ALPEA S.P.A.

STRADA CASTELLAMONTE, 4
10010 BAIRO (TO)
Tel: 0124501166 - Fax: 0124501169
P.IVA 02320320019
PEC: alpea@legalmail.it

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO: Gestione delle segnalazioni whistleblowing

ELENCO DEI TRATTAMENTI E DEI SOGGETTI INTERESSATI

Viene qui riportato un elenco dettagliato contenente la descrizione dei dati personali trattati suddivisi per sedi, trattamenti, ed archivi. È inoltre disponibile l'elenco dei soggetti interessati con relativi trattamenti coinvolti, dati trattati, finalità e liceità degli stessi.

La descrizione dettagliata delle aree di competenza, dei compiti e delle istruzioni affidati ai singoli soggetti è reperibile consultando la corrispondente nomina a responsabile od ad incaricato.

Titolare del Trattamento:	ALPEA S.P.A..

Elenco trattamenti da titolare

- **Gestione delle segnalazioni whistleblowing**

  Gestione dei dati personali forniti da soggetti che segnalino illeciti per l'analisi e la gestione della segnalazione, nonché per l'accertamento dei fatti oggetto della segnalazione e adozione dei conseguenti provvedimenti, in adempimento delle previsioni di cui al D. Lgs. 10 marzo 2023, n. 24

Dati Comuni trattati:	• nominativo, indirizzo o altri elementi di identificazione personale.
Dati Particolari trattati:	• Dati comuni ed eventuali dati particolari trattati nell'ambito della gestione delle segnalazioni whistleblowing.
Interessati al trattamento:	• Segnalante whistleblowing.

Archivi del trattamento

1 - Wall Breakers

Descrizione archivio:	• Sistema in cloud per la gestione delle segnalazioni di whistleblowing
Tipo di archivio:	• Archivio in Cloud.

Categorie di soggetti interessate al trattamento

Riportiamo ora in maggior dettaglio i trattamenti effettuati, distinguendo a quali soggetti interessati appartengono i dati oggetto di trattamento. Ulteriori informazioni a riguardo possono essere trovate, se previste, nelle relative informative.

- **Segnalante whistleblowing**

Trattamenti coinvolti:	• Gestione delle segnalazioni whistleblowing
Dati trattati:	• Dati comuni ed eventuali dati particolari trattati nell'ambito della gestione delle segnalazioni whistleblowing.; • nominativo, indirizzo o altri elementi di identificazione personale.
Finalità del trattamento: **[base giuridica]**	• rivelazione della sua identità a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni (comma 2 dell'art. 12 D.Lgs 24/2023) o nell'ambito del procedimento, ove la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza della sua identità sia indispensabile per la difesa dell'incolpato (comma 5 dell'art. 12 D.Lgs 24/2023). [richiesta di consenso]; • Attività di compliance in ambito D.Lgs 24/2023 [obbligo di legge o contrattuale]; • Ricezione, analisi e gestione della segnalazione, nonché per l'accertamento dei fatti oggetto della stessa e adozione dei conseguenti provvedimenti, in adempimento delle previsioni di cui al D. Lgs. 10 marzo 2023, n. 24 [obbligo di legge].
Tipologie di trattamento dei dati:	• a mezzo calcolatori elettronici con utilizzo di sistemi software gestiti da Terzi; • trattamento a mezzo di calcolatori elettronici; • Trattamento in forma orale; • trattamento temporaneo in Forma anonima/anonimizzata se scelto dal segnalante.
Tempo di conservazione dei dati:	• I dati potranno essere conservati fino a 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione (art. 14 D.Lgs. 24/2023); • stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati e nel rispetto dei tempi obbligatori prescritti dalla legge.; • stabilito in un arco di tempo non superiore all'espletamento degli obblighi di legge e per la tutela nel contenzioso.
I dati potranno essere comunicati a: **[base giuridica]**	• Autorità Giudiziaria [obbligo di legge]; • Comunicazione ad enti obbligatori per legge relativi alla normativa di whistleblowing secondo il D.Lgs 24/2023 [obbligo di legge]; • Enti preposti alle investigazioni [obbligo di legge]; • Piattaforma digitale di gestione whistleblowing Wallbreakers in qualità di Responsabile ex art. 28 GDPR [adempimento contrattuale].

ALPEA S.P.A.

STRADA CASTELLAMONTE, 4
10010 BAIRO (TO)
Tel: 0124501166 - Fax: 0124501169
P.IVA 02320320019
PEC: alpea@legalmail.it

ELENCO DEI RESPONSABILI ESTERNI

I dati personali in nostro possesso non sono affidati all'esterno della struttura del titolare.

ALPEA S.P.A.

STRADA CASTELLAMONTE, 4
10010 BAIRO (TO)
Tel: 0124501166 - Fax: 0124501169
P.IVA 02320320019
PEC: alpea@legalmail.it

ELENCO DELLE MISURE DI SICUREZZA ADOTTATE

Sono sotto riportate le misure di sicurezza implementate ai sensi dell'art.32 del Reg.to UE 2016/679.

Misure di sicurezza adottate a livello logico ed organizzativo

Misure di sicurezza adottate per trattamento

• Gestione delle segnalazioni whistleblowing

Gestione dei dati personali forniti da soggetti che segnalino illeciti per l'analisi e la gestione della segnalazione, nonché per l'accertamento dei fatti oggetto della segnalazione e adozione dei conseguenti provvedimenti, in adempimento delle previsioni di cui al D. Lgs. 10 marzo 2023, n. 24

Dati Comuni trattati:	• nominativo, indirizzo o altri elementi di identificazione personale.
Dati Particolari trattati:	• Dati comuni ed eventuali dati particolari trattati nell'ambito della gestione delle segnalazioni whistleblowing.
Archivi utilizzati per il trattamento	• Wall Breakers .

Misure Adottate

Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero. ► Back-Up in Cloud. Back-Up Su Sitemi in CLOUD
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali. ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Cifratura dei dati memorizzati.	I dati salvati su sistemi di archiviazione digitale vengono cifrati attraverso sistemi di protezione in ssl, PGP, o altri sistemi di cifratura proprietari
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Sospensione manuale delle sessioni di Lavoro.	Sospensione manuale delle sessioni di Lavoro.
Trattamento dei dati con protocolli criptati.	Trattamento dei dati con protocolli criptati ad es. SSL o criptazione dei dati tramite PGP

Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.
Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.
Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici	I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti
Pseudonimizzazione.	Pseudonimizzazione e cifratura dei dati personali
Separazione Fisica delle copie dei dati.	Le copie cartacee dei dati personali vengono conservati in un luogo differente da quello dove vengono effettuati i trattamenti.
Sicurezza Wall Breakers	Analisi di sicurezza e di Privacy by Design effettuata con metodologia NIST e criptazione separata di tutte le informazioni presenti