# DPIA MYS S.R.L.

Editing : Michele Pasqualotto
Evaluation : Fulvia Montagnani
Validation : Paolo Vianello

## Mappaggio dei rischi

## Piano d'azione

### Principi fondamentali

#### Adeguatezza dei dati

**Piano d'azione / misure correttive :**
Le tipologie di dati da trattare possono essere ulteriormente minimizzate, effettuando una maggiore selezione / filtro ab origine, a seconda delle aree di lavoro. Deve essere definita nei dettagli la portabilità dei dati in caso di richiesta del cliente.
**Commento di valutazione :**
Il livello di minimizzazione è buono, ma certamente migliorabile. La portabilità dei dati è in fase di inserimento nelle condizioni di contratto.
**Data prevista di implementazione :** 31.10.2023
**Responsabile dell'implementazione :** Paolo Vianello

## DPO and data subjects opinion

### Nome del DPO/RPD

Dott.ssa Fulvia Montagnani

### Posizione del DPO/RPD

Il trattamento può essere implementato in taluni aspetti del trattamento dei dati e delle misure di contenimento del rischio.

### Parere del DPO/RPD

Esistono aspetti che possono essere ulteriormente potenziati ed implementati, migliorando il contenuto del contratto coi clienti, nonché talune misure di sicurezza.

### Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

### Motivazione della mancata richiesta del parere degli interessati

Il trattamento è basato su rapporti contrattuali che mirano di per sé ad un alto livello di tutela dei diritti degli interessati.

# Contesto

## Panoramica del trattamento

### Quale è il trattamento in considerazione?

Trattamento dei dati dei clienti MYS attraverso WEBQUALITY.
WebQuality è un software di proprietà, creato e gestito direttamente da MYS, il quale consente ai clienti MYS, mediante le App integrate, la gestione e la condivisione dei propri processi aziendali.

### Quali sono le responsabilità connesse al trattamento?

Di norma, i clienti MYS sono Titolari del trattamento, poichè utilizzano la piattaforma WebQuality al fine di gestire i propri processi aziendali ed immettono dati propri (o di propri clienti/utenti).
MYS, fornendo la piattaforma WebQuality e la relativa assistenza softwaristica, ricopre il ruolo di Responsabile del trattamento (o, al più, di Sub-Responsabile) nominato dai propri clienti.

### Ci sono standard applicabili al trattamento?

Certificazione ISO 27000 in fase di accreditamento

**Valutazione : Accettabile**

# Contesto

## Dati, processi e risorse di supporto

### Quali sono i dati trattati?

Le tipologie di dati trattati sono eterogenee, poichè dipendono dal tipo di attività svolta dai clienti che utilizzano la piattaforma WebQuality.
Sovente, in particolare in relazione ai clienti che operano nel settore sanitario, i dati trattati possono avere natura di dati particolari ('sensibili').
I dati inseriti su WebQuality non sono oggetto di trasmissione o diffusione, tuttavia vi è l'utilizzo dell'infrastruttura Cloud Amazon per la collocazione dei server virtuali, come anche di talune terze parti per la fornitura di taluni servizi funzionali al cliente.
Solo il personale MYS è autorizzato all'accesso alla piattaforma WebQuality; i clienti accedono con propri account dedicati.

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

I dati vengono trattati dal momento dell'immissione degli stessi da parte del cliente sulla propria versione in uso di WebQuality.
Il trattamento ha la durata dell'utilizzo della piattaforma WebQuality da parte del cliente MYS; nel momento in cui cessa il rapporto contrattuale con il cliente per l'utilizzo della piattaforma, MYS offre al cliente la portabilità dei propri dati e provvede successivamente all'eliminazione degli stessi entro il termine contrattualmente definito.

**Valutazione : Accettabile**

### Quali sono le risorse di supporto ai dati?

Software WebQuality di proprietà MYS.
Il sofware è elaborato da Adobe Coldfusion ed entrambi sono installati su server Windows.
I server Windows sono su infrastruttura AWS (Amazon Italia).

**Valutazione : Accettabile**

# Principi Fondamentali

## Proporzionalità e necessità

### Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici, in quanto consistenti nella fornitura di servizi al cliente per la propria attività, nonchè nell'attività di assistenza informatica. Detti scopi sono altresì espliciti e legittimi in quanto formalizzati contrattualmente con i clienti.

