

Policy Whistleblowing

Allegato 2

Data di decorrenza:

31.07.2024.

Informativa sulla protezione dei dati

1. Ambito di applicazione della presente informativa sulla protezione dei dati

- (1) La presente informativa sulla protezione dei dati si applica a tutti i membri del gruppo OBO (di seguito: società del gruppo), ai loro dipendenti e membri degli organi gestori e ad altre persone interessate da una segnalazione, quando sono coinvolti nella gestione o nell'indagine di una segnalazione presentata a OBO Bettermann Holding GmbH & Co. KG con sede legale a Hüingser Ring 52, 58710 Menden (Sauerland), Germania, [numero di registro: HRA 4854, partita IVA: DE811792270] e/o a OBO Hungary Kft. con sede legale a Alsóráda 2, 2347 Bugyi, Ungheria, [numero di registro: 13-09-096185, partita IVA: HU10847392] come descritto nell'Allegato 1. Tutte le Società del Gruppo coinvolte nel trattamento dei dati personali oggetto di ciascuna segnalazione sono considerate contitolari del trattamento.
- (2) L'informativa sulla protezione dei dati di Gruppo OBO può essere consultata in qualsiasi momento al seguente [link](#).
- (3) Il Gruppo OBO si impegna a proteggere i dati personali dei whistleblower, delle altre persone coperte dalla Policy di Whistleblowing e di qualsiasi individuo menzionato o interessato da una segnalazione e attribuisce la massima importanza al rispetto del loro diritto all'autodeterminazione informativa. Il Gruppo OBO tratterà i dati personali con riservatezza e adotterà tutte le misure tecniche e organizzative per garantire la sicurezza dei dati.

2. Nome e indirizzo del/i responsabile/i del trattamento dei dati

- (1) Il responsabile principale ai fini della legge sulla protezione dei dati è la Società del Gruppo interessata al rapporto, come elencato nell'Allegato 3, insieme o indipendentemente da altre Società del Gruppo interessate, a seconda dei casi (di seguito "noi", "ci", "nostro", "responsabile/i del trattamento"):
 - Se all'ufficio competente in Germania il responsabile del trattamento è: **OBO Bettermann Holding GmbH & Co. KG**
Hüingser Ring 52
58710 Menden,
Germania

Telefono: +49 (0)2373 89-0

Fax: +49 (0)2373 89-238

E-mail: info@obo.de

[numero REA : HRA 4854, P.IVA : DE811792270] oppure

- Se all'ufficio competente in Ungheria il responsabile del trattamento è: **OBO BETTERMANN Hungary Kft.**
H-2347 Bugyi, Alsóráda str. 2.,
Ungheria
E-Mail: compliance@obo.de
Telefono: +0036 29 349-708
[numero REA : 13-09-096185, P.IVA : HU10847392]

(2) Dati di contatto del responsabile della protezione dei dati

OBO Bettermann Holding GmbH & Co. KG

Josef Honert

- Responsabile della protezione dei dati -

Hüingser Ring 52

58710 Menden

Germania

Tel.: +49 (0)2373 89-1351

E-mail: datenschutz@obo.de

(3) L'ufficio per il trattamento dei dati personali presso il Difensore civico (*Ombudsperson*) è:

DR. WEHBERG & PARTNER mbB

Revisori, consulenti fiscali e avvocati

Feithstraße 177, 58097 Hagen, Germania

Telefono: +49-(0)2331-1098-1234

E-mail: obo-hinweise@wehberg.de

Il referente per la protezione dei dati presso DR. WEHBERG & PARTNER mbB è:

DR. WEHBERG & PARTNER mbB

- Garante per la protezione dei dati personali -

Feithstraße 177, 58097 Hagen, Germania

E-mail: datenschutz@wehberg.de

Ulteriori informazioni sono disponibili alle pagine Internet <https://wehberg.de/impressum> e <https://wehberg.de/datenschutzerklaerung>.

3. Trattamento dei dati personali

Per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile, come nomi, indirizzi, numeri di telefono, indirizzi e-mail, dati anagrafici del contratto, dati contabili del contratto e dati di pagamento, nella misura in cui sono espressione dell'identità di una persona fisica. Trattiamo i dati personali solo se esiste una base giuridica per farlo.

Il processo decisionale automatizzato, compresa la profilazione, non è applicato in relazione all'utilizzo del sistema di whistleblowing del Gruppo OBO.

