ISTITUTO COMPRENSIVO STATALE IGEA

Sede legale: Via Nicolò Zeno, 21 – 47814 Igea (RN)

Sede operativa: Via Nicolò Zeno, 21 – 47814 Igea (RN)

Accettazione:

LA REDAZIONE DEL PRESENTE DOCUMENTO DI VALUTAZIONE D'IMPATTO È STATA ESEGUITA ED ACCETTATA DAL TITOLARE DEL TRATTAMENTO E DAL RESPONSABILE DEL TRATTAMENTO (*ai sensi dell'art. 35, del GDPR 2016/679*) CON LA CONSULTAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI OVE PREVISTO:

Titolare del trattamento: ***ISTITUTO COMPRENSIVO STATALE IGEA*** *Firma e Timbro* _____

Responsabile del trattamento: *Dott.ssa Myriam Toccafondo* *Firma e Timbro* _____

Responsabile della protezione dei dati: *Ing. Michele Manaresi* *Firma e Timbro* _____

Data certa:

QUESTO DOCUMENTO È COMPOSTO DA N.° _____ PAGINE.

Data _____ - _____ - _____
Scadenza _____ - _____ - _____

Data	*Revisione*	*Realizzazione*	*Approvazione*	*Commessa*
21/01/2019	*0*	*M. Ercolani*	*Ing. M. Manaresi*	*F.L.714-18*

INDICE

PREMESSA 3
DESCRIZIONE AZIENDALE 3
L'istituto svolge attività didattiche finalizzate alla fornitura di servizi scolastici. 3
VALUTAZIONE DELL'IMPATTO 4
ATTIVITÀ CHE RICHIEDONO LA REALIZZAZIONE DELLA VALUTAZIONE D'IMPATTO 5
RELAZIONE DPIA 6
ANALISI TRASVERSALE 39
CONCLUSIONI 46
SCADENZA DEL DOCUMENTO 47
ALLEGATI 48
DEFINIZIONI 49
FONTI NORMATIVE 55

PREMESSA

Il presente documento di valutazione d'impatto vuole ottemperare a quanto indicato dall'art. 35 del Regolamento UE 2016/679 (di seguito chiamato GDPR – General Data Protection Regulation).

Inoltre, costituisce parte integrante del presente documento, il Registro delle attività di trattamento (art. 30 – GDPR) e la Valutazione del rischio (D.V.R.) (art 32 – GDPR).

La Valutazione d'Impatto va effettuata per tutti quei trattamenti che per le caratteristiche attuative (ambito, finalità, dati personali raccolti, identità di titolari o destinatari, periodi di conservazione dei dati, misure tecniche e organizzative, ecc.) possono presentare un rischio elevato.

DESCRIZIONE AZIENDALE

L'istituto svolge attività didattiche finalizzate alla fornitura di servizi scolastici.

VALUTAZIONE DELL'IMPATTO

Art 35 GDPR 679/2016: "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura dell'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

- Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- Il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- La sorveglianza su larga scala di una zona accessibile al pubblico.

La valutazione contiene almeno:

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- Una valutazione delle necessità e proporzionalità dei trattamenti in relazione alle finalità (minimizzazione dei dati);
- Una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
- 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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione

Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività di trattamento."

ATTIVITÀ CHE RICHIEDONO LA REALIZZAZIONE DELLA VALUTAZIONE D'IMPATTO

1. GESTIONE DI CATEGORIE PARTICOLARI DI DATI PERSONALI DEGLI ALUNNI E DELLE FAMIGLIE DEGLI ALUNNI;
2. GESTIONE CATEGORIE PARTICOLARI DI DATI PERSONALI DEL PERSONALE INTERNO;
3. GESTIONE CATEGORIE PARTICOLARI DI DATI PERSONALI DEGLI ESPERTI ESTERNI.

RELAZIONE DPIA

Informazioni sulla PIA

Nome della PIA
IST. STATALE IGEA

Nome autore
Ercolani Martina

Nome valutatore
Manaresi Michele

Nome validatore
Manaresi Michele

Data di creazione
22/01/2019

Nome del DPO/RPD
Michele Manaresi

Parere del DPO/RPD
in quanto si ritiene che le misure di sicurezza adottate siano idonee a garantire la sicurezza dei dati.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
non richiesto.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Gestione attività che comportano la gestione di categorie particolari di dati personali degli alunni e delle famiglie degli alunni.

Il Titolare del Trattamento è l'ISTITUTO COMPRENSIVO STATALE IGEA e il Responsabile del Trattamento è la Dott.ssa Myriam Toccafondo.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità sono regolamentate internamente a mezzo di lettere di autorizzazione sottoposte dal responsabile del trattamento ai dipendenti incaricati ad effettuare l'attività in oggetto. Il responsabile del trattamento ha altresì firmato la lettera di nomina rilasciata dal titolare del trattamento.

Ci sono standard applicabili al trattamento?

I dipendenti si attengono ai contenuti dell'accordo tra le parti per regolamentare il rapporto di dipendenza che hanno sottoscritto.
Il responsabile del trattamento ed il responsabile della protezione dei dati ne verificano periodicamente la corretta applicazione.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Categorie particolari di dati personali come indicato dagli articoli 9 e 10 del GDPR 679/2016.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Tutti i dati vengono conservati su server, presso il comune di Bellaria-Igea, in rete protetto da PSW aggiornata periodicamente e a conoscenza del personale di segreteria.
Tutti i dati cartacei e digitali vengono conservati secondo norme di legge, presente segreteria digitale "NUVOLA".

I dati verranno trasmessi all'AUSL (riceve assolvimento degli obblighi vaccinali, e dati sanitari degli alunni)

I dati (nome, cognome, C.F. data di nascita e voti per erogazione delle borse di studio) verranno trasmessi al comune. I dati degli alunni non frequentanti per l'adempimento dell'obbligo scolastico vengono inviati al comune e ad altre pubbliche amministrazioni.

I dati (fascicolo personale degli alunni (verranno trasmessi ad altre pubbliche

Amministrazioni su richiesta in base alle pratiche.

L'INAIL e l'assicurazione ricevono i dati inerenti alla malattia o infortuni.

I dati sono presenti anche sulla piattaforma ministeriale "SIDI".

Sul "SIDI" sono presenti anche l'anagrafe nazionale degli studenti.

Le deleghe fornite a inizio anno vengono conservate per l'anno scolastico dai docenti presso le scuole primarie e di infanzia, mentre per le scuole secondarie presso gli uffici.

In caso di consegna di alunni minori a soggetti genitori (tutori o delegati) i collaboratori prendono visione del documento di identità di chi ritira l'alunno e fanno firmare allo stesso un "registro" interno.

Quali sono le risorse di supporto ai dati?

I dati sono presenti in formato cartaceo e digitale.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono indicate in modo specifico ed esplicito all'interno dell'informativa che viene sottoposta agli interessati.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La raccolta dei dati è necessaria per l'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e per assolvere ad obblighi di legge.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono quelli strettamente necessari all'attività svolta dal Titolare del Trattamento.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Gli interessati, in qualsiasi momento, possono chiedere al Titolare del trattamento la correzione e l'aggiornamento dei dati che lo riguardano. Per questo motivo si ritiene che i dati trattati siano esatti e aggiornati.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati sono conservati per i tempi previsti dalla legge.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Agli interessati viene sottoposta l'informativa con la richiesta di rilascio di consenso per ogni singola finalità.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

I dati sono trattati per assolvere a un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e per assolvere ad obblighi di legge in capo al titolare del trattamento.

