INFORMATIVA AI SENSI DELL'ART. 13 E 14 DEL REGOLAMENTO (UE) 2016/679 ("GDPR")
RELATIVA AL TRATTAMENTO DEI DATI PERSONALI DEI SEGNALANTI, SEGNALATI ED
EVENTUALI ALTRI SOGGETTI TERZI COINVOLTI ("INTERESSATI"), EFFETTUATI DA HFS E
LE SUE CONTROLLATE E/O PARTECIPATE, IN RELAZIONE ALLA GESTIONE DELLE SEGNALAZIONI
DISCIPLINATE DALLA "WHISTLEBLOWING POLICY".

Holding Ferrara Servizi (semplicemente "HFS", nel prosieguo) e le sue società controllate e/o partecipate (FERRARA TUA, AFM, ACOSEA, AMSEF, SIPRO) forniscono, qui di seguito, l'informativa sui trattamenti dei dati
personali dei segnalanti, segnalati ed eventuali altri soggetti terzi coinvolti (tutti "Interessati al trattamento", ai termini della normativa privacy applicabile), effettuati dalla stessa in relazione alla gestione delle segnalazioni disciplinate dalla "Whistleblowing Policy" approvata dal Consiglio di Amministrazione di HFS in data 29 gennaio 2019.

1. Dati personali trattati

Dati del segnalante, Dati del segnalato e Dati personali di terze persone che dovessero essere riportati nella segnalazione effettuata.

2. Categorie particolari di Dati personali trattati

Eventuali Dati cosiddetti "sensibili" (art. 9.1 GDPR, definizione degli ex "dati sensibili").

3. Fonte dei Dati e categorie di dati raccolti c/o terzi.

Il Titolare raccoglie i dati attraverso le segnalazioni. I dati degli Interessati possono essere forniti dal medesimo interessato, segnalante, oppure da terzi come, ad esempio, quelli della persona fisica oggetto di segnalazione (segnalato). Segnalanti possono essere dipendenti e/o collaboratori, amministratori, consulenti ed in generale tutti gli stakeholder del Titolare oppure di società del Gruppo. Le segnalazioni possono essere nominali oppure anonime. Per preservare le finalità investigative, l'interessato, oggetto di segnalazione, può non essere immediatamente messo a conoscenza del trattamento dei propri dati da parte del Titolare, fintanto che sussista il rischio di compromettere la possibilità di verificare efficacemente la fondatezza della denuncia o di raccogliere le prove necessarie. Tale rinvio verrà valutato caso per caso dai soggetti incaricati di svolgere le attività di indagine, in accordo con il Titolare, tenendo in debito conto l'interesse alla protezione delle prove, evitandone la distruzione o l'alterazione da parte del denunciato, e i più ampi interessi in gioco.

4. Finalità del trattamento e base giuridica

I dati personali degli interessati sono trattati per le finalità connesse all'applicazione della sopra citata "Whistleblowing Policy". L'adozione di tale Policy, nonché il trattamento dei dati avviene sulla scorta di un obbligo di legge a cui è assoggettato il Titolare. La Policy prevede la riservatezza dell'identità del segnalante, gestendo i dati personali separatamente dal contenuto della segnalazione effettuata. L'eventuale abbinamento può essere eseguito solo nei casi eccezionali indicati nella policy (es. per esercitare il diritto di difesa dell'incolpato, previo consenso del segnalante; nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione; nei casi di segnalazioni che si rivelino infondate, effettuate con dolo o colpa grave). L'interesse del Titolare ad utilizzare un sistema di ricognizione delle informazioni (anche se ottenute in forma anonima), tale da preservare la riservatezza dell'identità del segnalante, in relazione a possibili frodi, pericoli o altri seri rischi che possano minacciare la reputazione della società, prevale su quello dell'interessato ad esprimere il proprio consenso al trattamento dei dati personali, salvo che di quelli che afferiscono a categorie particolari.

