MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| Autore | Ufficio privacy |
| Approvazione | Ruggero Nicrosini |

Versione Revisione

| Versione | Autore | Consultazione DPO | Data emissione | Motivo della revisione |
|---|---|---|---|---|
| 0.0 | Ufficio privacy | 12/02/2021 | 15/02/2021 | Prima emissione |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

PARERE DPO
OK.

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

# MY GOVERNANCE

| RESPONSABILE DEL TRATTAMENTO | | | | | |
|---|---|---|---|---|---|
| **Denominazione** | MYGO SRL | | | | |
| **Partita Iva** | 14356531005 | | | | |
| **Indirizzo** | Via del Corso 92 – Sede legale Piazza Crati 20 | | | | |
| **Città** | Roma | **Cap** | 00199 | **PV** | RM |
| **Legale Rappresentante** | Davide Caiazzo | | | | |

| STRUTTURA ORGANIZZATIVA | | | |
|---|---|---|---|
| **Divisione** | Commerciale | Responsabile Divisione | Ruggero Nicrosini |

| INCARICATI DEL TRATTAMENTO |
|---|
| Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti |

| DATI DI CONTATTO | | | |
|---|---|---|---|
| **Responsabile del trattamento** | Davide Caiazzo | davide@mygovernance.it | |
| **Rappresentante del titolare** | N/A | | |
| **Responsabile protezione dati (DPO)** | N/A | | |

| DESCRIZIONE |
|---|
| My Whistleblowing è parte della suite My Governance, una soluzione in cloud che permette di digitalizzare i processi aziendali.<br>In particolare, My Whistleblowing è un sistema Saas che offre alle aziende un canale informatico per le segnalazioni di illeciti interni, garantendo la riservatezza delle informazioni ivi inserite, nonché, volendo, dando la possibilità di effettuare segnalazioni in forma anonima. La soluzione My Whistleblowing consente quindi da una parte ai dipendenti della azienda cliente di effettuare tali report e, dall'altra, ai responsabili interni identificati dall'azienda di accedere alle segnalazioni, gestirle e instaurare anche un dialogo con il segnalante, il tutto secondo i criteri di legge nel rispetto dei principi generali di riservatezza |

| FINALITA' DEL TRATTAMENTO |
|---|
| Il Responsabile del trattamento tratta i dati per finalità di creazione utenza, assistenza e manutenzione al Titolare. Si fa presente che il Responsabile non ha accesso alle informazioni contenute all'interno della singola segnalazione, che restano pertanto accessibili esclusivamente al Titolare |

| CATEGORIA INTERESSATI |
|---|
| Dipendenti, apprendisti, tirocinanti, stagisti, collaboratori, fornitori, appaltatori, visitatori, a seconda della scelta del Cliente su chi avrà accesso alla piattaforma My Whistleblowing. |

| CATEGORIE DI DATI PERSONALI |
|---|

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| |
|---|
| Come evidenziato, il Responsabile non ha accesso ai dati personali rilasciati all'interno della singola segnalazione. Il Responsabile ha unicamente accesso, ai fini della registrazione all'interno del Sistema e per la sua manutenzione, al nome, cognome e indirizzo email del segnalante |
| **CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI** |
| Aziende del gruppo Zucchetti<br>Subappaltatori<br>Microsoft Azure come provider di DC |
| **TRASFERIMENTO DATI ALL'ESTERO** |
| No |
| **TERMINI PER LA CANCELLAZIONE DEI DATI** |
| I dati conservati nel Data Center fornito in cloud da Microsoft Azure saranno conservati per tutta la durata del contratto e successivamente, su richiesta del Titolare, potranno essere consegnati con una estrazione unica al Titolare entro 30 giorni dalla fine del contratto.<br>I dati relativi alla gestione amministrativa e giuridica del rapporto contrattuale saranno conservati per 10 anni dalla cessazione del rapporto contrattuale. |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

# DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

## 1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

- *Gestione credenziali di accesso*

- User name: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede.
- Password: le regole di complessità della password sono quelli standard secondo le best practice di settore (minimo 8 caratteri, almeno una maiuscola, almeno un carattere speciale)
- Criteri di complessità per le impostazioni delle credenziali: le credenziali di accesso possono essere impostate secondo diversi criteri di complessità dal Titolare.
- Il Sistema prevede la funzione di blocco account a tempo oppure il blocco account per superamento tentativi di login fail.
- Disattivazione/disabilitazione credenziali: non appena comunicato dal Titolare, il Responsabile entro le successive 24 ore provvederà alla cancellazione delle credenziali.
- Il sistema è configurabile con un sistema SSO attraverso un token, active directory, ldap, SAML 2.0, injection header.
- È possibile implementare una two factor authentication anche attraverso un sistema di otp.
- C'è una funzione CAPTCHA Block User account enumeration.

- *Minimizzazione:*

- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti, in particolare nella individuazione admin/user.

- *Identificazione di chi ha trattato i dati:*

- Strumenti di log: su richiesta del Titolare il Responsabile potrà scaricare i log al sistema.

- *Tecniche di crittografia:*

- Crypting password DB service account.
- Crittografia della base dati: Il database è crittografato secondo gli standard di servizio offerti da Microsoft Azure.
- Crittografia file DMS: tutti i documenti generati dalle applicazioni e conservati nel DMS sono crittografati; la crittografia per eventuali documenti generati all'esterno e archiviati nel DMS, verrà applicata impostando correttamente i parametri sulla "Classe documentale" associata ai documenti stessi.

- *Privacy by default*

- Attivazione profilo utente: gli utenti nel portale sono attivati secondo una logica di non assegnare alcun profilo autorizzativo sui dati trattati. Sarà il Titolare in autonomia a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale. In particolare, il Titolare potrà individuare la funzione admin, ruolo che consente

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

di verificare le segnalazioni ricevute. Tale funzione viene assegnata o a un singolo ricevente, ovvero a un comitato di riceventi, a seconda delle necessità del Titolare.

- *Diritti degli interessati:*

- Diritti degli interessati: per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che potrà informare il Responsabile per provvedere alla cancellazione. Nei singoli applicativi saranno presenti quindi solo informazioni anonime non riconducibili neppure indirettamente ad alcun interessato. La funzione di cancellazione avviene per anagrafica soggetto.

