INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
WHISTLEBLOWING (D. Lgs. 24/2023)
ex art. 13 e 14 Reg. UE 2016/679 "GDPR"

La presente informativa è rivolta a tutti i soggetti interessati dal trattamento dei dati personali nell'ambito del sistema di segnalazione di violazioni (Whistleblowing) istituito dall'Agenzia Spaziale Italiana (ASI) ai sensi del D.Lgs. 10 marzo 2023, n. 24.

'L'informativa al Segnalato deve essere fornita solo dopo l'avvio dell'indagine e con le cautele necessarie a non compromettere la riservatezza del Segnalante.

1) TITOLARE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

Il **Titolare del trattamento** è l'**AGENZIA SPAZIALE ITALIANA - ASI** con sede legale in Roma, Via del Politecnico s.n.c., PEC asi@asi.postacert.it. Il **Responsabile della Protezione dei Dati (RPD)** è raggiungibile all'indirizzo mail: rpd@asi.it.

2) CATEGORIE DI INTERESSATI E DATI PERSONALI TRATTATI

Il trattamento riguarda i dati personali contenuti nelle segnalazioni effettuate ai sensi del D.Lgs. 24/2023, relativi alle seguenti categorie di interessati:

- **segnalante (Whistleblower):** la persona fisica che effettua la segnalazione;
- **segnalato:** la persona fisica menzionata nella segnalazione di condotta illecita come persona alla quale la violazione è attribuita;
- **terzi menzionati:** qualsiasi altra persona fisica o giuridica coinvolta o menzionata nella segnalazione.

I dati personali trattati includono:

- dati comuni identificativi e di contatto (se la segnalazione non è anonima);
- dati comuni relativi al contesto lavorativo e ai fatti oggetto di segnalazione;
- eventuali categorie particolari di dati personali (ex art. 9 GDPR) e dati relativi a condanne penali e reati (ex art. 10 GDPR), qualora siano strettamente pertinenti e necessari per la gestione della segnalazione.

3) FINALITA' E BASI GIURIDICHE DEL TRATTAMENTO

I dati personali sono trattati esclusivamente per le seguenti finalità:
a) gestione delle segnalazioni e adempimenti di legge:
ricezione, analisi, accertamento delle violazioni segnalate; comunicazione esito al segnalante; adozione di misure correttive o disciplinari; trasmissione alle autorità competenti (ANAC, Autorità Giudiziaria, altre autorità) ove previsto dalla legge; gestione di istanze di accesso documentale nei limiti dell'art. 12, co. 3, D.Lgs. 24/2023.
Base giuridica: necessità di adempimento di un obbligo giuridico (art. 6, par. 1, lett. c) GDPR) e necessità di esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e) GDPR), in combinato disposto con il D.Lgs. 24/2023. Per i dati particolari: art. 9, par. 2, lett. b) (obblighi in materia di diritto del lavoro) e lett. g) (interesse pubblico rilevante) GDPR, nonché art. 2-sexies del Codice Privacy. Per i dati giudiziari: art. 10 GDPR e art. 2-octies del Codice Privacy;
b) in caso di necessità rivelare l'identità della persona segnalante (o qualsiasi altra informazione da cui possa evincersi tale identità) a soggetti diversi dal RPCT e dal GdL,

qualora sia indispensabile per la difesa del segnalato in un procedimento disciplinare o penale; il Titolare procederà a richiedere al segnalante medesimo un espresso e specifico consenso [ai sensi dell'art. 12, commi 2 e 5 e ss. del D. Lgs. 24/2023 ed art. 6 §.1, lett. a) del GDPR]. Il consenso è facoltativo e può essere revocato in qualsiasi momento;

c) difesa di diritti in sede giudiziaria:

necessità di accertamento, esercizio o difesa di un diritto di ASI o di terzi in sede giudiziaria.

Base giuridica: per i dati comuni art. 6, par. 1, lett. e) GDPR (per ASI in qualità di ente pubblico); per dati particolari (art. 9) e giudiziari (art. 10): art. 9, par. 2, lett. f) GDPR.

4) MODALITÀ DI TRATTAMENTO E MISURE DI SICUREZZA

Il trattamento è svolto in modo da garantire la **massima riservatezza** dell'identità del Segnalante, del Segnalato e dei Terzi menzionati, nonché del contenuto della segnalazione e della relativa documentazione.

