

## ACCORDO DI CONTITOLARITÀ PER IL SISTEMA DI WHISTLEBLOWING

Pitagora S.p.A., P.IVA e C.F. 05488960013, con sede legale in Via Bisceglie 76, 20152 Milano (MI), nella persona del suo legale rappresentante *pro tempore* domiciliato presso la sede della società (di seguito anche solo la “Pitagora”)

e

Impresoft S.p.A., P.IVA e C.F. 03186830240, con sede legale in Via Bisceglie 76, 20152 Milano (MI), nella persona del suo legale rappresentante *pro tempore* domiciliato presso la sede della società (di seguito anche solo la “Impresoft”)

e

GN Techonomy S.r.l., P.IVA e C.F. 02391090160, con sede legale in Via G. Carducci 32 – 20123 Milano (MI), nella persona del suo legale rappresentante *pro tempore* domiciliato presso la sede della società (di seguito anche solo la “GN”)

e

4ward S.r.l., P.IVA e C.F. 03408060964, con sede legale in Via del Vigneto 31 – 39100 Bolzano (BZ), nella persona del suo legale rappresentante *pro tempore* domiciliato presso la sede della società (di seguito anche solo la “4ward”)

e

Qualitas S.p.A., P.IVA e C.F. 01833260241, con sede legale in Via Vecchia Ferriera 5 – 36100 Vicenza (VI), nella persona del suo legale rappresentante *pro tempore* domiciliato presso la sede della società (di seguito anche solo la “Qualitas”)

e

Opensymbol S.r.l., P.IVA e C.F. 03184500241, con sede legale in Via Vecchia Ferriera 5 – 36100 Vicenza (VI), nella persona del suo legale rappresentante *pro tempore* domiciliato presso la sede della società (di seguito anche solo la “GN”)

di seguito, congiuntamente, anche solo le “Parti” o i “Contitolari”.

### PREMESSO CHE

- Pitagora svolge attività di società di partecipazione – holding (Codice NACE 64.2);
- Impresoft svolge attività di società di partecipazione – holding (Codice NACE 64.2);
- GN Techonomy svolge attività di Progettazione, produzione di pacchetti software; progettazione di sistemi informativi; forniture di servizi ed assistenza in ambito informatico (Codice NACE: 62.01);
- 4ward svolge attività di Produzione di software non connesso all’edizione (Codice NACE: 62.01);
- Qualitas svolge attività di Sviluppo e realizzazione di software (Codice NACE: 62.01);
- Opensymbol svolge attività di Sviluppo di software applicativi e gestionali (Codice NACE: 62.01);
- in data 13 luglio 2023 Cerved Group S.p.A. concede in licenza la Piattaforma Whistleblowing a Impresoft S.p.A. per il ricevimento e la gestione delle Segnalazioni Whistleblowing da parte di tutte le Contitolari che fanno parte del Gruppo Impresoft nel rispetto delle disposizioni di cui al D. Lgs. 10 marzo 2023, n. 24 recante “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”;

  
CP

  
EM

  
SG

  
NB

  
AG

- Impresoft S.p.A., per conto anche delle Contitolari che fanno parte del Gruppo Impresoft, nomina Responsabili del Trattamento, ai sensi dell'art. 28 del GDPR i seguenti soggetti:
  - Cerved AML S.r.l. per l'attività di assistenza, manutenzione e supporto all'utilizzo della piattaforma fornita da Cerved Group S.p.A.;
  - MN Tax & Legal per la gestione delle Segnalazioni Whistleblowing tramite Piattaforma, posta cartacea e incontro diretto con i Gestori delle Segnalazioni;
- nell'ambito del rapporto instaurato tra le Parti, relativamente ai Trattamenti elencati nel presente Accordo, i Dati personali degli Interessati saranno trattati congiuntamente dalle Parti, le quali agiranno, pertanto, in qualità di Contitolari del Trattamento, determinando, congiuntamente, modalità e finalità dell'attività di Trattamento, ai sensi dell'articolo 26 del GDPR;
- le obbligazioni che sorgono in attuazione del presente Accordo di contitolarità non prevedono alcun corrispettivo;
- il contenuto essenziale del presente Accordo sarà reso accessibile agli Interessati.