Agli interessati viene comunque richiesto il consenso, in forma scritta, viene richiesto il consenso di entrambi i titolari della proprietà genitoriale.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

È presente un modello con cui l'interessato può richiedere al Titolare/Responsabile del trattamento di esercitare i propri diritti così come indicati all'interno dell'informativa.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

non applicabile.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

È presente un modello con cui l'interessato può richiedere al Titolare/Responsabile del trattamento di esercitare i propri diritti così come indicati all'interno dell'informativa.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del Responsabile del trattamento sono indicati nella lettera di nomina scritta, firmata dallo stesso per accettazione dell'incarico.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

non applicabile.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Controllo degli accessi logici

Credenziali personali per accedere al "SIDI" e a "NUVOLA" su cui sono contenuti i dati.

Valutazione : Accettabile

Archiviazione

Archivi cartacei chiusi a chiave.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

Cartelle personali degli studenti chiusi a chiave in possesso solo al titolare/responsabile del trattamento e agli autorizzati al trattamento.

Valutazione : Accettabile

Lotta contro il malware

Presenti e aggiornati antivirus e firewall.

Valutazione : Accettabile

Gestione postazioni

Tutti i terminali sono protetti da PSW.

Valutazione : Accettabile

Backup

Backup a carico del comune.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Lettera di nomina del Responsabile del Trattamento, firmata dallo stesso per accettazione dell'incarico.

Valutazione : Accettabile

Sicurezza dei canali informatici

Rete WIFI a carico del comune, che invia credenziali personali di accesso a ogni utente.

Valutazione : Accettabile

Controllo degli accessi fisici

L'accesso ai locali è consentito solo se accompagnati da personale autorizzato.

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Presente allarme antifurto

Valutazione : Accettabile

Politica di tutela della privacy

E' stato nominato un Responsabile della Protezione dei Dati esterno ed è stata effettuata la comunicazione dei suoi dati di contatto al Garante come indicato dall'articolo 37 del GDPR 679/2016.

Valutazione : Accettabile

Gestione delle politiche di tutela della privacy

Presente modulistica per regolamentare i rapporti con i dipendenti interni che accedono ai dati (Mod.0.3 accordo tra le parti per il rapporto di dipendenza - Mod.0.4 lettere di autorizzazione).

Valutazione : Accettabile

Gestione dei rischi

E' stata effettuata la Valutazione dei Rischi come indicato dall'articolo 32 del GDPR 679/2016.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Presente modulistica per regolamentare i rapporti con i terzi che accedono ai dati (Mod.0.2 accordo tra le parti, liberatoria).

Valutazione : Accettabile

Vigilanza sulla protezione dei dati

Sopralluoghi periodici del Responsabile della Protezione dei Dati.

Valutazione : Accettabile

Sicurezza dell'hardware

Server protetto da PSW; presente elenco delle misure minime di sicurezza adottate a livello informatico.

Valutazione : Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Discriminazione, Danno per la reputazione, Perdita di controllo dei dati, Altri svantaggi economici o sociali, Furto d'identità, Danni psicologici, Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

una terza parte malintenzionata, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un

tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Politica di tutela della privacy, Gestione dei rischi, Prevenzione delle fonti di rischio, Sicurezza dell'hardware, Vigilanza sulla protezione dei dati, Gestione dei terzi che accedono ai dati, Contratto con il responsabile del trattamento, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, In considerazione della tipologia di dati trattati e dell'età degli interessati si ritiene che la gravità del rischio sia "importante".

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la gravità del rischio sia "trascurabile".

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Discriminazione, Danno per la reputazione, Danni psicologici, Perdita di controllo dei dati, Altri svantaggi economici o sociali, Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni, una terza parte malintenzionata, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione dei rischi, Contratto con il responsabile del trattamento, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati, Sicurezza dell'hardware, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, In considerazione della tipologia di dati trattati e dell'età degli interessati si ritiene che la gravità del rischio sia "importante".

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la gravità del rischio sia "trascurabile".

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di controllo dei dati, Altri svantaggi economici o sociali, Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Distruzione e perdita dei dati, Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni, una terza parte malintenzionata, eventi catastrofici naturali o artificiali, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Backup, Controllo degli accessi fisici, Sicurezza dei canali informatici, Gestione dei rischi, Prevenzione delle fonti di rischio, Sicurezza dell'hardware, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Vigilanza sulla protezione dei dati, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, In considerazione della tipologia di dati trattati e dell'età degli interessati si ritiene che la gravità del rischio sia "importante".

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la gravità del rischio sia "trascurabile".

Valutazione : Accettabile

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Informativa
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

- Controllo degli accessi logici
- Archiviazione
- Sicurezza dei documenti cartacei
- Lotta contro il malware
- Gestione postazioni
- Backup
- Contratto con il responsabile del trattamento
- Sicurezza dei canali informatici
- Controllo degli accessi fisici
- Prevenzione delle fonti di rischio
- Politica di tutela della privacy
- Gestione delle politiche di tutela della privacy
- Gestione dei rischi
- Gestione dei terzi che accedono ai dati
- Vigilanza sulla protezione dei dati
- Sicurezza dell'hardware

