Data Protection Impact Assessment

Marini Carmine S.r.l.

Indice

1. Panoramica

La società Marini Carmine S.r.l. opera in diversi settori del mercato, occupandosi principalmente delle seguenti attività: commercio al minuto ed all'ingrosso di tutti i materiali per l'edilizia; vendita di mobili ed accessori per bagni e cucine e prodotti speciali per l'edilizia in generale; commercio al minuto ed all'ingrosso di materiali, beni ed arredi inerenti l'abitazione, l'ufficio e altri locali a destinazione pubblica e privata; provvede al commercio, all'ingrosso e al dettaglio, di vestiario di qualunque tipo e pregio, maglieria esterna e camiceria comprese; produzione di accessori per l'abbigliamento; provvede al commercio di articoli da regalo, articoli sportivi, materiale cartaceo e di cancelleria; provvede alla gestione diretta o indiretta di servizi di imballaggio, consegna, spedizione, distribuzione, trasporto e vendita dei prodotti di cui sopra; stipulazione di contratti di deposito e di rappresentanza per ogni tipo di materiale oggetto dei servizi resi.

I dati raccolti riguardano categorie di interessati al trattamento comuni nel settore, come per esempio clienti, fornitori e dipendenti, e comuni sono le tipologie dei dati trattati (anagrafiche, dati commerciali, codici INPS, etc), minimizzati e strettamente necessari, *by default*, per il conseguimento delle finalità aziendali.

Per quantità, natura dei dati trattati e le diverse tipologie del loro trattamento, non sono presenti rischi elevati per i diritti e le libertà delle persone fisiche, tuttavia la DPIA viene effettuata per limitare ulteriormente le possibilità che detti rischi si concretizzino, nonché al fine di dimostrare la responsabilizzazione e la trasparenza del titolare del trattamento.

Essendo i trattamenti simili tra loro viene effettuata una singola valutazione.
Non sono ancora disponibili codici di condotta ufficiali o condivisi.

Introduzione

La valutazione d'impatto sulla protezione dei dati (DPIA, acronimo di Data Protection Impact Assessment) rappresenta l'output del processo di analisi del trattamento dei dati personali per la Marini Carmine S.r.l. Questo documento è quindi un'analisi delle attività di trattamento attualmente gestite e delle relative valutazioni. Esso evidenzia i dettagli dell'attività di elaborazione stessa e fornisce una valutazione dei rischi associati al trattamento, suggerendo eventualmente le misure che possono essere adottate per mitigarli, anche grazie ad un'eventuale consultazione preliminare con il Responsabile per la Protezione dei Dati (RDP) competente.

Il titolare del trattamento elabora la DPIA ai sensi dell'articolo 35 del GDPR, laddove il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche (l'interessato).

Questo documento, nelle sue varie parti:

- valuta i rischi per la privacy personale nei processi di Marini Carmine;
- identifica le misure, le salvaguardie e i meccanismi esistenti o pianificati per garantire la protezione dei dati personali;
- identifica, ove ve ne sia necessità, il corretto bilanciamento tra i diritti alla privacy dell'individuo e quelli di raccolta ed elaborazione dei dati per finalità legittime di Marini Carmine.

Contesto

Il trattamento dei dati personali è realizzato per mezzo delle operazioni indicate all'art. 4 Codice Privacy e all'art. 4 n. 2) GDPR e precisamente: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione dei dati. I dati personali sono sottoposti a trattamento sia cartaceo che elettronico e/o automatizzato.
Il trattamento riguarda le seguenti categorie di dati:

- dei clienti e dei referenti commerciali delle aziende clienti/fornitori;
- dei dipendenti.

I dati relativi ai dipendenti riguardano: anagrafiche (nome, cognome, recapiti telefonici, residenza, e-mail), curriculum vitae, coordinate bancarie per pagamento degli stipendi. Tali dati sono acquisiti per consenso degli interessati al momento della sottoscrizione del contratto di lavoro e sono destinati all'amministrazione di Marini Carmine S.r.l. per le attività di gestione del rapporto d'impiego.

I dati relativi alla retribuzione del personale sono inviati tramite email in chiaro ad un consulente del lavoro esterno per la formulazione delle buste paga, le quali, una volta ricevute, vengono consegnate *brevi manu* ai dipendenti.

I dati relativi ai referenti commerciali delle imprese clienti/fornitrici riguardano: anagrafiche (come sopra), indicazione della azienda di appartenenza e tutti i dati necessari per l'esercizio del rapporto commerciale. Tali dati sono acquisiti per consenso degli interessati al momento della sottoscrizione del contratto commerciale e sono destinati al personale di Marini Carmine S.r.l.

Schema di riepilogo

Tavola di Riferimento con le Informazioni Chiave		
(a)	Titolare del trattamento	Marini Carmine S.r.l. Marini Edi
(b)	Responsabile del trattamento	Responsabill esterni Polymatic S.r.l P.IVA IT01871190698 1&1 Internet SE Germania
(c)	Descrizione del Trattamento	Trattamento commerciale Trattamento dipendenti
(d)	Scopo del Trattamento	Esecuzione contratti commerciali Esecuzione contratti lavorativi
(e)	Contesto, ambito e background	Ambito commerciale (dati relativi ai referenti) Ambito lavorativo (dati relativi ai dipendenti). Acquisiti contestualmente alla stipula dei contratti, con consenso.
(f)	Soggetti e relative mansioni, coinvolti nel trattamento	Titolare del trattamento Responsabili esterni Incaricati
(g)	Tipologia di dati personali	Anagrafici relativi ai referenti aziendali Anagrafici, codici malattia, presenze relativi ai dipendenti
(h)	Categorie speciali di dati	Assenti
(i)	Destinatari dei dati personali	Amministrazione e dirigenza, interni all'azienda Consulenti esterni

Il trattamento ha finalità legate all'esecuzione dei contratti (commerciali, di lavoro subordinato, mandati con agenti) e non eccede tale finalità. La società Marini Carmine S.r.l. non effettua alcun tipo di profilazione e la gestione del trattamento viene esplicitata nell'Informativa Aziendale. Il consenso viene esplicitamente richiesto ai soli lavoratori dipendenti ed in relazione al trattamento condiviso con il consulente del lavoro. I dati raccolti, sia come singolo record che come aggregati, non eccedono la portata strettamente necessaria alla finalità, dunque sono minimizzati, *by default*, le eventuali integrazioni richieste hanno esclusivamente relazione allo scopo definito.