**Valutazione : Accettabile**

### Quali sono le basi legali che rendono lecito il trattamento?

La base legale del trattamento è costituita dall'art. 6, par. 1, lett. b) del GDPR, in quanto i dati sono trattati in virtù di un contratto scritto che regola il rapporto col cliente. Poichè MYS riveste il ruolo di Responsabile del trattamento, al contratto è affiancato l'atto di designazione a Responsabile ai sensi dell'art. 28 del GDPR.

**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)?

Il trattamento dei dati è realizzato solo per quanto strettamente necessario alla gestione della piattaforma WebQuality e all'assistenza sistemistica.

**Valutazione : Migliorabile**

**Piano d'azione / misure correttive :**
Le tipologie di dati da trattare possono essere ulteriormente minimizzate, effettuando una maggiore selezione / filtro ab origine, a seconda delle aree di lavoro.
**Commento di valutazione :**
Il livello di minimizzazione è buono, ma certamente migliorabile.

### I dati sono esatti e aggiornati?

I dati sono esatti e aggiornati in quanto immessi direttamente dal cliente. Laddove modifiche ed aggiornamenti vengano richiesti dal cliente tramite assistenza sistemistica, i ticket di richiesta vengono assegnati ai diversi operatori MYS disponibili, di modo che la richiesta stessa sia gestita entro i termini contrattualmente stabiliti.

**Valutazione : Accettabile**

### Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati corrisponde alla durata del rapporto contrattuale con il cliente MYS. Alla cessazione del rapporto, viene assicurata la portabilità dei dati e la cancellazione degli stessi.

**Valutazione : Migliorabile**

**Commento di valutazione :**
L'aspetto della portabilità dei dati deve essere definito contrattualmente. Il contratto coi clienti è in fase di revisione.

# Principi Fondamentali

## Misure a tutela dei diritti degli interessati

### Come sono informati del trattamento gli interessati?

Poichè MYS opera quale Responsabile o Sub-Responsabile del trattamento, gli obblighi di informativa sono assolti dal Titolare del trattamento. La sussistenza di tali obblighi è evidenziata nell'atto di nomina di MYS a Responsabile.

**Valutazione : Accettabile**

## Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile

**Valutazione : Accettabile**

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

Gli interessati possono esercitare il diritto di accesso tramite il Titolare del trattamento, che fa pervenire l'istanza a MYS, oppure, a seconda del tipo di cliente, mediante apertura di un ticket di assistenza, a cui darà riscontro uno degli operatori MYS.
La portabilità dei dati riguarda il singolo cliente di MYS ed è regolamentata a contratto.

**Valutazione : Accettabile**

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

Gli interessati possono esercitare il diritto di rettifica e di cancellazione tramite il Titolare del trattamento, che fa pervenire l'istanza a MYS, oppure, a seconda del tipo di cliente, mediante apertura di un ticket di assistenza, a cui darà riscontro uno degli operatori MYS.

**Valutazione : Accettabile**

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

Ove del caso, gli interessati possono esercitare il diritto di limitazione o di opposizione tramite il Titolare del trattamento, che fa pervenire l'istanza a MYS, oppure, a seconda del tipo di cliente, mediante apertura di un ticket di assistenza, a cui darà riscontro uno degli operatori MYS.

**Valutazione : Accettabile**

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

I Responsabili del trattamento per le attività di MYS (che, di conseguenza, sono per lo più dei Sub-Responsabili) sono specificamente nominati con atto scritto o mediante inserimento di allegato/clausola contrattuale relativo alla nomina.

**Valutazione : Accettabile**

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

Non è previsto trasferimento di dati extra Unione.

**Valutazione : Accettabile**

# Rischi

## Misure esistenti o pianificate

### Controllo degli accessi logici

Il sistema di login degli operatori MYS a WebQuality è centralizzato sul servizio COGNITO di AWS (Amazon Web Services - servizio di gestione delle identità e degli accessi).
Tutti gli operatori MYS hanno le proprie credenziali in COGNITO ed effettuano login in COGNITO, per poi accedere in WebQuality come unico utente autenticato MYS (al fine di operare per l'assistenza ai clienti).
Gli operatori/utenti dei clienti MYS accedono con proprie credenziali personali a WebQuality per la gestione delle proprie attività aziendali; lo stesso avviene internamente a MYS nell'utilizzo di WebQuality per la gestione quotidiana delle attività proprie (cioè non su clienti).