4. Categorie di dati trattati

(1) L'utilizzo dei sistemi di whistleblowing del Gruppo OBO per una segnalazione è volontario. Se si decide di utilizzare il sistema, è necessario fornire informazioni sulle seguenti categorie di dati

- Dati di comunicazione (ad es. nome, telefono, e-mail, indirizzo)
- Dati dei dipendenti di OBO e
- Se del caso, i nomi e gli altri dati personali dei segnalanti, delle persone citate in una segnalazione, delle persone coinvolte (e delle persone identificate in relazione) all'elaborazione dei fatti segnalati e alle relative ulteriori indagini.

(2) Rispondere in modo completo a tutte le domande per la segnalazione aiuterà i responsabili del trattamento a elaborare la segnalazione. In caso di informazioni incomplete o anonimo del whistleblower, potremmo non essere in grado di elaborare la segnalazione o potremmo subire un ritardo nel farlo.

(3) Possiamo raccogliere ed elaborare le seguenti categorie di dati personali attraverso l'utilizzo del sistema di whistleblowing del Gruppo OBO:

- le violazioni e i relativi fatti segnalati (compresi i dati relativi a frodi o accuse di frode, o altre violazioni della legge, o relativi a sospetti o possibili reati penali solo nella misura consentita dalla legge applicabile, ad esempio per consentire alla Società del Gruppo interessata di gestire il proprio contenzioso), le comunicazioni e le informazioni raccolte/esaminate in relazione alla segnalazione e all'indagine dei fatti segnalati (nel rispetto dei requisiti applicabili ai sensi della legge applicabile), e il rapporto di indagine;
- le conseguenze dell'indagine, comprese eventuali misure disciplinari, nonché accuse, azioni penali o condanne, a seconda dei casi;
- protezione delle persone interessate contro le ritorsioni;
- follow-up della segnalazione.

I dati personali sensibili e i dati personali relativi a sospetti, procedimenti o condanne per reati penali saranno trattati solo come consentito dalle leggi sulla protezione dei dati applicabili.

Solitamente, riceviamo i dati personali dallo stesso individuo a cui si riferiscono (ad esempio, i dipendenti stessi) oltre che da fonti pubblicamente disponibili e/o da terzi in modo lecito, come descritto di seguito.

Possiamo raccogliere dati personali nei modi elencati di seguito:

- Raccolta di dati personali direttamente dall'interessato, ad esempio attraverso una relazione o altri moduli o informazioni che gli interessati ci forniscono in relazione al loro impiego;
- Raccolta di dati personali durante le attività degli interessati nel corso del loro impiego, ad esempio attraverso le loro prestazioni e interazioni con altri dipendenti, clienti o altri individui; e
- Raccolta di dati personali da altre parti, come i segnalanti e altri dipendenti.

5. Finalità del trattamento e base giuridica

(1) Lo scopo del sistema di whistleblowing del Gruppo OBO è quello di fornire un canale di comunicazione per le segnalazioni e di garantire che queste vengano gestite dal Gruppo OBO in conformità con i processi del sistema di gestione della conformità in attuazione dei requisiti del diritto societario.

(2) In particolare, i dati personali saranno trattati per le seguenti finalità

- Reportistica di conformità: Indicazione e follow-up delle segnalazioni relative a una possibile violazione dei requisiti di conformità. È possibile segnalare tali violazioni con il proprio nome o in forma anonima.

Base giuridica: Le attività di trattamento sono svolte sulla base di un obbligo legale a cui le Società del Gruppo sono soggette (art. 6 (1) (c) del GDPR), come previsto dalla normativa applicabile in materia di whistleblowing.

Nei Paesi in cui non esiste l'obbligo legale di istituire un sistema di whistleblowing, le attività di trattamento sono svolte sulla base del legittimo interesse del/i titolare/i del trattamento (art. 6, par. 1, lett. f) GDPR) a perseguire reati, a far valere pretese civili, a sviluppare o interrompere un rapporto di lavoro o a individuare reati in relazione al rapporto di lavoro.

- Gestione della conformità: Amministrazione centrale e assegnazione delle questioni di conformità a livello di Gruppo.

Base giuridica: Legittimo interesse del/i responsabile/i del trattamento a ottenere una panoramica centrale dei rapporti nell'ambito della funzione di governance (art. 6 (1) f) GDPR) e per l'esercizio e la difesa dei nostri diritti.