| Misure di sicurezza | Commenti |
|---|---|
| Mettere in sicurezza lo stabile che ospita l'infrastruttura IT utilizzata per elaborare e trasferire i dati | I dati della piattaforma My Governance sono conservati sui server Europei di AWS Amazon. |
| Limitare il numero di soggetti autorizzati ad accedere ai dati e all'infrastruttura IT utilizzata per elaborare e trasferire i dati | La società che fa manutenzione alla piattaforma è stata debitamente individuata come Amministratore di Sistema |
| Assicurare un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza | Grazie alla società terza che garantisce la continuità del Data Center (DC) si assicurerà un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza |
| Assicurare che l'accesso ai dati avvenga in maniera controllata | L'accesso ai dati può avvenire solo in maniera controllata, grazie agli alti standard di sicurezza con cui viene protetto il DC e alla criptazione dei dati |
| Assicurare che i dati siano protetti da perdita o distruzione accidentale | Per assicurare che i dati siano protetti da perdita o distruzione accidentale si utilizzano copie di backup dislocate in posizioni geografiche differenti. Tale livello di protezione ridurrà al minimo la possibilità di perdita e comunque nel caso dovesse avvenire sarà sicuramente molto limitata. |
| Assegnare ad ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione composte da un codice per l'identificazione ("User ID") associato a una parola chiave ("password") | Ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione composte da un codice per l'identificazione ("User ID") associato a una parola chiave ("password") secondo gli standard migliori oggi presenti sul mercato. Password con sicurezze minime garantite |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| La password riservata, conosciuta solamente dall'assegnatario ("Utente") deve avere quantomeno le seguenti caratteristiche:<br>1. essere composta da almeno 8 caratteri;<br>2. contenere lettere maiuscole e minuscole in combinazione con<br>3. numero o caratteri speciali;<br>4. non deve contenere lo User ID;<br>5. deve essere obbligatoriamente modificata al primo utilizzo e dopo il<br>6. reset della password;<br>7. deve essere modificata almeno ogni 60 giorni. | La password di accesso dovrà rispettare quantomeno i seguenti requisiti:<br>● almeno 8 caratteri<br>● almeno una lettera maiuscola<br>● almeno una lettera minuscola<br>● almeno un simbolo speciale<br>● almeno un numero<br>Al quinto tentativo errato di inserimento di una password l'utenza verrà bloccata per 30 minuti. |
| Assicurare che lo User ID assegnato ad un Utente non possa essere assegnato ad un altro incaricato in tempi diversi | Questo deve essere garantito dal Titolare in quanto lo user ID è l'indirizzo email |
| Assicurarsi che le credenziali vengano disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali | Questo dovrà essere eseguito dal Titolare che provvederà a rimuovere gli utenti dall'anagrafica. Tali utenti avranno in ogni caso accesso ai documenti già approvati. |
| Assicurare che:<br>i. quando per gli incaricati sono individuati profili di autorizzazione di<br>ambito diverso venga utilizzato un sistema di autorizzazione.<br>ii. i profili di autorizzazione, per ciascun incaricato o per classi<br>omogenee di incaricati, siano individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.<br>iii. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione | Confermato |
| Proteggere i dati il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale:<br>i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana;<br>ii. effettuare aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di | Confermato |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| strumenti elettronici e a correggerne difetti su base quotidiana | |
| Assicurare che il trattamento avvenga utilizzando software (ivi incluso il sistema operative, il middleware e le applicazioni) dotati di funzioni di sicurezza all'avanguardia | Confermato |
| Assicurare che sia effettuato un back-up almeno con frequenza quotidiana | Grazie alla società terza proprietaria dei server si assicurerà che sia effettuato un back-up almeno con frequenza quotidiana |
| Assicurare che i dati possano essere recuperati entro un determinato termine massimo (non più di 7 giorni) | Sì |
| Garantire che i dati utilizzati per l'autenticazione siano protetti con efficaci misure di sicurezza crittografica | Sì |
| Assicurarsi che i dati trasferiti siano protetti utilizzando procedure di crittografia aggiornate | Sì |
| Le categorie particolari di dati personali sono protette utilizzando procedure di crittografia aggiornate | Normalmente non vengono trattate categorie particolari di dati personali ma in ogni caso i dati in nostro possesso sono sempre crittografati |
| Assicurarsi che sia possibile verificare e stabilire se e chi ha avuto accesso o ha inserito, ha modificato o cancellato i dati nei sistemi di elaborazione dati. I log devono essere disponibili per almeno un anno | Confermato |
| Garantire che siano regolarmente eseguiti test di vulnerabilità e di penetrazione | Cadenza annuale |
| Qualora una violazione o vulnerabilità sia identificata nell'ambito del trattamento o in qualsiasi sistema utilizzato per fornire i servizi del Responsabile, informare immediatamente il Titolare del trattamento in merito all'evento e alle misure adottare per porvi rimedio | Sì |
| Garantire che l'accesso ai dati sia limitato ai soli dati necessari per effettuare le operazioni di trattamento. | Sì by default |
| Limitare il numero di Incaricati autorizzati a svolgere attività connesse al trattamento dei dati | Sì by default |
| Erogare apposita formazione nei confronti degli | Sì |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| Incaricati con riferimento alla normativa vigente in materia di tutela dei dati personali, alle misure di sicurezza | |
| Mantenere una lista aggiornata degli Incaricati | Presente |
| Mantenere una copia di riserva aggiornata dei dati e del software utilizzato per il trattamento | Presente |
| Garantire che i Dati vengano archiviati applicando misure idonee a proteggerli da accessi non autorizzati, modifiche, danni e distruzione | Presente |
| Assicurarsi che i dati vengano cancellati in modo irreversibile in caso di sostituzione o riutilizzo dell'hardware | Sì by default |
| Escludere o limitare le copie dei dati (incluse le stampe) e assicurare la corretta distruzione dopo l'utilizzo | Sì by default |
| Proteggere i documenti cartacei contenenti dati utilizzati durante l'elaborazione al momento della stampa, archiviazione, distruzione e scambio | Non viene utilizzato alcun documento cartaceo |
| Garantire la sicurezza della rete su cui viene eseguito il trattamento (sistema firewall, proxy, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi) | Presente |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

