Data protection impact assessment (DPIA)

Titolare del trattamento:

ZINCOGAM SPA

Sommario

Contesto

Questa sezione offre una visuale chiara del trattamento di dati personali in questione.

PANORAMICA

Questa parte permette di identificare e presentare l'oggetto dello studio.

Quale è il trattamento in considerazione?

La società ZINCOGAM SPA, di seguito Zincogam, Società o SPA, ai sensi dell'art.2325 c.c. e seguenti, è una società per azioni con sede in Galatina alla Via Pavia n.36.

L'Società, come si evince dallo statuto, e come riportato nella visura camerale, svolge le seguenti attività:

- attivita' di industria della zincatura in ogni sua forma e dimensione, nonchè il trattamento dei metalli in genere e la costruzione di carpenteria metallica varia;
- la costruzione e gestione degli impianti di produzione di energia elettrica da fonti rinnovabili (sole, vento, risorse idriche, risorse geotermiche, maree, moto ondoso, prodotti vegetali o rifiuti organici/inorganici, biogas, cogenerazione);
- la produzione di energia rinnovabile;
- la costruzione e gestione di impianti solari termici;
- la societa' potra' compiere qualsiasi operazione commerciale e finanziaria, mobiliare ed immobiliare necessaria o utile al conseguimento dell'oggetto sociale, compresa l'assunzione di finanziamenti e mutui ordinari e speciali da parte dello stato o degli enti locali, la ricezione o la prestazione di fideiussioni e l'assunzione sia direttamente che indirettamente di interessenze e partecipazioni in altre societa' o imprese, costituite o costituende, aventi oggetto analogo, affine, complementare o connesso al proprio.

Quali sono le responsabilità legate al trattamento?

I dati, solo occasionalmente (come agli artt.9 e 10 del Reg. UE 679/2016), sono ottenuti prevalentemente in maniera diretta, al fine di profilare, categorizzare, rielaborare ed utilizzare le informazioni ottenute in maniera pertinente e coerente con i sopra riportati scopi dell'attività.

A questo si aggiungono i dati relativi alla gestione interna tipica dell'Associazione, quali atti amministrativi, gestionali, contabili, fiscali, per via di rapporti formali con aziende e privati, collegati e interessati.

Visti gli obiettivi indicati nello Statuto, già richiamati al paragrafo precedente, l'Associazione, per lo svolgimento dell'attività, tratta le varie tipologie di dati nel rispetto dei propositi e dei vincoli del GDPR, tra i quali:

- ai sensi dell'art.5 i principi applicabili;
- ai sensi dell'art.6 le condizioni di liceità ed il legittimo interesse;
- ai sensi degli artt.7 e 8 il consenso dell'interessato;
- ai sensi degli artt. da 12 a 23 i diritti dell'interessato.

Al fine di realizzare l'accountability, e quindi di rendere attuabile tale normativa, si procede ad individuare i soggetti ai sensi dell'art.4, e le relative responsabilità.

In particolare, ai sensi degli artt.4 e 7, il TITOLARE DEL TRATTAMENTO è identificabile nella Società stessa in quanto soggetto dotato di personalità giuridica, e quindi al singolo socio a cui rivengono le responsabilità in caso di violazione e data breach, sebbene tale ambito non rientri direttamente nell'esercizio delle sue funzioni.

Ai sensi degli artt.4 e 8 vengono identificati i RESPONSABILI DEL TRATTAMENTO, intesi come responsabili interni, suddivisi per aree funzionali, che rispondono direttamente al titolare in base agli incarichi attribuitigli, oltre che alle casistiche obbligatorie ai sensi dell'art.29.

A tal punto si evidenzia la commistione tra titolari e responsabili, in quanto il responsabile di area spesso coincide, in base a mansioni e competenze, con uno dei componenti dell'asset societario; per meglio spiegare mansioni e relative responsabilità di soci e amministratori in materia di privacy e protezione dati, si rimanda all'organigramma allegato.

A suddette figure, ai sensi degli artt. 4 e 10, sono da associare gli AUTORIZZATI AL TRATTAMENTO, identificabili nei dipendenti e collaboratori a vario titolo, che sono di ausilio ai responsabili interni afferenti (di cui all'art.8), organizzati per settore di attività e per mansione, con accesso limitato ai soli documenti di competenza e le relative responsabilità.

Ci sono standard applicabili al trattamento?

Ai sensi dell'art.40 del Reg. UE 679/16, come disposto al paragrafo 5, l'Società si propone di seguire i seguenti codici di condotta:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dai titolari del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali (ove possibile);
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;
g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;

i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

Inoltre, ai sensi dell'art.42, l'Società, seppur non avesse alcun obbligo specifico, ha ritenuto opportuno strutturare un sistema di certificazione interno, integrando il registro dei trattamenti con il registro di protocollo, dando quindi data certa, immodificabilità e un ulteriore controllo.

Va poi precisato che, vista l'ingente quantità di dati trattati, le attività svolte, le complessità e responsabilità connesse, la società è strutturata in differenti Unità Operative, garantendo una prima frammentazione, minimizzazione e tutela dei dati, gestiti solo dal personale incaricato per competenza.

DATI, PROCESSI E RISORSE DI SUPPORTO

Questa parte permette di definire e descrivere lo scopo del trattamento nel dettaglio.

Quali sono i dati trattati?

Al fine di realizzare le attività sopra descritte, la Società acquisisce ed elabora dati su aziende e privati.

Va da subito precisato che i soggetti privati, figure principalmente tutelate dalla normativa che detta i principi del presente atto, sono marginali per numero e consistenza economica rispetto alla totalità degli stake holders.

La Società acquisisce ed elabora dati e documenti inerenti clienti, fornitori, dipendenti e collaboratori esterni. Da ciò si evince che i dati acquisiti, prodotti e gestiti sono prevalentemente di natura amministrativa, gestionale e fiscale.

Com'è il ciclo di vita del trattamento dei dati?

I dati sono comunicati direttamente dagli interessati verbalmente o a mezzo attestazioni, e vengono acquisiti a mezzo comunicazione verbale, in formato analogico o digitale, per poi essere acquisiti e rielaborati su specifici software e portali di competenza della Società e di eventuali contitolari, oltre che sul server di esclusiva competenza della Società.

Laddove opportuno gli stessi dati sono verificati tramite controllo incrociato su portali istituzionali.