In circostanze eccezionali, ad esempio quando intendiamo rivelare l'identità del segnalante a terzi, possiamo trattare i dati personali sulla base del consenso esplicito dell'interessato.

Nel caso in cui una segnalazione dovesse contenere categorie particolari di dati personali, tali dati saranno trattati solo

(i) se il trattamento è necessario per l'adempimento di obblighi e l'esercizio di diritti specifici del/dei responsabile/i del trattamento o dell'interessato nel campo del diritto del lavoro e della sicurezza sociale e della protezione sociale, nella misura consentita dal diritto dell'UE o nazionale o da un contratto collettivo di diritto nazionale che preveda adeguate garanzie per i diritti e gli interessi fondamentali dell'interessato (art. 9, par. 2, lett. b) GDPR), oppure

(ii) se il trattamento è necessario per l'istituzione, l'esercizio o la difesa di rivendicazioni legali (art. 9 (2) (f) GDPR). Nel caso in cui una segnalazione includa categorie speciali di dati personali che non sono chiaramente rilevanti per la questione segnalata, i dati di queste categorie saranno cancellati immediatamente e in modo sicuro.

I dati personali relativi a sospetti, procedimenti o condanne per reati saranno trattati solo in base a quanto specificamente autorizzato dal diritto unionale o nazionale.

6. Trasferimento dei dati ai dipendenti di OBO, a persone potenzialmente sospette e ad altri responsabili del trattamento dei dati

- (1) Quando si elabora una segnalazione, è necessario inoltrarla, in tutto o in parte, ai dipendenti di Gruppo OBO incaricati di elaborarla e ai dipendenti delle Società del Gruppo interessate dalla segnalazione. I dati saranno accessibili solo ai dipendenti che hanno la necessità di conoscerli per elaborare la segnalazione.
- (2) Il diritto dell'indagato di essere informato sul trattamento dei suoi dati personali può essere limitato o ritardato. Può essere limitato dalla legislazione nazionale vigente (art. 23 GDPR) o, in assenza di tale previsione, può essere ritardato in circostanze eccezionali, ad esempio in caso di rischio di distruzione di prove o quando è probabile che metta seriamente a rischio la finalità per cui le informazioni vengono trattate.
- (3) I dati personali saranno trasferiti alla Società del Gruppo interessata solo nella misura in cui ciò sia necessario per adempiere a ulteriori obblighi di legge. Inoltre, i dati possono essere trasferiti ad altri responsabili del trattamento (ad es. autorità) se richiesto a norma di legge o da ordini esecutivi di autorità o tribunali.

7. Trasferimento a destinatari al di fuori dell'UE e/o del SEE

I responsabili del trattamento possono trasferire dati personali dall'UE/SEE a terzi al di fuori dell'UE/SEE (compresa la concessione dell'accesso da un paese terzo) solo se

- il paese terzo offre un livello adeguato di protezione dei dati riconosciuto dalla Commissione UE e dal rispettivo paese, oppure
- il trasferimento è soggetto a clausole contrattuali standard dell'UE. È responsabilità del/i responsabile/i del trattamento, con l'assistenza della terza parte se necessario, valutare se il livello di protezione richiesto dal diritto dell'UE è rispettato nel paese terzo, al fine di determinare se le garanzie fornite dalle clausole contrattuali standard dell'UE possono essere soddisfatte nella pratica. In caso contrario, il terzo deve adottare misure aggiuntive per garantire un livello di protezione sostanzialmente equivalente a quello dell'UE/SEE, oppure
- in via eccezionale (cioè solo se le misure di cui ai punti precedenti non possono essere attuate), si applica un'esenzione per situazioni specifiche (ad esempio, il trasferimento è necessario per l'istituzione, l'esercizio o la difesa di rivendicazioni legali).

Una copia delle garanzie relative al trasferimento dei dati personali al di fuori del SEE può essere ottenuta contattandoci tramite i dettagli di contatto indicati nella precedente sezione 2.

8. Durata dell'archiviazione; periodi di conservazione

- (1) In linea di principio, conserveremo i dati per il tempo necessario a indagare sull'incidente di conformità oggetto della segnalazione. Al termine di tutte le attività relative alla segnalazione, cancelleremo i dati personali, ad eccezione di quelli che devono essere conservati ed elaborati per esercitare e difendere i nostri diritti.
- (2) Il momento in cui cancelleremo i dati personali che conserviamo ed elaboriamo per esercitare e difendere i nostri diritti dipenderà dallo scadere del periodo massimo di prescrizione per i reati di natura regolamentare e penale o per l'applicazione di rivendicazioni civili.
- (3) Quanto sopra non pregiudica i periodi specifici di conservazione dei dati applicabili in determinate giurisdizioni, secondo quanto previsto dalle normative nazionali elencate nell'Allegato 3, che prevarranno in caso di conflitto.

