Pubblicazione sul proprio sito istituzionale: http://www.agnochiampoambiente.it/amministrazione-trasparente/ in data 05.11.2026

AGNO CHIAMPO AMBIENTE S.r.l.

Novembre 2026

Valutazione d'impatto *ex* art. 35 GDPR

Glossario

DEFINIZIONE	DESCRIZIONE
Accountability	**È richiesto al Titolare di dimostrare, documentalmente, la conformità al GDPR.**
Categorie particolari di dati personali	**L'Origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.**

Dato personale	**Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.**
Diffusione	**La divulgazione di dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).**
DPIA (o PIA)	**Data Protection Impact Assessment (o Privacy Impact Assessment): è la valutazione d'impatto sulla protezione dei dati da eseguire in funzione.** **Tale processo è volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Lo stesso può riguardare una singola operazione di trattamento dei dati, ma potrebbe riferirsi anche a trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto e rischi.**
Interessato	**La persona fisica cui si riferiscono i dati personali.**
Liceità del trattamento	**Il Trattamento di dati personali può essere considerato lecito se ricorre almeno una delle seguenti condizioni;** **a) L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità** **b) Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso** **c) Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento** **d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica** **e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento**

	f) Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
Misure di sicurezza	**Insieme degli accorgimenti tecnici, organizzativi o fisici, dei dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, delle misure che permettano alle sole persone autorizzate di avere accesso ai dati; ulteriori accorgimenti atti ad evitare che siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti, ecc.**
Privacy by design	**Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.**
Responsabile del Trattamento	**La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.**
Titolare del Trattamento	**La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.**
Trattamento	**Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o**

	qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Premessa

Nell'ambito dell'implementazione del proprio modello di ricevimento e gestione delle segnalazioni interne, gli enti pubblici e privati destinatari delle nuove norme dovranno svolgere una valutazione di impatto (cd. "*Data Protection Impact Assesment*") *ex* art. 35 del GDPR al fine di individuare le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati.

Il D. Lgs. n. 24 del 2023 prescrive, per tutti i soggetti che devono predisporre canali di segnalazioni interni a disposizione dei whistleblower, l'obbligo di dar corso ad una valutazione d'impatto ai sensi del Regolamento 2016/679 (GDPR) che contenga:

a. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c. una valutazione dei rischi per i diritti e le libertà degli interessati;
d. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Più specificamente, il Decreto richiede che, nella fase di progettazione del canale di segnalazione whistleblowing, sia effettuata una DPIA ai sensi degli artt. 35 e 36 del Regolamento (UE) 679/2016 nel caso in cui il trattamento delle segnalazioni, divulgazioni pubbliche o denunce possa comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa, ad esempio, del gran numero di soggetti interessati o del ricorso a strumenti informatici e tecnologici nuovi), al fine di individuare ed applicare le necessarie misure tecniche per evitare tale rischio, includendo le garanzie per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento

(GDPR), tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte ai sensi del Decreto.
Si fa osservare, inoltre, che le tipologie di trattamenti, la necessità o meno del trattamento ed il bilanciamento fra rischi e tutele sono già normativamente definiti in modo compiuto. Ne consegue che la presente DPIA sarà focalizzata sui rischi e sulle misure di sicurezza previste per l'utilizzo dei canali di segnalazione informatico (piattaforma Mygo) e cartaceo.

La presente DPIA è stata redatta con l'ausilio del Responsabile del trattamento per l'utilizzo della piattaforma (Mygo S.r.l.), che ha individuato i rischi e le misure di sicurezza previste in materia di segnalazioni whistleblowing.

Tutte le misure di seguito indicate, si intendono adeguate ed idonee a rendere trascurabile o limitato il rischio di dispersione dei dati, di accesso abusivo al sistema informatico o al rischio di modifica o alterazione dei dati.

CONTESTO

Quale è il trattamento in considerazione?

Il trattamento in esame riguarda i dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite, delle quali sia venuto a conoscenza, commesse dai soggetti che a vario titolo interagiscono con la Società, allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.
La ricezione e la gestione delle segnalazioni dà luogo a trattamenti di dati personali riferiti al segnalante tra i quali principalmente dati anagrafici e di contatto e eventualmente, secondo il contenuto della segnalazione, a soggetti terzi.
Ed appunto, il trattamento in questione comporta il conferimento – di persona al Gestore, tramite invio di segnalazione – di dati anagrafici, codice fiscale, dati di contatto e, eventualmente, dati sulla qualifica professionale, nonché di dati e informazioni ulteriori connessi alla condotta illecita riportata.
La segnalazione potrebbe, altresì, comprendere dati personali riferiti alle persone indicate come possibili responsabili delle condotte illecite, nonché delle persone a vario titolo coinvolte nelle vicende segnalate.
I predetti dati saranno trattati con supporti informatici e cartacei che ne garantiscono la sicurezza e la

riservatezza.

La documentazione in formato cartaceo è limitata al minimo indispensabile ed è archiviata e custodita in armadi e locali dotati di serrature di sicurezza.

Con riguardo alla piattaforma, la trasmissione dei dati forniti dal segnalante mediante compilazione del *form* sul portale "MY WHISTLEBLOWING".

Sono inoltre applicate tecniche di cifratura basate su Algoritmo AES e tutti i dati sono completamente criptati, garantendo in questo modo la riservatezza delle informazioni trasmesse.

I dati sono trattati dal Gestore delle segnalazioni, adeguatamente formato, che opera in qualità di personale autorizzato al trattamento del dato, secondo principi di correttezza, liceità, trasparenza, pertinenza e non eccedenza rispetto alle finalità della raccolta e di successivo trattamento.

Il Gestore tratterà i dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite, delle quali sia venuto a conoscenza, allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

Al fine di garantire la riservatezza del segnalante per tutta la durata della gestione della segnalazione, l'identità dello stesso sarà conosciuta solo dal Gestore e, se del caso, da eventuali altri soggetti, previamente autorizzati, di cui quest'ultimo dovesse avvalersi durante la fase istruttoria.