Attualmente i dati hanno un periodo di archiviazione indefinito, ma viene proposto, tra i remedies di limitarne l'archiviazione ai soli fini legali (creditizi o fiscali) i dati vengono aggiornati con regolarità nell'interesse delle imprese clienti o del lavoratore.

2. Processo di valutazione dei trattamenti

Flusso operativo

Le operazioni di elaborazione previste nel processo di valutazione dei trattamenti possono essere suddivise in sei fasi:

1. **Pianificazione della Valutazione**
   Sono individuate le funzioni aziendali e le persone che possono rendere disponibili le conoscenze, le prassi e la documentazione presenti in azienda, per quanto riguarda il trattamento dei dati e le esigenze tecniche e normative del GDPR. E si stabilisce un piano di attività per lo svolgimento del processo di valutazione.

2. **Raccolta e analisi dei dati**
   In questa fase vengono raccolte tutte le informazioni necessarie a mappare i sistemi informativi ed il flusso di gestione documentale presenti in Marini Carmine. L'obiettivo è che lo sforzo di adeguamento alle linee guida del GDPR comporti un complessivo miglioramento degli asset aziendali, informativi e tecnici.

3. **Stesura e redazione della DPIA**
   In base alle risultanze delle interviste ed all'analisi dei dati viene redatta la DPIA, che può anche essere in versione preliminare, valida per un periodo pilota, trascorso il quale dovrà essere rivista ed aggiornata. È previsto in ogni caso un aggiornamento con cadenza almeno annuale.

4. **Revisione di gruppo**
   Il documento finale viene revisionato alla presenza del Responsabile IT, nella persona del titolare Marini Edi, e quindi sottoposto agli organi amministrativi dell'azienda e, per presa visione, agli stakeholders che ne facciano richiesta.

5. **Redazione dei report**
   Una volta terminata la valutazione, con cadenza annuale, si procede alla redazione di report, che costituiranno parte integrante di un processo di revisione atto a garantire che l'analisi del rischio venga effettuata correttamente, innescando un processo di revisione e aggiornamento continuo.

6. **Condivisione dei risultati**
   A revisioni concluse, e dopo aver contribuito alla redazione dell'informativa e alla costruzione del registro dei trattamenti, i risultati sono condivisi tra il titolare e chi è intervenuto nel processo.

Mappatura dei Dati

In questa sezione della DPIA è presentata una mappatura approfondita di tutti i dati personali presenti nei contesti aziendali della Marini Carmine srl.

Le attività di archiviazione sono effettuate, per i dati digitali, su un software gestionale ad uso interno, su un server aziendale locale, gestito da un'azienda esterna (Polymatic); i dati cartacei, invece, sono conservati in archivio, sito nei locali degli uffici amministrativi, il cui accesso è ristretto ai soli autorizzati.

Sul sito web è presente un modulo di contatto clienti con il quale vengono raccolti i dati dei clienti che ne fanno uso, dati che poi vengono inviati via mail ai dipendenti di Marini Carmine S.r.l. e che vengono conservati nel server aziendale per non più di 90 giorni. Salvo quest'ultimo, non sono attualmente definiti ulteriori termini massimi di conservazione dei dati.

Dati gestione Dipendenti:

- Nome, Cognome, Recapiti telefonici, Indirizzi residenza e mail, Coordinate bancarie per pagamento stipendi, Curriculum Vitae
- Destinati a: Amministrazione Marini Carmine S.r.l.

Dati gestione commerciale referenti clienti e fornitori

- Nome, Cognome, Recapiti telefonici, indirizzi Mail, Azienda di appartenenza.
- Destinatari: personale Marini Carmine srl, di cui un Dirigente, 3 Amministrazione, 2 Commessi e 4 Operai; per un totale di circa 12 dipendenti, sono incaricati a trattare i dati personali di Marini Carmine S.r.l.)

Archiviati su:

- Software gestionale per uso interno installato su server aziendale locale, ma gestito da azienda esterna (Polymatic)
- Armadio in archivio cartaceo negli uffici amministrativi di Marini Carmine (restrizione degli accessi all'archivio ai soli autorizzati)

Modulo di contatto clienti su sito web dell'azienda (il sito è gestito da azienda esterna ed è basato sul CMS WordPress). Il modulo raccoglie dati personali (Nome, Cognome ed Email) di chi utilizza la form contatti, li memorizza su un DB interno e li invia via mail ai dipendenti Marini Carmine S.r.l. I dati vengono archiviati nel DB per una durata di 90 giorni prima di essere cancellati.

Non sono definite durate massime del tempo di vita dei dati. Alcuni dati in archivio cartaceo potrebbero aver superato il tempo di vita massimo stimato e andrebbero eliminati.

I dati riguardo le prestazioni lavorative dei dipendenti Marini Carmine S.r.l. vengono inviati via mail ad un consulente del lavoro esterno per la preparazione delle buste paga; le quali vengono inviate all'amministrazione della Marini Carmine sempre via mail, per poi essere consegnate brevi manu ai dipendenti.

Risorse coinvolte nel processo di trattamento dei dati

Questa sezione della DPIA contiene un elenco delle risorse attraverso le quali avviene l'elaborazione dei dati personali, sia interni che esterni alla Marini Carmine.

Internal IT

(Sistemi IT interni all'azienda/Ente)

Postazioni PC dei dipendenti, per elaborazione dati ed accesso al software gestionale.

Un server aziendale locale, su cui è installato un software gestionale, prodotto da Polymatic, utilizzato internamente.

External IT

(Sistemi IT esterni all'azienda/Ente)

Sito web con form di contatto. (Il sito è su dominio 1&1).

Not IT Assessment

(Sistemi di trattamento non informatizzati)

Archivio cartaceo presso gli uffici amministrativi di Marini Carmine.