Se appositamente richiesto dalle procedure, o laddove ritenuto opportuno per una corretta gestione delle attività, i dati e le relative rielaborazioni possono essere soggetti a stampe, affiancando all'archiviazione digitale, anche quella analogica.

La Società si propone di mantenere la proprietà dei dati secondo i dettami del codice civile, comunque non oltre un periodo limite definito in 10 anni; fanno eccezione i riepiloghi e le rielaborazioni con fine statistico, a disposizione dell’attività, le quali riportano solo dati riepilogativi e non riferibili a singoli soggetti.

Quali sono le risorse di supporto ai dati?

I dati sono gestiti con file del pacchetto office appositamente personalizzati, e sono acquisiti sul server in sede e soggetti a backup, al fine di adempiere alle attività di gestione interna.

Ai fini delle procedure e di adempiere a incarichi ed eventuali obblighi, gli stessi dati, o parte di essi, vengono condivisi tramite caricamento manuale effettuato dal personale preposto.

Parte dei dati può essere soggetta a stampe, al fine di consentire una più facile gestione delle attività, e favorire eventuali verifiche; in tal caso, i dati in formato cartceo saranno soggetti a partizione per attività, e fascicolati in appositi faldoni nell'archivio fisico.

Solo per le attività amministrative e gestionali, la Società si avvale di mail e PEC.

Si prevede invece l'utilizzo di social network a fini promozionali, anche con riepiloghi statistici anonimi.

Principi Fondamentali

Questa sezione permette di generare lo schema di adeguamento secondo i principi considerati.

PROPORZIONALITÀ, NECESSITÀ

Questa sezione permette di dimostrare l'implementazione dei mezzi necessari per abilitare le persone interessate ad esercitare i loro diritti.

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità dei trattamenti risultano rispondenti ai principi riportati nell'art.5 del Reg. UE 679/2016.

Ai sensi dell'art.5 comma 1 punto b) gli scopi dei trattamenti risultano specifici, espliciti e legittimi.

Di fatto i trattamenti sono specifici, ovvero necessari e mirati al raggiungimento degli obiettivi prefissati nello statuto, secondo i dettami normativi e procedurali.

Gli stessi risultano espliciti, in quanto preventivamente esplicitati dalle sopra citate normative e da prassi operative e procedurali definite dall'ordinamento nazionale e regionale; inoltre gli interessati vengono edotti entro e non oltre il momento di acquisizione dei dati stessi.

Gli scopi sono legittimi in quanto effettuati con il consenso e su richiesta degli interessati, e rispondenti agli specifici dettami normativi nazionali e regionali di riferimento.

Ai sensi dell'art.5 comma 1 punto a) i dati sono trattati secondo i principi di liceità, correttezza e trasparenza.

Di fatto il trattamento è lecito poiché richiesto direttamente dagli interessati, e svolto nell'interesse degli stessi.

Il trattamento è corretto in base alle modalità prestabilite e predeterminate da specifiche procedure, nonché alle competenze degli operatori.

Quali sono le basi legali che rendono il trattamento legittimo?

Ai sensi dell'art. 6 del Reg. UE 679/2016, i trattamenti rispondono al principio di liceità e rispettano l'interesse legittimo delle parti; peraltro le operazioni svolte in collaborazione con Enti Pubblici, rispettano i dettami e le normative in materia di regolamentazione degli enti pubblici di fonte nazionale - art.14 L.124/2015, L.191/1998, D.Lgs.165/2001, D.Lgs.33/2013, D.Lgs.97/2016 e D.Lgs.36/2006 - e regionale - L.15/2018, Reg.20/2009 e linee guida in materia di trattamento dati -, nonché con atti intrinseci alla buona amministrazione della Società e della tutela dei soggetti terzi beneficiari ai sensi del C.C.

Di fatto l'interessato acconsente al trattamento dei propri dati personali per uno o più scopi specifici.

Tale trattamento risulta necessario per:

- l'esecuzione di un contratto di cui l'interessato è parte o per prendere provvedimenti alla richiesta dell'interessato prima di stipulare un contratto;
- per adempiere a un obbligo giuridico a cui è soggetto il titolare del trattamento;
- tutelare gli interessi legittimi dell'interessato;
- l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri conferiti al titolare del trattamento;
- gli interessi legittimi perseguiti dal titolare del trattamento o da una terza parte, eccetto laddove tali interessi violino i diritti e le libertà fondamentali dell'interessato.

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

Ai sensi dell'art. 5 comma 1 punto c), Zincogam predilige la buona pratica della minimizzazione delle informazioni, di fatto riducendo al minimo il numero di dati personali che verranno acquisiti ed elaborati, a quanto strettamente necessario per gli scopi adeguati, come ai punti precedenti.

Di fatto le tipologie di dati sono standardizzate a mezzo di specifici software gestionali e procedure affiate nel tempo.

Resta ovviamente l'eccezione di documenti e informazioni inviati dagli interessati. Tale possibilità è prevenuta con una corretta informativa da parte della Società, e correttamente gestita eliminando i dati in eccesso.

La riduzione del numero di dati si traduce in una riduzione dei rischi e dell'impatto che gli stessi potrebbero avere, oltre a garantire una più facile gestione degli stessi.

Ovviamente i dati devono essere sufficienti ed adeguati per le finalità, gli scopi e le funzioni della gestione tipica della società.

Commento:

- Fermi restando i principi sopra enunciati, va precisato che la Zincogam demanda ai fruitori dei servizi il compito di verificare e dimostrare l'autenticità delle informazioni.

I dati sono accurati e mantenuti aggiornati?

Ai sensi dall'art. 5 comma 1 punto d) del Reg. UE 679/2016, l'Ente garantisce la qualità dei dati.

Di fatto, le informazioni sono fornite direttamente dagli interessati, tanto a voce quanto tramite la compilazione di appositi moduli cartacei o telematici.

Tali informazioni sono inoltre controllate tramite l'incrocio di dati tra quanto dichiarato e quanto in possesso della società.

Al fine di garantire l'accuratezza dei dati, la Società si riserva di effettuare verifiche presso enti pubblici ad uopo preposti e organizzati.

Quale è la durata della conservazione dei dati?

