati = **pericoli**)

C = conseguenze generate dall'evento (stima della gravità dei danni attesi rispetto all'accadimento di un determinato evento)

V = vulnerabilità rispetto al grado di adeguatezza delle misure (grado di adeguatezza delle misure che contrastano il manifestarsi degli eventi)

In prima battuta viene ricavato il **rischio intrinseco Ri** come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITÀ	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze C è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

La **matrice** che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

PROBABILITA'	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

Per ricavare il **Rischio Normalizzato RN**, viene introdotto il fattore Vulnerabilità che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla vulnerabilità V è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		VALORE
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

□ 0,25; □ 0,5; □ 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

VULNERABILITA'	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		RISCHIO INTRINSECO			

RISCHIO NORMALIZZATO	
RN = Ri x V	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

b) definizione di aree di pericolo, rischi generati e valutazione del livello di rischio intrinseco

Di seguito la suddivisione delle principali aree di pericolo con i rischi generati, e le relative stime su probabilità di accadimento e conseguenze:

PERICOLO	RISCHI	PROBABILITA' stimata	CONSEGUENZE stimate
Agenti fisici (incendio, allagamento, attacchi esterni)	□ Danneggiamento □ Perdita □ Distruzione non autorizzata	□ Improbabile	□ Limitate
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	□ Danneggiamento □ Perdita □ Distruzione non autorizzata	□ Improbabile	□ Limitate
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	□ Danneggiamento □ Perdita □ Distruzione non autorizzata	□ Poco probabile	□ Limitate
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	□ Danneggiamento □ Perdita □ Distruzione non autorizzata □ Accesso dati non autorizzato	□ Poco probabile	□ Limitate
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	□ Perdita □ Distruzione non autorizzata □ Accesso dati non autorizzato	□ Poco probabile	□ Limitate
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	□ Danneggiamento □ Perdita □ Distruzione non autorizzata □ Accesso dati non autorizzato □ Trattamento non autorizzato □ Trattamento non conforme alla finalità della raccolta o illecito	□ Poco probabile	□ Limitate

Rischio intrinseco *(valutato sulla base della media dei valori peggiori di probabilità e conseguenza stimati per rischio specifico)*

□ RISCHIO: Danneggiamento / Perdita / Distruzione non autorizzata		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante

RISCHIO: Accesso non autorizzato		
PROBABILITA’	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante

RISCHIO: Trattamento non autorizzato		
PROBABILITA’	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante

RISCHIO: Trattamento non conforme alla finalità della raccolta o illecito		
PROBABILITA’	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante

c) valutazione dell’idoneità delle misure di sicurezza tecniche e organizzative a rendere il rischio accettabile

TRATTAMENTO CON L’AUSILIO DI STRUMENTI ELETTRONICI

Rischio	**Misure**	**Idoneità**
danneggiamento, distruzione o perdita del dato	- effettuazione di copie di sicurezza, salvataggio settimanale dei dati, backup centralizzato periodico, aggiornamento annuale dei programmi di protezione per elaboratore (semestrale per trattamento di dati sensibili o giudiziari) - effettuazione di backup full dei database dei gestionali giornalieri conservando gli ultimi 7 - crittografia dei dati - doppio livello di autenticazione - effettuazione periodica di restore (dei dati di backup) del database del gestionale principale; - ripristino periodico di snapshot. - utilizzo di infrastrutture servite da alimentazione privilegiata (gruppo elettrogeno) ed UPS per i sistemi di produzione	ADEGUATE

accesso non autorizzato (ai locali, al sistema ed ai dati)	- i server aziendali sono collocati in locali chiusi a chiave (porte blindate o tradizionali), di norma senza finestre e in taluni casi dotati di telecamera IP con registrazione remota - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate - assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate - adozione di sistema di gestione degli utenti che associa il data base degli stessi con le rispettive autorizzazioni, disponibile centralmente in rete al fine di un eventuale recupero su richiesta dei soggetti autorizzati al trattamento dei dati - firewall di rete - sistema di anonimizzazione dei dati biometrici - crittografia dei dischi di rete - utilizzo di salvaschermo protetti da password in caso di inattività	ADEGUATE
	- tutti i PC fissi e mobili e gli elaboratori sono coperti da sistemi di rilevamento e di prevenzione delle intrusioni e anti-hackers, firewall di sistema, antivirus, antispyware la cui efficacia è periodicamente verificata ed aggiornata	
trattamento non autorizzato	- ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore - di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative	ADEGUATE
trattamento non conforme alla finalità della raccolta o illecito	- è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.	ADEGUATE

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Rischio	**Misure**	**Idoneità**
accesso non autorizzato	- la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro - i documenti contenenti dati sensibili, se affidati all'incaricato del trattamento, devono da questo essere conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio - l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni - i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro - fare attendere soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, avere cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c. - evitare l'esportazione di dati personali e/o l'installazione degli stessi su attrezzature diverse da quelle messe a disposizione dall'Azienda (ad es.	ADEGUATE

	computer di casa)	
<u>trattamento non autorizzato</u>	- gli incaricati al trattamento sono autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento - divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Azienda avviene in modo da garantirne la riservatezza	ADEGUATE
<u>trattamento non conforme alla finalità della raccolta o illecito</u>	- i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo - è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili. - i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti	ADEGUATE

d) valutazione rischio normalizzato (sulla base del valore peggiore assegnato alle misure di sicurezza relativamente al rischio specifico).

RISCHIO: Danneggiamento / Perdita / Distruzione non autorizzata		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

RISCHIO: Accesso non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

RISCHIO: Trattamento non autorizzato		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante

VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

RISCHIO: Trattamento non conforme alla finalità della raccolta o illecito		
PROBABILITA'	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il rischio*		
RISCHIO INTRINSECO	VULNERABILITA'	RISCHIO NORMALIZZATO
Rilevante	0,25	BASSO

Risultati DPIA

A valle dell'indagine DPIA condotta l'attività ricade in fascia BASSA.

Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati

Secondo le buone prassi, è opportuno che la presente valutazione d'impatto venga riesaminata periodicamente, e particolarmente quando nell'intervallo di tempo trascorso dal completamento della DPIA si siano verificate delle modifiche nei rischi connessi al trattamento o vengano messe in evidenza delle anomalie.
A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale che debbono indurre ad una revisione della DPIA:
- Cambiamento sulle attività di trattamento, in termini di:
  - Contesto o finalità del trattamento,
  - Tipologia di dati personali trattati
  - Destinatari o modalità di raccolta dei dati personali
  - Combinazioni di dati provenienti da fonti differenti
  - Trasferimento di dati all'estero
- Modifica ai rischi con impatto sui diritti degli interessati derivati da:
  - Presenza di nuove minacce
  - Modifica ai sistemi informativi a supporto del trattamento
  - Soppressione di contromisure esistenti
  - Nuovi scenari di rischio
  - Nuovi potenziali impatti sulle dimensioni di analisi (Riservatezza, Integrità, Disponibilità)
  - Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

Inoltre, si rende comunque necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in esser