**Valutazione : Accettabile**

### Vulnerabilità

MYS rilascia periodicamente degli aggiornamenti di sistema per WebQuality.
WebQuality è un sofware scritto su linguaggio CFM ed elaborato da Adobe Coldfusion, che rilascia periodicamente aggiornamenti e patch di sicurezza.
Poichè sia WebQuality sia Adobe Coldfusion sono installati su server Windows, beneficiano degli aggiornamenti periodici di sistema rilasciati da Microsoft.
I server Windows sono su infrastruttura AWS e beneficiano degli aggiornamenti di sicurezza effettuati centralmente da Amazon.

**Valutazione : Accettabile**

### Lotta contro il malware

Una volta effettuato l'accesso in WebQuality gli input degli utenti (che siano in forma di testo o di file caricati) sono processati dal Firewall di Amazon e successivamente analizzati e schermati da

Adobe Coldfusion.
E' inoltre attiva la protezione da malware di Windows.

**Valutazione : Accettabile**

## Gestione postazioni

I notebook degli operatori MYS hanno sistemi operativi Windows o MAC di ultima generazione aggiornati e dotati di sistema di sicurezza Sophos.

**Valutazione : Accettabile**

## Backup

Il backup dei dati contenuti in WebQuality è gestito automaticamente, con cadenza giornaliera (1 backup al giorno per 1 mese, poi 1 backup il primo del mese - fino a risalire indietro ad 1 anno) dall'infrastruttura Amazon, sul proprio servizio backup su server in Italia.

**Valutazione : Accettabile**

## Contratto con il responsabile del trattamento

Ai Responsabili e Sub-responsabili del trattamento sono applicate almeno le medesime condizioni previste dal rapporto contrattuale tra il Titolare del trattamento (cliente MYS) e MYS stessa.

**Valutazione : Accettabile**

## Tracciabilità

E' stata adottata la Procedura di Gestione Data Breach ed è stato creato il Registro Data Breach.

**Valutazione : Accettabile**

## Politica di tutela della privacy

All'interno dell'organizzazione di MYS sono previste specifiche procedure (relativamente alla gestione del rapporto con il cliente, allo svolgimento delle attività di progettazione e di assistenza, alla condotta sul luogo di lavoro o presso i clienti, alla gestione dei device forniti dall'azienda ecc.) e modulistiche per la corretta gestione dei dati personali.
Sono adottati il Registro dei trattamenti come Titolare del trattamento, nonché, ove del caso, le

schede registro da Responsabile / Sub-Responsabile per ciascun cliente MYS.
Sono adottati una procedura di gestione Data Breach e il Registro Data Breach.
E' stato nominato un DPO esterno per lo svolgimento delle attività di verifica sulla corretta gestione della privacy.

**Valutazione : Accettabile**

## Gestire gli incidenti di sicurezza e le violazioni dei dati personali

E' stata adottata la Procedura di Gestione Data Breach ed è stato creato il Registro Data Breach.
Sono adottate procedure per Penetration Test e Disaster Recovery.

**Valutazione : Accettabile**

## Vigilanza sulla protezione dei dati

I registri dei trattamenti, così come tutta la documentazione privacy adottata, sono sottoposti a verifica periodica con cadenza almeno annuale, che viene evidenziata alla scadenza mediante l'applicazione di gestione dei documenti all'interno dell'area riservata MYS su WebQuality.
Specifica attività di vigilanza è svolta dal DPO incaricato.

**Valutazione : Accettabile**

## Sicurezza dei documenti cartacei

L'utilizzo di supporti cartacei è massimamente ridotta, in ragione della specifica attività svolta da MYS.
Sono disponibili due stampanti comuni negli uffici del co-working ove si trova la sede operativa MYS.
Inoltre, presso gli uffici in uso a MYS (uffici con porte con chiusura a chiave - accesso al solo personale MYS) è in uso uno schedario con chiusura a chiave (gestita dai legali rappresentanti di MYS), per l'archiviazione, ed una macchina distruggi-documenti per l'eliminazione dei documenti cartacei.

**Valutazione : Accettabile**

## Crittografia

Il disco fisso dei notebook in uso al personale MYS sono crittati da Microsoft / Apple.
Gli applicativi di WebQuality sono tutti raggiungibili tramite protocollo HTTPS.
L'accesso ai sistemi Cloud avviene in VPN (canale crittografato).
In fase di implementazione la crittografazione totale del canale (all'interno del data center AWS).

