ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679 ("REGOLAMENTO")

TRA

Whistleblowing Solutions Impresa Sociale S.r.l. (Titolare)

E

Seeweb S.p.A. (Responsabile del Trattamento)

In relazione alla fornitura specifica dei seguenti prodotti: "Foundation Server PRO (fs20585), Cloud Data Protection (cdp000132), Appliance VPN OPNsense (vm9619)"

1. PREMESSA

1.1. Premesso che:

A. Le vigenti disposizioni in materia di Trattamento dei Dati Personali prevedono che qualora un Trattamento sia effettuato per conto di **Whistleblowing Solutions IS S.r.l.** ("**WBS**") - Titolare da una persona fisica o giuridica, una pubblica amministrazione o qualsiasi altro ente o associazione quale Responsabile del Trattamento, WBS in qualità di Titolare ricorra a soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento dei Dati Personali, ivi compreso il profilo della sicurezza; pertanto il Responsabile del Trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalle Leggi applicabili in materia di protezione dei Dati Personali pro tempore vigenti in materia e garantisca la tutela dei diritti dell'Interessato;

B. SEEWEB S.r.l. ("**SEEWEB**") dichiara di avere tutte le competenze tecniche e organizzative idonee ai sensi e per gli effetti dell'art. 28 del Regolamento al ruolo di Responsabile del Trattamento dei Dati Personali necessario all'esecuzione del Contratto di cui il presente documento costituisce un allegato.

C. WBS e SEEWEB si danno reciprocamente atto che:

a) il Cliente (WBS) è Titolare dei Dati Personali determinando le finalità e le modalità del loro Trattamento nell'erogazione del Servizio oggetto del Contratto;
b) il Prestatore (SEEWEB) è Responsabile dei Dati Personali Trattati in esecuzione del Servizio oggetto del Contratto; in particolare, pertanto, i compiti e le responsabilità di SEEWEB sono strettamente legati al diretto adempimento delle obbligazioni assunte nell'ambito del Contratto, con esclusione di ogni altra responsabilità
c) il presente accordo e le sue appendici (congiuntamente denominati "Accordo per il Trattamento dei Dati Personali" o anche "Accordo TDP"), sono sottoscritti da WBS e SEEWEB al fine di dettagliare le istruzioni del Titolare e regolare il rapporto tra il Titolare e il Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento, anche con riferimento ai rispettivi diritti e obblighi relativi al Trattamento dei Dati Personali posto in essere dal Responsabile del Trattamento ed in particolare per stabilire misure di sicurezza e procedure idonee per procedere al legittimo Trattamento dei Dati Personali; il presente Accordo TDP è a titolo gratuito in quanto collegato alla fornitura del Servizio;
d) con il presente Accordo TDP, il Titolare affida al Responsabile del Trattamento tutte ed esclusivamente le operazioni di Trattamento dei Dati Personali necessarie per dare piena esecuzione al Servizio, come descritto nel Contratto e nei suoi allegati. In caso di danni derivanti dal Trattamento dei Dati Personali posto in essere dal Responsabile del Trattamento, questi ne risponderà solo qualora non abbia adempiuto agli obblighi derivanti dalle Leggi applicabili in materia di protezione dei Dati Personali specificatamente diretti ai responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare.

D. In particolare, la finalità perseguita, la tipologia, e le modalità del Trattamento dei Dati Personali sono descritti nell'**Appendice 1**.

E. In caso di contrasto o incongruenze per quanto riguarda gli accordi tra le Parti in materia di protezione dei Dati Personali tra il presente Accordo TDP e il Contratto, prevale quanto stabilito nell'Accordo TDP ed in eventuali accordi integrativi o modificativi di quest'ultimo.

F. La presente premessa forma parte integrante dell'Accordo TDP.

2. DEFINIZIONI

2.1. Salvo che sia diversamente definito nel presente Accordo TDP, tutti i termini in maiuscolo utilizzati nel presente documento e nelle sue appendici hanno il significato loro attribuito nel Contratto.

"**Accordo per il Trattamento dei Dati Personali" o "Accordo TDP**" indica il presente accordo per il Trattamento dei Dati Personali comprensivo delle Appendici 1, 2 e 3, nonché di eventuali accordi modificativi o integrativi;

"AEE" indica l'Area Economica Europea;

"**Autorità di Controllo**" indica ogni autorità competente a vigilare ed assicurare l'applicazione delle Leggi applicabili in materia di protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali svolti per mezzo del Servizio;

"Categorie Particolari di Dati Personali" indica i Dati Personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

"Clausole Contrattuali Tipo" indica le cd. "Standard Contractual Clauses" (controller to processor), clausole contrattuali tipo adottate dalla Commissione Europea per il trasferimento dei Dati Personali da un verso organismI extra SEE.