5. Modalità, logica del trattamento e tempi di conservazione

I trattamenti dei dati sono effettuati manualmente (ad esempio, su supporto cartaceo) e/o attraverso strumenti automatizzati (oltre che tramite la piattaforma Whistleblowing, ad esempio, utilizzando procedure e supporti elettronici), con logiche correlate alle finalità sopraindicate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati. In particolare, i dati trattati sono conservati per un tempo almeno sufficiente per l'espletamento delle finalità indicate e, comunque, sono cancellati al massimo entro sei mesi dalla chiusura di tutte le eventuali attività conseguenti all'accertamento dei fatti esposti nella segnalazione.

6.DPO.
HFS ha nominato un Data Protection Officer, "DPO" ai sensi degli articoli 37-39 del GDPR. Il DPO di HFS può essere contattato, mediante e-mail all'indirizzo: dpo@holdingferrara.it, da qualsiasi Interessato per ogni questione relativa ai propri dati personali od all'esercizio dei diritti che gli derivano dal GDPR (segnatamente, articoli da 15 a 22).

7. Natura del conferimento e conseguenze dell'eventuale rifiuto
Il conferimento dei dati del segnalante è obbligatorio nella "segnalazione nominativa". Un eventuale rifiuto al conferimento dei dati nella "segnalazione nominativa" rende impossibile seguire l'iter della procedura descritta nella "Whistleblowing Policy". Il conferimento dei dati del segnalante è facoltativo nella "segnalazione anonima", tuttavia l'applicazione della procedura di segnalazione sarà possibile solo qualora le segnalazioni siano adeguatamente circostanziate e rese con dovizia di particolari, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

8. Categorie di soggetti terzi ai quali i dati potrebbero essere comunicati
I soggetti terzi a cui i dati potrebbero essere comunicati sono ricompresi nelle seguenti categorie: a) Consulenti (Studi Legali, ecc.) b) Società incaricate per la gestione degli archivi aziendali, ivi inclusi i dati personali dei dipendenti cessati dal servizio c) Istituzioni e/o Autorità Pubbliche, Autorità Giudiziaria, Organi di Polizia, Agenzie investigative d) OdV. In casi eccezionali, quando la segnalazione abbia dato origine ad un procedimento disciplinare e si basi unicamente sulla denuncia del segnalante, l'identità di quest'ultimo può essere comunicata a colui che è sottoposto al procedimento disciplinare, se ciò sia assolutamente indispensabile per esercitare il suo diritto di difesa. In tali casi la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

9. Diritto di accesso ai dati personali ed altri diritti dell'Interessato
Gli Interessati possono chiedere al Titolare, mediante richiesta e-mail all'indirizzo DPO@holdingferrara.it, l'accesso ai dati che li riguardano, la loro rettifica, l'integrazione o la loro cancellazione, nonché la limitazione del trattamento o qualsiasi altro diritto di cui agli articoli da 15 a 22 del GDPR, ricorrendone i presupposti da evidenziare nella richiesta; ciò, comunque, salvo l'esistenza di motivi legittimi prevalenti sugli interessi, diritti e libertà dell'interessato, l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o altri obblighi di legge che il Titolare deve assolvere o diversa disposizione eventuale delle Autorità Pubbliche o dell'Autorità Giudiziaria o degli Organi di Polizia. Gli interessati hanno altresì diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali in caso di trattamento illegittimo od illecito dei propri dati da parte del Titolare.

La legge 30 novembre 2017, n. 179, recante "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" ha riformato la materia del *whistleblowing* nel settore pubblico e in quello privato.
Tutti i dipendenti, gli amministratori**,** i collaboratori, e comunque i soggetti che svolgono attività e servizi in favore di Holding devono effettuare segnalazioni all'Organismo di Vigilanza (OdV) di condotte illecite rilevanti ai sensi del D. Lgs. 231/2001 o di violazioni del Modello organizzativo adottato.
I dipendenti possono inoltre effettuare segnalazioni al Responsabile per la prevenzione della corruzione e trasparenza (RPCT) e/o all'ANAC o denunce all'Autorità Giudiziaria o Amministrativa contabile riguardo a condotte genericamente illecite di cui siano venuti a conoscenza in ragione del proprio rapporto di lavoro.