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

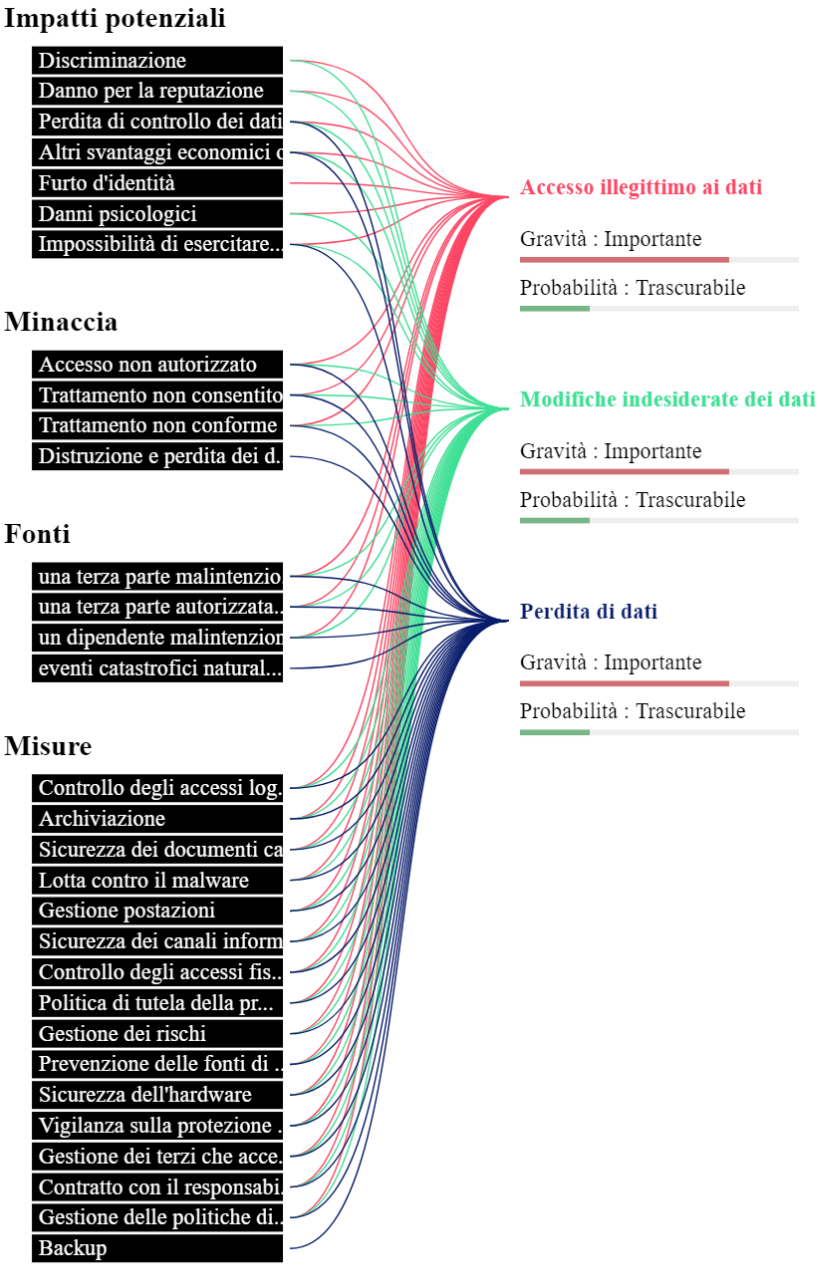
Misure esistenti o pianificate

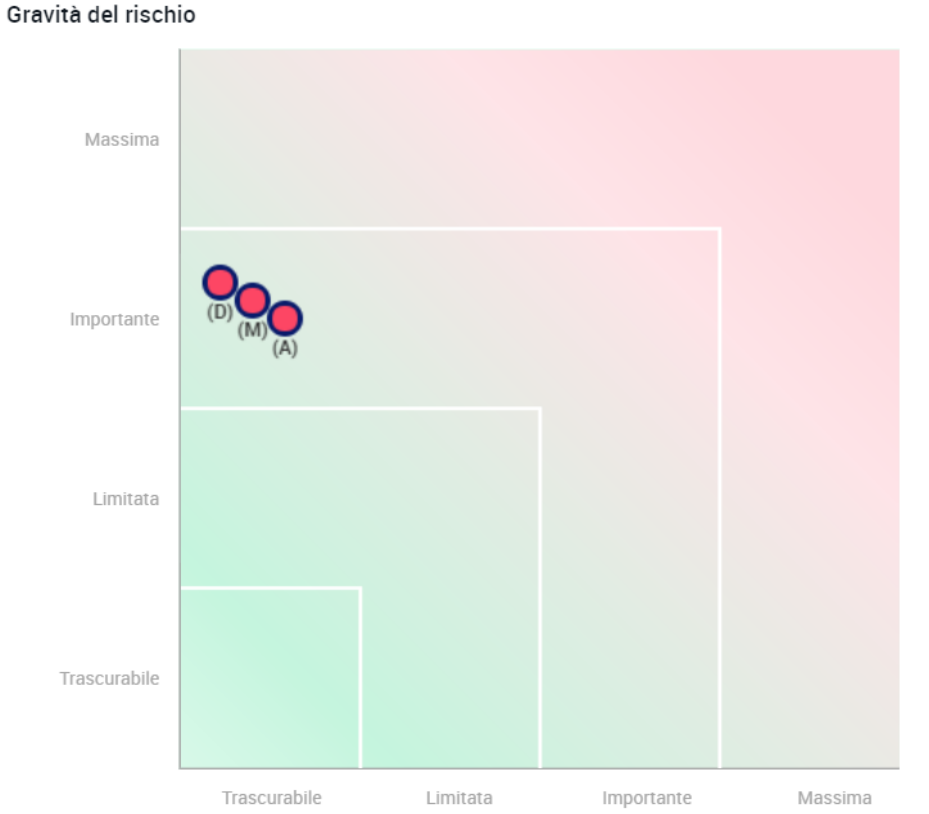
Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.


PRIVACY
INFORMATION
DATA
PERSONAL
INDIVIDUALS
LAWS
PRIVATE
PUBLIC
CASES
SOMETHING
CONSIDERED
RIGHT


Impatti potenziali
Discriminazione
Danno per la reputazione
Perdita di controllo dei dati
Altri svantaggi economici c
Furto d'identità
Danni psicologici
Impossibilità di esercitare..
Minaccia
Accesso non autorizzato
Trattamento non consentito
Trattamento non conforme
Distruzione e perdita dei d.
Fonti
una terza parte malintenzio
una terza parte autorizzata..
un dipendente malintenzior
eventi catastrofici natural...
Misure
Controllo degli accessi log.
Archiviazione
Sicurezza dei documenti ca
Lotta contro il malware
Gestione postazioni
Sicurezza dei canali inform
Controllo degli accessi fis..
Politica di tutela della pr...
Gestione dei rischi
Prevenzione delle fonti di ..
Sicurezza dell'hardware
Vigilanza sulla protezione .
Gestione dei terzi che acce.
Contratto con il responsabi.
Gestione delle politiche di..
Backup
Accesso illegittimo ai dati
Gravità : Importante
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Importante
Probabilità : Trascurabile
Perdita di dati
Gravità : Importante
Probabilità : Trascurabile



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

22/01/2019

Informazioni sulla PIA

Nome della PIA
IST. STATALE IGEA

Nome autore
Ercolani Martina

Nome valutatore
Manaresi Michele

Nome validatore
Manaresi Michele

Data di creazione
22/01/2019

Nome del DPO/RPD
Michele Manaresi

Parere del DPO/RPD
in quanto si ritiene che le misure di sicurezza adottate siano idonee a garantire la sicurezza dei dati.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
non richiesto.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Attività che comportano la gestione di categorie particolari di dati personali dei dipendenti interni.

Il Titolare del Trattamento è l'ISTITUTO COMPRENSIVO STATALE IGEA e il Responsabile del Trattamento è la Dott.ssa Myriam Toccafondo.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità sono regolamentate internamente a mezzo di lettere di autorizzazione sottoposte dal responsabile del trattamento ai dipendenti incaricati ad effettuare l'attività in oggetto. Il responsabile del trattamento ha altresì firmato la lettera di nomina rilasciata dal titolare del trattamento.

Ci sono standard applicabili al trattamento?

I dipendenti si attengono ai contenuti dell'accordo tra le parti per regolamentare il rapporto di dipendenza che hanno sottoscritto.
Il responsabile del trattamento ed il responsabile della protezione dei dati ne verificano periodicamente la corretta applicazione.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Categorie particolari di dati personali come indicato dagli articoli 9 e 10 del GDPR 679/2016.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati del personale interno vengono trasmessi su carta, per le pratiche per cui è possibile, o via email alla controparte del contratto ed elaborati su piattaforma "SIDI".

Gli estremi del contratto vengono trasmessi alla piattaforma "SARE" (centro per l'impiego) nel rispetto dei termini contrattuali e comunque entro 15 giorni dalla stipula del contratto.

I dati saranno conservati per il tempo previsto dalla legge.

Quali sono le risorse di supporto ai dati?

I dati sono conservati in formato cartaceo e digitale.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono indicate in modo specifico ed esplicito all'interno dell'informativa che viene sottoposta agli interessati.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La raccolta dei dati è necessaria per l'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e per assolvere ad obblighi di legge.