Ai sensi dall'art. 5 comma 1 punto d) del Reg. UE 679/2016, seguendo le indicazione riportate nel Bollettino n. 30 (pag.43) del Garante della Privacy, fermi restando i principi di tracciabilità e trasparenza, e in conformità con i presupposti del comma 1 punto c) sopra richiamato, la società si impegna a conservare i dati solo per il tempo strettamente necessario.

Va però precisato che tali tempistiche variano in funzione della tipologia di dato.

In via generale l'Ente tenderà a lasciare traccia degli atti di gestione tipica ai fini della trasparenza, limitando i termini di conservazione a 5 anni per dati di interesse contabile e fiscale, 10 anni per dati di interesse civilistico, e, secondo le direttive del Garante, si riserva il potere di anticipare l'eliminazione laddove venga meno l'utilità per cui il dato era stato acquisito.

CONTROLLI PER PROTEGGERE I DIRITTI PERSONALI DEI SOGGETTI INTERESSATI

Questa sezione permette di dimostrare l'implementazione dei mezzi necessari per abilitare le persone interessate ad esercitare i loro diritti.

I soggetti interessati come sono informati del trattamento?

Al fine di adempiere a pieno ai doveri di cui all'art. 13, l'Associazione ha predisposto un'informativa adeguata, da sottoporre agli interessati al fine di rendergli edotti sulle modalità di recepimento e acquisizione dei dati, nonché sull'utilizzo e sulla conservazione.

Tale informativa è a disposizione degli interessati su apposita modulistica, sul portale a disposizione dei potenziali clienti, nonché esposta in sede, al fine di rendere edotti gli interessati, e permettere la sottoscrizione della stessa.

Inoltre, per meglio rispondere ai dettami dell'art.13, la medesima informativa è a disposizione nell'apposita sezione del sito. Per lo stesso motivo, ogni mail inviata dall'Ente è corredata da un richiamo alla normativa e al link del sito.

Come si ottiene il consenso dei soggetti interessati?

Al fine di adempiere a pieno alla compliance del GDPR, pur prevedendo casi residuali, la Zincogam, ai sensi degli artt. 6 e 9, e nel rispetto dell'art. 7 comma 1 del medesimo regolamento, ha predisposto apposita modulistica per acquisire il consenso per iscritto, da allegare all'informativa di cui al punto precedente. In caso di relazione con clienti esclusivamente con modalità telematiche, è previsto sul portale un apposito spazio con possibilità di spunta per testimoniare l'avvenuta presa di consapevolezza dell'informativa e relativa accettazione delle condizioni inerenti. Inoltre, in funzione del ruolo assunto, delle attività svolte e delle modalità di svolgimento, ai sensi dell'art. 7 del Reg. U.E. 679/2016, si avvale del consenso implicito.

Nel rispetto dell'art. 7 commi 1 e 2, l'Ente si avvale espressamente del consenso prestato dagli interessati ai Contitolari e agli altri collegati; ovviamente, ai sensi del comma 3, l'utilizzo dei dati è limitato alle finalità riportate nella documentazione dei soggetti terzi.

Ai sensi dell'art. 7 comma 4, è espressamente data facoltà agli interessati di revocare il consenso a mezzo richiesta scritta consegnata a mano; l'Ente si impegna a rispondere tempestivamente alla richiesta, nel minor tempo possibile, e comunque entro 90 giorni lavorativi.

Inoltre il Reg. UE 679/16 introduce il concetto di legittimo interesse quale base giuridica su cui valutare la liceità delle operazioni di trattamento di dati personali.

Si tratta di un concetto nuovo per il nostro ordinamento che, ai sensi dell'art. 6 comma 1 lett. f, consente di considerare legittimo il trattamento dei dati oltre che nelle ipotesi già previste dal Codice per la protezione dei dati anche qualora lo stesso sia effettuato per perseguire uno scopo legittimo del titolare a condizione che non siano prevalenti su tale scopo gli interessi o i diritti e le libertà fondamentali dell'interessato.

Si chiarisce che, secondo il considerando n. 47 del GDPR, per la valutazione della sussistenza di un legittimo interesse del titolare deve innanzitutto tenersi conto delle "ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento". Tale valutazione, che nell'impostazione del Regolamento Europeo è svolta autonomamente dal titolare, deve quindi basarsi su ciò che l'interessato potrebbe ragionevolmente attendersi rispetto al trattamento dei propri dati da parte del titolare con cui abbia rapporti (o venga in contatto).

Tutto ciò premesso, analizzando in dettaglio il settore di attività e le modalità attuative, sempre nel rispetto della normativa nazionale in materia fiscale, tributaria e commerciale, è evidente come il legittimo interesse sia sufficiente a giustificare le procedure ad ora menzionate e di seguito dettagliate.

I soggetti interessati come esercitano i loro diritti di acceso alla portabilità dei dati?

Zincogam offre la possibilità di ricevere gli interessati in sede, o di essere contattato a mezzo pec personale all'indirizzo info@pec.zincogam.it per sollecitare e garantire il rispetto del diritto di accesso, nonché alla portabilità dei dati, secondo le modalità e prassi indicate dal C.C..

Di fatto, nel rispetto dei limiti dettati dalla trasparenza e dalla tracciabilità che la natura societaria impone, sono garantiti, ai sensi dell'art. 15 del Reg. UE 679/16 il diritto di ottenere dal titolare del trattamento l'accesso ai dati personali comunicati o rielaborati e, ai sensi dell'art. 20 il diritto di far trasmettere i dati personali ad un ulteriore titolare del trattamento in un formato strutturato, comunemente utilizzato e leggibile.

Commento:

- Fermo restando quanto riportato dagli artt. 15 e 20, è preferibile che gli interessati esercitino il diritto alla portabilità presentandosi di persona presso la sede legale.

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

Zincogam offre la possibilità, di persona previo appuntamento o a mezzo PEC all'indirizzo info@pec.zincogam.it, per chiedere, sollecitare e garantire il rispetto dei diritti di rettifica e cancellazione da parte degli uffici amministrativi.

Ai sensi dell'art. 16 del Reg. UE 679/16, l'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa ferma restando la coerenza tra i dati e le finalità del trattamento.

Ai sensi dell'art. 17 l'interessato ha il diritto di ottenere dalla titolare e dagli altri contitolari del trattamento la cancellazione nel minor tempo possibile.