Gestione degli accessi ai trattamenti

In questa sezione vengono descritte le misure, regole, procedure e norme per la gestione degli accessi ai trattamenti.

Identificazione e autenticazione

I PC sono privi di password, le credenziali vengono attribuite ai dipendenti, non viene seguita una password policy.

Controllo accessi

Software gestionale ad accesso ristretto e riservato (Polymatic).

Gestione dei supporti e dei documenti cartacei

Archivi documentali cartacei in locali ad accesso ristretto.

Gestione delle risorse umane

In questa sezione vengono descritte le procedure di gestione delle risorse umane coinvolte nel trattamente dei dati personali: politiche di formazione, funzioni e obblighi ed eventuali previsioni sanzionatorie per i trasgressori.

Formazione

Viene effettuato un intervento di formazione a seguito della compliance al GDPR

Funzioni e obblighi

Non sono previsti attualmente, obblighi specifici per il trattamento dei dati personali.

Conseguenze per violazioni

Attualmente non sono previste sanzioni contrattuali per violazione degli obblighi di tutela della privacy.

Acquisizione dati personali

Questa sezione descrive in dettaglio i tipi di informazioni personali che l'azienda/Ente raccoglie dagli interessati:

I soggetti interessati vengono informati del trattamento, tramite il rimando all'Informativa aziendale e con il consenso inserito a latere del contratto (commerciale e di lavoro). Il consenso viene firmato contestualmente al contratto. Su richiesta firmata, i dati vengono concessi ai fini della portabilità. Il diritto alla cancellazione viene concesso su richiesta firmata, salvo finalità legali o fiscali che lo rendano illegittimo. Non sono definite durate massime del tempo di vita dei dati. Alcuni dati in archivio cartaceo potrebbero aver superato il tempo di vita massimo stimato e andrebbero eliminati.
Dipendenti:

- Nome, Cognome
- Indirizzo
- Indirizzo Email
- Numeri di telefono fisso e cellulare
- Dati finanziari
- Codice Fiscale o Partita IVA
- Curriculum Vitae
- Orari di entrata e uscita del dipendente

Referenti Commerciali:

- Nome, Cognome
- Indirizzo
- Azienda per cui lavora e posizione aziendale
- Numeri di telefono fisso e cellulare
- Codice Fiscale o Partita IVA

L'eventuale collezione di dati appartenenti alle cosiddette categorie particolari di dati personali (Art. 9 Reg. UE 679/2016) è indicata nel riquadro seguente:

Assenti.

3. Necessità e proporzionalità del trattamento

La validità di quanto dedotto durante il processo di valutazione è direttamente connesso all'integrità e alla completezza delle informazioni raccolte nello svolgimento dello stesso.

Contesto generale che giustifica il trattamento e la valutazione d'impatto

Considerata la natura dei dati raccolti, il contesto, l'ambito e le finalità legittime dei trattamenti, tenuto conto delle indicazioni contenute nei "*considerando dal 47 al 51"* del *Regolamento (UE) 2016/679*, la valutazione d'impatto non risulta obbligatoria, tuttavia viene effettuata al fine di ridurre ulteriormente il rischio di eventuali minacce all'integrità dei diritti e le libertà degli interessati. La raccolta dei dati è limitata a quelli necessari per l'esecuzione dei contratti commerciali e di lavoro, la valutazione d'impatto, non obbligatoria, viene effettuata al fine di ridurre il rischio di possibili violazioni.

Interessi legittimi

La Marini Carmine gestisce trattamenti come descritto in **Sezione 1** e **Sezione 2**. I trattamenti dei dati personali sono funzionali all'ottenimento degli interessi legittimi di Marini Carmine e non vengono usati per altri fini.

Marini Carmine ha pertanto un legittimo interesse:

I trattamenti descritti e mappati nella DPIA sono conformi con le indicazioni del considerando 47 (GDPR) e non sussistono altre finalità oltre quelle relative alla corretta esecuzione dei contratti commerciali e di lavoro, stipulati dal titolare del trattamento
Come datore di lavoro, la Marini Carmine s.r.l. raccoglie dati del personale e partner esterni al fine di:

- Offrire corretta esecuzione dei rapporti contrattuali
- Migliorare le capacità personali
- Rispondere alle esigenze di conformità normativa
- Garantire produttività e retribuzione del personale dipendente
- Misurare la qualità dei programmi aziendali e performance

Come partner commerciale delle aziende clienti per

- Migliorare la comunicazione commerciale e la produttività
- implementare delle performance commerciali
- Fornire una base su cui assegnare titoli o certificati
- Offrire corretta esecuzioni dei contratti

4. Rischi e Correttivi

Metodologia di valutazione del rischio

Il campo di applicazione di questa valutazione è limitato ai rischi che potrebbero comportare danni fisici, materiali o immateriali alla persona interessata (soggetto portatore di interessi), comprese eventuali discriminazioni, danni alla reputazione, perdita di riservatezza dei dati protetti dal segreto professionale, o qualsiasi altro significativo svantaggio economico o sociale. Eventuali altri rischi cui l'organizzazione può esporsi, ma che non incidono sulla privacy, sono oltre lo scopo della presente DPIA.

Nella analisi, tutti i rischi sono anche associati a una probabilità:

- ❑ **4: Quasi certo.** Probabilità estremamente alta. Il verificarsi dello scenario costituisce un evento quasi certo.
- ❑ **3: Probabile.** Alta possibilità che lo scenario descritto possa verificarsi.
- ❑ **2: Possibile.** Possibilità media che lo scenario descritto possa verificarsi.
- ❑ **1: Improbabile**. Possibilità bassa che lo scenario possa verificarsi.
- ❑ **0: Quasi impossibile.** Possibilità quasi nulla che lo scenario possa verificarsi.

I rischi sono anche associati a una gravità.