I dati sono trattati per dare esecuzione a misure precontrattuali di cui l'interessato è parte o per assolvere ad obblighi legali e contrattuali derivanti da un contratto di cui l'interessato è parte.
Agli interessati viene comunque richiesto il consenso per la finalità in oggetto.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono quelli strettamente necessarie all'attività svolta dal titolare del trattamento.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Gli interessati, in qualsiasi momento, possono chiedere al Titolare del trattamento la correzione e l'aggiornamento dei dati che lo riguardano. Per questo motivo si ritiene che i dati trattati siano esatti e aggiornati.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati sono conservati per l'intera durata del rapporto di lavoro, a seguito di trasferimento il fascicolo personale segue l'interessato.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Agli interessati viene sottoposta l'informativa con la richiesta di rilascio di consenso per ogni singola finalità.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

I dati sono trattati per assolvere a un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e per assolvere ad obblighi di legge in capo al titolare del trattamento.

Agli interessati viene comunque richiesto il consenso, in forma scritta.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

È presente un modello con cui l'interessato può richiedere al Titolare/Responsabile del trattamento di esercitare i propri diritti così come indicati all'interno dell'informativa.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

non applicabile.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

È presente un modello con cui l'interessato può richiedere al Titolare/Responsabile del trattamento di esercitare i propri diritti così come indicati all'interno dell'informativa.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del Responsabile del trattamento sono indicati nella lettera di nomina scritta, firmata dallo stesso per accettazione dell'incarico.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

non applicabile.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Controllo degli accessi logici

Credenziali personali di accesso al "SIDI", a "NUVOLA" e al "SARE".

Valutazione : Accettabile

Archiviazione

Archivio cartaceo chiuso a chiave. La chiave di accesso all'archivio è in possesso solo agli autorizzati al trattamento e al titolare/responsabile del trattamento.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

Documenti cartacei conservati in armadi chiusi a chiave, la cui chiave è in possesso solo agli autorizzati al trattamento.

Valutazione : Accettabile

Lotta contro il malware

Presenti e aggiornati antivirus e firewall a carico del comune.

Valutazione : Accettabile

Gestione postazioni

Tutti i terminali sono protetti da PSW personali.

Valutazione : Accettabile

Backup

Backup a carico del comune.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Lettera di nomina del Responsabile del Trattamento, firmata dallo stesso per accettazione dell'incarico (Mod.0.5).

Valutazione : Accettabile

Sicurezza dei canali informatici

Rete WIFI a carico del comune che fornisce credenziali personali a ogni utente autorizzato.

Valutazione : Accettabile

Controllo degli accessi fisici

Accesso ai locali consentito solo se accompagnati da personale autorizzato.

Valutazione : Accettabile

Sicurezza dell'hardware

Server protetto da PSW; presente elenco delle misure minime di sicurezza adottate.

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Presente allarme antifurto.

Valutazione : Accettabile

Politica di tutela della privacy

E' stato nominato un Responsabile della Protezione dei Dati esterno ed è stata effettuata la comunicazione dei suoi dati di contatto al Garante.

Valutazione : Accettabile

Gestione delle politiche di tutela della privacy

Presente modulistica per regolamentare i rapporti con i dipendenti interni che accedono ai dati (Mod.0.3 accordo tra le parti per il rapporto di dipendenza - Mod.0.4 lettera di autorizzazione).

Valutazione : Accettabile

Gestione dei rischi

E' stata effettuata la Valutazione dei Rischi come indicato dall'articolo 32 del GDPR 679/2016.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Presente modulisitca per regolamentare i rapporti con i terzi che accedono ai dati (Mod.0.2 accordo tra le parti - liberatoria9.

Valutazione : Accettabile

Vigilanza sulla protezione dei dati

Sopralluoghi periodici del Responsabile della Protezione dei Dati.

Valutazione : Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Discriminazione, Danno per la reputazione, Furto d'identità, Perdita di controllo dei dati, Altri svantaggi economici o sociali, Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

una terza parte malintenzionata, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Gestione dei rischi, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Vigilanza sulla protezione dei dati, Contratto con il responsabile del trattamento, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In considerazione della tipologia di dati trattati si ritiene che la gravità del rischio sia "limitata".

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la probabilità del rischio sia "trascurabile".

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Discriminazione, Danno per la reputazione, Perdite finanziarie, Perdita di controllo dei dati, Altri svantaggi economici o sociali, Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza, una terza parte malintenzionata, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In considerazione della tipologia di dati trattati si ritiene che la gravità del rischio sia "limitata".

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la probabilità del rischio sia "trascurabile".

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di controllo dei dati, Impossibilità di esercitare diritti, servizi o opportunità, Altri svantaggi economici o sociali

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Distruzione e perdita dei dati, Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza, una terza

parte malintenzionata, eventi catastrofici naturali o artificiali, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Backup, Controllo degli accessi fisici, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione dei rischi, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati, Gestione delle politiche di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In considerazione della tipologia di dati trattati si ritiene che la gravità del rischio sia "limitata".

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la probabilità del rischio sia "trascurabile".

Valutazione : Accettabile

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Informativa
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

- Controllo degli accessi logici
- Archiviazione
- Sicurezza dei documenti cartacei
- Lotta contro il malware
- Gestione postazioni
- Backup
- Contratto con il responsabile del trattamento
- Sicurezza dei canali informatici
- Controllo degli accessi fisici
- Sicurezza dell'hardware
- Prevenzione delle fonti di rischio
- Politica di tutela della privacy
- Gestione delle politiche di tutela della privacy
- Gestione dei rischi
- Gestione dei terzi che accedono ai dati
- Vigilanza sulla protezione dei dati

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

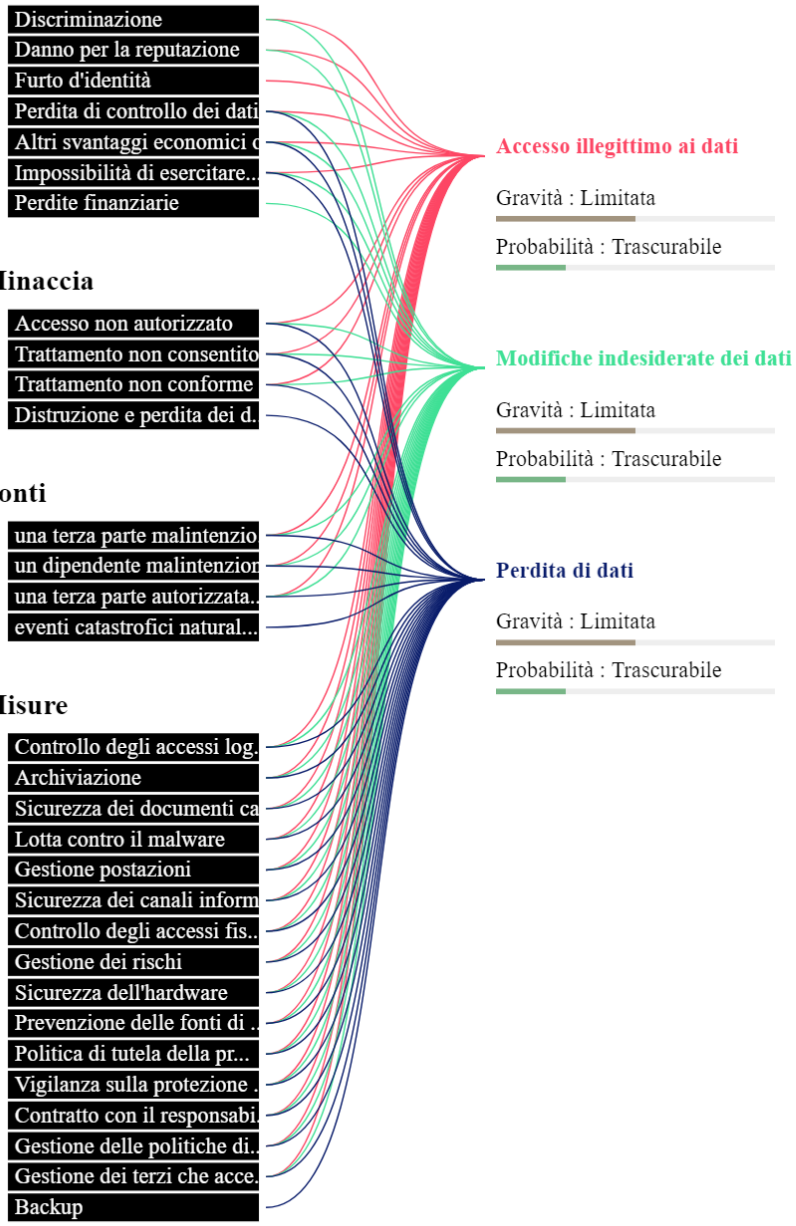
Nessun piano d'azione registrato.