Commento:

- Fermo restando quanto riportato dagli artt. 16 e 17, è preferibile che gli interessati esercitino il diritto alla portabilità presentandosi di persona presso la sede legale, sempre nel rispetto dei diritti, dei doveri e del legittimo interesse dell'Ente, oltre che di eventuali stake-holder.

I soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

Zincogam offre la possibilità, in sede previo appuntamento o a mezzo PEC all'indirizzo info@pec.zincogam.it, per chiedere, sollecitare e garantire il rispetto dei diritti di restrizione e obiezione.

Ai sensi dell'art. 18 del Reg. UE 679/16, l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

In particolare, ai sensi dell'art. 21 l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni; il titolare del trattamento dovrà astenersi dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Tale diritto è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Commento:

- Fermo restando quanto riportato dagli artt. 18 e 21, gli interessati possono godere dei diritti di restrizione e obiezione preferibilmente presentandosi di persona presso la sede legale, contestualmente all'avviamento di attività a loro riferite, o in momenti successivi.

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto scritto e dalle prassi operative.

Si precisa che i ruoli e le responsabilità sono ben definiti e sottoscritti tanto per i responsabili interni, soggetti a specifica formazione e modulistica (oltre che dalla normativa in materia di contrattazione collettiva), quanto per i responsabili esterni, soggetti anch'essi a specifica contrattazione e modulistica.

Ai sensi dell'art. 28 del GDPR, tale modulistica deve riportare durata, ambito, finalità, istruzioni di elaborazione documentate, autorizzazione preventiva in cui è coinvolto l'incaricato, fornitura di qualsiasi documentazione che dimostri la conformità al GDPR, notifica tempestiva di eventuali violazioni dei dati, ecc.

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

Zincogam ha affrontato attentamente l'argomento al fine di perseguire i principi di cui all'art. 44 e seguenti del Reg. UE 679/16.

In merito a potenziali trasferimenti di dati in Paesi esteri, ed in particolare in Paesi extra-UE, l'Ente, non avendo qualifica per svolgere controlli preventivi e volendo agevolare le volontà degli interessati in tempi ragionevoli, si propone di inoltrare i dati direttamente agli interessati, delegandoli quali mediatori.

In merito a potenziali trasferimenti di dati in Paesi comunitari, L'Ente, intratterrà sicuramente rapporti con enti analoghi, con i quali condividerà solo dati statistici e riepilogativi, senza riferimenti specifici. In caso di diverse esigenze degli interessati, dovendo relazionarsi con organizzazioni private, si rimanda a quanto esposto per i soggetti extra-UE.

Commento:

- In merito all'attività amministrativa, la Società valuta preventivamente e con attenzione le garanzie offerte da eventuali contitolari, ancor più se soggetti esteri.

Rischi

Questa sezione permette di valutare i rischi della privacy, prendendo in considerazione controlli esistenti o pianificati.

CONTROLLI ESISTENTI O PIANIFICATI

Questa sezione permette di identificare i controlli (esistenti o pianificati) che contribuiscono alla sicurezza dei dati

Crittografia

I dati, archiviati su un sever e occasionalmente transitanti su cloud, sono protetti da un sistema di crittografia.

Quanto presente in copia di dato in formato analogico e/o digitale, è metodicamente fascicolato ed archiviato con diverse chiavi d'accesso e livelli di autorizzazione.

Anonimizzazione

I dati sono raggruppati per progetti ed attività, spesso indicati con un codice numerico, non riportando in alcun modo dati riconducibili ad un singolo soggetto.

Partizionamento dei dati

I dati sono suddivisi e fascicolati in base all'attività di riferimento, suddivisi e smistati ai settori di competenza per le attività a cui gli stessi dati sono soggetti e/o per cui sono propedeutici.

Controllo degli accessi

Ogni incaricato al trattamento ha una postazione personale. In funzione di mansioni, incarichi e competenze, utilizza software o strumenti specifici, munito di credenziali personali o specifica autorizzazione, pertanto risulta facilmente desumibile la responsabilità.

Tracciabilità

Qualunque operazione, in funzione di incarichi e mansioni predeterminate, è soggetta a tracciabilità. Ancor più evidenza assume la tracciabilità in caso di utilizzo hardware e software.

In caso di trattamenti a mezzo pc, avendo ogni autorizzato un proprio pc, qualunque accesso o operazione è attribuibile a mezzo indirizzo IP.

Archiviazione

L'archiviazione avviene in maniera metodica e puntuale.

I dati digitali (nativi digitali e di seconda generazione) vengono acquisiti, fascicolati e conservati su server; inoltre, dove richiesto dalle normative, dalla natura dell'Ente oggetto di analisi e delle misure attivate, i dati sono condivisi con portali istituzionali.

La documentazione cartacea, se relativa a fatti interni di gestione viene suddivisa per tipologia, smistata agli uffici di competenza, lavorata, protocollata e conservata secondo un ordine funzionale, in faldoni stipati in arredi dotati di serratura; la documentazione relativa a specifiche misure, soggetta ad acquisizione in digitale (seconda generazione), è suddivisa e conservata in faldoni in base ad un ordine ed una classificazione specifica:

I. misura;
II. tipologia dei dati;
III. ordine cronologico.

Sicurezza dei documenti cartacei

Oltre quanto riportato nel paragrafo, va precisato che i faldoni delle varie attività vengono fascicolati e conservati in un archivio appositamente strutturato e rigorosamente chiuso a chiave, dotato di appositi arredi muniti di serratura.

Minimizzare la quantità di dati personali

In quanto alla minimizzazione dei dati, la Società acquisisce solo i dati necessari, seguendo le linee guida dell'apposita modulistica e dei software specifici.

Inoltre, i dati sono mirati per misura e settori di attività coinvolti, garantendo anche un ulteriore livello di minimizzazione.

Vulnerabilità

Ad oggi, viste la metodicità della progettazione dei processi e delle prassi operative, la grande attenzione alle strutture informatiche adottate e la responsabilizzazione degli operatori tramite formazione, tracciabilità e controllo degli accessi, eventuali vulnerabilità possono essere preventivate principalmente per i rapporti con eventuali contitolari, in quanto soggetti terzi.

Per gli stessi motivi, si cerca di regolarizzare al meglio il rapporto e le prassi operative con i contitolari al fine di prevenire eventuali errori, anche e non solo in materia di protezione dati.