- ❑ **4: Critico.** Danno significativo e reale a un gran numero di interessati (soggetti dei dati), ad esempio una violazione dei dati su larga scala.
- ❑ **3: Grave.** Danno significativo e reale a uno o ad un numero limitato di interessati o danno di entità minore a un gran numero di interessati.
- ❑ **2: Moderato.** Danno di entità limitata a uno o ad un numero limitato di interessati o invece danno di entità minima a un gran numero di interessati.
- ❑ **1: Minimo.** Problema minore o procedurale che non comporta danni significativi.
- ❑ **0: Quasi nullo.** Non vi è praticamente alcun danno reale *(e.g. furto/perdita di dati anonimizzati o pseudonimizzati)*.

Minacce ai dati personali

A seguire vengono indicate le possibili minacce alla privacy, dal punto di vista dell'interessato:

1. **Divulgazione di dati personali.** Le informazioni fornite al titolare del trattamento sono confidenziali e potrebbero arrecare un danno all'interessato se circolassero impropriamente.
2. **Integrità dei dati personali.** L'interessato potrebbe subire un danno qualora i suoi dati personali - sebbene utilizzati legittimamente - risultassero non corretti, o venissero corrotti durante il trasporto/elaborazione/archiviazione, oppure risultassero confusi erroneamente con i dati di un'altra persona.
3. **Perdita di dati personali.** L'interessato ha la legittima aspettativa che i propri dati vengano custoditi in maniera sicura e possano essere recuperati durante l'intero periodo di conservazione.
4. **Mancanza di capacità di esercitare i diritti previsti dalla legge sulla protezione dei dati.** L'interessato ha la legittima aspettativa di poter esercitare i diritti garantiti dal Regolamento UE 679/2016 e potrebbe subire un danno dalla mancata capacità del Titolare del trattamento di adempiere ai suoi doveri.

Le sezioni seguenti trattano i rischi relativi a queste minacce, considerando separatamente:

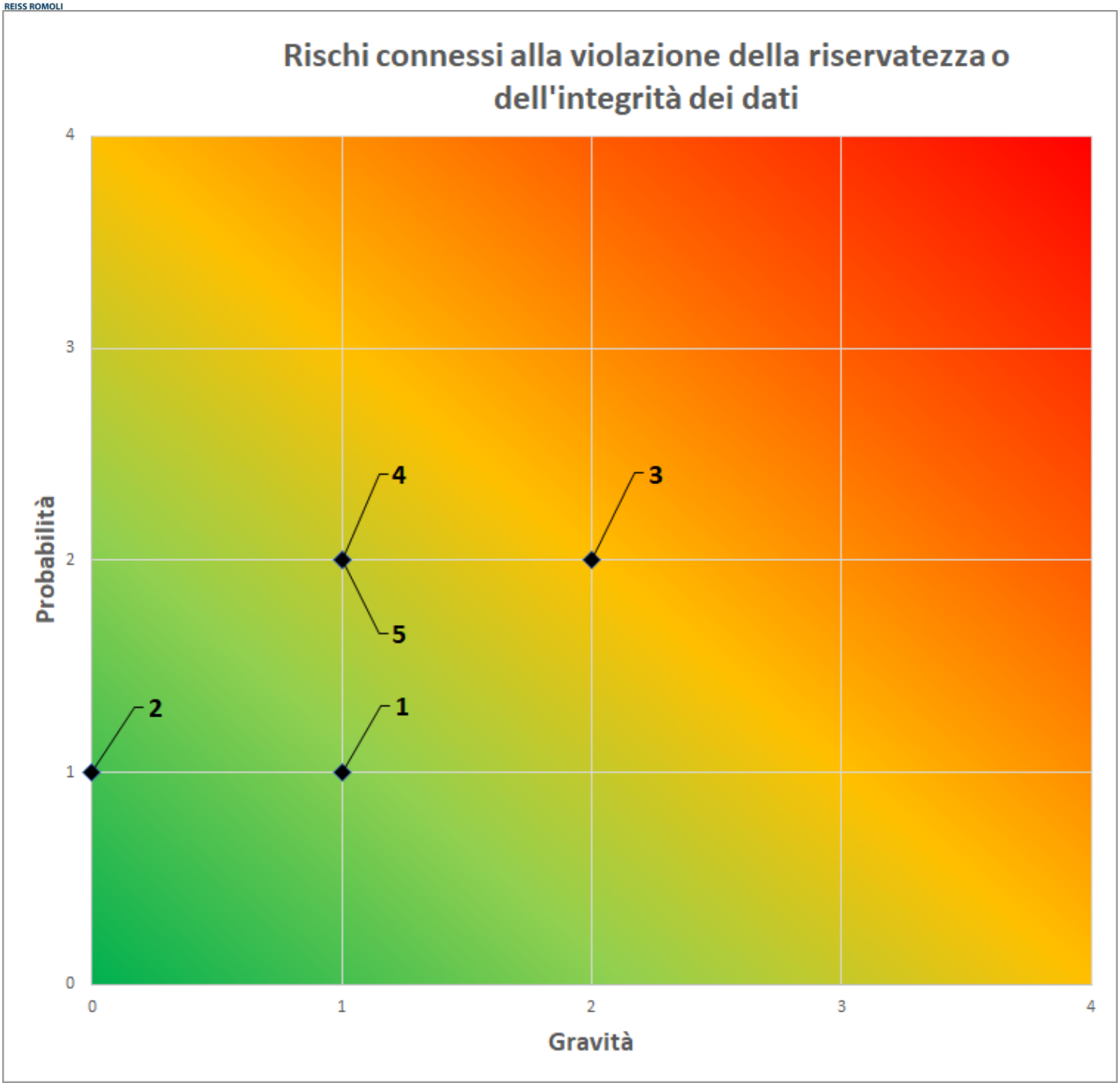
- Minacce alla riservatezza o all'integrità dei dati personali (punti 1 e 2 dell'elenco);
- Minacce alla perdita o alla disponibilità di dati personali (punto 3 dell'elenco);
- Minacce alla facoltà di esercitare i propri diritti secondo GDPR (punto 4 dell'elenco).

Rischi connessi alla violazione della riservatezza o dell'integrità dei dati

La tabella seguente mostra i rischi relativi alla violazione della riservatezza o dell'integrità dei dati personali.