- **misure tecniche:** la gestione avviene tramite piattaforma informatica (GlobaLeaks) che garantisce la crittografia *in-transit* e *at-rest*, l'utilizzo di meccanismi di anonimizzazione (es. Rete TOR) e rigorosi controlli di accesso. La piattaforma è configurata per garantire la non tracciabilità della persona segnalante nel momento in cui viene stabilita la connessione al canale interno, anche quando l'accesso avviene dalla rete dati interna di ASI. Sono adottate misure tecniche sugli apparati di rete (es. firewall, proxy) per prevenire il tracciamento degli accessi alla piattaforma;
- **misure organizzative:** l'accesso ai dati è consentito esclusivamente al personale specificamente autorizzato e formato (RPCT e GdL). Il RPCT procede all'**anonimizzazione del contenuto** della segnalazione prima di trasmettere il fascicolo d'indagine a soggetti terzi o interni all'Ente, al fine di mitigare il rischio di re-identificazione del Segnalante.

5) CATEGORIE DI DESTINATARI DEI DATI PERSONALI

I dati personali conferiti vengono trattati e comunicati (cioè trasmessi o messi a disposizione) alle seguenti categorie di destinatari, nella misura minima necessaria al raggiungimento delle finalità:

a) Personale interno di ASI:

- **RPCT e componenti del GdL**, espressamente autorizzati, per la gestione della segnalazione; - Altri uffici interni di ASI (es. Direzione Risorse Umane, Ufficio Legale), solo su documenti anonimizzati e nei limiti necessari alle misure conseguenti.

b) Responsabili del trattamento esterni (art. 28 GDPR):

- **ISWEB S.p.A.** (fornitore piattaforma) gestisce esclusivamente l'infrastruttura tecnologica (*hosting*, manutenzione software, sicurezza informatica); - **Seeweb S.r.l**. (gestore *data center*): gestisce l'infrastruttura fisica del *data center*.

Tali soggetti non hanno accesso ai contenuti delle segnalazioni né ai dati identificativi dei segnalanti.

c) Autorità pubbliche e organismi di controllo:

- **ANAC (Autorità Nazionale Anticorruzione)**, ove la segnalazione sia inoltrata dall'ASI secondo le previsioni del D.Lgs. 24/2023;
- **Autorità Giudiziaria** (Procura della Repubblica, Corte dei conti), ove la segnalazione configuri ipotesi di reato o danno erariale;

- **altre Autorità amministrative competenti** (es. Ispettorato del Lavoro, ASL, Autorità di settore), ove la segnalazione riguardi materie di loro competenza;
- **Garante per la Protezione dei Dati Personali**, in caso di violazione dei dati personali o per richieste di accertamento.

d) Difensori e consulenti tecnici:

- avvocati e consulenti legali dell'ASI, nell'ambito di procedimenti giudiziari o stragiudiziali, cui vengono trasmessi **esclusivamente documenti anonimizzati**, salvo i casi eccezionali di cui all'art. 12, co. 5, D.Lgs. 24/2023.

e) Ulteriori soggetti:

- persona segnalata (in presenza del consenso del segnalante), qualora si apra un procedimento disciplinare nei confronti di quest'ultima e la contestazione sia fondata, in tutto o in parte, sulla segnalazione, nonché la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato;
- altri soggetti pubblici o privati cui la comunicazione sia obbligatoria per legge o necessaria per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Importanti precisazioni:
La segnalazione è sottratta all'accesso documentale (L. 241/1990), all'accesso civico e all'accesso civico generalizzato (D.Lgs. 33/2013), ai sensi dell'art. 12, co. 3, D.Lgs. 24/2023;

6) TRASFERIMENTI DATI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO

Non è previsto il trasferimento di dati personali al di fuori dello Spazio Economico Europeo. L'infrastruttura tecnologica (*data center* Seeweb s.r.l.) è interamente localizzata in Italia.