## TUTTO CIÒ PREMESSO LE PARTI CONVENGONO E STIPULANO QUANTO SEGUE

### 1. PREMESSE

1.1 Le premesse e gli allegati al presente Accordo di contitolarità costituiscono parte integrante e sostanziale dello stesso.

### 2. DEFINIZIONI

2.1 Con il termine:

- «**Accordo**»: si intende il presente Accordo di contitolarità;
- «**Canale di Segnalazione**»: si intendono i canali implementati dal Titolare per la comunicazione e gestione delle Segnalazioni. In particolare, si intendono: la Piattaforma Whistleblowing, la posta cartacea e l'incontro diretto con i Gestori delle Segnalazioni.
- «**Dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessati»); 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.
- «**DPIA**»: valutazione d'impatto c.d. *Data Privacy Impact Assessment*.
- «**GDPR**»: Regolamento UE del Parlamento Europeo e del Consiglio n. 679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione di tali Dati e che abroga la direttiva 95/46/CE.
- «**Gestore delle Segnalazioni**»: soggetto/i deputato/i alla ricezione delle Segnalazioni, nominato in conformità all'art. 4 co.2 del D.Lgs. 24/2023.
- «**Interessati**»: persona fisica cui si riferiscono i Dati personali. In particolare, ai fini della presente DPIA per Interessati si intendono i Segnalanti e/o le Personale coinvolte.
- «**Persona coinvolta**»: la persona fisica o giuridica menzionata nella Segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata.

  
CP

  
EM

  
SG

  
NB

  
AG

- «**Piattaforma Whistleblowing**» o «**Piattaforma**»: Piattaforma Cerved accessibile via Internet tramite un'applicazione web o un'applicazione remota utilizzabile per effettuare Segnalazioni e per la gestione delle stesse.
- «**Procedura Whistleblowing**»: procedura adottata dalla Società recante i principi di comportamento e le modalità operative da seguire per le Segnalazioni coerentemente alle previsioni di cui al D.Lgs. 24/2023.
- «**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 in conformità all'art. 28 del GDPR.
- «**Segnalante**»: soggetti che effettuano Segnalazioni tramite i Canali di Segnalazione. In particolare, possono effettuare Segnalazioni i seguenti soggetti:
  - o i lavoratori subordinati della Società, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81<sup>1</sup>, o dall'articolo 54-bis del decreto-legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n. 96<sup>2</sup>;
  - o i lavoratori autonomi, ivi compresi quelli indicati al capo I della legge 22 maggio 2017, n. 81<sup>3</sup>, nonché i titolari di un rapporto di collaborazione di cui all'articolo 409 del codice di procedura civile e all'articolo 2 del decreto legislativo n. 81 del 2015, che svolgono la propria attività lavorativa presso la Società;
  - o i lavoratori o i collaboratori, che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato che forniscono beni o servizi che realizzano opere in favore di terzi;
  - o i liberi professionisti e i consulenti che prestano la propria attività presso la Società;
  - o i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Società;
  - o gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso la Società.
- «**Segnalazione**» o «**Segnalazione Whistleblowing**»: comunicazione di informazioni sulle violazioni, presentata tramite la Piattaforma Whistleblowing e/o altri Canali di Segnalazione.
- «**Titolare/i del Trattamento**» e «**Contitolare/i**»: 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. Ai fini della presente DPIA sono Contitolari le Parti.
- «**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.

<sup>1</sup> i.e. "Rapporti di collaborazione che si concretano in prestazioni di lavoro esclusivamente personali, continuative e le cui modalità di esecuzione sono organizzate dal committente anche con riferimento ai tempi e al luogo di lavoro; lavoro a tempo parziale; lavoro intermittente; lavoro a tempo determinato; somministrazione; apprendistato; lavoro accessorio".

<sup>2</sup> i.e. "Per ciascun prestatore, con riferimento alla totalità degli utilizzatori, a compensi di importo complessivamente non superiore a 5.000 euro; per ciascun utilizzatore, con riferimento alla totalità dei prestatori, a compensi di importo complessivamente non superiore a 10.000 euro; per le prestazioni complessivamente rese da ogni prestatore in favore del medesimo utilizzatore, a compensi di importo non superiore a 2.500 euro; per ciascun prestatore, per le attività di cui al decreto del Ministro dell'interno 8 agosto 2007, pubblicato nella Gazzetta Ufficiale n. 195 del 23 agosto 2007, svolte nei confronti di ciascun utilizzatore di cui alla legge 23 marzo 1981, n. 91, a compensi di importo complessivo non superiore a 5.000 euro."