**Valutazione : Accettabile**

## Anonimizzazione

MYS predispone un ambiente di staging, a cui possono accedere i programmatori, con meccanismo di anonimizzazione.

**Valutazione : Accettabile**

## Minimizzazione dei dati

**In fase di implementazione**

**Valutazione : Migliorabile**

## Sicurezza dei siti web

Gli applicativi di WebQuality sono tutti raggiungibili tramite protocollo HTTPS.

**Valutazione : Accettabile**

## Controllo degli accessi fisici

Gli uffici della sede operativa di MYS sono ubicati in una struttura di co-working.
L'accesso alla struttura è regolato mediante APP per l'apertura del cancello carraio e della porta di ingresso.
Gli uffici non sono aperti al pubblico e ogni ufficio è dotato di porta con chiusura a chiave.
L'eventuale accesso di soggetti esterni avviene solo alla presenza di personale MYS.
La struttura è dotata di un sistema di allarme anti-intrusione centralizzato.

**Valutazione : Accettabile**

## Sicurezza dell'hardware

Al personale MYS è assegnato un proprio notebook aziendale che non viene mai lasciato presso la sede operativa.
Tutti i notebook prevedono credenziali di accesso univoche e disco fisso crittato.

**Valutazione : Accettabile**

## Gestione del personale

Al personale MYS viene fornita apposita informativa privacy e documento di autorizzazione al trattamento dei dati personali, con le istruzioni basilari. E' inoltre prevista la formazione privacy periodica.
Alla cessazione del rapporto, i device aziendali vengono recuperati e formattati (o smaltito, se del caso) e le credenziali sono resettate/eliminate.

**Valutazione : Accettabile**

## Gestione delle politiche di tutela della privacy

La documentazione privacy di MYS è soggetta a revisione periodica almeno con cadenza annuale, con evidenziazione della scadenza da parte dell'applicativo WebQuality.

**Valutazione : Accettabile**

## Protezione contro fonti di rischio non umane

- Sistema antincendio presso la sede del co-working
- La struttura del co-working è di recente ristrutturazione
- Backup fuori sede
- Misure di sicurezza presso infrastruttura Amazon (in Italia)

**Valutazione : Accettabile**

## Prevenzione delle fonti di rischio

- Nessun trasferimento dati extra Unione
- Accesso agli uffici non aperto al pubblico
- Sede collocata in area geografica non pericolosa
- Infrastruttura Amazon Italia collocata a Milano

**Valutazione : Accettabile**

# Rischi

## Accesso illegittimo ai dati

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

Perdita di dati, Divulgazione di dati e informazioni riservati, Divulgazione di dati particolari (sensibili), Ritardo nell'erogazione dei servizi, Perdita economica, Danno alla salute.

### Quali sono le principali minacce che potrebbero concretizzare il rischio?

Violazione del sistema informatico, Errore umano.

### Quali sono le fonti di rischio?

Operatore/utente del cliente, Operatore MYS, Hacker esterno, Virus/malware.

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

Lotta contro il malware, Controllo degli accessi logici, Backup, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vulnerabilità, Protezione contro fonti di rischio non umane, Prevenzione delle fonti di rischio, Gestione del personale, Anonimizzazione, Crittografia, Vigilanza sulla protezione dei dati.

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

Importante, Il rischio è grave, tenuto conto della tipologia di dati trattati e, quindi, degli impatti potenziali sia sui clienti MYS, sia sui diretti interessati. Tuttavia, le misure pianificate sono consistenti e potenzialmente efficaci.

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

Limitata, poichè le minacce possono essere significative e ad alto impatto, l'esistenza di misure di sicurezza importanti e strutturate mitiga in maniera rilevante il rischio, non potendolo tuttavia rendere trascurabile.

**Valutazione : Accettabile**

# Rischi

## Modifiche indesiderate dei dati

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

Danno alla salute, Perdita economica, Ritardo nell'erogazione dei servizi.

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

Errore umano, Violazione del sistema informatico.

### Quali sono le fonti di rischio?

Operatore MYS, Operatore/utente del cliente.