Impatti potenziali

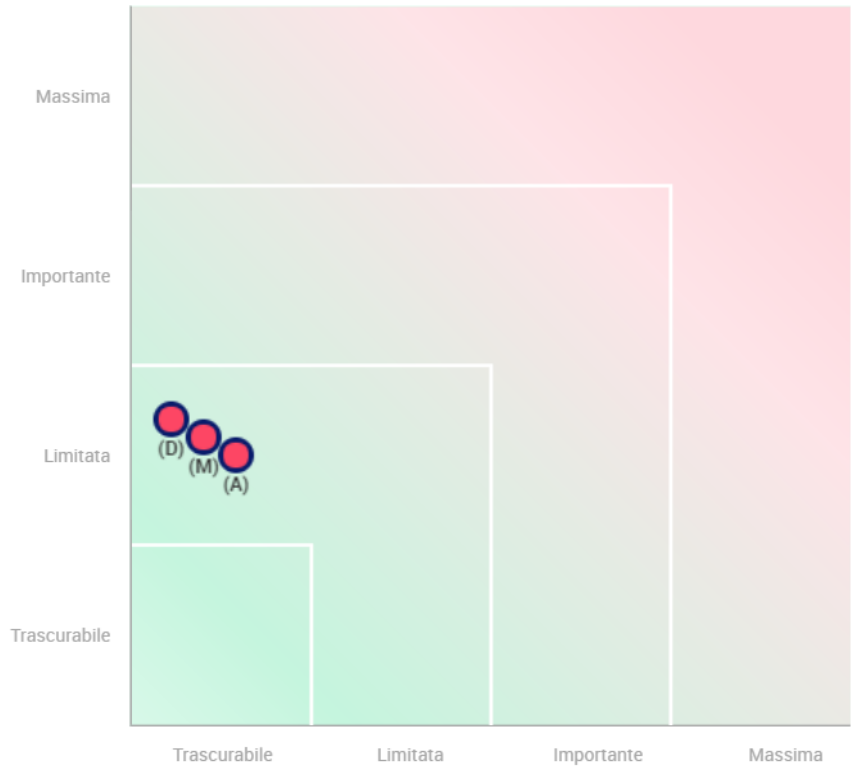
Minaccia

Fonti

Misure



Gravità del rischio



Probabilità del rischio

- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

22/01/2019

Informazioni sulla PIA

Nome della PIA
IST. STATALE IGEA

Nome autore
Ercolani Martina

Nome valutatore
Manaresi Michele

Nome validatore
Manaresi Michele

Data di creazione
22/01/2019

Nome del DPO/RPD
Michele Manaresi

Parere del DPO/RPD
in quanto si ritiene che le msiure di sicurezza adottate siano idonee a garantire la sicurezza dei dati

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
non richiesto.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Attività che comportano la gestione di categorie particolari di dati personali degli esperti esterni.

Il Titolare del Trattamento è l'ISTITUTO COMPRENSIVO STATALE IGEA e il Responsabile del Trattamento è la Dott.ssa Myriam Toccafondo.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità sono regolamentate internamente a mezzo di lettere di autorizzazione sottoposte dal responsabile del trattamento ai dipendenti incaricati ad effettuare l'attività in oggetto. Il responsabile del trattamento ha altresì firmato la lettera di nomina rilasciata dal titolare del trattamento.

Ci sono standard applicabili al trattamento?

I dipendenti si attengono ai contenuti dell'accordo tra le parti per regolamentare il rapporto di dipendenza che hanno sottoscritto.
Il responsabile del trattamento ed il responsabile della protezione dei dati ne verificano periodicamente la corretta applicazione.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Categorie particolari di dati personali come indicato dagli articoli 9 e 10 del GDPR 679/2016.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati del personale interno vengono trasmessi su carta, per le pratiche per cui è possibile, o via email alla controparte del contratto ed elaborati su piattaforma "SIDI".

Gli estremi del contratto vengono trasmessi alla piattaforma "SARE" (centro per l'impiego) nel rispetto dei termini contrattuali e comunque entro 15 giorni dalla stipula del contratto.

I dati saranno conservati per il tempo previsto dalla legge.

Quali sono le risorse di supporto ai dati?

I dati sono conservati in formato cartaceo e digitale.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono indicate in modo specifico ed esplicito all'interno dell'informativa che viene sottoposta agli interessati.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

I dati sono trattati per dare esecuzione a misure precontrattuali di cui l'interessato è parte o per assolvere ad obblighi legali e contrattuali derivanti da un contratto di cui l'interessato è parte.
Agli interessati viene comunque richiesto il consenso per la finalità in oggetto.

La raccolta dei dati è necessaria per l'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e per assolvere ad obblighi di legge.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono solo quelli strettamente necessari all'attività svolta dal titolare del trattamento.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Gli interessati, in qualsiasi momento, possono chiedere al Titolare del trattamento la correzione e l'aggiornamento dei dati che lo riguardano. Per questo motivo si ritiene che i dati trattati siano esatti e aggiornati.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati sono conservati per i tempi previsti dalla legge.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Agli interessati viene sottoposta l'informativa con la richiesta di rilascio di consenso per ogni singola finalità.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

I dati sono trattati per dare esecuzione a misure precontrattuali di cui l'interessato è parte o per assolvere ad obblighi legali e contrattuali derivanti da un contratto di cui l'interessato è parte.
Agli interessati viene comunque richiesto il consenso, in forma scritta, per ogni finalità.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

È presente un modello con cui l'interessato può richiedere al Titolare/Responsabile del trattamento di esercitare i propri diritti così come indicati all'interno dell'informativa.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

non applicabile.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

È presente un modello con cui l'interessato può richiedere al Titolare/Responsabile del trattamento di esercitare i propri diritti così come indicati all'interno dell'informativa.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del Responsabile del trattamento sono indicati nella lettera di nomina scritta, firmata dallo stesso per accettazione dell'incarico.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

non applicabile.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Controllo degli accessi logici

Credenziali personali per accedere al "SIDI", a "NUVOLA" e al "SARE".