<sup>3</sup> i.e. Contratto d'opera (ex artt. 2222 c.c. e ss.) e Contratto di prestazione d'opera intellettuale (ex artt. 2229 c.c. e ss), esclusi i piccoli imprenditori (ex art. 2083 c.c.).

- «**Violazione dei Dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali trasmessi, conservati o comunque trattati;
- «**Autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. In Italia l'Autorità di controllo è l'Autorità Garante per la protezione dei Dati personali.

### 3. FINALITÀ DELL'ACCORDO

3.1 Congiuntamente, le Parti, con il presente Accordo intendono condividere le risorse per la ricezione e la gestione delle Segnalazioni Whistleblowing. In particolare, le Parti condividono le seguenti risorse:

- a) Gestori delle Segnalazioni;
- b) Piattaforma Whistleblowing;
- c) canale di segnalazione per la ricezione della posta cartacea.

3.2 Le Parti attraverso il presente Accordo intendono, in conformità a quanto stabilito dall'art. 26 del GDPR, determinare congiuntamente le finalità e mezzi del Trattamento, e, in modo trasparente, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dallo stesso, con particolare riguardo ai rispettivi ruoli e rapporti nei confronti degli Interessati.

### 4. DESCRIZIONE DEL TRATTAMENTO

4.1 Il Trattamento posto in essere in qualità di Contitolari consiste nella ricezione e gestione delle Segnalazioni Whistleblowing.

4.2 Per l'elenco in merito a persone che hanno accesso ai dati, finalità del Trattamento, categoria di Interessati, tipologia di Dati trattati, base giuridica, archivio, eventuali trasferimenti al di fuori dello Spazio Economico Europeo (c.d. SEE) e destinatari/responsabili del Trattamento si rimanda all'allegato 1 "Descrizione del Trattamento" (**Allegato 1**) del presente Accordo.

### 5. MODALITÀ DEL TRATTAMENTO

5.1 Il Trattamento effettuato da parte dei Contitolari avverrà tramite i seguenti canali:

- posta cartacea riservata al Gestore delle Segnalazioni presso MN Tax & Legal in Corso di Porta Nuova, 46 – 20121 Milano;
- piattaforma informatica all'indirizzo: <https://whistleblowing-impresoftgroup.hawk-aml.com/Whistleblowing/home>;
- incontro diretto con il Gestore delle Segnalazioni presso MN Tax & Legal in Corso di Porta Nuova, 46 – 20121 Milano da organizzare via e-mail al seguente indirizzo [whistleblowing@impresoft.com](mailto:whistleblowing@impresoft.com).

5.2 Ciascun Contitolare si impegna a trattare i Dati nel rispetto dei principi di liceità, correttezza, trasparenza, esattezza, integrità e non eccedenza, pertinenza e necessità rispetto alle finalità perseguite, garantendo la tutela della riservatezza e dei diritti dell'Interessati.

### 6. DIRITTI DEGLI INTERESSATI

6.1 Le Parti gestiscono le richieste degli Interessati di cui trattano i dati. Le Parti concordano nel fornire agli interessati il medesimo indirizzo per presentare le proprie richieste di esercizio dei diritti previsti dal GDPR e che poi queste richieste verranno gestite dalla singola Società

  
CP

  
EM

  
SG

  
NB

  
AG

competente. L'indirizzo e-mail verso il quale gli interessati possono esercitare i propri diritti è il seguente [gdpr@impresoft.com](mailto:gdpr@impresoft.com).

6.2 Le Parti si impegnano a dare riscontro alle richieste degli interessati entro i termini e secondo le modalità previste dal GDPR. Pertanto, gli Interessati potranno esercitare i diritti attribuitigli dal GDPR con richiesta rivolta senza formalità all'indirizzo sopra riportato.

6.3 Resta inteso che, indipendentemente dal presente Accordo, l'Interessato potrà contattare qualsiasi Contitolare.

## 7. OBBLIGHI DI CIASCUN CONTITOLARE

7.1 Le Parti si impegnano a rispettare i punti che seguono.

7.1.1 Informazioni da fornire al Segnalante e alla Persona coinvolta ai sensi dell'art. 13 e 14 del GDPR: le informative privacy saranno rese disponibili sul sito web delle Parti nell'area dedicata alla tematica whistleblowing e nella Piattaforma Whistleblowing all'indirizzo <https://whistleblowing-impresoftgroup.hawk-aml.com/Whistleblowing/home>.