"**Contratto**" indica il Contratto per i prodotti "**Foundation Server PRO (fs20585), Cloud Data Protection (cdp000132), Appliance VPN OPNsense (vm9619)"** qualificati da AgID per erogare servizi IaaS alla Pubblica Amministrazione;

"Dati Giudiziari" indica o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;

"**Dati Personali del Cliente**" indica i Dati Personali trattati in relazione al Servizio fornito dal Responsabile per conto del Cliente per l'esecuzione del Contratto;

"Dati Personali" significa qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato") oggetto di Trattamento da parte del Prestatore per conto del Titolare in esecuzione del Contratto; 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; al fine di evitare contrasti interpretativi, ha in ogni caso il significato previsto dal Regolamento e dalle Leggi applicabili in materia di protezione dei Dati Personali;

"Diritti dell'Interessato" sono i diritti riconosciuti all'Interessato dalle Leggi applicabili in materia di protezione dei Dati Personali come, nei limiti di applicabilità del Regolamento, ad esempio, il diritto di chiedere al Titolare l'accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del

Trattamento dei dati dell'Interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;

"**Elenco dei Sub-Responsabili**" indica l'elenco disponibile nell'**Appendice 3**;

"Incaricato/i" il personale, dipendenti, collaboratori a qualsiasi titolo del Prestatore che abbiano accesso ai Dati Personali e agiscono sotto l'autorità del Responsabile del Trattamento ai sensi dell'art. 29 del Regolamento;

"Interessato/i" ha il significato previsto dal Regolamento;

"Leggi applicabili in materia di protezione dei Dati Personali" indica, negli Stati membri dell'Unione Europea, il Regolamento e le complementari legislazioni nazionali in materia di protezione dei Dati Personali, comprensivi di ogni orientamento e/o *code of pratice* emessi dalla competente Autorità di controllo all'interno dell'Unione Europea (inclusi i provvedimenti e/o delle Autorizzazioni e/o Linee Guida del Garante per la protezione dei dati personali in quanto applicabili); e/o, negli Stati extra UE, ogni vigente legislazione in materia di protezione dei Dati Personali relativa alla tutela ed al legittimo Trattamento di Dati Personali;

"Regolamento" indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio 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;

"Responsabile del Trattamento" indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che effettua un Trattamento dei Dati Personali per conto del Titolare. Ai fini del presente Accordo TDP, il Responsabile è **SEEWEB** (anche "**Prestatore**");

"**SEE**" indica lo Spazio Economico Europeo;

"**Servizio**" indica il servizio oggetto del Contratto di cui il presente Accordo TDP costituisce allegato;

"**Sub-Responsabile**" indica un organismo individuato dal Responsabile per assisterlo nel (o che intraprenda direttamente qualsivoglia) Trattamento dei Dati Personali nel rispetto delle obbligazioni previste dal Responsabile e di cui al presente Accordo TDP, che sia stato autorizzato dal Titolare ai sensi dell'Art. 5 del presente Accordo TDP;

"Titolare" indica la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali. Ai fini del presente Accordo TDP, il Titolare è **WBS** (anche "**Cliente**);

"Trattare" o "**Trattamento**" significa 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;

"**UE**" indica l'Unione Europea;

"Violazione dei Dati Personali" indica 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.

3. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

3.1. Il Responsabile del Trattamento, per quanto di competenza, è tenuto, in forza di legge e di contratto, per sé e per gli Incaricati e per qualunque soggetto collabori con la sua attività, al rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.