Ar	ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
T	**1**	Intercettazione di dati in transito nel software gestionale interno durante la trasmissione, l'utilizzo o la visualizzazione.	1	1	**Correttivi in atto**: - Il software gestionale accessibile solo dalla intranet aziendale. - La rete wi-fi è protetta da protocollo crittografico WPA2. **Correttivi suggeriti**: - **Correttivi possibili**: -
T	**2**	Accesso fisico ai dati in trattamento memorizzati nei server.	0	1	**Correttivi in atto**: - Il server e le workstation dei dipendenti sono in locali ad accesso ristretto, protetti con sistemi anti intrusione. **Correttivi suggeriti**: - **Correttivi possibili**: -
T	**3**	La vulnerabilità del software, la mancata patch o il malware nel sistema consentono l'accesso di un utente malintenzionato e causano una violazione dei dati.	2	2	**Correttivi in atto**: - Antivirus installati sulle workstation dei dipendenti, tuttavia non è in atto una soluzione omogenea (AV di diverse marche, sia pro che free) **Correttivi suggeriti**: - Utilizzare una soluzione Antivirus omogenea per i sistemi. - Pianificare aggiornamenti costanti o utilizzare un sistema di distribuzione automatica per l'update dei sistemi operativi delle workstation. **Correttivi possibili**: - Pianificare ed implementare l'attivazione di un dominio Active Directory.
T	**4**	La password dell'amministratore o degli incaricati per l'accesso al software gestionale interno viene indovinata, trovata, o ottenuta consentendo	1	2	**Correttivi in atto**:

		l'accesso ai dati nel sistema o nei sistemi organizzativi.			- Password policy in atto per la definizione delle credenziali dei dipendenti aziendali. - Accessi al gestionale distinti per ogni dipendente. **Correttivi suggeriti**: - Definire password complesse (o direttamente nuove password policy) anche per l'accesso alle workstation. **Correttivi possibili**: -
T	**5**	Le informazioni vengono recuperate in modo illecito dall'accesso non autorizzato ai sistemi della Marini Carmine S.r.l. da locazioni remote.	1	2	**Correttivi in atto**: - Firewall personali attivi sulle workstation. - Firewall perimetrale presente nel router dell'ISP. **Correttivi suggeriti**: - **Correttivi possibili**: - Installazione di un firewall aziendale perimetrale, a protezione della rete interna.

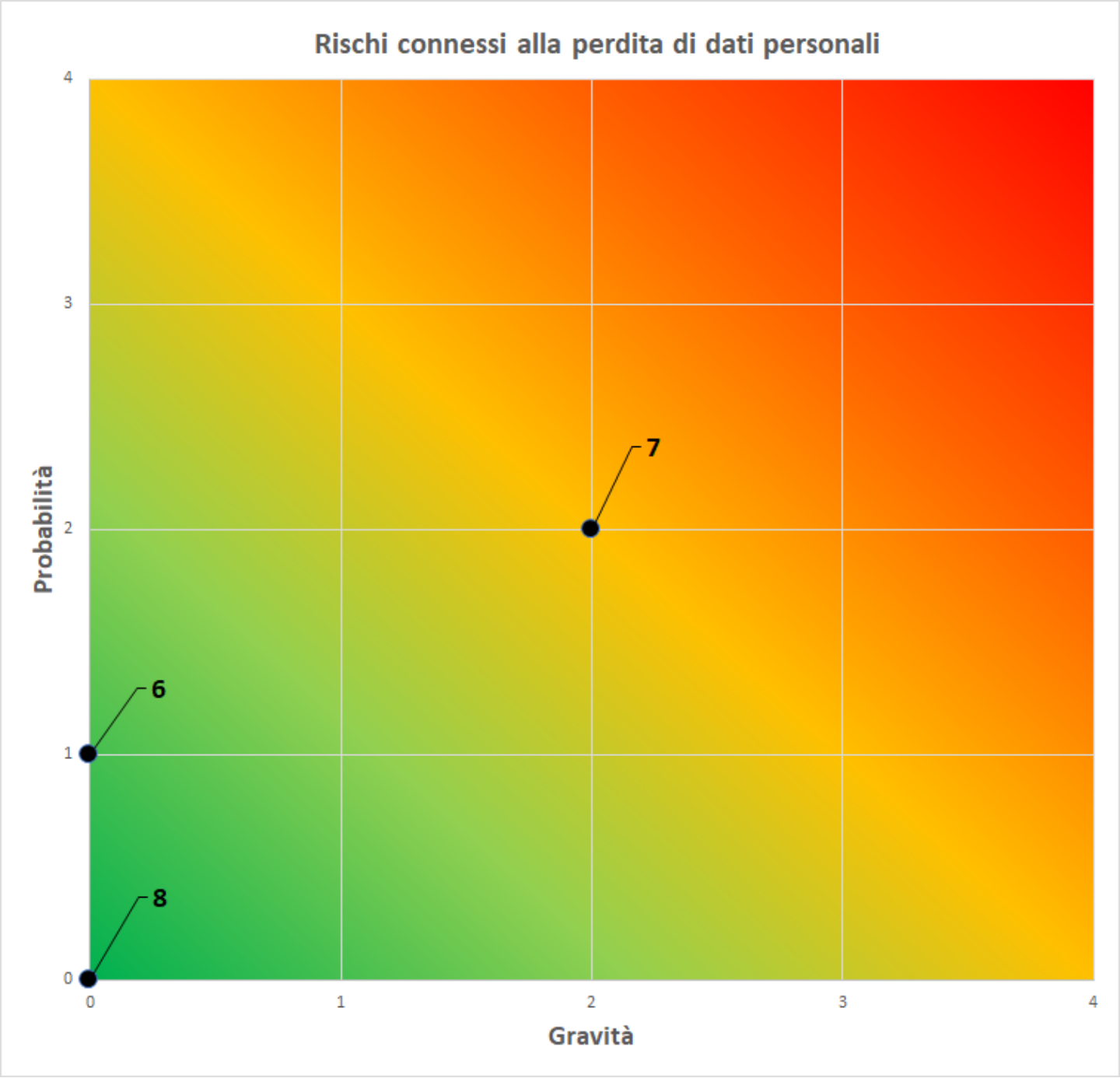


Rischi connessi alla perdita di dati personali

La tabella seguente mostra i rischi relativi alla perdita o alla cancellazione dei dati personali. Si noti che alcuni dei rischi valutati nella precedente tabella potrebbero anche comportare la cancellazione/perdita dei dati, e pertanto figurare anche nella presente Sezione.