7.1.2 Raccolta e gestione dei consensi: le Parti raccolgono i seguenti consensi del Segnalante:

- a) alla rivelazione della propria identità e di qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità a persone diverse dal Gestore delle Segnalazioni e da altre persone specificatamente autorizzate dal Titolare;
- b) alla rivelazione della propria identità e di qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità nell'ambito del procedimento disciplinare ove la contestazione sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato;
- c) alla documentazione della Segnalazione quando questa viene effettuata oralmente nel corso di un incontro con il Gestore delle Segnalazioni.

Quando la Segnalazione è effettuata oralmente nel corso di un incontro con il Gestore delle Segnalazioni, la documentazione della Segnalazione avverrà a cura dello stesso mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, il Segnalante dovrà verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

7.1.3 Conservazione dei Dati personali: le Parti si impegneranno a conservare i Dati raccolti in nella Piattaforma e, in caso di Segnalazioni ricevute mediante posta cartacea o in occasione di un incontro diretto, nella Piattaforma e/o in un archivio cartaceo utilizzando modalità idonee a prevenirne la perdita, la distruzione e l'accesso non autorizzato e per il tempo necessario al trattamento delle Segnalazioni e comunque per non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di Segnalazione nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del D. Lgs. 24/2023 e del principio di limitazione della conservazione di cui alla normativa privacy.

7.1.4 Nomina Responsabili del Trattamento (ex art. 28 GDPR): Impresoft S.p.A., per conto anche delle Contitolari che fanno parte del Gruppo Impresoft, nomina Responsabili del Trattamento, ai sensi dell'art. 28 del GDPR i seguenti soggetti:

- Cerved AML S.r.l. per l'attività di assistenza, manutenzione e supporto all'utilizzo della piattaforma fornita da Cerved Group S.p.A.;
- MN Tax & Legal per la gestione delle Segnalazioni Whistleblowing tramite Piattaforma, posta cartacea e incontro diretto;

Qualora nel corso del presente Accordo dovesse essere necessario avvalersi di altri fornitori/consulenti da nominare, ai sensi dell'art. 28 del GDPR, Responsabili del Trattamento, le Parti condivideranno l'aggiunta o la sostituzione di altri Responsabili e valuteranno

  
CP

  
EM

  
SG

  
NB

  
AG

congiuntamente se procedere con l'aggiunta o la sostituzione di altri Responsabili. Le eventuali nuove nomine dovranno essere inserite nell'Allegato 1 da ciascuna Parte e tale documento verrà condiviso con l'altra Parte.

7.1.5 Adozione di misure di sicurezza idonee ex art. 32 GDPR: le Parti si impegnano – anche per il tramite dei Responsabili del trattamento nominati ai sensi dell'art. 28 del GDPR - attraverso l'adozione di tutti gli strumenti necessari, a garantire un livello di sicurezza adeguato ad eventuali rischi che potrebbero derivare da specifici Trattamenti effettuati nell'ambito del presente Accordo (a titolo esemplificativo e non esaustivo, distruzione o perdita, anche accidentale dei Dati, accesso non autorizzato, non consentito o difforme dalle finalità della raccolta dei Dati medesimi). In particolare, le misure di sicurezza adottate dal Responsabile del trattamento Cerved AML S.r.l. con riferimento alla Piattaforma sono i seguenti:

▪ **Crittografia**

- I mezzi implementati per assicurare la confidenzialità dei dati archiviati sono Database MSSQL cifrato con TDE (Transparent Data Encryption) nativa del prodotto.
- I backup sono compressi e protetti con password.
- L'accesso all'applicazione avviene in https con certificato, protocollo TLS 1.2 e chiave di cifratura a 2048 bit; Lo scambio flussi da/verso Cliente avviene con protocollo SFTP ed autenticazione con username/password e/o chiave pubblica/privata.
- I dati acquisiti sono suddivisi in più DB e stoccati in cloud per proteggere i contenuti nelle segnalazioni dagli utenti.
- Riguardo alla chiave asimmetrica la metodologia utilizzata recupera una chiave da codice java su uno specifico percorso, mentre l'altra chiave è generata per ogni segnalazione.