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

Controllo degli accessi logici, Backup, Controllo degli accessi fisici, Gestione del personale, Prevenzione delle fonti di rischio, Protezione contro fonti di rischio non umane, Minimizzazione dei dati, Vigilanza sulla protezione dei dati.

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

Limitata, La gravità del rischio è limitata, in quanto, benchè l'impatto potenziale possa risultare significativo, le misure pianificate sono numerose e ad alto tasso di efficacia specifica.

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

Limitata. La probabilità del rischio è molto limitata, quasi trascurabile, sia alla luce della natura delle fonti di rischio, sia soprattutto per l'efficacia specifica della tipologia di misure di sicurezza adottate.

**Valutazione : Accettabile**

# Rischi

## Perdita di dati

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

Danno alla salute, Perdita di dati, Perdita economica, Ritardo nell'erogazione dei servizi.

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

Errore umano, Violazione del sistema informatico.

### Quali sono le fonti di rischio?

Hacker esterno, Operatore MYS, Operatore/utente del cliente, Virus/malware.

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

Controllo degli accessi logici, Vulnerabilità, Lotta contro il malware, Backup, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Crittografia, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Protezione contro fonti di rischio non umane, Vigilanza sulla protezione dei dati.

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

Importante, Il rischio è grave, tenuto conto della tipologia di dati trattati e, quindi, degli impatti potenziali sia sui clienti MYS, sia sui diretti interessati. Tuttavia, le misure pianificate sono consistenti e potenzialmente efficaci.

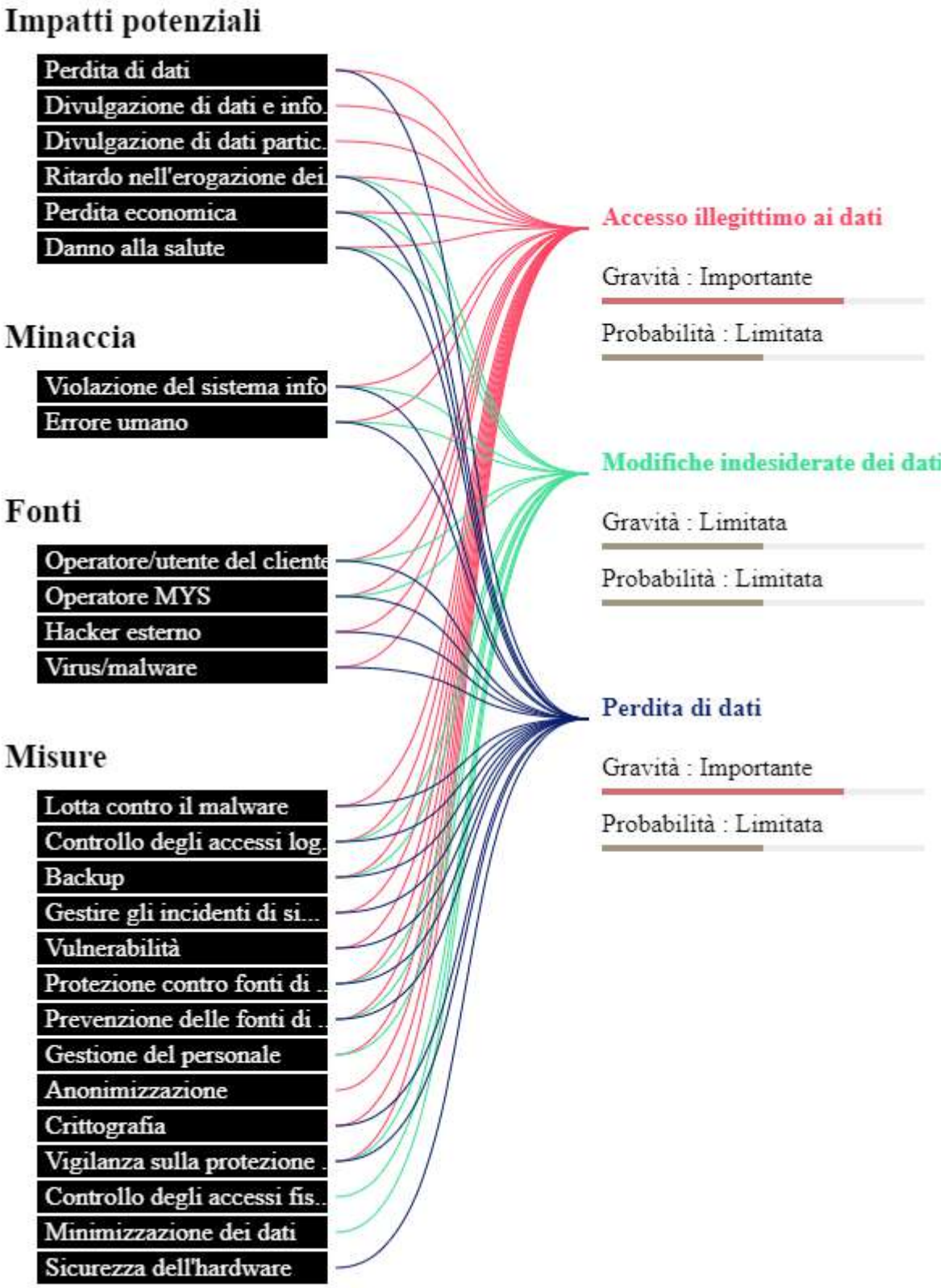
### Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, poichè le minacce possono essere significative e ad alto impatto, l'esistenza di misure di sicurezza importanti e strutturate mitiga in maniera rilevante il rischio, non potendolo tuttavia rendere trascurabile.