Le segnalazioni dovranno essere circostanziate e fondate su elementi di fatto precisi e concordanti.

La segnalazione è **circostanziata** quando la narrazione da parte dell'autore, di fatti, eventi o circostanze che costituiscono gli elementi fondanti dell'asserito illecito (ad esempio tipologia di illecito commesso, periodo di riferimento, valore, cause e finalità dell'illecito, aree e persone interessate o coinvolte, anomalia sul sistema interno di controllo etc…) è effettuata con un grado di dettaglio sufficiente a consentire, almeno astrattamente, di identificare elementi utili o decisivi ai fini della verifica della fondatezza della segnalazione stessa. Le segnalazioni circostanziate si distinguono a loro volta in:
– **segnalazioni circostanziate verificabili:** qualora, considerati i contenuti della segnalazione, sia possibile in concreto, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla veridicità della segnalazione.
– **segnalazioni circostanziate non verificabili:** qualora, considerati i contenuti della segnalazione, non sia possibile, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla veridicità della segnalazione e pertanto procedere alla successiva fase di accertamento.

Segnalazioni in materia di corruzione (rif. segnalazioni al RCPT e ANAC):
comprendono non solo l'intera gamma dei delitti contro la pubblica amministrazione (ad es. ipotesi di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri d'ufficio e corruzione in atti giudiziari), ma anche le situazioni in cui, nel corso dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati, nonché i fatti in cui – a prescindere dalla rilevanza penale

– venga in evidenza un mal funzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite, ivi compreso l'inquinamento dell'azione amministrativa *ab externo*.

Segnalazioni violazione Codice Etico e Modello 231:
si considerano tali tutte le segnalazioni afferenti alla violazione dei principi del Codice Etico nonché eventi idonei, anche astrattamente, a cagionare una responsabilità amministrativa della Società ai sensi del D.lgs. 231/2001.

Segnalazione anonima:
è consentita la segnalazione in cui le generalità del segnalante non siano esplicitate, né siano individuabili in maniera univoca, ma in tal caso essa deve essere resa con dovizia di particolari e in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

Segnalazione in malafede:
segnalazione che dagli esiti della fase istruttoria si rilevi priva di fondamento sulla base di elementi oggettivi comprovanti la malafede del segnalante, fatta allo scopo di arrecare un danno ingiusto alla persona segnalata.

L'accesso al Portale Whistleblowing della Holding è soggetto alla politica "no log" al fine di impedire l'identificazione del segnalante che intenda rimanere anonimo, che significa che i sistemi informatici aziendali non sono in grado di identificare il punto di accesso al portale (indirizzo IP) anche nel caso in cui l'accesso venisse effettuato da un computer connesso alla rete aziendale.

Dopo l'accesso al Portale il segnalante sarà guidato nella compilazione di un questionario formato da domande aperte e/o chiuse che gli permetteranno di fornire gli elementi caratterizzanti la segnalazione (fatti, contesto temporale, dimensione economica, ecc.).

Il Portale chiederà al segnalante se intende o meno fornire la propria identità. In ogni caso, il segnalante potrà fornire la propria identità in un secondo momento sempre attraverso il Portale.

Nel momento dell'invio della segnalazione il Portale rilascerà al segnalante un codice identificativo univoco (ticket); questo numero, conosciuto unicamente dal segnalante, non potrà essere recuperato in alcun modo in caso di smarrimento. Il ticket servirà al segnalante per accedere, sempre attraverso il Portale, alla propria segnalazione al fine di monitorare lo stato di avanzamento, inserire ulteriori elementi per circostanziare la segnalazione, fornire le proprie generalità.

La segnalazione tramite portale è ricevuta contemporaneamente dal RPCT aziendale e dall'Organismo di Vigilanza aziendale e di gruppo.