Valutazione : Accettabile

Archiviazione

Archivi cartacei sono conservati chiusi a chiave.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

Documenti cartacei conservati in armadi chiusi a chiave.

Valutazione : Accettabile

Lotta contro il malware

Presenti e aggiornati antivirus e firewall a carico del comune.

Valutazione : Accettabile

Gestione postazioni

Tutti i terminali sono protetti da PSW di accesso.

Valutazione : Accettabile

Backup

Backup a carico del comune.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Lettera di nomina del Responsabile del Trattamento, firmata dallo stesso per accettazione dell'incarico (Mod.0.5).

Valutazione : Accettabile

Sicurezza dei canali informatici

Rete WIFI a carico del comune che consegna credenziali personali di accesso a ogni utente autorizzato.

Valutazione : Accettabile

Controllo degli accessi fisici

Accesso ai locali consentito solo se accompagnati da personale autorizzato.

Valutazione : Accettabile

Sicurezza dell'hardware

server protetto da PSW, presente elenco delle misure minine di sicurezza adottate.

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Presente sistema di allarme.

Valutazione : Accettabile

Politica di tutela della privacy

E' stato nominato un Responsabile della Protezione dei Dati esterno ed è stata effettuata la comunicazione dei suoi dati di contatto al Garante.

Valutazione : Accettabile

Gestione delle politiche di tutela della privacy

Presente modulistica per regolamentare i rapporti con i dipendenti interni che accedono ai dati (Mod.0.3 accordo tra le parti per il rapporto di dipendenza - Mod.0.4 lettera di autorizzazione).

Valutazione : Accettabile

Gestione dei rischi

E' stata effettuata la Valutazione dei Rischi come richiesto dall'articolo 32 del GDPR 679/2016.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Presente modulistica per regolamentare i rapporti con i terzi che accedono ai dati (Mod.0.2 accordo tra le parti, liberatoria).

Valutazione : Accettabile

Vigilanza sulla protezione dei dati

Sopralluoghi periodici del Responsabile della Protezione dei Dati.

Valutazione : Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Discriminazione, Danno per la reputazione, Furto d'identità, Altri svantaggi economici o sociali, Perdita di controllo dei dati, Impossibilità di esercitare diritti, servizi o opportuntià

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

una terza parte malintenzionata, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Gestione dei rischi, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Vigilanza sulla protezione dei dati, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In considerazione della tipologia di dati trattati si ritiene che la gravità del rischio sia "limitato".

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la gravità del rischio sia "trascurabile".

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Discriminazione, Danno per la reputazione, Perdite finanziarie, Perdita di controllo dei dati, Altri svantaggi economici o sociali, Imposisbilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

una terza parte malintenzionata, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Gestione dei rischi, Politica di tutela della privacy, Contratto con il responsabile del trattamento, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In considerazione della tipologia di dati trattati si ritiene che la gravità del rischio sia "limitato".

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la gravità del rischio sia "trascurabile".

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di controllo dei dati, Altri svantaggi economici o sociali, Impossibilità di esercitare diritti, servizi o opportunità

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Distruzione e perdita dei dati, Accesso non autorizzato, Trattamento non consentito, Trattamento non conforme alle finalità

Quali sono le fonti di rischio?

eventi catastrofici ntaurali o artificiai, una terza parte malintenzionata, un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Lotta contro il malware, Backup, Gestione postazioni, Sicurezza dell'hardware, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Gestione dei rischi, Controllo degli accessi fisici, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In considerazione della tipologia di dati trattati si ritiene che la gravità del rischio sia "limitato".

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, In considerazione delle misure di sicurezza adottate si ritiene che la gravità del rischio sia "trascurabile".

Valutazione : Accettabile

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Informativa
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

- Controllo degli accessi logici
- Archiviazione
- Sicurezza dei documenti cartacei
- Lotta contro il malware
- Gestione postazioni
- Backup
- Contratto con il responsabile del trattamento
- Sicurezza dei canali informatici
- Controllo degli accessi fisici
- Sicurezza dell'hardware
- Prevenzione delle fonti di rischio
- Politica di tutela della privacy
- Gestione delle politiche di tutela della privacy
- Gestione dei rischi
- Gestione dei terzi che accedono ai dati
- Vigilanza sulla protezione dei dati

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

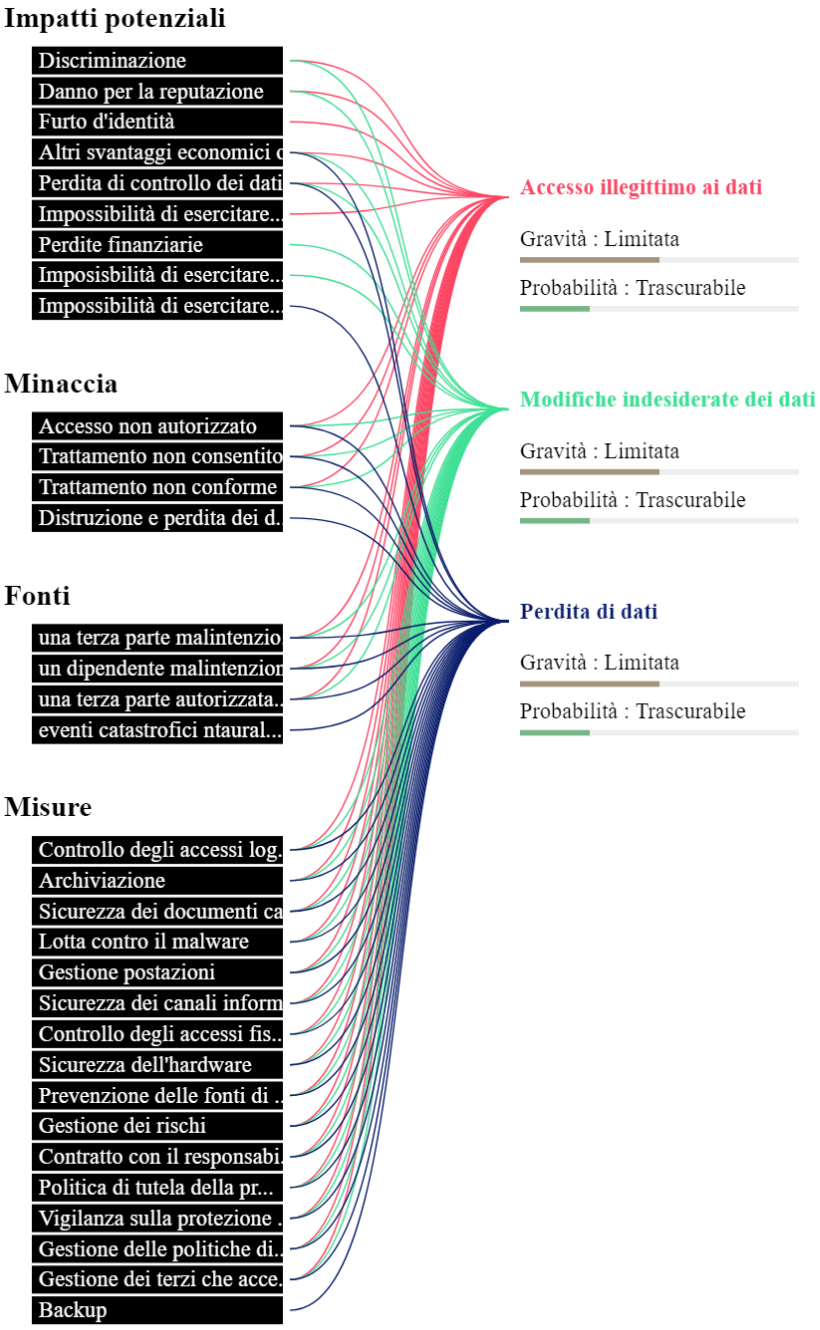
Misure esistenti o pianificate

Nessun piano d'azione registrato.