Quali sono le responsabilità connesse al trattamento?

Titolari del trattamento: AGNO CHIAMPO AMBIENTE S.R.L.

Responsabile del trattamento: MYGO PIATTAFORMA MY WHISTLEBLOWING

Ci sono standard applicabili al trattamento?

- Art. 35, Regolamento UE 2016/679 (c.d. GDPR)
- Linee Guida concernenti la valutazione d'impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, WP248 rev.1, revisionate il 04 ottobre 2017
- Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 – 11 ottobre 2018 [doc. web. n. 9058979]
- Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979], Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto
- i codici di condotta approvati (vedi Art. 40 del RGPD)
- le regole deontologiche e le prescrizioni del Garante per la protezione dei dati personali o da altri

soggetti competenti ai sensi del d.lgs. 196/2003 (art. 2-quater, art. 2-quinquiesdecies, art. 2-septies, art. 2-octies)

Quali sono i dati trattati?

I dati personali oggetto di trattamento si riferiscono, in particolare, a:

- dati personali del segnalante, a seguito di una segnalazione effettuata in forma non anonima, quali nome, cognome ed eventuali altre informazioni che il segnalante volesse rilasciare quali recapito telefonico, indirizzo mail, indirizzo postale;
- dati personali ed informazioni sul segnalato o su altri soggetti coinvolti, che potranno essere inserite nell'apposito percorso digitale attivato dalla Società per consentire l'inoltro della segnalazione.
- dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite o non improntate a principi di eticità ed integrità delle quali sia venuto a conoscenza.

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

1) Fase di inserimento della segnalazione da parte del segnalante

2) Fase di ricezione e gestione della segnalazione da parte del Gestore preposto e relativa attività istruttoria

3) Fase decisoria da parte del Gestore

4) Fase di archiviazione cartacea o informatica della segnalazione e dei relativi provvedimenti

5) Fase (eventuale) di cancellazione di distruzione o cancellazione del dato se valutato irrilevante o superfluo

6 - Fase di cancellazione nei termini di legge (5 anni)

Quali sono le risorse di supporto ai dati?

- Supporti cartacei e persone per il canale di posta cartacea
- Piattaforma *My whislteblowing*

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati personali devono essere raccolti per scopi specificati, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi. (art. 5.1 b) del GDPR).

I dati forniti verranno trattati esclusivamente per l'istruttoria della segnalazione ai sensi della normativa

whistleblowing.

Vengono trattati solamente i dati personali adeguati, pertinenti e limitatamente a quanto necessario rispetto alle finalità per le quali sono raccolti e trattati.

I dati sono trattati da personale adeguatamente istruito, che opera in qualità di personale autorizzato al trattamento del dato, secondo principi di correttezza, liceità, trasparenza, pertinenza e non eccedenza rispetto alle finalità della raccolta e di successivo trattamento.

Il trattamento avviene in maniera da garantire un'adeguata sicurezza dei dati personali, mediante l'utilizzo di strumenti automatizzati, nonché la riservatezza e la protezione, attraverso misure tecnico organizzative volte a prevenire la perdita dei dati, gli usi illeciti o non corretti e gli accessi non autorizzati.

Quali sono le basi legali che rendono lecito il trattamento?

Per le finalità sopra indicate, la base di legittimità dei trattamenti dei Dati Personali è rappresentata da:

a) il consenso *ex* artt. 6, par. 1, lett. a) e art. 9, par. 2, lett. a), del GDPR che Lei potrà manifestare prima di procedere all'invio della segnalazione, sul Modello di segnalazione messo a diposizione dai Titolari e pubblicato sulla pagina web delle Società;

b) l'interesse legittimo dei Titolari, ai sensi dell'art. 6, co.1, lett. f) del GDPR, che venuto a conoscenza della segnalazione da Lei presentata, intenda garantire e preservare gli interessi della società;

c) la necessità di adempiere ad obblighi legali cui sono soggetti i Titolari (in particolare l'art. 4 e ss. del D.Lgs. n. 24 del 2023 e l'art. 6., co. 2 bis e ss. del D. Lgs. 8 giugno 2001, n. 231);

d) la necessita di accertare, esercitare o difendere un diritto in sede giudiziaria, in caso fosse necessari.

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

In base alle previsioni della normativa in materia di dati personali e del D.lgs. n. 24 del 2023 ed alle Linee Guida ANAC (Delibera n.311 del 2023), i Titolari del trattamento, i Responsabili del trattamento e le persone autorizzate a trattare i dati personali relativi alle segnalazioni *whistleblowing* sono tenuti a rispettare anche i seguenti principi fondamentali:

· Trattare i dati in modo lecito, corretto e trasparente nei confronti dei soggetti interessati («**liceità, correttezza e trasparenza**»).

· Raccogliere i dati solo al fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce effettuate da parte dei soggetti tutelati dal D.lgs. 24/2023 («**limitazione della finalità**»).

· Garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»). A tal riguardo il decreto precisa, infatti, che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati senza indugio.

· Assicurare che i dati siano esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione, divulgazione pubblica o denuncia che viene gestita («**esattezza**»).

· Conservare i dati in una forma che consenta l'identificazione degli interessati per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione («**limitazione della conservazione**»).

· Rendere *ex ante* ai possibili interessati (ad es. segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) un'informativa sul trattamento dei dati personali mediante la pubblicazione di documenti informativi ad esempio tramite sito web, piattaforma, informative brevi in occasione dell'utilizzo degli altri canali previsti dal decreto. Non devono invece essere fornite informative *ad hoc* ai vari soggetti interessati.

· Assicurare l'aggiornamento del registro delle attività di trattamento, integrandolo con le informazioni connesse a quelle di acquisizione e gestione delle segnalazioni.