9. Sicurezza

- (1) I nostri dipendenti e fornitori di servizi sono tenuti a mantenere riservate le nostre informazioni e a rispettare le leggi vigenti in materia di protezione dei dati.
- (2) Tutte le segnalazioni in arrivo vengono ricevute da un numero ristretto di dipendenti autorizzati e appositamente formati da Gruppo OBO e sono sempre trattate in modo riservato. I dipendenti del Gruppo OBO esamineranno i fatti e condurranno eventuali ulteriori indagini richieste dal caso specifico. Tutte le persone che hanno accesso ai dati sono tenute alla riservatezza.

10. Diritto di informazione e accesso

Il soggetto interessato ha il diritto di ottenere dal/i responsabile/i del trattamento informazioni sul fatto che i suoi dati siano o meno oggetto di trattamento e, in tal caso, di accedere ai suoi dati personali che stiamo trattando.

11. Diritto alla rettifica

Il soggetto interessato ha il diritto di correggere o integrare i dati personali se sono errati o incompleti.

12. Diritto alla cancellazione

Il soggetto interessato ha il diritto di richiedere la cancellazione dei dati personali che lo riguardano nelle circostanze specifiche previste dalla legge applicabile sulla protezione dei dati (ad esempio, il GDPR). I periodi di conservazione esistenti e gli interessi degni di protezione che vietano la cancellazione devono essere rispettati.

13. Limitazione del trattamento

Il soggetto interessato ha il diritto di limitare il trattamento dei propri dati se ne viene contestata l'esattezza o se il responsabile del trattamento non ha più bisogno di tali dati, e al contempo lo stesso soggetto interessato ne ha bisogno per le proprie rivendicazioni legali. È anche possibile richiedere che il responsabile del trattamento limiti il trattamento dei dati se altrimenti dovrebbe cancellarli o quando sta esaminando un'obiezione da parte dell'utente.

14. Portabilità dei dati

Il soggetto interessato ha il diritto di ricevere i dati personali che lo riguardano, forniti dall'utente stesso, in un formato strutturato, di uso comune e leggibile da un dispositivo automatico e può avere il diritto di trasmettere tali dati a un altro soggetto.

15. Obiezione al trattamento dei dati

Il soggetto interessato ha inoltre il diritto di opporsi in qualsiasi momento al trattamento dei propri dati da parte del/i responsabile/i del trattamento per motivi legati alla sua situazione particolare, a condizione che il trattamento sia effettuato sulla base giuridica del "legittimo interesse". In tal caso, interromperemo il trattamento dei dati, a meno che non possiamo dimostrare - in conformità con i requisiti di legge - motivi legittimi impellenti per un ulteriore trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato o per l'istituzione, l'esercizio o la difesa di rivendicazioni legali (articolo 21 del GDPR).

16. Diritto di revoca del consenso

Nel caso in cui il trattamento dei dati personali sia basato sul consenso del soggetto interessato, quest'ultimo può revocare il proprio consenso in qualsiasi momento. Tale revoca non pregiudica la liceità del trattamento precedente alla revoca del consenso.

17. Diritto a presentare un reclamo a un'autorità di controllo

Il soggetto interessato ha il diritto di presentare un reclamo a un'autorità di protezione dei dati. È possibile rivolgersi all'autorità di protezione dei dati competente per il luogo o Paese di residenza o per il luogo di sede di lavoro o per il luogo di una presunta violazione del GDPR. L'elenco e i dettagli di contatto delle autorità per la protezione dei dati sono riportati nell'Allegato 3. L'elenco delle autorità nazionali di protezione dei dati dell'UE è disponibile all'indirizzo https://edpb.europa.eu/about-edpb/about-edpb/members_en.

18. Modifiche all'Informativa sulla protezione dei dati

Ci riserviamo il diritto di modificare le nostre pratiche di sicurezza e privacy. In tal caso, aggiorneremo la nostra informativa sulla privacy e, nella misura in cui ciò sia richiesto dalla legge applicabile, informeremo l'utente di conseguenza.