▪ **Anonimizzazione**

- Viene utilizzata una keycode, restituita a video, per ogni segnalazione inserita, unica chiave per richiamare successivamente la segnalazione inserita.
- È inoltre prevista la figura del "gestore delle identità", addetto all'esclusiva gestione delle richieste di accesso ai dati anagrafici legati alla segnalazione al fine di tutelare il segnalante durante l'indagine.

▪ **Partizionamento**

- I dati acquisiti vengono salvati su più database (database 1 per dati utenti e profili utente; database2 per segnalazioni; database3 gestione pratiche/segnalazioni)

▪ **Controllo degli accessi logici**

- I mezzi di autenticazione implementati prevedono una password con lunghezza minima pari a 12 caratteri alfanumerici (1 Maiuscola, 1 minuscola, 1 numerico e 1 special)
- La validità della password ha una durata pari a 3 mesi standard, impostabile dal cliente e prevede tre tentativi prima del blocco dell'account.

▪ **Tracciabilità**

- La procedura traccia gli accessi, le attività, l'esecuzione dei processi e tutte le operazioni effettuate dagli utenti, con la relativa data e ora ed indirizzo IP.
- Lo storico del log viene mantenuto per una durata pari alla durata del contratto.
- È prevista operatività SOC H24.

▪ **Archiviazione**

- I dati anagrafici sono custoditi all'interno del database applicativo, per il quale è prevista la cifratura mediante Transparent Data Encryption (TDE).
- Il database risiede in area protetta, non raggiungibile da internet, presso infrastruttura Infodata in Private Cloud.

▪ **Vulnerabilità**

- Le risorse utilizzate sono regolamentate e gestite attraverso procedure e soluzioni interne (es. versionamento, archiviazione, procedure di deploy automatici, VAPT e relativi rientri ecc.). È inoltre prevista una policy di BCDR per ridurre i rischi ai livelli minimi.

▪ **Lotta contro il malware**

- È prevista la soluzione DarkTrace per le funzionalità di controllo e contrasto delle minacce legate alla componente network e di scambio flussi.
- È prevista la soluzione CyberReason per le funzionalità di controllo delle minacce.
- Entrambe le soluzioni contemplano l'operatività di SOC H24.

▪ **Sicurezza dei siti web**

- L'accesso all'applicazione avviene in https con certificato, protocollo SSL/TLS 1.2 e chiave di cifratura a 2048 bit; E' prevista l'esecuzione periodica di VAPT con successiva applicazione delle contromisure atte a ripristinare i corretti livelli di sicurezza. Sono inoltre previste verifiche periodiche da parte della funzione Internal Audit e di soggetti terzi certificatori ISO27001.

▪ **Backup**

- I database applicativi prevedono esecuzione di backup giornalieri con retention di una settimana. I backup vengono archiviati in forma compressa e cifrata e custoditi su sito secondario, collocato geograficamente a distanza maggiore di 300km.

▪ **Contratto con il responsabile del trattamento**

- È prevista la cifratura mediante Transparent Data Encryption.
- La trasmissione delle informazioni avviene mediante protocolli HTTPS e SFTP.
- È prevista la tracciatura applicativa con retention pari alla durata del contratto.
- Le utenze vengono configurate e profilate in base al concetto di minima accessibilità ai dati ("least privilege" e "need to know"), compatibilmente con il ruolo assegnato.
- L'autenticazione avviene mediante password gestite in base alle policy GDPR
- Il Contratto stipulato con Infodata recepisce quanto riportato.

▪ **Prevenzione delle fonti di rischio**

- I dati sono in Cloud ed ubicati solo su territorio Nazionale.

▪ **Protezione contro fonti di rischio non umane**

- I dati personali risiedono presso Webfarm Infodata. La totalità delle misure riportate è recepita ed implementata dal fornitore.

7.1.6 **Nomina Autorizzati al Trattamento (ex art. 29 GDPR)**: ciascuna Parte si impegna a istruire e vincolare alla riservatezza i propri dipendenti e/o collaboratori coinvolti nelle operazioni di Trattamento oggetto del presente Accordo quali le persone autorizzate a dare seguito alle



Segnalazioni. MN Tax & Legal, quale Responsabile del trattamento ai sensi dell'art. 28 del GDPR, nomina, per conto delle Società del Gruppo, i Gestori delle Segnalazioni ai sensi dell'art. 29 del GDPR.