· Garantire il divieto di tracciamento dei canali di segnalazione. Nel caso in cui l'accesso ai canali interni e al canale esterno di segnalazione avvenga dalla rete dati interna del soggetto obbligato e sia mediato da dispositivi *firewall* o *proxy*, deve essere garantita la non tracciabilità – sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - del segnalante nel momento in cui viene stabilita la connessione a tali canali.

· Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante.

· Effettuare il trattamento in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»). Nel contesto in esame, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, il ricorso a strumenti di crittografia nell'ambito dei canali interni e del canale esterno di segnalazione, è di regola da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al predetto principio di integrità e riservatezza. Le misure di sicurezza adottate devono, comunque, essere

periodicamente riesaminate e aggiornate.

· Definire un modello di gestione delle segnalazioni in conformità ai principi di protezione dei dati personali. In particolare, tali misure devono fare in modo che non siano resi accessibili, in via automatica senza il tramite del titolare del trattamento o soggetto autorizzato, dati personali a un numero indefinito di soggetti.

· Effettuare, nella fase di progettazione del canale di segnalazione e dunque prima dell'inizio del trattamento, **una valutazione d'impatto sulla protezione dei dati ai sensi degli artt. 35 e 36 del Regolamento (UE) 679/2016** nei casi in cui il trattamento delle segnalazioni, divulgazioni pubbliche o denunce può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa, ad esempio, del gran numero dei soggetti interessati di cui sono magari trattati anche dati sensibili o del ricorso a strumenti informatici e tecnologici nuovi) al fine di individuare ed applicare le necessarie misure tecniche per evitare tale rischio.

I dati sono esatti e aggiornati?

La Società adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione, ove consentito dalla legge.

L'esattezza dei dati è garantita dalla conservazione dei dati relativi alla segnalazione e delle policy di seguito indicate che consentono di mitigare adeguatamente il rischio di modifica o alterazione dei dati.

Qual è il periodo di conservazione dei dati?

I Dati Personali, nel rispetto del principio di minimizzazione di cui all'articolo 5, comma 1, lett. c), del GDPR nonché degli obblighi di legge cui sono tenuti i Titolari, il Responsabile di trattamento e il Gestore delle segnalazioni, saranno conservati per il tempo necessario per elaborare e indagare su una segnalazione di irregolarità e per il tempo necessario per decidere e applicare sanzioni o altre misure o comunque non oltre i cinque anni (art. 14 del D.Lgs. n. 24 2023) prevista dalla legge.

MISURE SPECIFICHE DI SICUREZZA GENERALI

Come sono informati del trattamento gli interessati?

Gli interessati sono adeguatamente informati mediante l'Informativa *privacy* e la Procedura *Whistleblowing* pubblicate sul sito istituzionale della Società

Ove applicabile: come si ottiene il consenso degli interessati?

All'Interessato/segnalante è sottoposta l'informativa *privacy* da sottoscrivere/flaggare per attestarne la presa visione.

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

Ai sensi degli articoli dal 15 al 22 del GDPR, in qualità di interessato, l'interessato ha il diritto di:

- ottenere da parte dei Titolari la conferma che sia o meno in corso un trattamento di dati personali che la riguardano e in tal caso, ottenere l'accesso ai suoi dati, nonché, qualora i dati non siano raccolti presso, ricevere tutte le informazioni disponibili sulla loro origine;
- conoscere le finalità del trattamento, le categorie dei dati in questione, i destinatari o le categorie di destinatari cui i dati sono stati o saranno comunicati, il periodo di conservazione dei dati previsto o i criteri utilizzati per determinare tale periodo;
- chiedere ai Titolari la cancellazione dei dati o la limitazione del trattamento dei dati che la riguardano, nei casi previsti dalla legge;
- opporsi al trattamento dei dati, fatto salvo il diritto dei Titolari di valutare la Sua istanza, che potrebbe non essere accettata in caso di esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgano sui Suoi interessi, diritti e libertà;
- richiedere la portabilità dei dati, nei casi previsti dalla legge, se compatibile con la disciplina del *whistleblowing*.

Si precisa, inoltre, che ai sensi dell'art.2-*undecies*, co.1, lett. f) del D.Lgs. 101/2018, i Titolari garantiscono la riservatezza della identità del segnalante.

L'interessato che ritenga che il trattamento dei dati personali avvenga in violazione di quanto previsto dal Regolamento ha, inoltre, il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

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

Sì, sono disciplinati da un *Data Protection Agreement ex* art. 28 del GDPR.

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

Non sono previsti trasferimenti dei dati fuori dall'UE.

MISURE ESISTENTI O PIANIFICATE

SICUREZZA DEI DOCUMENTI CARTACEI

Presidi relativo all'utilizzo ed all'archiviazione dei documenti cartacei (ad es. segnalazione pervenuta attraverso il canale di posta ordinaria), tra cui: archiviazione in armadio custodito ed accessibile solo da parte del Gestore).

GESTIONE DEGLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

Un incidente nell'ambito della sicurezza dei sistemi informativi è un evento o una vulnerabilità, in grado di violare l'integrità, la confidenzialità o la disponibilità delle applicazioni o dei dati del sistema.

È necessario quindi attivare le opportune procedure per minimizzare il rischio derivante da violazioni delle misure di sicurezza, per garantire adeguata e tempestiva segnalazione dei reali o sospetti incidenti o violazioni.

Sono stabiliti i seguenti obiettivi in materia di gestione degli incidenti:

- contenere i possibili danni dovuti ad un incidente mediante la definizione di responsabilità chiare e procedure corrette che assicurino una risposta tempestiva;
- misurare l'efficacia ed adeguatezza delle politiche di sicurezza e delle contromisure attuate mediante la registrazione e la successiva analisi degli incidenti.

Per il raggiungimento degli obiettivi definiti si stabilisce di:

- sensibilizzare il personale coinvolto nel trattamento dei dati. Infatti, l'efficacia del sistema di gestione degli incidenti può essere inficiata o annullata dalla mancata osservanza delle norme comportamentali e dalla mancata segnalazione alle funzioni competenti di eventuali debolezze del sistema;
- definire canali che consentano al personale di comunicare nel più breve tempo possibile alla struttura preposta le situazioni di incidente e/o di attacco e/o di evento sospetto.