7) PERIODO DI CONSERVAZIONE DEI DATI

a) Segnalazioni e documentazione:
conservate per il tempo necessario alla gestione della segnalazione e **comunque non oltre cinque anni** dalla comunicazione dell'esito finale della segnalazione (art. 14 D.Lgs. 24/2023);
b) atti di procedimenti conseguenti:
gli atti relativi a procedimenti conseguenti (disciplinari, giudiziari, amministrativi) sono conservati separatamente, nei termini di legge previsti per ciascun procedimento. Tali atti non contengono riferimenti identificativi del Segnalante, salvo i casi di rivelazione obbligatoria previsti dalla legge (art. 12, co. 5, D.Lgs. 24/2023);
c) dati manifestamente non utili:
i dati personali che, in fase di screening preliminare, risultino **manifestamente non utili** alla gestione della specifica segnalazione (es. dati irrilevanti, sovrabbondanti, non pertinenti) sono **cancellati immediatamente** (art. 13, co. 1, lett. a), D.Lgs. 24/2023). Questa valutazione è effettuata dal RPCT caso per caso, nel rispetto del principio di minimizzazione;
d) segnalazioni non rilevanti:
qualora la segnalazione non rientri nell'ambito applicativo del D.Lgs. 24/2023 (es. natura sindacale, rivendicativa, personale), il **RPCT garantisce comunque la riservatezza del segnalante**, in ragione della ragionevole aspettativa di riservatezza e tutela della persona che abbia erroneamente assunto di poter beneficiare delle garanzie della normativa *whistleblowing*.

Il segnalante è informato dell'esito negativo e i dati acquisiti sono cancellati, salvo eventuale inoltro a canali più appropriati.

Al termine dei periodi di conservazione, i dati sono distrutti o resi anonimi per finalità statistiche aggregate.

8) DIRITTI DEGLI INTERESSATI E LORO LIMITAZIONE

Il GDPR riconosce agli interessati (segnalante, segnalato/i, terzi) i diritti di cui agli articoli da 15 a 22 (diritto di accesso, rettifica, cancellazione, limitazione di trattamento, opposizione).

In conformità con l'art. 13, comma 1, lett. d) del D.Lgs. 24/2023, e l'art. 2-*undecies* del D.Lgs. 196/2003 (Codice Privacy), **l'esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR può essere limitato, ritardato o escluso** per la durata e nei limiti in cui ciò costituisca una misura necessaria e proporzionata per:

a) garantire la **riservatezza dell'identità del segnalante** (*whistleblower*);
b) tutelare l'**integrità del processo di gestione della segnalazione** e l'accertamento delle violazioni;
c) prevenire un **pregiudizio effettivo e concreto** alla tutela giurisdizionale dei diritti del segnalante.

In particolare, il diritto di accesso del segnalato (art. 15 GDPR) e gli altri diritti non possono essere esercitati se, con riferimento al caso concreto, la loro attuazione possa compromettere la riservatezza dell'identità del segnalante.
Diritto di revoca del consenso: è possibile revocare il consenso prestato in qualsiasi momento, ma la revoca non pregiudica la liceità del trattamento dei dati effettuato nel periodo precedente alla revoca.
Per esercitare i Suoi diritti può contattare il Responsabile della Protezione dei Dati all'indirizzo e-mail rpd@asi.it
Le **limitazioni** sono valutate caso per caso dal Titolare del trattamento, in applicazione del principio di proporzionalità, e sono applicate solo nella misura e per il periodo strettamente necessari a tutelare la riservatezza del Segnalante e l'integrità del processo di gestione della segnalazione.
Qualora ritenga che il trattamento dei Suoi dati personali avvenga in violazione di quanto previsto dal Regolamento, può **proporre reclamo al Garante per la Protezione dei Dati Personali**, come previsto dall'art. 77 GDPR, oppure adire le opportune sedi giudiziarie ai sensi dell'art. 79 GDPR.

9) NATURA DEL CONFERIMENTO E CONSEGUENZE DEL RIFIUTO

Il conferimento dei dati personali da parte del Segnalante è volontario. Il mancato conferimento dei dati identificativi comporta l'impossibilità di beneficiare delle tutele previste dal D.Lgs. 24/2023 in caso di ritorsioni, sebbene la segnalazione possa comunque essere gestita in forma anonima

Il trattamento dei dati del Segnalato e dei Terzi menzionati è obbligatorio per il Titolare del Trattamento, in quanto necessario per adempiere a un obbligo legale. Non è possibile opporsi al trattamento per motivi connessi alla situazione particolare, salvo che l'opposizione sia motivata da un'inesattezza o illiceità del trattamento stesso.