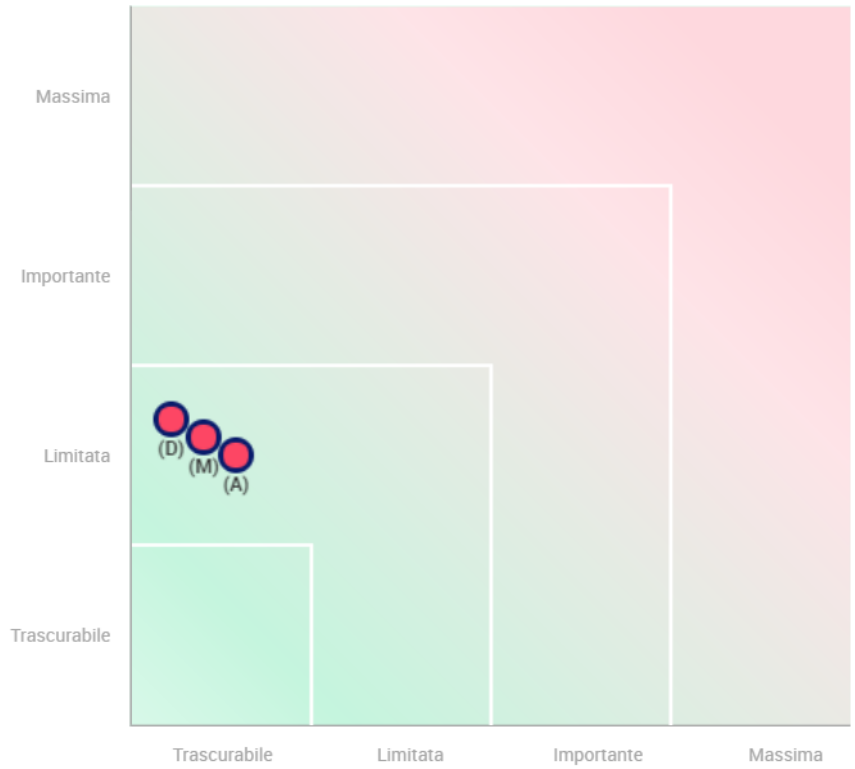
Rischi

Nessun piano d'azione registrato.


PRIVACY
INFORMATION
DATA
PERSONAL
INDIVIDUALS
LAWS
PRIVATE
PUBLIC
CASES
COUNTRIES
SOMETHING
CONSIDERED
RIGHT


Impatti potenziali
Discriminazione
Danno per la reputazione
Furto d'identità
Altri svantaggi economici c
Perdita di controllo dei dati
Impossibilità di esercitare..
Perdite finanziarie
Imposisbilità di esercitare..
Impossibilità di esercitare..
Minaccia
Accesso non autorizzato
Trattamento non consentito
Trattamento non conforme
Distruzione e perdita dei d.
Fonti
una terza parte malintenzio
un dipendente malintenzior
una terza parte autorizzata..
eventi catastrofici ntaural...
Misure
Controllo degli accessi log.
Archiviazione
Sicurezza dei documenti ca
Lotta contro il malware
Gestione postazioni
Sicurezza dei canali inform
Controllo degli accessi fis..
Sicurezza dell'hardware
Prevenzione delle fonti di ..
Gestione dei rischi
Contratto con il responsabi
Politica di tutela della pr...
Vigilanza sulla protezione .
Gestione delle politiche di..
Gestione dei terzi che acce.
Backup
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile

Gravità del rischio



Probabilità del rischio

- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

22/01/2019

ANALISI TRASVERSALE

Questa sezione di analisi del presente Documento di Valutazione dell'Impatto prende in considerazione tutti quei fattori che sono indipendenti dalle attività di trattamento, ma che di fatto costituiscono fattori di rischio oggettivo per la privacy all'interno dell'azienda.

Punto di Controllo	Indicazione misure tecniche e organizzative (già attuate)	P	M	R	Programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza	P	M	R	TEMPI
Nomina e formazione delle figure dell'organigramma privacy – Artt. 24 - 26 - 27 - 28 - 29 - 37, Capo IV, GDPR	Presente la lettera di nomina firmata per accettazione da parte di titolare del trattamento, responsabile del trattamento, responsabile della protezione dei dati ed autorizzati al trattamento. Gli autorizzati al trattamento sono stati istruiti dal titolare del trattamento come richiesto dall'art. 29 – GDPR.	1	1	**1**	Realizzare le nuove lettere di nomina qualora dovessero cambiare i nominativi delle figure in azienda. Mantenere periodicamente aggiornata la formazione degli autorizzati al trattamento.	1	1	**1**	Monitor
Informativa – Art. 12, GDPR	Risultano presenti le informative specifiche nel caso in cui il titolare del trattamento debba fornire informazioni all'interessato. Le informative vengono fornite per iscritto o con mezzi elettronici a secondo dell'attività di trattamento.	1	1	**1**	Nel caso in cui si introducano nuove attività di trattamento, occorre informare il Responsabile della protezione dei dati al fine di realizzare opportuna informativa specifica.	1	1	**1**	Monitor
Consenso – Art. 7, GDPR	Il titolare del trattamento richiede il consenso esplicito per ciascuna finalità di trattamento.	1	1	**1**	//	1	1	**1**	Monitor
Notifica di una violazione dei dati personali all'autorità di controllo – Art. 33, GDPR	Presente la modulistica specifica per la notificazione di una violazione dei dati personali all'autorità di controllo.	1	1	**1**	I titolari dovranno notificare all'autorità di controllo violazioni di dati personali di cui siano a conoscenza entro 72 ore, se ritengono che da tale violazione derivino dei rischi.	1	1	**1**	Monitor
Registro delle attività di trattamento – Art. 30, GDPR	Presente il registro delle attività di trattamento, realizzato in conformità all'art. 30 del GDPR.	1	1	**1**	Nel caso in cui si introducano nuove attività di trattamento, occorre informare il Responsabile della protezione dei dati al fine di aggiornare il registro delle attività di trattamento.	1	1	**1**	Monitor

Punto di Controllo	Indicazione misure tecniche e organizzative (già attuate)	P	M	R	Programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza	P	M	R	TEMPI
Valutazione di impatto sulla protezione dei dati – Art. 35, GDPR	È stata effettuata la Valutazione d'impatto.	1	1	**1**	Nel caso in cui vi sia un nuovo tipo di trattamento che prevede l'uso di nuove tecnologie e che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali, con la consultazione del responsabile della protezione dei dati.	1	1	**1**	Monitor
Consultazione preventiva del Garante – Art. 36	Non applicabile allo stato attuale in quanto al momento non si ritiene necessario procedere con la valutazione di impatto sulla protezione dei dati.	1	1	**1**	//	1	1	**1**	Monitor
Accordo scritto tra aziende, se presente un accordo di partnership	Non applicabile allo stato attuale.	1	1	**1**	//	1	1	**1**	Monitor
Accordo scritto tra Titolare del Trattamento e Responsabile del trattamento, se quest'ultimo è di una società esterna	Presente un modulo di "accordo tra le parti" per regolamentare le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento europeo 2016/679.	1	1	**1**	Compilare il modulo qualora risulti necessario.	1	1	**1**	Monitor