SICUREZZA DEI CANALI INFORMATICI

La sicurezza delle informazioni è caratterizzata dai seguenti aspetti:

- Confidenzialità: garantisce che l'informazione sia accessibile solamente da coloro che sono autorizzati ad accedervi;
- Integrità: garantisce l'accuratezza, la completezza e quindi l'affidabilità dell'informazione e dei metodi utilizzati per la sua elaborazione;
- Disponibilità: garantisce che gli utenti autorizzati possono accedere all'informazione.

La sicurezza delle informazioni viene conseguita attraverso l'implementazione di policy, procedure, strutture organizzative, processi operativi, strumenti software e tutti gli altri controlli ritenuti necessari in funzione del risk appetite aziendali.

Commento alla valutazione: le reti, i sistemi, i server e le apparecchiature informatiche utilizzati dal Titolare per il trattamento dei dati personali sono adeguatamente protetti dai rischi di sottrazione, accesso abusivo, perdita, modifica non autorizzata o corruzione dei dati mediante impiego di software antivirus e firewall. Inoltre, gli applicativi impiegati sono costantemente aggiornati.

MISURE SPECIFICHE DI SICUREZZA PIATTAFORMA MYGO

Crittografia	*Se si, descrivere i mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup ecc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di sospetta compromissione ecc.).* *Specificare i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, ecc.) implementati nel trattamento.*	L'intero ciclo di gestione dei dati viene crittografato utilizzando l'algoritmo di crittografia AES256 (Crypting protocol: "Advanced Encryption Standard" (lo stesso che usa il governo USA) AES / CBC / NOPADDING),. Durante la comunicazione "in transito" tramite TLS / Protocolli HTTPS. Tutto lo spazio di archiviazione è crittografato AES256 e i dati sensibili sono crittografati nel database.
Anonimizzazione	*Indicare qui i meccanismi di anonimizzazione implementati, le garanzie da essi introdotte contro l'eventuale reidentificazione e per quali finalità sono implementati.*	Il sistema separa logicamente i contenuti del database in modo tale per cui i dati delle segnalazioni risultano separati dai dati del segnalante. Senza esplicita volontà del segnalante non è mai possibile associare una segnalazione al ID di un segnalante
Controllo degli accessi logici	*Descrivere in che modo sono definiti e attribuiti i profili degli utenti. Specificare i mezzi di autenticazione implementati precisando, ove applicabile, le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numero di tentativi prima del blocco dell'account, ecc.).*	● Ogni soggetto coinvolto nel trattamento delle credenziali di autenticazione riceverà un codice identificativo (“User ID”) associato ad una parola chiave (“password”) secondo i migliori standard attualmente in commercio. Password con requisiti minimi di sicurezza garantiti.● La password di accesso deve soddisfare almeno i seguenti requisiti: almeno 8 caratteri, una lettera maiuscola, una lettera minuscola, un simbolo speciale e un numero. Al quinto tentativo errato di immissione di una password, l'utente verrà bloccato per 30 minuti.● Gli account utente verranno disabilitati dopo 12 mesi di inattività, ovvero verranno immediatamente disabilitati o cancellati quando l'utente cesserà la propria attività. Gli account utente esistenti e i diritti di accesso verranno rivisti almeno una volta all'anno al fine di rilevare account inattivi o account con privilegi eccessivi.● E' possibile attivare una Strong Authentication attraverso la quale verrà richiesto di inserire un secondo fattore, un codice numerico, inviato via mail per accedere alla propria area personale.. La password di accesso al software deve essere composta da caratteri alfanumerici e caratteri speciali, deve essere cambiata ogni 90 giorni, con una password diversa dalle tre precedenti dello storico. Una volta comunicato al Cliente ne viene richiesta la modifica al primo utilizzo. Gli Account di accesso al software sono nominativi e forniti al Cliente nella misura necessaria e sufficiente per lo sfruttamento di un software adeguato. Abbiamo impostato un meccanismo di blocco dell'accesso dopo 10 tentativi di accesso non riusciti, garantendo che la connessione al Software si interrompa dopo un'ora di inattività.

Tracciabilità	*Politiche che definiscono la tracciabilità degli eventi e la gestione dei relativi log.*	My Whistleblowing traccia e registra una serie di informazioni che vengono salvati in file LOG. I file rispondono alle seguenti funzionalità: ▪ AnagraficaRubricaLOG: viene salvato un record quandosi fa un update di una rubrica (ma non quando viene inserita), vengono salvati i nuovi dati della rubrica insieme all'id dello user che ha fatto la modifica ▪ ArchivioDocumentiDownloadLOG : viene inserito un record quando viene fatto un download di un report d flussi (myApprovals) o della rubrica; viene salvato chi fa i downlad ▪ UtentiLOG : viene salvato lo stato dell'utente insieme a chi a fatto la modifica quando ▪ si fa un update alla rubrica ▪ Vengono reinviate le credenziali ▪ MWBFlussiLog : Viene inserito un record ogni volta che viene fatta una modifica a una segnalazione (cambio di stato, conferma disclaimer) ▪ MWBFlussiCommentiLogLettura : Si inserisce un record quando si fa un commento a una segnalazione (sono le notifiche che vengono mostrate col pallino rosso in interfaccia, si riesce a capire se un utente ha visto il commento di un altro utente oppure no).