- 7.1.7 Nomina Amministratore di Sistema: le Parti si impegnano, ove necessario, a nominare un Amministratore di Sistema, rispettando quanto dettato dal Provvedimento del 27 novembre 2008 del Garante per la protezione dei Dati personali recante "*Misure e accorgimenti prescritti ai titolari dei Trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".
- 7.1.8 Valutazione d'impatto (c.d. DPIA): le Parti si impegnano a redigere una valutazione d'impatto sui Trattamenti connessi alla gestione delle Segnalazioni Whistleblowing.
- 7.1.9 Registro dei Trattamenti: le Parti si impegnano a tenere un registro delle attività di Trattamento secondo quanto previsto dall'art. 30 del GDPR.
- 7.1.10 Trasferimenti al di fuori dello SEE e garanzie previste: le Parti si impegnano a rispettare quanto previsto dal Capo V del GDPR in caso di eventuali trasferimenti di dati al di fuori dello SEE. Sul punto si rinvia all'Allegato 1 del presente Accordo;
- 7.1.11 Notifica di eventuali violazioni di Dati personali (c.d. Data Breach): fatta salva la reciproca collaborazione tra le Parti, ognuna provvede autonomamente a notificare tempestivamente, secondo i termini e le modalità descritte dagli artt. 33 e 34 del GDPR, eventuali violazioni di Dati personali alle Autorità di controllo competenti.
- 7.1.12 Rapporti con le Autorità di controllo: le Parti si impegnano a collaborare al fine di rispondere a qualsiasi richiesta proveniente da soggetti terzi, quali, enti pubblici, l'Autorità Garante per la Protezione dei Dati Personali e consentire agli stessi, ed ai propri rappresentanti, tutti i controlli e gli accessi che dovessero rendersi opportuni e/o necessari;
- 7.1.13 Pubblicazione dell'estratto dell'Accordo di Contitolarità: le Parti, nel pieno rispetto dell'art. 26 par. 2 del GDPR, pubblicano nel proprio sito web nella sezione dedicata al Whistleblowing l'estratto del presente Accordo disponibile in allegato (**Allegato 2**).

## **8. RESPONSABILITÀ DEI CONTITOLARI E MANLEVA**

- 8.1 Ciascun Contitolare è responsabile, nell'ambito delle attività di Trattamento di Dati effettuate, per la violazione degli obblighi di cui al paragrafo precedente.
- 8.2 La Parte che violerà gli obblighi di cui al paragrafo precedente si impegna a tenere manlevata e indenne l'altra Parte da qualsiasi pretesa, danno, responsabilità, spesa - comprese le eventuali spese legali - che possa derivare da tale inadempimento e/o dal mancato rispetto delle prescrizioni di cui al presente Accordo.

## **9. MANDATO**

- 9.1 Le Parti conferiscono mandato a Impresoft S.p.A. affinché la stessa possa concludere accordi / contratti / atti, anche con riferimento alla normativa privacy, e sottoscrivere informative ai sensi all'articolo 13 del GDPR, in nome e per conto delle Società del Gruppo ai fini di poter dare esecuzione al presente Accordo.

## **10. DECORRENZA, DURATA E RECESSO**

- 10.1 Il presente Accordo ha validità dal momento della sua sottoscrizione da parte dei Contitolari e avrà la medesima durata del rapporto intercorrente tra gli stessi, salvo recesso anticipato di una delle Parti, da esercitarsi secondo quanto previsto dal seguente punto 10.3.

  
CP

  
EM

  
SG

  
NB

  
AG



10.2 Al termine del presente Accordo – a qualsiasi titolo e causa - le Parti si impegnano a cancellare eventuali copie esistenti dei Dati personali trattati, salvo che la normativa vigente preveda la conservazione dei Dati; in entrambi i casi, le Parti dovranno dare atto, per iscritto, dell'avvenuta cancellazione dei Dati.

10.3 Ciascuna delle Parti potrà recedere dal presente Accordo con un preavviso di 30 giorni, da comunicarsi alle altre Parti a mezzo Raccomandata A/R o PEC. Il citato preavviso decorre dalla data di ricevimento dalle altre Parti della comunicazione di recesso. L'eventuale recesso determinerà la cessazione dei Trattamenti oggetto del presente Accordo.