Punto di Controllo	Indicazione misure tecniche e organizzative (già attuate)	P	M	R	Programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza	P	M	R	TEMPI
Cifratura dei dati personali (art. 32, comma 1, lett. a – GDPR)	//	2	2	**4**	Il Titolare del trattamento, o il responsabile del trattamento, devono adottare misure per limitare i rischi tra i quali la cifratura dei dati (o crittografia), basata su un algoritmo di cifratura e su una passphrase (psw più lunga e complessa) che "apre" e "chiude" i dati (di solito al momento dell'autenticazione). Verificare, con l'ausilio della Software House che tale sistema sia presente nel caso di server, di sistemi che gestiscono credenziali, di quelli che trattano dati sensibili, dei computer che processano una grande mole di informazioni per profilare consumatori e, in generale di tutti quegli archivi che contengono dati personali. Stabilire inoltre una corretta gestione del sistema mediante la chiara identificazione di chi detiene le chiavi di cifratura oppure all'obbligatorietà, per tutti i dipendenti, di ricevere eventuali smartphone, chiavette USB e portatili già cifrati.	1	1	**1**	Medio
Pseudonimizzazione (art. 32, comma 1, lett. a – GDPR)	//	2	2	**4**	Il Titolare del trattamento, o il responsabile del trattamento, devono adottare misure per limitare i rischi tra i quali la pseudonimizzazione delle informazioni, basata sull'uso di codici e pseudonimi per fare in modo che i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, le quali devono essere conservate separatamente e soggette a misure tecniche ed organizzative adeguate. Verificare, con l'ausilio della Software	1	1	**1**	Medio

					House che tale sistema sia presente.				

Punto di Controllo	Indicazione misure tecniche e organizzative (già attuate)	P	M	R	Programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza	P	M	R	TEMPI
Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (art. 32, comma 1, lett. b – GDPR)	//	2	2	**4**	Assicurarsi, mediante la Software House, che i sistemi presenti siano capaci di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati. Adottare, con l'ausilio di Software House, misure atte a impedire l'accesso non autorizzato a reti di comunicazione elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.	1	1	**1**	Medio
Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (art. 32, comma 1, lett. c – GDPR)	//	2	2	**4**	Assicurarsi, mediante la Software House, che i sistemi presenti siano capaci di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidenti fisici o tecnici. Predisporre un piano di emergenza informatico, che ricomprende, in particolare, procedure per l'impiego provvisorio di un centro di elaborazione dati alternativo o comunque l'utilizzo di macchine di soccorso da utilizzare in attesa della riattivazione. Messa a disposizione dei dati che sono stati salvati nei dischi di back-up esterni. Presenza di rete GPS sconnessa a cavi che potrebbero tranciarsi.	1	1	**1**	Medio

Procedure per testare l'efficacia delle misure tecniche ed organizzative adottate *(es. audit interni; piani di controlli a campione, ecc.)* (art. 32, comma 1, lett. d – GDPR)	Allo stato attuale si effettuano periodici audit da parte del Responsabile della protezione dei dati.	1	1	**1**	Continuare ad effettuare periodici audit per testare l'efficacia delle misure tecniche ed organizzative adottate.	1	1	**1**	Monitor

CONCLUSIONI

Dopo un'attenta analisi delle attività di trattamento dei dati personali in azienda, alla luce dei risultati ottenuti si conclude che:

RISCHIO	Attività di trattamento
BASSO	*Tutte le attività di trattamento*
ELEVATO*	*Nessuna*

N.B. Si effettuano in ogni caso nr. 2 check registrati all'anno, al fine di valutare l'idoneità delle misure di sicurezza riferite alle attività di trattamento in essere e contestualmente si rende obbligatorio intervenire sulle misure integrative inserite nella pesatura di rischio di ogni trattamento e trasversale.

Nel caso in cui la Valutazione d'Impatto dia rischio sia elevato, si rende necessario realizzare la consultazione preventiva da effettuare prima di procedere al trattamento dei dati ai sensi dell'art. 36 del GDPR.

SCADENZA DEL DOCUMENTO

Il Titolare del trattamento dovrà revisionare il D.P.I.A. (Valutazione di Impatto) ogniqualvolta vi sia un cambiamento nelle caratteristiche attuative di un trattamento, all'introduzione di una nuova attività di trattamento che per le sue caratteristiche necessiti la redazione del documento in oggetto, al fine di mantenere invariato il livello di protezione dei dati nel tempo *(Rif. "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del Regolamento 2016/679").*

Se necessario, il Titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento *(Rif. Comma 11, Art. 35, Sez. 3, Regolamento 2016/679).*


PERSONAL
CASES
PERSONS
PEOPLE
SOMETHING
SELF-SYNCHRONIZATION
COUNTRIES
INFORMATION
PRIVATE
PUBLIC
PERSON
INDIVIDUAL
WAY
CONSIDERED
PRIVACY
INTERESTS
STAKEHOLDERS
RIGHT
DATA
INDIVIDUALS
LAWS

ALLEGATI

DEFINIZIONI

«**GDPR**»: General Data Protecion Regulation

«**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;

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

«**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«**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;

«**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;

«**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;

«**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;

«**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;

«**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;

«**stabilimento principale**»: per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

«**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

«**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

OBBLIGHI GENERALI

Responsabilità del titolare del trattamento - *Articolo 25*

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure sopra citate includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta di cui all'articolo 40 – GDPR o a un meccanismo di certificazione di cui all'articolo 42 – GDPR può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita - *Articolo 25*

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Contitolari del trattamento - *Articolo 26*

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le

rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle

informazioni di cui agli articoli 13 e 14 – GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

L'accordo sopra citato riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo sopra citato, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione - *Articolo 27*

Ove si applichi l'articolo 3, paragrafo 2 del GDPR, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione.
L'obbligo di designare un rappresentante nell'Unione non si applica:
a) al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1 – GDPR o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 – GDPR, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure
b) alle autorità pubbliche o agli organismi pubblici.

Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.

Ai fini della conformità con il GDPR, il rappresentante è incaricato dal titolare del trattamento o dal responsabile del trattamento a fungere da interlocutore, in aggiunta o in sostituzione del titolare del trattamento o del responsabile del trattamento, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.

La designazione di un rappresentante a cura del titolare del trattamento o del responsabile del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso titolare del trattamento o responsabile del trattamento.

Responsabile del trattamento - *Articolo 28*

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate
alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32 - GDPR;
d) rispetti le condizioni sopra citate per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III - GDPR;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 - GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.
Con riguardo alla lettera h) il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 – GDPR o a un meccanismo di certificazione approvato di cui all'articolo
42 – GDPR può essere utilizzata come elemento per dimostrare le garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del GDPR.

FONTI NORMATIVE

- Regolamento UE 2016/679 (GDPR) – Art. 35 “Valutazione d’Impatto sulla protezione dei dati”
- PIA – Privacy Impact Assessment.