## 2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

### ASSISTENZA ON SITE

Gli addetti My Governance offrono al Titolare formazione e sono disponibili a recarsi anche on site per eventuali supporti, ferma restando l'assistenza continua da remoto secondo gli SLA condivisi con il cliente.
In questo caso gli addetti My Governance lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezze implementate dallo stesso. I Titolari potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale.
Qualora durante l'attività di assistenza l'addetto My Governance abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolari e registri tale attività sulla Nota di intervento.

### ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

### ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email i tecnici My Governance rendono sempre disponibile tramite link la possibilità per Titolare di leggere l'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.
L'addetto My Governance non è autorizzato a farsi mandare le credenziali di accesso del Titolare via email né tantomeno potrà salvarle sullo strumento di ticketing.
Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico My Governance è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico My Governance dovrà richiedere credenziali individuali oppure collegamento tramite Team Viewer.

### ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO

Personale di Help Desk

La creazione dell'utenza deve essere richiesta solo al Titolare che, attraverso l'amministratore di applicazione, potrà creare il nuovo utente.
Non deve mai essere utilizzato l'utente amministratore da parte degli operatori di assistenza.

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

## 3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS- PAAS

La sicurezza, la riservatezza e la salvaguardia del patrimonio informativo vengono prima di tutto e costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di My Governance.

Gli obiettivi di My Governance sono:

- dimostrare al mercato la propria capacità di fornire con regolarità un Software sicuro e reliable, massimizzando gli obiettivi di business dei propri Clienti;
- minimizzare il rischio di perdita e indisponibilità dei dati dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere di conseguenza una adeguata analisi dei rischi, determinando il valore delle risorse informative coinvolte e valutando il rischio conseguente, attraverso l'esame delle vulnerabilità e delle minacce associate;
- rispettare e far rispettare ai propri Clienti le leggi, i regolamenti, le disposizioni vigenti, i requisiti contrattuali, le norme e le procedure aziendali;
- promuovere lo sviluppo Digitale anche attraverso la collaborazione, la comprensione e la consapevolezza dei propri Clienti e Fornitori strategici, e
- conformarsi a tutte le norme e regolamenti che disciplinano le attività di business in cui opera.
- Tutta l'organizzazione è impegnata a supportare l'implementazione, la messa in opera e il riesame periodico di MY GOVERNANCE.

Il vertice aziendale si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi di questa politica.
My Governance pone i propri sistemi sul server certificato di Microsoft – Azure – che garantisce la massima sicurezza.

| | |
|---|---|
| Data Center principale | Microsoft Azure APP Service - Location West Europe |
| Data Center di emergenza | Microsoft Azure APP Service - Location West Europe |
| Memorizzazione Dati | Microsoft Azure SQL Server - Location West Europe |
| Back up Memorizzazione Dati | Microsoft Azure SQL Server - Location West Europe |
| Archivio | Microsoft Azure Storage Account - Location West Europe |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

Non sono stati sottoscritti dei contratti ad hoc con Microsoft, in quanto le funzionalità di Microsoft Azure sono acquistabili on line tramite adesione a condizioni generali di servizio.

Ai seguenti link si possono trovare i T&C e il service agreement con Microsoft Azure, oltre agli SLA per gli applicativi utilizzati:

- https://www.microsoft.com/it-it/licensing/product-licensing/products?rtc=1
- https://docs.microsoft.com/it-it/azure/azure-resource-manager/management/policy-reference
- https://azure.microsoft.com/it-it/support/legal/subscription-agreement-nov-2014/
- https://azure.microsoft.com/it-it/support/legal/
- https://azure.microsoft.com/it-it/support/legal/sla/
- https://docs.microsoft.com/it-it/compliance/regulatory/gdpr-arc-azure-dynamics