Ar	ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
T	6	Il fallimento del backup che implica una perdita permanente di dati	0	1	**Correttivi in atto**:

					- (Pianificato) Backup da effettuare, con regolarità, sul NAS interno ai locali Marini. (NOTA: i dati di Marini ricevevano un Backup regolare online a cura di Euro Service, tuttavia il contratto è stato interrotto circa un anno e mezzo fa ed i dati di Marini potrebbero essere presenti ancora presso gli archivi Euro Service, a cui è stato chiesto di eliminarli. Si potrebbe pensare di avviare nuovamente un contratto di questo tipo). **Correttivi suggeriti**: - **Correttivi possibili**: - Possibilità di eseguire una copia mensile dei backup, dal NAS ad un servizio Cloud.
T	**7**	La vulnerabilità del software, le mancata patch o il malware possono causare la perdita di dati di dati (Ex. ransomware)	2	2	**Correttivi in atto**: - Antivirus installati sulle workstation dei dipendenti, tuttavia non è in atto una soluzione omogenea (AV di diverse marche, sia pro che free). **Correttivi suggeriti**: - Utilizzare una soluzione Antivirus omogenea per i sistemi. - Pianificare aggiornamenti costanti o utilizzare un sistema di distribuzione automatica per l'update dei sistemi operativi delle workstation. **Correttivi possibili**: - Pianificare e implementare l'attivazione di un dominio Active Directory.
T	**8**	Interruzione durante il trattamento (ad esempio guasto dell'attrezzatura, guasto della connettività, allarme antincendio)	0	0	**Correttivi in atto**: - Vengono eseguiti controlli regolari, ed aggiornati annualmente, sullo stato di sicurezza fisica dell'edificio e delle strutture annesse. **Correttivi suggeriti**: - **Correttivi possibili**: - Installazione di un UPS a cui connettere i sistemi su cui è in esecuzione il gestionale.