3.2. Fatti salvi gli obblighi stabiliti da altre disposizioni del presente Accordo TDP, il Responsabile del Trattamento è obbligato a:

a) trattare i Dati Personali solo per quanto strettamente necessario all'erogazione del Servizio e solo limitatamente alla conduzione tecnico funzionale dei sistemi/servizi oggetto del Contratto;

b) rispettare le istruzioni impartite dal Titolare per iscritto con il presente Accordo TDP e con eventuali accordi scritti successivi, avvertendo il Titolare qualora ritenga che le istruzioni impartite si pongano in violazione delle Leggi applicabili in materia di protezione dei Dati Personali;

c) contestualmente alla designazione, fornire adeguate istruzioni scritte agli Incaricati circa le modalità del Trattamento dei Dati Personali in ottemperanza a quanto disposto dalle Leggi applicabili in materia di protezione dei Dati Personale e dal presente Accordo TDP. A titolo esemplificativo e non esaustivo, il Responsabile del Trattamento, nel designare per iscritto gli Incaricati, dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Inoltre, ove occorrer possa, per i Trattamenti effettuati per fornire il Servizio dagli Incaricati con mansioni di "Amministratore di Sistema", il Responsabile del Trattamento è tenuto altresì al rispetto del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (modificato in base al provvedimento del 25 giugno 2009) e delle Leggi applicabili in materia di protezione dei Dati Personali pro tempore applicabili relative alla disciplina sugli amministratori di sistema. La versione aggiornata dell'elenco contenente gli estremi identificativi (nome, cognome, funzione o area organizzativa di appartenenza) degli Amministratori di Sistema dovrà essere consegnato senza indugio a semplice richiesta anche solo verbale di WBS, a quest'ultimo e/o alle competenti Autorità e ad eventuali ulteriori terzi aventi diritto;

d) vincolare gli Incaricati alla riservatezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto, in relazione alle operazioni di Trattamento da essi eseguite;

e) verificare che gli Incaricati di cui al punto precedente applichino tutte le disposizioni in materia di sicurezza adottate ai sensi dell'art. 32 del Regolamento (per quanto di loro competenza) e in conformità ai principi generali di cui all'art. 5 del Regolamento. In particolare, il Responsabile del Trattamento dovrà verificare che gli Incaricati applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave (trattamenti elettronici) e che conservino in luogo sicuro i supporti non informatici contenenti eventuali atti o documenti con categorie particolari di dati (dati sensibili o giudiziari) o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei di dati sensibili);

f) assicurare l'adozione, l'implementazione e l'utilizzo delle misure tecniche ed organizzative di cui all'**Appendice 2** del presente Accordo TDP, nonché di tutte le ulteriori misure tecniche ed organizzative che si dovessero rendere necessarie per proteggere i Dati Personali (compresi i Dati

Giudiziari e le Categorie Particolari di Dati Personali, qualora presenti) ai sensi degli artt. 25 e 32 del Regolamento, in particolare contro:

(i) - distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.

(ii) - Trattamento dei Dati Personali non consentito o non conforme alle finalità delle operazioni di Trattamento;

Al fine in particolare di prevenire il Trattamento non consentito di Dati Personali, NTT si impegna a comunicare tempestivamente a WBS la necessità di revocare il profilo autorizzativo del proprio personale che non ha più accesso ai sistemi di WBS.

g) applicare le misure di sicurezza di cui al punto precedente al fine di garantire:
- se del caso, la pseudonimizzazione o la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

h) adottare ed aggiornare, secondo criteri di diligenza professionale, protocolli di *disaster recovery e business continuity*, garantendo, in ogni caso, che i Dati Personali siano conservati con regolari operazioni di backup cifrati;

i) implementare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento, trasmettendo tempestivamente al Titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate; a tal fine, il Responsabile del Trattamento informerà immediatamente il Titolare qualora, a suo parere, un'istruzione violi le Leggi applicabili in materia di protezione dei Dati Personali;

j) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento; inoltre, consentirà e contribuirà alle attività di revisione, comprese eventuali ispezioni, realizzati dal Titolare o da un altro soggetto da questi incaricato. A tale scopo il Responsabile del Trattamento riconosce al Titolare, e agli incaricati dal medesimo, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di Trattamento o dove sono custoditi dati o documentazione relativi al presente Accordo TDP. In ogni caso il Titolare si impegna a mantenere la riservatezza sulle informazioni raccolte durante le operazioni di verifica e pertanto a non comunicarle a soggetti terzi salvo sia necessario in adempimento di un obbligo previsto dalla legge o dal presente Accordo TDP;

k) cooperare con il Titolare del trattamento nel riscontro alle richieste degli interessati ai sensi dell'articolo 28, par. 3, lett. e), fornendo tempestivamente le informazioni eventualmente in proprio possesso;

l) comunicare tempestivamente, senza indebito ritardo, ogni contatto o comunicazione ricevuta da un'Autorità di Controllo in relazione al Trattamento dei Dati Personali. In difetto, la responsabilità

del mancato riscontro alle suddette richieste resterà esclusivamente in capo al Responsabile del Trattamento;

4. OBBLIGHI DEL TITOLARE

4.1. Il Cliente è consapevole e accetta che, nella misura necessaria a consentire l'erogazione del Servizio, comunicherà i Dati Personali di cui è Titolare al Prestatore o ne consentirà a quest'ultimo l'accesso.