Lotta contro il malware

La Società, sempre attenta all'evoluzione tecnologica e a sistemi di implementazione dei servizi, comprendendo chiaramente l'importanza dei dati e i rischi connessi, cura costantemente la lotta ai malware tramite appositi software accuratamente selezionati e tenuti sempre aggiornati.

Gestione postazioni

Le postazioni sono personali e dotate di chiave d'accesso e diversi livelli autorizzativi, limitando i rischi e responsabilizzando gli operatori.

Sicurezza dei siti web

Il sito istituzionale https://zincogam.it/ risponde agli standard di sicurezza, in quanto vengono applicati protocolli "per la comunicazione sicura".

Inoltre il sito ha solo funzione di vetrina, riportando dati sulle attività produttive che la Ditta svolge abitualmente.

In merito ad altri portali con i quali l'Società si interfaccia a vario titolo, bisogna precisare che ciò avviene per dovere istituzionale, trattando dati statistici riepilogativi previsti da apposite normative regionali e nazionali in base alle specifiche attività svolte.

Si precisa che tali siti non sono gestiti dall'Ente, e pertanto si declinano eventuali responsabilità sugli stessi.

Restano comunque salde buone pratiche quali la mancata memorizzazione di credenziali sui dispositivi, e l'accesso ai suddetti portali solo da personale specializzato.

Backup

La Società si è dotata di un doppio sistema di Backup, come di seguito dettagliato.

Il primo step è dato da un server fisico, sito e messo in sicurezza nella sede centrale dell'Società, che ha una funzione di supporto temporaneo alla connettività delle varie fasi dell’attività produttiva, gestionale ed amministrativa.

Il secondo step è la postposizione di tali dati su:

- memorie esterne, al fine di garantire la conservazione dei dati e l'ottimale funzionalità del server fisico;
- conservazione di documenti in formato analogico.

Manutenzione

La manutenzione preventiva è affidata a società esterne, specializzate nei sistemi e sugli strumenti adottati, tramite formale contratto.

Contratti di trattamento

Qualunque rapporto instaurato dalla Società con i collaboratori/professionisti, con società e aziende eroganti servizi, con società e aziende richiedenti servizi, nonché con privati che volontariamente si interfaccino, è regolato da specifico contratto scritto e controfirmato dalle parti, al fine di rendere edotti gli interlocutori ai sensi del Reg. UE 679/2016, fermo quanto evidenziato in merito al legittimo interesse delle parti.

Sicurezza della rete

Per quanto concerne la sicurezza della rete si conferma quanto riportato al paragrafo "manutenzione".

Controllo degli accessi fisici

Le attività sono monitorate e tracciate istantaneamente, nonché rendicontate direttamente dall'organo amministrativo.

Monitoraggio dell'attività della rete

Le attività sono monitorate e tracciate istantaneamente, nonchè rendicontate direttamente dall'organo amministrativo.

Sicurezza dell'hardware

Per quanto concerne la sicurezza dell'hardware si conferma quanto riportato al paragrafo "manutenzione".

Evitare le fonti di rischio

Le best practice sino ad ora descritte, nonchè i dettami che seguiranno, evidenziano la volontà dell’Azienda di prevenire ed evitare alcuna fonte di rischio, fino a limitare gli accessi fisici al solo personale di fiducia, debitamente formato.

Protezione contro fonti di rischio non umane

In merito a fonti di rischio non umane, ad oggi sovviene solo l'eventualità di problemi legati alla sicurezza dei luoghi, demandando tale aspetto alla garanzia data dal rispetto dei dettami del D. Lgs. n.81/2009 e del D.M. 163/2013.

Commento:

- La posizione dei singoli centri operativi in merito a fonti di rischio non umane sarà oggetto di adeguamenti specifici, conformemente a quanto riportato nel DVR.

Organizzazione

In materia di privacy i ruoli sono assegnati in maniera conforme a quelli operativi, meglio desumibili dall'organigramma allegato alla presente relazione.

Politiche

Le politiche interne, volte a definire, coinvolgere, formare ed informare gli operatori su obiettivi, best practice e modalità operative sono esplicitati in fase di formazione, nonché accompagnati da un documento scritto con funzione di vademecum.

Gestione dei rischi sulla privacy

La formazione mirata, le procedure di gestione dei dati e di verifica costante, limitano i rischi sulla privacy.

La gestione di tali rischi, demandata ai responsabili, è parte integrante della formazione e delle buone pratiche.

Integrare la protezione della privacy nei progetti

Analizzando la gestione della protezione dati e tutela della privacy per singoli progetti, questi:

- rientrano nella privacy by design per quanto concerne modulistica, formazione e registri;
- rientrano nella privacy by default in merito all'attuazione specifica e al monitoraggio.

Gestione del personale

Il personale tratta esclusivamente dati essenziali per lo svolgimento dell'attività specifica, in proporzione al ruolo e in base alla competenza.

Lo stesso personale, adeguatamente formato, diventa elemento di gestione, monitoraggio e implementazione dei processi.

Gestire le violazioni dei dati personali

L'obiettivo primario, in materia di protezione dati, è la prevenzione di eventuali violazioni.

Inoltre, ai sensi dell'art. 33 del Reg. UE 679/16, in caso di DATA BREACH, la Società si obbliga ad avvisare gli interessati, nonchè a tracciare, monitorare e studiare l'evento al fine di determinare eventuali responsabilità, errori e possibili soluzioni.

Relazioni con terze parti

Le relazioni con parti terze saranno tutte normate da accordi e informative controfirmate.

Supervisione

Una ulteriore supervisione sull'Ente, oltre quanto già specificato, per la natura e per le finalità sociali dello stesso, nonché per la mole di dati particolari trattati, è demandata al RDP.

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?

Nella mole di dati trattati, spiccano quali dati particolari quelli legati a clienti non titolari di partita iva e a dipendenti, relativamente ad aspetti economici e fiscali, oltre a casi ex L.68 o L.104, ma si ricorda che le stesse informazioni sono condivise con contitolari afferenti all'amministrazione pubblica, al fine di garantire l'operatività dei contitolari stessi, nonché il legittimo interesse degli interessati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Ad oggi, visto l’approccio statistico e riepilogativo dei dati trattati dall'Ente, nonché la scarsa rilevanza del singolo dato, non si rilevano minacce specifiche.