Si riporta inoltre, di seguito, il dettaglio dei servizi attivi su Microsoft Azure:

| **Servizi attivi su AZURE** | **Plan** | **Location** | **Dettagli** | | |
|---|---|---|---|---|---|
| App Service | P1V2 | West Europe | 210 Total ACU | 3.5 GB memory | Dv2-series compute equivalent |
| SQL Database | Standard S1 | West Europe | 20 DTUs | - | - |
| SQL Server | n/a | n/a | n/a | n/a | n/a |
| Storage account | Standard | West Europe | Locally-redundant storage (LRS) | Storage (general purpose v1) | - |
| Storage account BKP | Standard | West Europe | Locally-redundant storage (LRS) | Storage (general purpose v1) | - |
| Azure function | Consumption | n/a | Serverless | n/a | n/a |
| Virtual Network | Azure provided DNS service | West Europe | Subnet enable | | |
| Application Gateway | WAF | West Europe | NET-AppGateway-01/default | | |

Ulteriori informazioni utili e le specifiche di sicurezza del servizio che fornisce Microsoft Azure sono consultabili ai seguenti link:

- https://docs.microsoft.com/it-it/azure/security
- https://docs.microsoft.com/it-it/azure/security/fundamentals/log-audit

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

- https://docs.microsoft.com/it-it/azure/security/fundamentals/technical-capabilities

Fatta salva la responsabilità ed il dovere del Responsabile di valutare e adottare ogni ulteriore misura tecnica e organizzativa adeguata per garantire che il trattamento posto in essere avvenga nel rispetto dei requisiti richiesti dal Regolamento GDPR ed assicuri la protezione dei diritti degli Interessati, il presente allegato descrive le misure minime di sicurezza che devono essere adottate dal Responsabile del trattamento (ove applicabile).