4.2. Il Titolare si impegna a comunicare al Responsabile del Trattamento qualsiasi variazione si dovesse rendere necessaria nelle operazioni di Trattamento dei Dati Personali.

4.3. Il Cliente dichiara, inoltre, che i Dati Personali trasmessi al Responsabile:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i Dati Personali e/o le categorie particolari di Dati Personali, oggetto delle operazioni di trattamento affidate al Prestatore, sono raccolti e trasmessi rispettando le prescrizioni delle Leggi applicabili in materia di protezione dei Dati Personali pro tempore applicabili.

4.4. Il Cliente assicura e garantisce che sussiste un'idonea base legale per consentire al Prestatore il Trattamento dei Dati Personali come parte della fornitura del Servizio.

5. AUTORIZZAZIONE AL TRATTAMENTO DA PARTE DI SUB-RESPONSABILI

5.1. Il Titolare conferisce autorizzazione scritta generale al Responsabile del Trattamento a poter ricorrere a eventuali ulteriori responsabili del trattamento nella prestazione del Servizio.

5.2. Nel caso in cui il Responsabile del Trattamento faccia ricorso a Sub-responsabili, il medesimo si impegna a selezionare Sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti di cui alle Leggi applicabili in materia di protezione dei Dati Personali e garantisca la tutela dei diritti degli Interessati e a comunicare il nominativo del Sub-responsabile fornendo le informazioni di cui all'Appendice 3.

5.3. Il Responsabile del Trattamento si impegna altresì a stipulare specifici contratti o altri atti giuridici con i Sub-responsabili a mezzo dei quali siano descritti analiticamente i loro compiti e sia imposto a tali soggetti il rispetto dei medesimi obblighi di cui alle Leggi applicabili in materia di protezione dei Dati Personali ed al presente Accordo TDP, prevedendo in particolare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa applicabile e i provvedimenti emessi dall'Autorità di controllo.

5.4. Qualora il Sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei Dati Personali, il Responsabile del Trattamento riconosce di conservare nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei Sub-responsabili coinvolti, nonché si impegna a manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al Titolare dalla mancata osservanza di tali obblighi e più in generale dalla violazione della applicabile normativa sulla tutela dei dati personali da parte del Responsabile e dei suoi sub-fornitori.

Tale manleva opererà nel rispetto nelle seguenti condizioni:

-tempestiva informazione al Responsabile-la responsabilità del Responsabile opererà indipendentemente dalle coperture assicurative eventualmente applicate al Titolare;
-il Titolare farà ogni sforzo per attenuare le conseguenze dannose della violazione e nella sua sfera di controllo.
5.5. Il Responsabile del Trattamento si impegna altresì ad informare il Titolare di eventuali modifiche o sostituzioni previste riguardanti i Sub-responsabili, dando così al Titolare la possibilità di opporsi a tali modifiche.
5.6. Su richiesta del Titolare, il Responsabile fornisce tempestivamente al Titolare adeguate informazioni in merito alle azioni e alle misure che il Responsabile ed i suoi Sub-Responsabili hanno adottato per assicurare il rispetto delle previsioni del presente Accordo TDP.

6. TRASFERIMENTO DEI DATI PERSONALI

6.1. I dati devono essere trattati ed utilizzati esclusivamente nel territorio di uno Stato Membro dell'Unione Europea (EU) o di altro firmatario della presente Nomina nell'Area Economica Europea (AEE).

7. OBBLIGHI IN TEMA DI COOPERAZIONE E RESPONSABILITÀ

7.1. Il Cliente e i Prestatore, si impegnano a collaborare in buona fede per assicurare il rispetto delle previsioni del presente Accordo TDP, tra cui, ma non solo, il dovere di assicurare il corretto e tempestivo esercizio dei diritti dell'Interessato, gestire incidenti di sicurezza/Violazioni dei Dati Personali al fine di mitigare i possibili effetti avversi da essi derivanti.
7.2. Il Cliente e i Prestatore collaborano in buona fede per rendere disponibile reciprocamente e verso l'Autorità di Controllo le informazioni necessarie a dimostrare il rispetto delle Leggi applicabili in materia di protezione dei Dati Personali.