		▪ L'accesso ai file di log è possibile solo tramite il nostro supporto: l'utente non accede direttamente ai file di sistema.
Archiviazione	*Politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, ecc.).*	I dati verranno conservati nel sistema ed eventualmente soggetti a cancellazione logica secondo in armonia con le regole di conservazione richieste dal client I dati verranno eliminati dal nostro database in base ai tempi concordati con il cliente all'atto della comunicazione di interruzione del contratto. In caso di interruzione del rapporto contrattuale i dati verranno, in primis, consegnati in formato da concordare al cliente. Dopo di che verranno distrutti all'interno del nostro database con tempi da concordare.
Sicurezza dei document icartacei	*Politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento. Tali politiche descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.*	Non sono utilizzati documenti cartacei
Minimizzazione dei dati	*Si possono utilizzare i seguenti metodi: filtraggio e rimozione, riduzione del potenziale identificativo attraverso trasformazione, riduzione della natura identificativa del dato, riduzione dell'accumulazione dei dati, limitazione dell'accesso ai dati*	Non applicabile
Vulnerabilità	*Politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività (documentare le procedure operative, inventariazione e aggiornamento di software e hardware, correzione di vulnerabilità, duplicazione dei dati, limitazioni all'accesso fisico al materiale, ecc.).*	Per la valutazione delle vulnerabilità dei sistemi, My Governance può avvalersi di consulenti esterni individuati allo scopo di effettuare test di penetrazione (con frequenza almeno biennale), ovvero utilizzando software ad hoc che effettueranno test di vulnerabilità automatici su base ricorrente . Al ricevimento di qualsiasi segnalazione, il team operativo sarà responsabile di: ● Fornire un rimedio modificando la configurazione o distribuendo le patch di sicurezza ● Implementare altre misure di mitigazione ● Rivedere il risultato ● Documentare correttamente ogni possibile eccezione La correzione della vulnerabilità deve essere completata il più rapidamente possibile, in ogni caso seguendo queste linee guida: Qualunque esito che debba essere mitigato in un arco di tempo superiore alla tempistica di delibera sopra indicata, deve essere approvato dal Management Team e documentato in via eccezionale. Ogni caso di vulnerabilità deve generare una specifica segnalazione. Tali segnalazioni di vulnerabilità devono essere condivise con l'Alta Direzione. Le segnalazioni di vulnerabilità avranno una frequenza massima mensile o trimestrale, a seconda delle circostanze. I report sono archiviati in cartelle condivise accessibili dal Top Management. Il Cliente può condurre test di penetrazione, valutazioni di

		vulnerabilità e sopralluoghi presso le sedi di My Governance per esaminare e valutare l'adeguatezza delle misure tecniche e organizzative poste in essere con riferimento ai Servizi erogati. My Governance dichiara di aver implementato un processo di monitoraggio delle vulnerabilità e di aver adottato una policy di patch che prevede la fornitura di patch di sicurezza periodiche, infine implementate anti-malware sui componenti. My Governance si impegna ad inoltrare al Cliente nel più breve tempo possibile, per il momento a conoscenza, qualsiasi richiesta inerente i dati del Cliente o attività prestata al Cliente ai sensi del presente contratto pervenuta da qualsiasi Autorità Pubblica.
Lotta contro il malware	*Misure volte a proteggere l'accesso a reti pubbliche (Internet) o non controllate (di partner) nonché postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati personali.*	My Governance ha implementato un sistema antimalware sui propri sistemi che garantisce il processo di monitoraggio delle vulnerabilità e una politica di patch che fornisce patch di sicurezza regolari
Gestione postazioni	*Misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni ecc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accessi, lavoro su uno spazio di rete protetto, controllidi integrità, logging, ecc.).*	Il software My Whistleblowing è un sistema cloud e non ha componenti software installati localmente. Il download dei dati avviene attraverso l'applicazione che risponde ai criteri di sicurezza visti ai punti precedenti, è quindi escluso il rischio che i documenti o i dati scaricati attraverso il nostro sistema possano essere fonte diretta oindiretta di danni ai sistemi locali.

Sicurezza dei siti web	*Metodi e strumenti implementati per ridurre il rischio che le caratteristiche di un sito web siano sfruttate al fine di pregiudicare dati personali (disciplinare generale di sicurezza, cifratura TLS dei flussi di dati, politica di rilascio dei cookie, audit di sicurezza, ecc.) .*	Il sito web è integrato nel sistema, e quindi risulta soggetto alle stesse regole e procedure già illustrate
Backup	*Esistenza di politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.).*	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 ridurra` al minimo la possibilita`di perdita e comunque nel caso dovesse avvenire sara`sicuramente molto limitata. Il back-up avviene almeno con frequenza quotidiana. Le applicazioni oggetto del Contratto risiedono su server certificato di Microsoft – Azure. Sono attualmente configurati i backup sulle risorse, in particolare: - Azure AppService backup (applicazione software) - Azure Database backup (dati dell'applicazione) Il backup del database è schedulato con la seguente retention policy: - Backup giornaliero per gli ultimi 7 giorni - Backup settimanale per le ultime 5 settimane - Backup mensile per gli ultimi 6 mesi - Backup annuale per l'anno in corso. I dati risiedono in zona Azure West-Europe.
Manutenzione	*Esistenza di una politica di manutenzione fisica dei dispositivi, specificando l'eventuale ricorso all'outsourcing.* *Dovrà comprendere la manutenzione remota, ove autorizzata, e specificare i metodi di gestione dei materiali difettosi*	Non applicabile: l'applicazione non gestisce dispositivi hardware locali
Sicurezza dei canali informatici	*A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o Internet), il titolare del trattamento deve implementare sistemi di protezione adeguati: firewall, sonde anti-intrusione o altri dispositivi (attivi o passivi) volti a garantire la sicurezza della rete.*	My Governance utilizza le applicazioni Microsoft Rete di produzione di Azure | Microsoft Docs per proteggere le nostre applicazioni Web o API da exploit Web e bot comuni che possono influire sulla disponibilità e compromettere la sicurezza.