## **11. MODIFICHE ALL'ACCORDO**

11.1 Le Parti, congiuntamente, si impegnano a valutare, in maniera periodica, i risultati raggiunti per il tramite del presente Accordo.

11.2 Le Parti potranno valutare, tenendo conto anche dei risultati ottenuti di cui al punto precedente, di modificare il presente Accordo laddove lo ritengano necessario e/o alla luce degli aggiornamenti applicativi e interpretativi delle norme in materia di protezione dei Dati personali.

11.3 Le Parti, inoltre, concordano che qualsiasi modifica dell'Accordo in oggetto debba avvenire in forma scritta e sottoscritta da entrambe le Parti.

## **12. RISERVATEZZA**

12.1 Le Parti si impegnano reciprocamente, anche mediante l'adozione di idonee misure tecniche e organizzative, a mantenere la massima riservatezza, confidenzialità e segretezza su tutte le informazioni riservate ricevute o in qualunque maniera apprese durante l'esecuzione del presente Accordo. In particolare, le Parti non copieranno, tratteranno, comunicheranno, diffonderanno, divulgheranno, né comunque utilizzeranno le informazioni riservate, in qualsiasi modo o forma e anche in via indiretta, per fini diversi da quelli previsti nel presente Accordo.

## **13. LEGGE APPLICABILE E FORO COMPETENTE**

13.1 Tutte le controversie derivanti dal presente Accordo, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, saranno di esclusiva competenza del foro di Milano.

## **14. DISPOSIZIONI FINALI**

14.1 L'invalidità o la nullità di una o più delle clausole del presente Accordo non comprometterà la validità delle rimanenti clausole che conserveranno in ogni caso pieno vigore ed efficacia.

14.2 Resta inteso tra le Parti che le disposizioni del presente Accordo che sono adatte, per loro natura, a sopravvivere alla scadenza o alla risoluzione dello stesso per qualsiasi causa, manterranno efficacia anche dopo la data di scadenza o risoluzione dello stesso.

14.3 Le Parti dichiarano di aver negoziato le clausole del presente accordo e che, pertanto, le previsioni di cui agli artt. 1341 e 1342 c.c. non sono applicabili.

## **15. ESTENSIONE DELL'ACCORDO**

15.1 Le Parti accettano e concordano sin da ora che nel caso di ingresso di altre società nel Gruppo, quest'ultime potranno partecipare all'Accordo mediante adesione allo stesso con contratto sottoscritto con Impresoft S.p.A.

  
CP

  
EM


  
SG

  
NB


  
AG

• Allegato 1 – DESCRIZIONE OPERAZIONI DI TRATTAMENTO


Milano, 5 dicembre 2023


Pitagora S.p.A. - Alessandro Geraldi – Amministratore Delegato   
Alessandro Geraldi (05/dic/2023 14:51 GMT+1)

Impresoft S.p.A. - Alessandro Geraldi – Amministratore Delegato   
Alessandro Geraldi (05/dic/2023 14:51 GMT+1)

GN Techonomy S.r.l. – Nives Borroni - Presidente   
Nives Borroni (06/dic/2023 10:44 GMT+1)

4ward S.r.l. – Christian Parmigiani – Presidente ed Amministratore Delegato   
Christian Parmigiani (05/dic/2023 14:36 GMT+1)

Qualitas S.p.A. – Sergio Gasparin – Amministratore Delegato   
Sergio Gasparin (06/dic/2023 10:03 GMT+1)