| Misure di sicurezza | Commenti |
|---|---|
| Mettere in sicurezza lo stabile che ospita l'infrastruttura IT utilizzata per elaborare e trasferire i dati | I dati sono conservati presso i server di Microsoft Azure in Italia |
| Limitare il numero di soggetti autorizzati ad accedere ai dati e all'infrastruttura IT utilizzata per elaborare e trasferire i dati | La società che fa manutenzione alla piattaforma è stata debitamente individuata come Amministratore di Sistema |
| Assicurare un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza | Grazie alla società terza che garantisce la continuità del Data Center (DC) si assicurerà un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza |
| Assicurare che l'accesso ai dati avvenga in maniera controllata | L'accesso ai dati può avvenire solo in maniera controllata, grazie agli alti standard di sicurezza con cui viene protetto il DC e alla criptazione dei dati |
| Assicurare che i dati siano protetti da perdita o distruzione accidentale | Per assicurare che i dati siano protetti da perdita o distruzione accidentale si utilizzano copie di backup dislocate in posizioni geografiche differenti. Tale livello di protezione ridurrà al minimo la possibilità di perdita e comunque nel caso dovesse avvenire sarà sicuramente molto limitata. |
| Assegnare ad ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione composte da un codice per l'identificazione ("User ID") associato a una parola chiave ("password") | Ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione composte da un codice per l'identificazione ("User ID") associato a una parola chiave ("password") secondo gli standard migliori oggi presenti sul mercato. Password con sicurezze minime garantite |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| La password riservata, conosciuta solamente dall'assegnatario ("Utente") deve avere quantomeno le seguenti caratteristiche:<br>1. essere composta da almeno 8 caratteri;<br>2. contenere lettere maiuscole e minuscole in combinazione con<br>3. numero o caratteri speciali;<br>4. non deve contenere lo User ID;<br>5. deve essere obbligatoriamente modificata al primo utilizzo e dopo il<br>6. reset della password;<br>7. deve essere modificata almeno ogni 60 giorni. | La password di accesso dovrà rispettare quantomeno i seguenti requisiti:<br>● almeno 8 caratteri<br>● almeno una lettera maiuscola<br>● almeno una lettera minuscola<br>● almeno un simbolo speciale<br>● almeno un numero<br>Al quinto tentativo errato di inserimento di una password l'utenza verrà bloccata per 30 minuti. |
| Assicurare che lo User ID assegnato ad un Utente non possa essere assegnato ad un altro incaricato in tempi diversi | Questo deve essere garantito dal Titolare in quanto lo user ID è l'indirizzo email |
| Assicurarsi che le credenziali vengano disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali | Questo dovrà essere eseguito dal Titolare che provvederà a rimuovere gli utenti dall'anagrafica. Tali utenti avranno in ogni caso accesso ai documenti già approvati. |
| Assicurare che:<br>i. quando per gli incaricati sono individuati profili di autorizzazione di<br>ambito diverso venga utilizzato un sistema di autorizzazione.<br>ii. i profili di autorizzazione, per ciascun incaricato o per classi<br>omogenee di incaricati, siano individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.<br>iii. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione | Confermato |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| Proteggere i dati il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale:<br>i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana;<br>ii. effettuare aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti su base quotidiana | Confermato |
| Assicurare che il trattamento avvenga utilizzando software (ivi incluso il sistema operative, il middleware e le applicazioni) dotati di funzioni di sicurezza all'avanguardia | Confermato |
| Assicurare che sia effettuato un back-up almeno con frequenza quotidiana | Grazie alla società terza proprietaria dei server si assicurerà che sia effettuato un back-up almeno con frequenza quotidiana |
| Assicurare che i dati possano essere recuperati entro un determinato termine massimo (non più di 7 giorni) | Sì |
| Garantire che i dati utilizzati per l'autenticazione siano protetti con efficaci misure di sicurezza crittografica | Sì |
| Assicurarsi che i dati trasferiti siano protetti utilizzando procedure di crittografia aggiornate | Sì |
| Le categorie particolari di dati personali sono protette utilizzando procedure di crittografia aggiornate | Normalmente non vengono trattate categorie particolari di dati personali ma in ogni caso i dati in nostro possesso sono sempre crittografati |
| Assicurarsi che sia possibile verificare e stabilire se e chi ha avuto accesso o ha inserito, ha modificato o cancellato i dati nei sistemi di elaborazione dati. I log devono essere disponibili per almeno un anno | Confermato |
| Garantire che siano regolarmente eseguiti test di vulnerabilità e di penetrazione | Cadenza annuale |
| Qualora una violazione o vulnerabilità sia identificata nell'ambito del trattamento o in qualsiasi sistema utilizzato per fornire i servizi del Responsabile, informare immediatamente il Titolare del trattamento in merito all'evento e alle misure adottare per porvi rimedio | Sì |

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

| | |
|---|---|
| Garantire che l'accesso ai dati sia limitato ai soli dati necessari per effettuare le operazioni di trattamento. | Sì by default |
| Limitare il numero di Incaricati autorizzati a svolgere attività connesse al trattamento dei dati | Sì by default |
| Erogare apposita formazione nei confronti degli Incaricati con riferimento alla normativa vigente in materia di tutela dei dati personali, alle misure di sicurezza | Sì |
| Mantenere una lista aggiornata degli Incaricati | Presente |
| Mantenere una copia di riserva aggiornata dei dati e del software utilizzato per il trattamento | Presente |
| Garantire che i Dati vengano archiviati applicando misure idonee a proteggerli da accessi non autorizzati, modifiche, danni e distruzione | Presente |
| Assicurarsi che i dati vengano cancellati in modo irreversibile in caso di sostituzione o riutilizzo dell'hardware | Sì by default |
| Escludere o limitare le copie dei dati (incluse le stampe) e assicurare la corretta distruzione dopo l'utilizzo | Sì by default |
| Proteggere i documenti cartacei contenenti dati utilizzati durante l'elaborazione al momento della stampa, archiviazione, distruzione e scambio | Non viene utilizzato alcun documento cartaceo |
| Garantire la sicurezza della rete su cui viene eseguito il trattamento (sistema firewall, proxy, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi) | Presente |