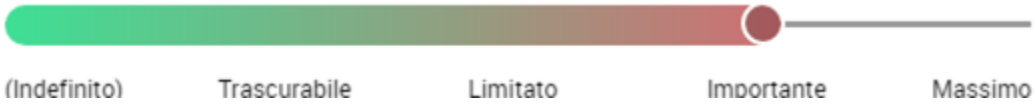
Quali sono le fonti di rischio?

Visto l'alto livello informatico-amministrativo dell'Ente, il rischio principale è dato dall'errore umano.

Quali dei controlli identificati contribuiscono a gestire il rischio?

Crittografia - Partizionamento dei dati - Anonimizzazione - Controllo degli accessi - Archiviazione - Tracciabilità - Sicurezza dei documenti cartacei - Vulnerabilità - Lotta contro il malware - Minimizzare la quantità di dati personali - Sicurezza dei siti web - Backup - Contratti di trattamento - Manutenzione - Sicurezza della rete - Politiche - Gestione dei rischi sulla privacy - Gestione postazioni - Monitoraggio dell'attività della rete - Controllo degli accessi fisici

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?



Secondo una stima prudenziale,che imputa alla Zincogam anche responsabilità di competenza dei contitolari, la gravità stimata risulta essere IMPORTANTE.

Questa metodologia di valutazione vuole dimostrare l'attenzione della Società verso gli Interessati, e l'impegno verso il rispetto della normativa.

Di fatto, a fronte di una gravità LIMITATA per le sole competenze della Zincogam, ulteriormente mitigata da procedure standardizzate obbligatorie soggette a tracciabilità e trasparenza, il Titolare del trattamento, consapevole delle complessità legate alla presenza di Contitolari, a tutela degli Interessati, si erge a garante e controllore, attuando best practice operative e di monitoraggio tanto per le attività interne quanto per i rapporti con l'esterno.

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?

Si ricorda quanto il Titolare del trattamento si spenda per best practice in materia di impostazione del lavoro, formazione, organizzazione e monitoraggio.

Tenendo conto che le medesime "informazioni" sono reperibili a mezzo dell'Ente, ma ancor più facilmente, purtroppo con meno limitazioni e accortezze, a mezzo dei Contitolari, la probabilità in capo al Titolare risulta LIMITATA.

MODIFICHE INDESIDERATE DEI DATI

Analizzare le cause e le conseguenze di modifiche indesiderate ai dati, e stimare la gravità la probabilità dell'evento.

Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?

Nella mole di dati trattati, spiccano quali dati particolari quelli legati a L. 104 e a soggetti con bisogni particolari ex L.68, e più in generale dati inerenti situazioni reddituali/lavorative/familiari.

P.Q.M.

Eventuali modifiche indesiderate potrebbero comportare l'errata attribuzione di diritti reali a danno di trasparenza e concorrenza, la pregiudizievole impossibilità di godere di diritti reali spettanti, nonché violazioni rimandabili al DVR.

Quali sono le principali minacce che possono portare al rischio?

Non si rilevano minacce specifiche, in quanto i dati particolari sono presenti anche, e con informazioni più complete, in database di terzi, permettendo la ricostruzione dell'informazione.

Quali sono le fonti di rischio?

Tra le fonti di rischio si annoverano:

- fonti umane interne;
- fonti umane esterne;
- automazzioni di sistema;
- danneggiamento hardware;
- disallineamento software.

Quali dei controlli identificati contribuiscono a gestire il rischio?

Partizionamento dei dati - Controllo degli accessi – Tracciabilità - Archiviazione - Sicurezza dei documenti cartacei - Minimizzare la quantità di dati personali - Lotta contro il malware - Gestione postazioni - Sicurezza dei siti web – Backup - Manutenzione - Sicurezza della rete - Controllo degli accessi fisici - Monitoraggio dell'attività della rete -
Sicurezza dell'hardware - Evitare le fonti di rischio - Protezione contro fonti di rischio non umane - Organizzazione - Politiche - Gestione dei rischi sulla privacy - Integrare la protezione della privacy nei progetti - Gestire le violazioni dei dati personali - Gestione del personale - Supervisione - Relazione con terze parti

Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

La gravità, seppur rilevante per impatto sugli interessati, è stimata LIMITATA in quanto mitigata dalle best practice e dai controlli pianificati dell'Ente.

Inoltre si precisa che i dati gestiti dall'Ente sono condivisi e finalizzati da Pubbliche Amministrazioni Contitolari, permettendo un controllo ulteriore, nonché una eventuale correzione immediata.

Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

Si ricorda quanto il Titolare del trattamento si spenda per best practice in materia di impostazione del lavoro, formazione, organizzazione e monitoraggio.

Tenendo conto che le medesime "informazioni" sono reperibili a mezzo dell'Ente, ma ancor più facilmente, purtroppo con meno limitazioni e accortezze, a mezzo dei Contitolari, la probabilità in capo al Titolare risulta LIMITATA.

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?

Nella mole di dati trattati, spiccano quali dati particolari quelli legati a L. 104 e a soggetti con bisogni particolari ex L.68, e più in generale dati inerenti situazioni reddituali/lavorative/familiari.

P.Q.M.

Eventuali perdite “temporanee” potrebbero comportare l’errata attribuzione di diritti reali a danno di trasparenza e concorrenza, la pregiudizievole impossibilità di godere di diritti reali spettanti, nonché violazioni rimandabili al DVR.

Quali sono le minacce che potrebbero portare al rischio?

Non si rilevano minacce specifiche, in quanto i dati particolari sono presenti anche, e con informazioni più complete, in database di terzi, permettendo la ricostruzione dell’informazione e la finalizzazione delle procedure.

Quali sono le fonti di rischio?

Tra le fonti di rischio si annoverano:

- Fonti umane interne
- Fonti umane esterne
- Automazioni di sistema
- Danneggiamento Hardware
- Disallineamento software

Quali dei controlli identificati contribuisce a gestire il rischio?

Anonimizzazione - Partizionamento dei dati - Controllo degli accessi - Tracciabilità - Archiviazione - Minimizzare la quantità di dati personali - Lotta contro il malware - Gestione postazioni - Sicurezza dei siti web - Backup - Manutenzione - Sicurezza della rete - Controllo degli accessi fisici - Monitoraggio dell'attività della rete - Sicurezza dell'hardware - Evitare le fonti di rischio - Protezione contro fonti - di rischio non umane - Organizzazione - Politiche - Gestione dei rischi sulla privacy - Integrare la protezione della privacy nei progetti - Gestione del personale - Relazioni con terze parti - Supervisione

Come stimeresti la gravità del rischio, specialmente riguardo il potenziale impatto e i controlli pianificati?