Controllo degli accessi fisici	*Esistenza di un controllo degli accessi fisici ai locali che ospitano il trattamento (zonizzazione, accompagnamento di visitatori, assegnazione di badge, porte chiuse, e così via).* *Indicare se sono in atto procedure di allarme in caso di irruzione.*	I dati sono conservati presso i server Microsoft situati in Europa. MIcrosoft fornisce l'accesso fisico al data center solo ai dipendenti autorizzati. Tutti i dipendenti che necessitano dell'accesso al data center devono prima richiedere l'accesso e fornire una giustificazione aziendale valida. Queste richieste vengono concesse in base al principio del privilegio minimo, in cui le richieste devono specificare a quale livello del data center l'individuo deve accedere e sono limitate nel tempo. Le richieste vengono esaminate e approvate da personale autorizzato e l'accesso viene revocato allo scadere del tempo richiesto. Una volta concessa l'ammissione, le persone sono limitate alle aree specificate nelle loro autorizzazioni. L'accesso fisico ai data center Microsoft viene registrato, monitorato e conservato. L'accesso fisico è controllato ai punti di ingresso dell'edificio da personale di sicurezza professionale che utilizza sistemi di sorveglianza, rilevamento e altri mezzi elettronici. Il personale autorizzato utilizza meccanismi di autenticazione a più fattori per accedere ai data center. Gli ingressi alle sale server sono protetti con dispositivi che emettono allarmi per avviare una risposta a un incidente se la porta viene forzata o tenuta aperta. I sistemi elettronici di rilevamento delle intrusioni sono installati all'interno del livello dati per monitorare, rilevare e avvisare automaticamente il personale appropriato di incidenti di sicurezza. I punti di ingresso e di uscita verso le sale server sono protetti con dispositivi che richiedono a ciascun individuo di fornire l'autenticazione a più fattori prima di concedere l'ingresso o l'uscita. Questi dispositivi emetterannoallarmi se la porta viene forzata aperta senza autenticazione o tenuta aperta. I dispositivi di allarme porta sono inoltre configurati per rilevare le istanze in cui un individuo esce o entra in un livello dati senza fornire l'autenticazione a più fattori
Tracciabilità	*Esistenza di misure messe in atto per rilevare tempestivamente incidenti relativi a dati personali e*	My Governance attua misure proporzionate alla protezione dei sistemi informatici attraverso:● monitorare il traffico sulle

	disporre di elementi utilizzabili per studiarli o per fornire prove nel contesto di indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati ecc.)	proprie reti e sui sistemi informatici al fine di rilevare possibili attacchi alla sicurezza informatica e interruzioni del sistema e informare il personale;● mantenere registri ed effettuare prove adeguate per consentire l'indagine sugli incidenti e preservare la custodia di tali dati, anche per procedimenti giudiziari o di prova. La gestione dell'incidente avviene seguendo questo schema: Rilevamento dell'incidente: Il problema viene rilevato nella sua fase iniziale e le sue caratteristiche debitamente registrate e segnalate attraverso la creazione di un ticket specifico per ogni singolo incidente. Classificazione di un incidente: l'incidente viene classificato in base alla tipologia di rischio ad esso connesso (incidente a Basso, Medio o Alto Rischio) e viene definito il supporto iniziale per gestirlo. Inizio indagine e contenimento: viene avviata un'indagine volta a individuare la causa dell'incidente e vengono implementati tutti i mezzi necessari per limitare e contenere l'incidente e i relativi impatti, soprattutto se riguardano il Cliente. Lancio di una linea di comunicazione interna per risolvere l'incidente: viene stabilita una linea di comunicazione interna per gestire l'incidente, quindi verrà risolta utilizzando i dati acquisiti nella fase precedente. La soluzione finale è disponibile internamente per ulteriori referenze. Chiusura dell'incidente: l'incidente è ufficialmente chiuso. Problema risolto: il problema è stato risolto. E il sistema viene periodicamente controllato per la probabilità di ulteriori interruzioni. Creazione di un quadro: viene stabilito un quadro di riferimento che dovrebbe essere utilizzato per la risoluzione di incidenti simili. Valutazione del quadro: il quadro degli incidenti viene ulteriormente valutato per garantire un metodo semplice e sicuro per risolvere il problema.
Sicurezza dell'hardware	*Esistenza di misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso ecc.)*	*Non applicabile*
Prevenzione delle fonti di rischio	*Esistenza di misure per evitare che fonti di rischio, umane o non umane, anche se scarsamente probabili, arrechino pregiudizio ai dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE, ecc.)*	*Non applicabile*

Protezione contro fonti di rischio non umane	*Esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendi, danni provocati dall'acqua, incidenti interni o esterni, animali, ecc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, di rilevamento, protezione, ecc.)*	*L'applicazione si appoggia su infrastruttura HW e SW gestita da Microsoft. A questo link la descrizione delle misure di sicurezza specifica dei datacenter Microsoft:* Panoramica sulla sicurezza del datacenter - Microsoft Service Assurance | Microsoft Docs
Politica di tutela della privacy	*Esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio, ecc.)*	La verifica e la responsabilità di quanto attinente alla privacy è nella responsabilità del DPO
Gestione delle politiche di tutela della privacy	*Il titolare del trattamento deve disporre di una base documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, ecc.)*	La verifica e la responsabilità di quanto attinente alla privacy è nella responsabilità del DPO.
Gestione dei rischi	*Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.)*	La verifica e la responsabilità di quanto attinente alla privacy è nella responsabilità del DPO.
Integrare la protezione della	*Esistenza di procedure che descrivono i metodi volti a tenere conto della protezione dei dati personali in ogni nuovo trattamento (certificazioni, specifiche di*	Non applicabile