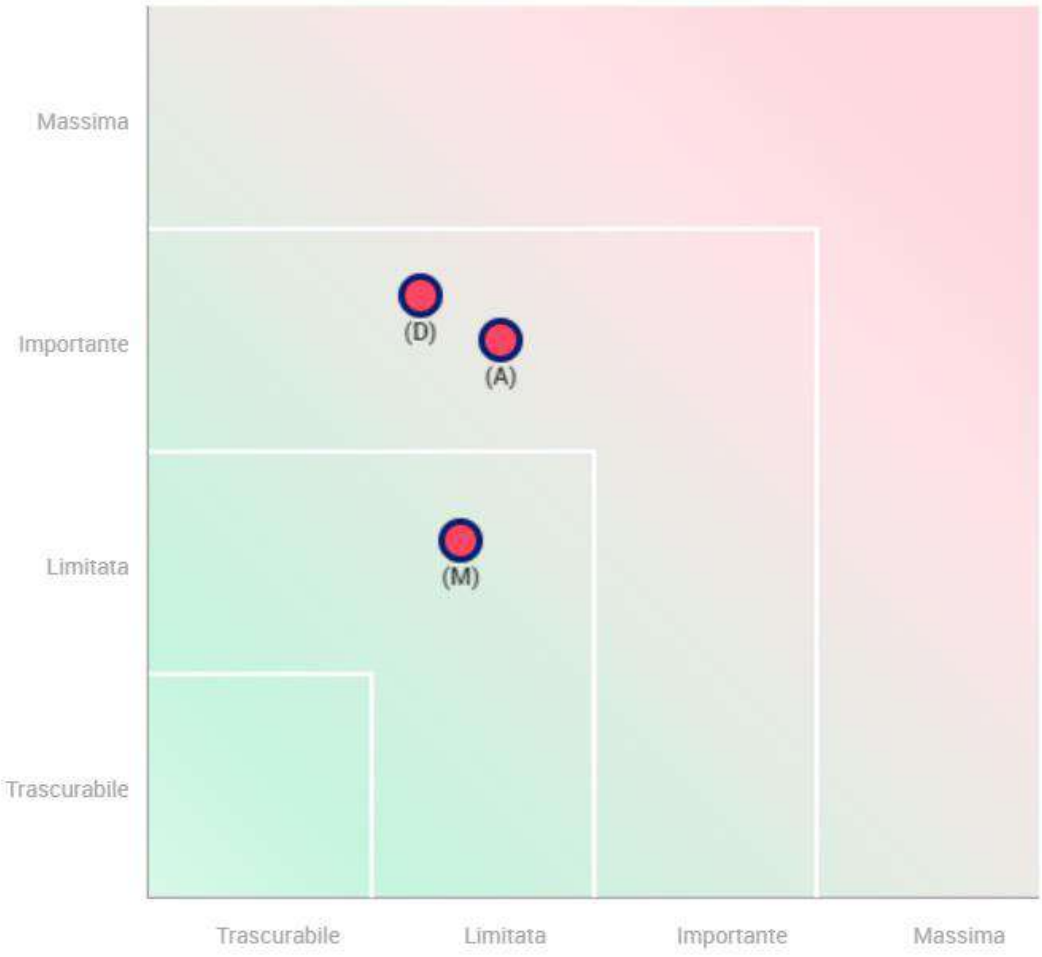
**Valutazione : Accettabile**

# Rischi

## Panoramica dei rischi



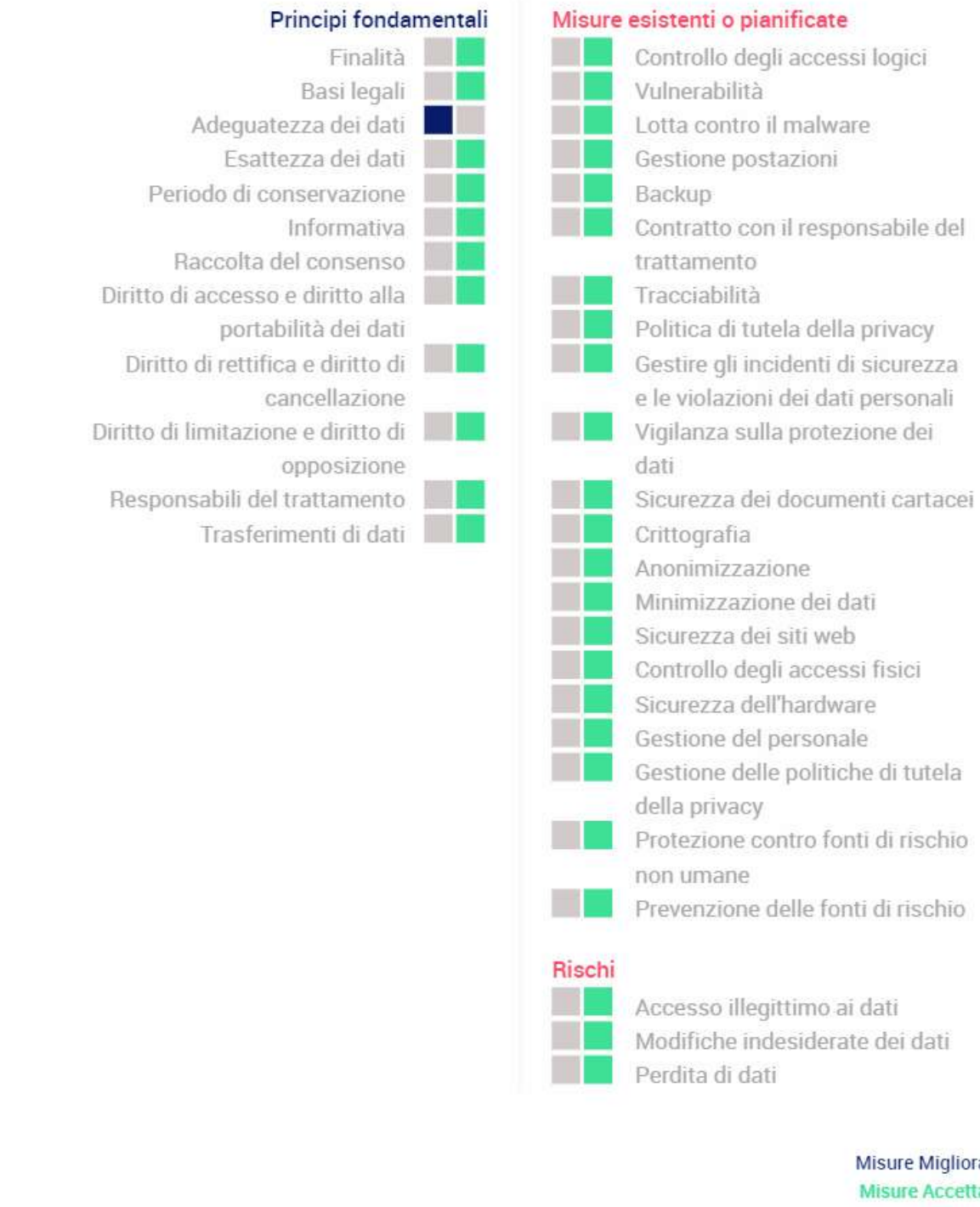
Gravità del rischio




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

## Panoramica




Rovigo, lì 02 ottobre 2023

MYS S.r.l.