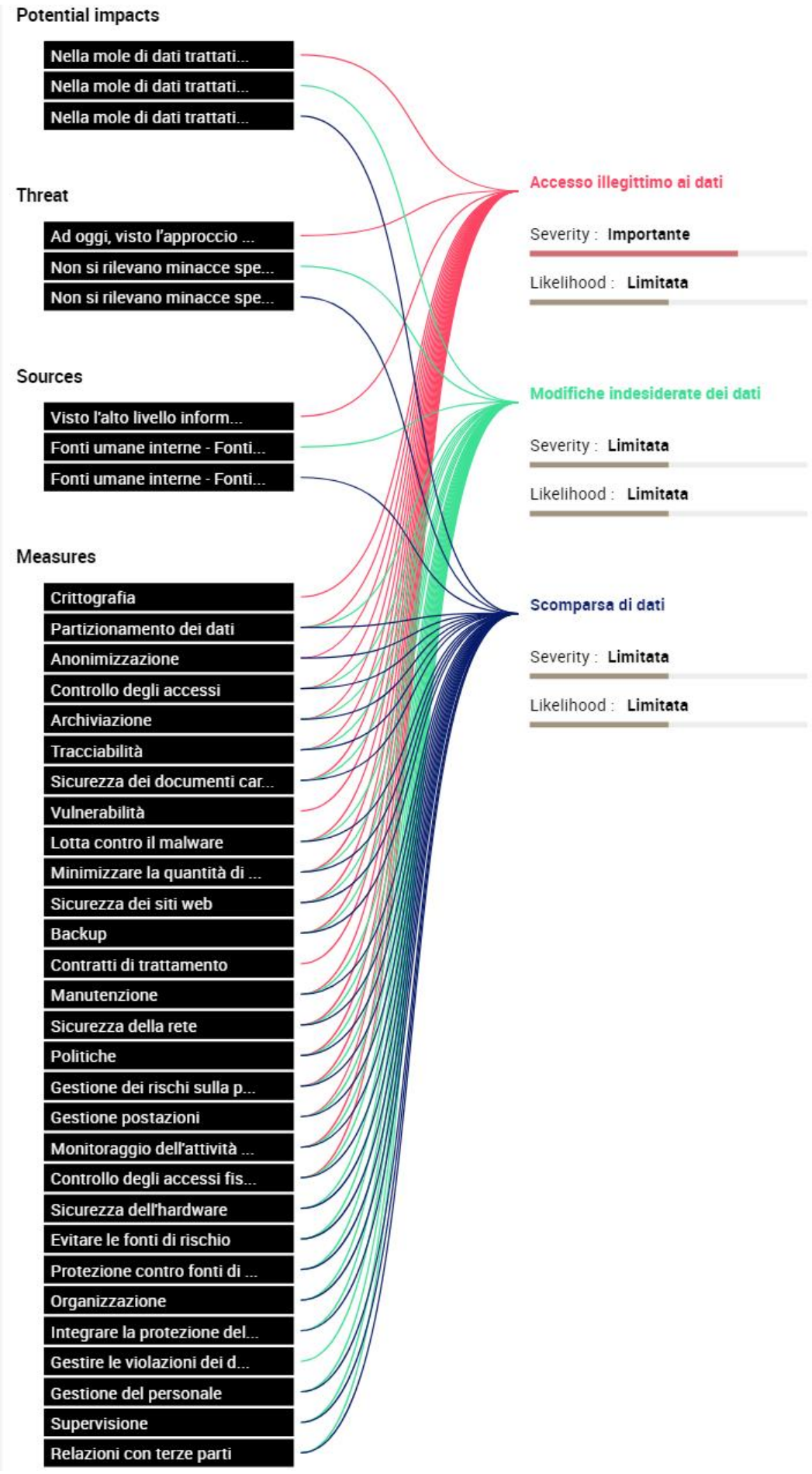
Ai fini della stima della gravità del rischio di perdita dei dati si demanda a quanto riportato nel paragrafo "MODIFICHE INDESIDERATE DEI DATI".

Come stimeresti la probabilità del rischio, specialmente rispetto le minacce, fonti di rischio e i controlli pianficati?

Ai fini della stima della gravità del rischio di perdita dei dati si demanda a quanto riportato nel paragrafo "MODIFICHE INDESIDERATE DEI DATI".

PANORAMICA DEL RISCHIO

Questa visualizzazione permette di avere una visuale globale e sintetica degli effetti dei controlli sui rischi che gestiscono.