privacy nei progetti	*riferimento, gestione del rischio per la persona interessata secondo una metodologia interna o indicata dall'autorità di controllo, ecc.)*	
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	*Esistenza di un'organizzazione operativa per rilevaree gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.)*	My Governance attua misure proporzionate alla protezione dei sistemi informatici attraverso: ● monitorare il traffico sulle proprie reti e sui sistemi informatici al fine di rilevare possibili attacchi alla sicurezza informatica e interruzioni del sistema e informare il personale; ● mantenere registri ed effettuare prove adeguate per consentire l'indagine sugli incidenti e preservare la custodia di tali dati, anche per procedimenti giudiziari o di prova. La gestione dell'incidente avviene seguendo questo schema: Rilevamento dell'incidente: Il problema viene rilevato nella sua fase iniziale e le sue caratteristiche debitamente registrate e segnalate attraverso la creazione di un ticket specifico per ogni singolo incidente. Classificazione di un incidente: l'incidente viene classificato in base alla tipologia di rischio ad esso connesso (incidente a Basso, Medio o Alto Rischio) e viene definito il supporto iniziale per gestirlo. Inizio indagine e contenimento: viene avviata un'indagine volta a individuare la causa dell'incidente e vengono implementati tutti i mezzi necessari per limitare e contenere l'incidente e i relativi impatti, soprattutto se riguardano il Cliente. Lancio di una linea di comunicazione interna per risolvere l'incidente: viene stabilita una linea di comunicazione interna per gestire l'incidente, quindi verrà risolta utilizzando i dati acquisiti nella fase precedente. La soluzione finale è disponibile internamente per ulteriori referenze. Chiusura dell'incidente: l'incidente è ufficialmente chiuso. Problema risolto: il problema è stato risolto. E il sistema viene periodicamente controllato per la probabilità di ulteriori interruzioni. Creazione di un quadro: viene stabilito un quadro di riferimento che dovrebbe essere utilizzato per la risoluzione di incidenti simili. Valutazione del quadro: il quadro degli incidenti viene ulteriormente valutato per garantire un metodo semplice e sicuro per risolvere il problema.

Gestione del personale	*Esistenza di un piano che preveda le misure di sensibilizzazione adottate al momento della presa in carico di un dipendente, e di una procedura che descriva le misure adottate una volta cessato il rapporto di lavoro con i soggetti che accedono ai dati.*	Con l'assunzione vengono resi disponibili i documenti di sistema per la nuova risorsa e più precisamente: - la politica di sicurezza delle informazioni; - la disciplina sul corretto utilizzo degli strumenti assegnati al fine di non compromettere la sicurezza delle risorse aziendali; - le procedure e le istruzioni relative al ruolo e ai compiti. La nuova risorsa deve impegnarsi a rispettare le politiche di sicurezza delle informazioni (in materia di riservatezza, integrità e disponibilità delle stesse) e i principi etici stabiliti dalla società, nonché a sottoscrivere un accordo di riservatezza o non divulgazione, in relazione alle informazioni di cui verrà a conoscenza, sia durante che dopo la relazione. Formazione sulla sicurezza informatica È prevista un'adeguata formazione sulla Cyber Security, al fine di garantire che tutto il personale sia informato sui rischi per la sicurezza incorsi nell'utilizzo delle risorse aziendali e adeguatamente formato per consentire allo stesso di riconoscere situazioni di potenziale e/o concreta minaccia per la sicurezza. Viene inoltre svolta una formazione specifica per i rischi di cybersecurity come quelli legati al phishing e tutte le problematiche connesse al GDPR. Il tema della formazione è sempre stato molto sentito per My Governance, non solo per il background giuridico di alcuni di noi, ma anche e soprattutto perché riteniamo questa materia di fondamentale importanza, sia per il lavoro di tutti noi, ma anche per il nostro sviluppo personale per comprendere: - problemi di sicurezza; - i rischi che incidono sul patrimonio informativo; - gli obiettivi di sicurezza e le modalità per il loro raggiungimento. Il personale è inoltre a conoscenza di:

		- le procedure operative di sicurezza da adottare nello svolgimento dell'attività lavorativa; - il corretto utilizzo degli strumenti assegnati al fine di non compromettere la sicurezza delle risorse aziendali. Il programma di formazione è costruito e adattato ai diversi ruoli e compiti svolti in azienda. L'efficacia di tale programma è verificata periodicamente, e comunque almeno annualmente, al fine di intraprendere le necessarie azioni correttive e/o integrarlo alle nuove esigenze conoscitive che possono sorgere. Agli utenti, ai key user e all'Amministratore è prevista una formazione adeguata, che comprende gli elementi di protezione dei dati che saranno gestiti dal servizio. Cessazione del rapporto di lavoro Al termine del rapporto di lavoro l'ufficio informatico, tempestivamente informato dalla funzione HR, provvede al ripristino dei dispositivi aziendali assegnati a ciascun dipendente e alla chiusura/cancellazione dei profili/utenti in nome dello stesso. Inoltre, sulla base delle indicazioni ricevute dai Responsabili e al fine di garantire la continuità delle attività lavorative, può essere richiesto dal Responsabile della Direzione Operazioni Informatiche il backup dei dati sui dispositivi e la deviazione delle email aziendali ad altri destinatari. Sono definite adeguate procedure per la restituzione dei beni (es. computer portatili, cellulari, documenti, software, manuali, carte di credito) assegnati al personale che ha cessato il rapporto di lavoro. Tutti i permessi di accesso, logici o fisici (quali credenziali, smart card, chiavi, badge), assegnati al personale che ha cessato il rapporto di lavoro vengono verificati e revocati.
Gestione dei terzi che accedono ai dati	*Esistenza di una procedura volta a ridurre i rischi per le libertà e la vita privata degli interessati potenzialmente conseguenti all'accesso legittimo ai dati da parte di terzi (identificazione dei soggetti terzi, contratto di outsourcing, convenzione, BCR, ecc.)*	La verifica e la responsabilità di quanto attinente alla privacy è nella responsabilità del DPO.
Vigilanza sulla protezione deidati	*Esistenza di misure che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.).*	La verifica e la responsabilità di quanto attinente alla privacy è nella responsabilità del DPO.

POLICY A SUPPORTO DELLA DPIA DEL RESPONSABILE DEL TRATTAMENTO

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)	Mario Brocca	dpo@zucchetti.it

DESCRIZIONE
My Whistleblowing è parte della suite My Governance, una soluzione in cloud che permette di digitalizzare i processi aziendali. 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
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 Subappaltatori 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. I dati relativi alla gestione amministrativa e giuridica del rapporto contrattuale saranno conservati per 10 anni dalla cessazione del rapporto contrattuale.