8. RESTITUZIONE DEI DATI E DISTRUZIONE

8.1. Il Responsabile del Trattamento, senza porre costi aggiuntivi a carico del Titolare, restituirà o distruggerà prontamente i Dati Personali alla scadenza o risoluzione anticipata del Contratto in base alla scelta comunicata dal Titolare o in ogni caso su richiesta del Titolare, da comunicare al Responsabile del Trattamento per iscritto, salvo che sussistano specifici obblighi di conservazione previsti dalla legge (inclusi, a titolo esemplificativo ma non esaustivo, quelli previsti dalle normative previste dalla Pubblica Amministrazione in riferimento ai servizi cloud, Leggi applicabili in materia di protezione dei Dati Personali o richieste provenienti dall'autorità giudiziaria), tra cui, ma non solo, quelli provenienti dall'Autorità di Controllo.
8.2. Al fine di adempiere all'obbligo di pronta restituzione di cui al precedente art. 9.1, il Responsabile del Trattamento dovrà procedere senza ingiustificato ritardo e non oltre 7 giorni dalla richiesta del Titolare. Resta inteso che il Responsabile del Trattamento dovrà altresì procedere prontamente alla distruzione di ogni copia dei Dati Personali in suo possesso.
8.3. Nel caso in cui il Titolare richieda la pronta distruzione dei Dati Personali e fatto salvo quanto previsto dal successivo art. 8.4, il Responsabile fornirà un'attestazione che assicuri tale pronta distruzione.

8.4. Ai fini del presente Accordo TDP e di quanto stabilito ai punti precedenti, il Cliente dichiara di optare per la scelta di distruggere i Dati Personali una volta terminato il rapporto contrattuale e trascorsi i periodi di conservazione indicati dalla legge applicabile o richiesti dalle autorità competenti.

8.5 La presente disposizione non incide sui doveri di legge del Responsabile del Trattamento di conservare le registrazioni per i periodi di conservazione indicati dalla legge applicabile o richiesti dalle autorità competenti.

9. VIOLAZIONE DEI DATI PERSONALI

9.1. Il Titolare è consapevole e acconsente che il Responsabile del Trattamento non sarà ritenuto responsabile in caso di Violazione dei Dati Personali che non sia imputabile a colpa di quest'ultimo.

9.2. Nel caso in cui il Responsabile venga a conoscenza di una Violazione dei Dati Personali, dovrà:

a) adottare le misure tecniche e organizzative appropriate per contenere e mitigare tale Violazione dei Dati Personali;

b) informare prontamente e senza ingiustificato ritardo il Titolare e, in ogni caso, non oltre ventiquattro (24) ore dalla conoscenza della Violazione dei Dati Personali, al fine di consentire al Titolare l'adempimento degli obblighi di notifica e comunicazione previsti dagli artt. 33 e 34 del Regolamento e la rapida adozione delle possibili contromisure necessarie;

c) collaborare con il Titolare per indagare: la natura, le categorie ed il numero approssimativo di Interessati coinvolti, le categorie ed il numero approssimativo di Dati Personali coinvolti e le probabili conseguenze di tale violazione con modalità commisurate alla serietà ed al suo impatto complessivo sul Titolare e sull'erogazione del Servizio previsto dal Contratto;

d) ove le Leggi applicabili in materia di protezione dei Dati Personali richiedano la notificazione alle competenti Autorità di Controllo o la comunicazione agli Interessati della Violazione dei Dati Personali, e nel caso essa si riferisca a Dati Personali, il Responsabile del Trattamento dovrà deferire e assumere istruzioni dal Titolare, che – salvo quanto previsto dalla lettera a) del presente articolo - sarà l'unico ad avere il diritto di determinare le ulteriori misure che dovranno essere adottate nel rispetto delle Leggi applicabili in materia di protezione dei Dati Personali o il diritto porre rimedio a qualsivoglia rischio, tra cui ma non solo:

i. determinare se l'avviso debba essere fornito a qualsivoglia individuo, autorità di regolamentazione, autorità giudiziaria, enti a tutela dei consumatori o altri come richiesto dalle Leggi applicabili in materia di protezione dei Dati Personali, o richiesto a discrezione del Titolare;
ii. determinare il contenuto di tale avviso e comunicarlo ai soggetti individuati dal Titolare;
iii. se sia possibile offrire all'Interessato dalla violazione qualsivoglia tipologia di rimedio riparatorio, nonché la natura e l'estensione di tale rimedio.