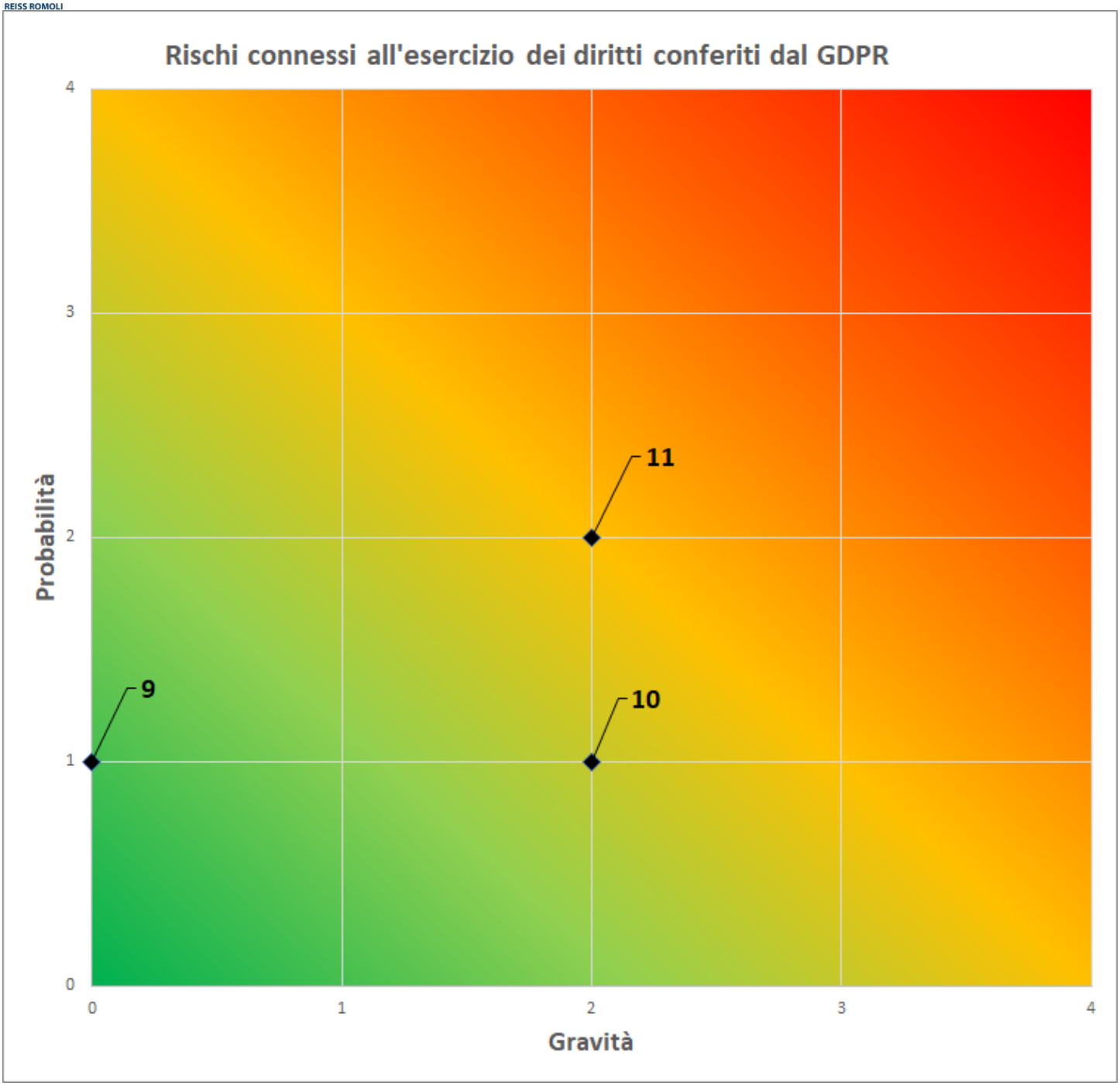


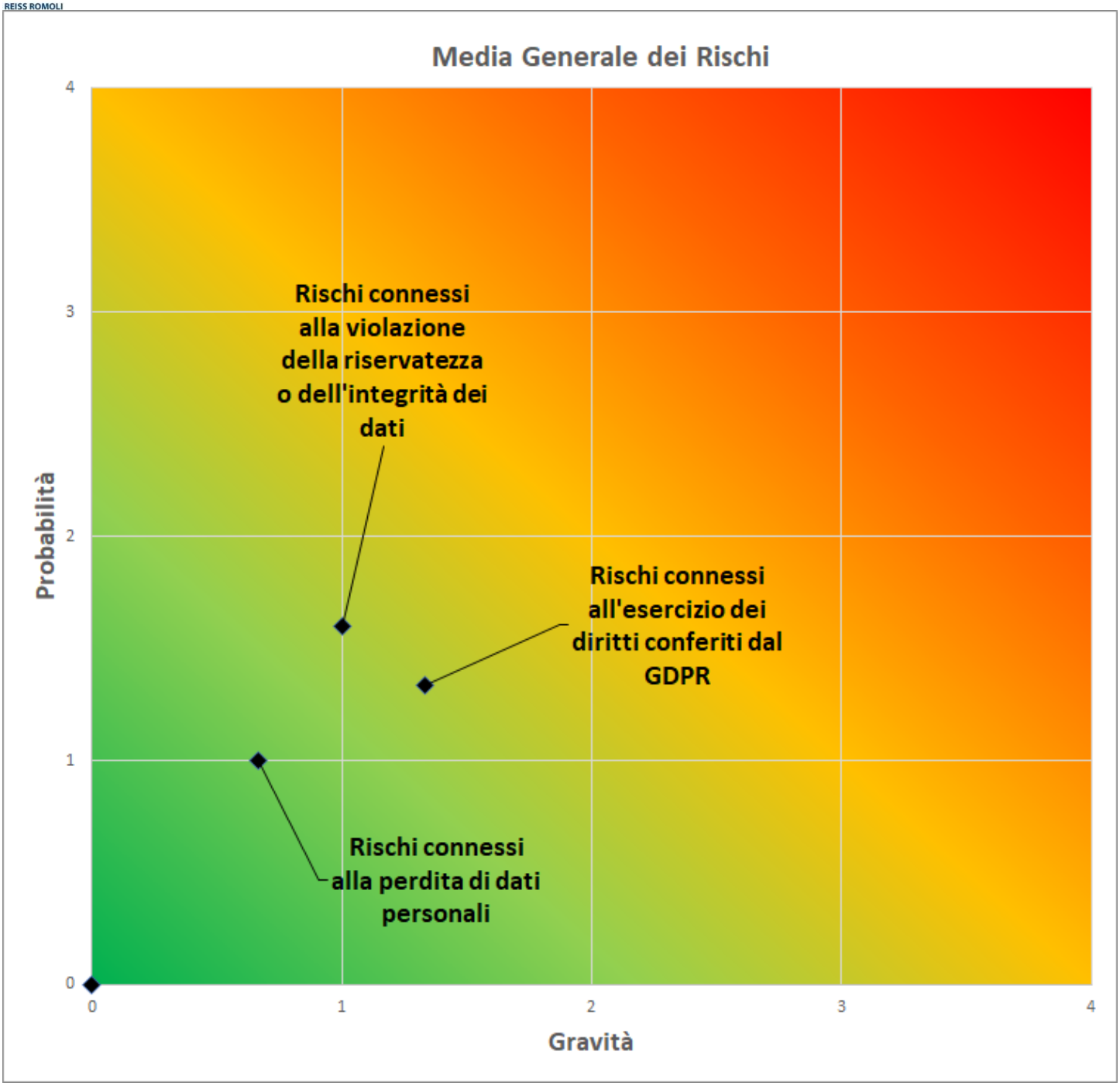
Rischi connessi all'esercizio dei diritti conferiti dal GDPR

La tabella seguente mostra i rischi relativi alla mancata facoltà di esercitare i propri diritti.

Ar	ID	Natura del rischio	Probabilità	Gravità	Correttivi e adeguamenti possibili
T	**9**	Rischio che i dati vengano elaborati da un incaricato (al trattamento dei dati	0	1	**Correttivi in atto**:

		personali) che non soddisfa i requisiti di protezione dei dati			- Gli incaricati che hanno accesso ai dati personali sono definiti chiaramente nell'organigramma aziendale. - L'accesso all'archivio cartaceo è ristretto e limitato ai soli aventi diritto. - Esistono account distinti, per ciascun dipendente, per l'accesso al gestionale. **Correttivi suggeriti**: - Definire un tempo di vita massimo per tutti i dati ed un processo interno per cancellare quei dati che hanno oltrepassato il tempo di vita massimo **Correttivi possibili**: -
T	**10**	I dati personali vengono conservati più a lungo del necessario	2	1	**Correttivi in atto**: - È facile tracciare i dati immagazzinati nel software gestionale a fine di cancellazione. **Correttivi suggeriti**: - **Correttivi possibili**: -
T	**11**	Difficoltà e non immediatezza nel rilevare ed identificare una fuoriuscita dei dati archiviati nelle Basi di Dati del software gestionale interno, può condurre alla non possibilità di ottemperare all'obbligo di notifica al Garante.	2	2	**Correttivi in atto**: - **Correttivi suggeriti**: - Richiedere alla Polymatic l'attivazione della feature che abilita il controllo e la notifica degli accessi al software gestionale. **Correttivi possibili**: - Backup dei log degli accessi al server e delle operazioni utente.