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 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 Microsoft Azure.
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 uncodice per l'identificazione (“User ID”) associato a una parola chiave (“password”) secondo gli standard migliori oggi presenti sul mercato. Password con sicurezze minime garantite

La password riservata, conosciuta solamente dall'assegnatario ("Utente") deve avere quantomeno le seguenti caratteristiche: 1. essere composta da almeno 8 caratteri; 2. contenere lettere maiuscole e minuscole in combinazione con 3. numero o caratteri speciali; 4. non deve contenere lo User ID; 5. deve essere obbligatoriamente modificata al primo utilizzo e dopo il 6. reset della password; 7. deve essere modificata almeno ogni 60 giorni.	La password di accesso dovrà rispettare quantomeno i seguenti requisiti: ● almeno 8 caratteri ● almeno una lettera maiuscola ● almeno una lettera minuscola ● almeno un simbolo speciale ● almeno un numero 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: i. quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso venga utilizzato un sistema di autorizzazione. ii. i profili di autorizzazione, per ciascun incaricato o per classi 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. 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: i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana; 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 middlewaree 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 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,	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

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 esercitarei 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.

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

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 pergli 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
- 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
La password riservata, conosciuta solamente dall'assegnatario ("Utente") deve avere quantomeno le seguenti caratteristiche: 1. essere composta da almeno 8 caratteri; 2. contenere lettere maiuscole e minuscole in combinazione con 3. numero o caratteri speciali; 4. non deve contenere lo User ID; 5. deve essere obbligatoriamente modificata al primo utilizzo e dopo il 6. reset della password; 7. deve essere modificata almeno ogni 60 giorni.	La password di accesso dovrà rispettare quantomeno i seguenti requisiti: ● almeno 8 caratteri ● almeno una lettera maiuscola ● almeno una lettera minuscola ● almeno un simbolo speciale ● almeno un numero 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: i. quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso venga utilizzato un sistema di autorizzazione. ii. i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, siano individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari	Confermato

per effettuare le operazioni di trattamento. iii. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	

Proteggere i dati il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale: i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana; 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, 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 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 datie 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.
- 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.

PARERE DPO ok

Autore	Ufficio privacy
Approvazione	Ruggero Nicrosini

RISCHI

1) ACCESSO ILLEGITTIMO AI DATI

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

Violazione di norme di legge (GDPR e D.Lgs. n. 24 del 2023), danno reputazionale, richieste di risarcimento, data breach, comportamenti ritorsivi.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

trattamenti di dati personali invasivi a causa di accesso a soggetti non autorizzati, divulgazione di dati, modifica intenzionale o alterazione da parte dell'AS o di altri soggetti.

Quali sono le fonti di rischio?

Accesso abusivo da parte di soggetti non autorizzati. Furto di apparecchiature ; Virus informatici;;

Trattamento illecito dei dati; Ignoranza procedure di gestione; Diffusione illegale dei dati; Errore nello svolgimento di mansioni; Carenza di consapevolezza, disattenzione o incuria; Presa visione abusiva; Uso non autorizzato dei dati.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

CRITTOGRAFIA, SICUREZZA DEI CANALI INFORMATICI, ARCHIVIAZIONE, TRACCIABILITA', BACKUP, LOTTA CONTRO IL MALWARE, GESTIONE DELLE VULNERABILITA' TECNICHE

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

Valutazione: Limitata

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

Valutazione: Limitata

2) MODIFICHE INDESIDERATE DEI DATI

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

Violazione di norme di legge (GDPR e D.Lgs. n. 24 del 2023), comportamenti ritorsivi, danno reputazionale.

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

Modifica intenzionale o alterazione da parte dell'AS o di altri soggetti, trattamenti di dati personali invasivi a causa di accesso a soggetti non autorizzati.

Quali sono le fonti di rischio?

Fonti umane interne od esterne che dolosamente o colposamente accedano o modifichino i dati, accesso abusi da parte di soggetti non autorizzati, distruzione, deterioramento del supporto (portatile, computer, etc.), comportamenti sleali o fraudolenti, malfunzionamento, copia e modifica abusiva dei dati, etc.

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

BACKUP, TRACCIABILITA', CRITTOGRAFIA, LOTTA CONTRO IL MALWARE, MANUTENZIONE, SICUREZZA DEI CANALI INFORMATICI.

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

Valutazione: Limitata

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

Valutazione: Medio-bassa

3) PERDITA DI DATI

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

Violazione di norme di legge (GDPR e D.Lgs. n. 24 del 2023), comportamenti ritorsivi, danno reputazionale, richieste di risarcimento, *data breach.*

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

Perdita accidentale o furto del supporto, divulgazione di dati, trattamenti di dati personali invasivi a causa di accesso a soggetti non autorizzati.

Quali sono le fonti di rischio?

fonti umane interne od esterne che colposamente o dolosamente perdano i dati o il supporto, distruzione, deterioramento del supporto (portatile, computer, etc.).

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

ARCHIVIAZIONE, SICUREZZA DEI CANALI INFORMATICI, TRACCIABILITA', BACKUP, PROTEZIONE CONTRO FONTI DI RISCHIO NON UMANE, MANUTENZIONE.

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

Valutazione: Limitata

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

Valutazione: Medio-bassa

* * * * * *

Il sottoscritto, in qualità di titolare del trattamento in oggetto, dopo aver esaminato l'intera valutazione di impatto effettuata con l'ausilio del Responsabile del trattamento:

- conferma che la descrizione del contesto del trattamento è coerente con la realtà;
- prendo atto delle misure individuate dal Responsabile del trattamento;
- approva le misure correttive indicate;
- prende atto del parere del DPO
- si impegna ad attuare quanto prima le misure correttive indicate.

IL TITOLARE DEL TRATTAMENTO DI AGNO CHIAMPO AMBIENTE S.R.L.