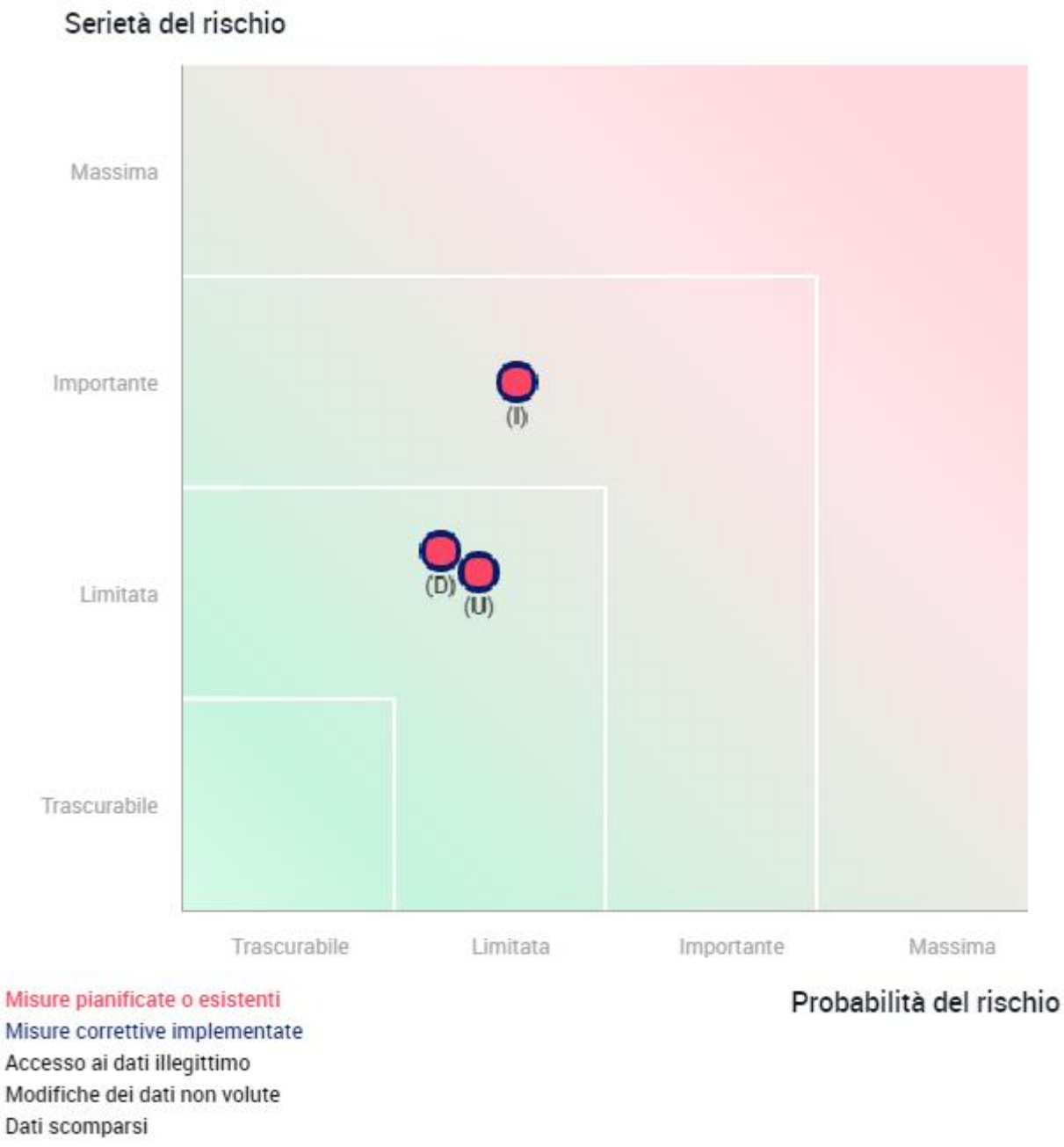


Convalida

Questa sezione permette di preparare e formalizzare la convalida PIA.

MAPPATURA DEL RISCHIO

Questa visualizzazione permette di comparare il posizionamento del rischio prima e dopo l'applicazione dei controlli complementari.



PIANO D'AZIONE

Pianificare in dettaglio l'implementazione di controlli aggiuntivi identificati durante il PIA.

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Dati adeguati
- Accuratezza dei dati
- Durata dell'archiviazione
- Informazioni per i soggetti interessati
- Ottenere il consenso
- Informazioni per i soggetti interessati
- Diritto di rettifica e cancellazione
- Diritto di restrizione e obiezione
- Subappalto
- Trasferimenti

Rischi

- Accesso illegittimo ai dati
- Modifiche dei dati non volute
- Dati scomparsi

Controlli pianificati o esistenti

- Anonimizzazione
- Partizionamento dei dati
- Controllo degli accessi
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti cartacei
- Minimizzare la quantità di dati personali
- Vulnerabilità
- Lotta contro il malware
- Gestione postazioni
- Sicurezza dei siti web
- Backup
- Manutenzione
- Contratti di trattamento
- Sicurezza della rete
- Controllo degli accessi fisici
- Monitoraggio dell'attività della rete
- Evitare le fonti di rischio
- Protezione contro fonti di rischio non umane
- Organizzazione
- Politiche
- Gestione dei rischi sulla privacy
- Integrare la protezione della privacy nei progetti
- Gestione del personale
- Gestire le violazioni dei dati personali
- Relazioni con terze parti
- Supervisione
- Sicurezza dell'hardware

Principi fondamentali

I Principi fondamentali sopra richiamati sono garantiti come riportato nelle best practice operative e nei codici di condotta (art.40 Reg. UE 679/2016).

Controlli pianificati o esistenti

Ad oggi i controlli pianificati sopra elencati risultano in linea con il contesto operativo, e sufficienti a garantire livelli adeguati di sicurezza rispetto ai rischi evidenziati.

Il relatore sottolinea come un controllo costante e il prosieguo delle attività istituzionali potranno suggerire eventuali implementazioni alla gestione dati e ai controlli stessi.

Rischi

I rischi sopra richiamati sembrano ben prevenuti e gestiti a mezzo delle best practice e dei controlli connessi.

Particolare rilevanza assume l'errata variazione di dati, che, nei rari casi di relazione con il pubblico, può derivare da fraintendimenti tra operatore e interessato al trattamento; in tal caso, al fine di tutelare l'interesse legittimo, è preferibile acquisire ulteriori dati certificati, allentando i limiti imposti dalla minimizzazione.

Di fatto i sistemi informatici su cui la Società opera svolgono una funzione di verifica, inabilitando la possibilità di operare in caso di dati incongruenti.

PARERI DI DPO E SOGGETTI INTERESSATI

Presentare l'opinione delle persone responsabili della protezione dei dati e dei problemi di privacy (o eventuali delegati). Presentare anche le opinioni dei soggetti interessati o di loro rappresentanti.

Parere DPO

Il DPO (Data Protection Officer) incaricato, Dott. Francesco Fasiello, verificate le informazioni riportate nella presente relazione, prende atto degli esiti dell'analisi dei rischi e la delle misure di sicurezza adottate.

Il DPO suggerisce di verificare metodicamente la corretta attuazione delle buone pratiche e delle misure di sicurezza, nonché di valutare eventuali misure ulteriori atte a migliorare il sistema di prevenzione e protezione.

Parere delle persone interessate

La società Zincogam spa resta a disposizione di tutti gli stake holder al fine di garantire i diritti degli stessi in materia di privacy e protezione dati.

Si invitano gli interessati e i portatori di interesse a interagire con la stessa a mezzo PEC all'indirizzo info@pec.zincogam.it al fine di prevenire e correggere potenziali disservizi, nonché di suggerire eventuali implementazioni del sistema di prevenzione e protezione.