Inoltre,

- Certificazioni: My Governance ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza. L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure chiaramente definiti a presidio dei processi aziendali. Certificazioni: ISO 9001 e ISO 27001
- Compliance: i processi aziendali di My Governance rispondono alle normative vigenti, in particolare per quanto riguarda la rispondenza ai requisiti di privacy. In tale ambito l'azienda ha adeguato il proprio sistema di gestione alle richieste del provvedimento del Garante per la Protezione dei Dati Personali riguardo gli amministratori di sistema. Qualora le prescrizioni di legge vengano modificate My

MYGO SRL
Via del Corso, 92
00186 – Roma, Italia
T. (+39) 06.45214912
E. info@mygovernance.it
W. www.mygovernance.it

Governance adeguerà immediatamente le modalità di erogazione del servizio e le caratteristiche tecniche per essere conforme alle eventuali modifiche.

- Accesso alle informazioni: il sistema di gestione di My Governance prevede l'esplicita classificazione del livello di riservatezza di ogni documento. In particolare i documenti contenenti informazioni sui sistemi di sicurezza vengono classificati come riservati e non sono diffusi all'esterno dell'azienda.
- Accesso ai sistemi: gli accessi ai sistemi sono sempre classificabili in accessi di produzione e accessi di amministrazione. Gli accessi di produzione sono quelli oggetto della fornitura del servizio. Gli accessi di amministrazione sono quelli effettuati da My Governance o dal cliente con finalità diverse quali la manutenzione, la verifica di anomalie, l'acquisizione di dati. Gli accessi di amministrazione da parte di My Governance sono riservati a personale con la qualifica ("ruolo") di amministratore di sistema. L'azienda pone particolare attenzione all'assegnazione di tale ruolo soltanto a personale di elevate capacità tecniche e avente caratteristiche di comprovata affidabilità e moralità. L'accesso amministrativo ai sistemi da parte di personale del cliente avverrà attraverso l'assegnazione nominale di personale a ruoli ai quali sono assegnati privilegi di accesso.
- Auditing: nell'ambito del proprio sistema di gestione My Governance pone particolare attenzione all'audit dei sistemi e delle attività amministrative compiute sugli stessi. L'accesso al sistema di gestione dei log è riservato al personale di My Governance avente ruolo di auditor ed è inaccessibile al personale addetto all'amministrazione di sistema.
- Riservatezza dei dati: My Governance non potrà conoscere in nessun modo i dati personali inseriti dagli utenti del cliente all'interno della singola segnalazione. My Governance non si assume alcuna responsabilità riguardo all'uso che di tali dati viene fatto da parte del cliente o da società incaricate dal cliente stesso che gestiscono o utilizzano il servizio. My Governance gestirà e conserverà le informazioni in conformità alle norme espresse dalla vigente normativa.
- Log Management: i log dei sistemi contengono informazioni necessarie alle attività amministrative, di diagnostica e di sicurezza. Ogni sistema viene configurato per loggare ogni evento significativo. I log generati da ogni sistema vengono trasferiti ad un repository centrale. La conservazione dei log avviene secondo le norme di legge, in particolare il Codice Privacy e le norme sulla conservazione dei dati di traffico telefonico e telematico. I log dei sistemi riportano tutte le attività significative ai fini della sicurezza quali gli accessi amministrativi, le modifiche ai permessi e alle configurazioni di sistema e di sicurezza, le anomalie.
- Sicurezza dei sistemi: i servizi di sicurezza si ritengono attivi e funzionanti a protezione delle componenti ospitate in Datacenter. I sistemi di protezione sono progettati in modo da massimizzare la protezione e sono amministrati da personale con formazione specifica che segue procedure operative stringenti.
- Controlli di sicurezza: sull'intera infrastruttura sono svolti Penetration Test e Vulnerability Assessment con cadenza semestrale
- Firewalling: I flussi dati vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati.
- Filesystem Antivirus: tutti i server dispongono di moduli Antivirus
- Security Patch Management: la piattaforma è sottoposta ad un processo periodico di verifica delle patch o delle fix rilasciate dal produttore e ritenute critiche per l'erogazione del servizio o per la sicurezza. L'applicazione delle patch verrà sottoposta a preventiva comunicazione al cliente e la schedulazione avverrà in accordo con quest'ultimo.