10. TRASMISSIONE

10.1. I Dati Personali trasmessi dal Responsabile in relazione al Servizio attraverso Internet dovranno essere cifrati in modo appropriato in osservanza delle disposizioni di cui all'Allegato A2 del Contratto. Le Parti

sono altresì consapevoli che la sicurezza delle trasmissioni su Internet non potrà essere completamente garantita.

10.2. In caso si sospetti una Violazione dei Dati Personali, il Responsabile potrà sospendere, immediatamente in attesa delle indagini sulle cause, l'utilizzo del Servizio via Internet da parte del Titolare, a condizione che il Responsabile notifichi tale sospensione non appena ciò sia ragionevolmente possibile, nonché adotti tutte le misure adeguate per ripristinare prontamente la fruizione del Servizio via Internet e cooperi con il Titolare al fine di proseguire l'erogazione del Servizio tramite altri canali di comunicazione disponibili.

11. DURATA E VALIDITÀ

11.1. Il presente Accordo TDP avrà la medesima durata del Contratto di cui il presente documento costituisce un allegato. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche il presente Accordo TDP verrà automaticamente meno, senza bisogno di comunicazioni o revoche, ed il Responsabile del Trattamento non sarà più legittimato a Trattare i Dati Personali cessando lo status di Responsabile.

11.2. Con il presente Accordo TDP, il Cliente e il Responsabile intendono espressamente revocare e sostituire ogni altra eventuale nomina e accordo per qualsivoglia tipologia di Dati Personali del Cliente.

Questo documento sostituisce integralmente e annulla il documento di nomina del 21/05/21.

MILANO, 10/12/21

Per conto del Titolare (WBS):

Giovanni Pellerano,
Amministratore Delegato

Per conto del Responsabile (SEEWEB S.p.A.):

APPENDICE 1

Categorie di interessati: i Dati Personali riguardano le seguenti categorie di Interessati: Personale e collaboratori di WBS; Referenti di clienti che attivano il servizio di digital whistleblowing, soggetti riceventi le segnalazioni (Responsabili Anticorruzione, Organismi di Vigilanza, Audit, ecc.); soggetti che inviano le segnalazioni (dipendenti, collaboratori, consulenti, clienti, fornitori); Terzi indeterminati.

Tipo di Dati Personali oggetto di trattamento: i Dati Personali oggetto di trattamento si riferiscono alle seguenti tipologie di dati:

- Dati comuni: dati anagrafici, di contatto, professionali, indirizzi IP, log, ID utenti, codici di identificazione, dati bancari;
- Categorie particolari di dati personali: dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti allegati, relativi alla salute eventualmente contenuti nella segnalazione.

Natura e finalità del trattamento: il trattamento dei Dati Personali è obbligatorio per l'esecuzione del Servizio oggetto del Contratto.

Descrizione delle attività di trattamento: operazioni di trattamento necessarie per l'esecuzione del Servizio oggetto del Contratto.

Modalità di Trattamento

I Dati Personali sono trattati secondo modalità cartacea e elettronica.

APPENDICE 2

1. Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile ed i Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte (misure standard suggerite dallo standard ISO 27001).

2. Informazioni sulle misure di sicurezza

2.1 Gestione della sicurezza delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a definire una serie di politiche e misure per chiarire gli obiettivi al fine di supportare la sicurezza delle informazioni. A livello apicale, il Responsabile ed i Sub-Responsabili si impegnano a definire una "Policy per la sicurezza delle informazioni" di carattere generale, come specificato nella sezione 5.2 della ISO/IEC27001.

2.2 Organizzazione della sicurezza delle informazioni

2.2.1 Organizzazione interna

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'organizzazione definisca i ruoli e le responsabilità per la sicurezza delle informazioni e assegnarli singolarmente a soggetti determinati. Ove necessario, i compiti devono essere separati per ruoli e persone al fine di evitare conflitti di interesse e prevenire attività inappropriate.