Rischi connessi all'esercizio dei diritti conferiti dal GDPR
Probabilità
Gravità
0
1
2
3
4
9
10
11



Misure relative alla sicurezza e controlli esistenti o pianificati

Ar	ID	Misura di sicurezza	Tipologia	SI	NO
T	1	Crittografia			x
T	2	Anonimizzazione			x
T	3	Partizionamento dei dati			x
T	4	Controllo degli accessi	Locali protetti da sistemi anti intrusione. Archivi di Dati personali in locali ad accesso ristretto ai soli aventi diritto.	x	
T	5	Tracciabilità			x

T	6	**Archiviazione**			x
T	7	**Sicurezza dei documenti cartacei**	Archivio documentale cartaceo ad accesso ristretto.	x	
L T	8	**Minimizzazione dei dati**	Marini Carmine acquisisce una quantità di dati minimizzati.	x	
T	9	**Vulnerabilità**			x
T	10	**Prevenzione malware**	Postazioni PC con antivirus installati (non omogenei: sia pro che free e di diversi brand).	x	
T	11	**Gestione postazioni**			x
T	12	**Sicurezza dei siti web**			x
T	13	**Backup**	Pianificato: backup regolari su NAS dei dati presenti nelle Basi di Dati del software gestionale.	x	
T	14	**Manutenzione**	Marini Carmine ha un contratto per la manutenzione dei propri sistemi (hardware e software) con aziende esterna.	x	
L	15	**Contratti di trattamento**	I responsabili esterni hanno adeguato i prodotti al GDPR. Stipulare nomine agli incaricati.	x	
T	16	**Sicurezza della rete**			x
L T	17	**Controllo degli accessi fisici**	Locali ad accesso ristretto, protetti da sistemi anti intrusione.	x	
T	18	**Monitoraggio dell'attività della rete**			x
T	19	**Sicurezza dell'hardware**			x
L	20	**Prevenzione dalle fonti di rischio**	Controlli regolari ed aggiornati annualmente sullo stato di sicurezza fisica dell'edificio e delle strutture annesse. Sistemi antintrusione e videosorveglianza per proteggere gli accessi alla struttura.	x	
L	21	**Protezione contro le fonti di rischio**	Controlli regolari ed aggiornati annualmente sullo stato di sicurezza fisica dell'edificio e delle struttura annesse.	x	
L	22	**Organizzazione**			x
L T	23	**Politiche**			x
L T	24	**Gestione dei rischi sulla privacy**			x
T	25	**Privacy by Design**			x
L T	26	**Gestire le violazioni della privacy**			x
L	27	**Gestione del personale**			x
L	28	**Relazioni con terze parti**			x
L	29	**Supervisione**			x
T	30	**Pseudonimizzazione**			x

5. Informazioni di supporto

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per:
    - "affrontare i rischi";
    - "dimostrare la conformità al regolamento".

Nel valutare l'impatto di un trattamento va tenuto conto (articolo 35, paragrafo 8) del rispetto di un codice di condotta (articolo 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche certificazioni, sigilli e marchi al fine di dimostrare la conformità rispetto al GDPR dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42), nonché rispetto alle norme nazionali vincolanti nella attività d'impresa.

Codici di condotta

Non sono presenti codici di condotta di categoria approvati.

Certificazioni

Non sono indicate certificazioni aziendali di tipo ISO, certificazioni di qualità o procedurali, certificazioni tecniche, che riducono la responsabilità diretta del titolare del trattamento.

Richieste degli interessati

L'articolo 35, paragrafo 9, del GDPR stabilisce che, se del caso, il Titolare del trattamento deve chiedere il parere degli interessati o dei loro rappresentanti in merito al trattamento previsto. Il parere non è stato richiesto poiché non necessario.

Consultazione con il responsabile della protezione dei dati (DPO)/Indicazione dei remedies

Ai fini di una corretta ed adeguata *compliance* si consigliano le seguenti attività:

- Definizione di tempi di vita massima dei dati raccolti;
- Attivare procedure di controllo a cadenza (almeno) annuale dei rimedi messi in atto;
- Previsione di un vademecum (codice di condotta) da sottoporre al personale incaricato al momento del conferimento dell'incarico e della sottoscrizione del consenso. Il codice deve contenere una sanzione per la violazione degli obblighi di correttezza nel trattamento dei dati personali;
- Fissare un periodo campione al termine del quale effettuare una nuova valutazione d'impatto al fine di verificare l'efficacia dei rimedi messi in atto;
- Formazione specifica privacy e gestione data breach;
- Registro accessi esterni;
- Redigere i contratti di nomina dei responsabili esterni;
- Redigere le lettere d'incarico per il personale interno.

6. Conclusioni

Valutazione finale

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

Nelle precedenti sezioni di questa DPIA:

- è stato presentato il processo di trattamento dei dati personali e fornita una panoramica funzionale;
- è stata descritta la mappatura dei dati personali identificati ed è stato evidenziato il loro percorso nel contesto di Marini Carmine;
- sono stati identificati i trattamenti, i loro scopi e gli interessi legittimi nel condurre tale elaborazione;
- sono stati analizzati e mappati i rischi per la privacy dell'interessato e le contromisure in atto per la mitigazione di tali rischi;
- sono state identificate le criticità e le mancanze che sono causa di rischio e proposti rimedi atti alla mitigazione del rischio.

Nella Sezione successiva si andrà a valutare se permane un rischio residuo elevato e se risulti pertanto necessaria una consultazione con l'autorità di controllo.

Rischio residuale

Ai sensi del GDPR, se il rischio residuo dopo le attenuazioni adottate rimane elevato, deve essere consultata l'autorità di vigilanza.

Il Gruppo dell'articolo 29 (WP29) per la tutela dei dati, nelle Linee Guida sulla DPIA, fornisce una definizione di rischio residuo elevato inaccettabile: "*casi in cui le persone gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota*)".

Nei trattamenti di Marini Carmine srl, non si rilevano condizioni di rischio residuo elevato. La Marini Carmine gestisce il suo programma di valutazione in modo professionale e attenua i rischi in larga misura.

Un rischio marginale di violazione dati potrebbe derivare nel caso di un attacco informatico portato con successo (virus) o in caso di furto di macchinari.

Non sembra che il rischio residuo esista in quest'area.

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi elevati residui e che pertanto non è necessario consultare l'autorità di vigilanza.

25,maggio2018

Il Titolare del Trattamento

_____