Opensymbol S.r.l. – Enrico Maggi – Amministratore Delegato 

## ALLEGATO 1

### DESCRIZIONE OPERAZIONI DI TRATTAMENTO

Tipologia di Trattamento	Persone che hanno accesso ai dati	Finalità di Trattamento	Interessati	Dati personali	Base giuridica	Archivio	Trasferimenti extra UE e Garanzie previste (Capo V GDPR)	Destinatari / Responsabili
Gestione delle segnalazioni whistleblowing mediante Piattaforma	Gestore delle segnalazioni  Soggetti competenti a dare seguito alle segnalazioni	Ricevere, analizzare, e gestire la segnalazione whistleblowing, accertare i fatti oggetto della stessa e adottare i conseguenti provvedimenti.	Segnalante  Persona coinvolta	Dati personali (tra cui dati identificativi e anagrafici, indirizzo e-mail e numero di telefono, voce del segnalante e immagini)  Categorie particolari di dati personali  Dati giudiziari (ovvero dati relativi a condanne penali e reati)	Adempimento delle previsioni di cui alla D.lgs. 10 marzo 2023, n. 24  Consenso del Segnalante per rivelare la sua identità a terzi o in un procedimento disciplinare	Piattaforma Cerved	No	Eventuali consulenti legali esterni che possano fornire attività di consulenza alla società relativamente alle attività di gestione della segnalazione whistleblowing;  Soggetti, enti o autorità a cui sia obbligatorio comunicare i dati in forza di disposizioni di legge o di ordini delle autorità.  MN Tax & Legal  Cerved
Gestione delle segnalazioni whistleblowing mediante Piattaforma	Admin	Accedere alla Piattaforma	Gestore delle Segnalazioni  Admin	Dati personali (nome, cognome e indirizzo e-mail)	Esecuzione dell'incarico di gestore delle segnalazioni affidato in adempimento delle previsioni di cui alla D.lgs. 10 marzo 2023, n. 24	Piattaforma Cerved	No	Cerved

<p>Gestione delle segnalazioni whistleblowing mediante posta cartacea</p>	<p>Gestore delle segnalazioni</p> <p>Soggetti competenti a dare seguito alle segnalazioni</p>	<p>Ricevere, analizzare, e gestire la segnalazione whistleblowing, accertare i fatti oggetto della stessa e adottare i conseguenti provvedimenti.</p>	<p>Segnalante</p> <p>Persona coinvolta</p>	<p>Dati personali (tra cui dati identificativi e anagrafici, eventuale indirizzo e-mail e numero di telefono, indirizzo di residenza o domicilio)</p> <p>Categorie particolari di dati personali</p> <p>Dati giudiziari (ovvero dati relativi a condanne penali e reati)</p>	<p>Adempimento delle previsioni di cui alla D.lgs. 10 marzo 2023, n. 24</p> <p>Consenso del Segnalante per rivelare la sua identità a terzi o in un procedimento disciplinare</p>	<p>Archivio cartaceo chiuso a chiave in ufficio chiuso a chiave</p> <p>Registro segnalazioni</p> <p>Piattaforma Cerved (eventuale per archiviazione)</p>	<p>No</p>	<p>'Eventuali consulenti legali esterni che possano fornire attività di consulenza alla società relativamente alle attività di gestione della segnalazione whistleblowing;</p> <p>Soggetti, enti o autorità a cui sia obbligatorio comunicare i dati in forza di disposizioni di legge o di ordini delle autorità</p> <p>MN Tax &amp; Legal</p> <p>Cerved</p>
<p>Gestione delle segnalazioni whistleblowing mediante incontro diretto</p>	<p>Gestore delle segnalazioni</p> <p>Soggetti competenti a dare seguito alle segnalazioni</p>	<p>Ricevere, analizzare, documentare e gestire la segnalazione whistleblowing, accertare i fatti oggetto della stessa e adottare i conseguenti provvedimenti.</p>	<p>Segnalante</p> <p>Persona coinvolta</p>	<p>Dati personali (tra cui dati identificativi e anagrafici, dati di contatto)</p> <p>Categorie particolari di dati personali</p> <p>Dati giudiziari (ovvero dati relativi a condanne penali e reati)</p>	<p>Adempimento delle previsioni di cui alla D.lgs. 10 marzo 2023, n. 24</p> <p>Consenso del Segnalante per rivelare la sua identità a terzi o in un procedimento disciplinare e per la documentazione della segnalazione</p>	<p>Archivio cartaceo chiuso a chiave in ufficio chiuso a chiave</p> <p>Registro segnalazioni</p> <p>Piattaforma Cerved (eventuale per archiviazione)</p>	<p>No</p>	<p>Eventuali consulenti legali esterni che possano fornire attività di consulenza alla società relativamente alle attività di gestione della segnalazione whistleblowing;</p> <p>Soggetti, enti o autorità a cui sia obbligatorio comunicare i dati in forza di disposizioni di legge o di ordini delle autorità.</p> <p>MN Tax &amp; Legal</p> <p>Cerved</p>