2.2.2 Dispositivi mobili e telelavoro

Il Responsabile ed i Sub-Responsabili si impegnano a definire una Policy di sicurezza e adeguati controlli per i dispositivi mobili (come laptop, tablet, PC, dispositivi indossabili, smartphone, strumenti USB e altri) e per il telelavoro (come coloro che lavorano da casa, quelli che viaggiano assiduamente e le postazioni di lavoro da remoto/virtuali).

2.2.3 Sicurezza delle risorse umane

Prima dell'instaurazione del rapporto di lavoro

Il Responsabile ed i Sub-Responsabili si impegnano a prendere in considerazione le responsabilità della sicurezza delle informazioni durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e ad inserirle all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

Durante il rapporto di lavoro

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i manager si assicurino che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni. Il Responsabile ed i Sub-Responsabili si impegnano altresì a formalizzare un procedimento disciplinare per gestire gli incidenti relativi alla sicurezza delle informazioni presumibilmente causati dai lavoratori.

Conclusione o modifiche al rapporto di lavoro

Il Responsabile ed i Sub-Responsabili si impegnano a gestire gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.

2.2.4 Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale

Il Responsabile ed i Sub-Responsabili si impegnano a inventariare tutte le informazioni relative alle risorse del patrimonio aziendale e ad identificare i relativi soggetti di riferimento al fine di individuare le responsabilità per la loro sicurezza. Il Responsabile ed i Sub-Responsabili si impegnano altresì a definire una Policy per un "uso corretto" delle stesse e a far rientrare le risorse all'interno dell'organizzazione al momento dell'uscita dei soggetti coinvolti.

Classificazione delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a classificare e a catalogare le informazioni dai rispettivi soggetti di riferimento in linea con quanto previsto dalle esigenze di sicurezza, nonché a trattarle in modo appropriato.

Gestione dei media

Il Responsabile ed i Sub-Responsabili si impegnano a gestire, controllare, modificare ed utilizzare le informazioni conservate sui media in modo tale da non comprometterne il loro contenuto.

2.2.5 Controllo degli accessi

Requisiti aziendali per il controllo degli accessi

Il Responsabile ed i Sub-Responsabili si impegnano a documentare chiaramente i requisiti previsti dall'organizzazione per controllare l'accesso alle informazioni relative al patrimonio aziendale in una Policy per il controllo degli accessi e delle relative procedure. Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'accesso alla rete e le connessioni prevedano delle limitazioni.

Gestione dell'accesso degli utenti

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'allocazione dei diritti d'accesso da parte degli utenti sia controllata dalla registrazione iniziale dell'utente fino alla rimozione del profilo quando esso non sia più necessario, incluse speciali restrizioni per i diritti di accesso privilegiato e la gestione delle password (definita come "informazione di autenticazione segreta"); Il Responsabile ed i Sub-Responsabili si impegnano, peraltro, a procedere regolarmente alla revisione e all'aggiornamento dei diritti di accesso.

Responsabilità degli utenti

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che gli utenti siano consapevoli delle loro responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad es. scegliendo password complesse e mantenendole riservate.

Sistemi e applicazioni per il controllo degli accessi

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'accesso alle informazioni sia limitato coerentemente a quanto previsto dalla Policy sul controllo degli accessi, ad es. attraverso autenticazioni sicure, gestione delle password, controllo delle utilità privilegiate e limitazioni all'accesso ai codici sorgente dei programmi.

2.2.6 Crittografia

Controllo crittografico

Il Responsabile ed i Sub-Responsabili si impegnano a definire una Policy sull'uso della cifratura dei dati, oltre ad autenticazioni criptate e controlli di integrità, come firme digitali e messaggi con codici di autenticazione, nonché una gestione delle chiavi di cifratura.

2.2.7 Sicurezza fisica e ambientale

Aree sicure

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che un perimetro fisico e una recinzione, con controllo fisico degli accessi e procedure operative, sia in grado di proteggere i locali, gli uffici, le stanze, le

aree di carico/scarico da accessi non autorizzati. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire la consulenza di uno specialista per quanto riguarda le misure di protezione contro incendi, allagamenti, terremoti, esplosioni, ecc.

Apparecchiatura

Il Responsabile ed i Sub-Responsabili si impegnano a rendere sicuri e manutenuti l'apparecchiatura (intesa perlopiù come apparecchiatura in ambito ICT), i servizi di supporto e il cablaggio. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire che:

a) l'apparecchiatura e le informazioni non escano dal loro luogo di riferimento se non previa autorizzazione, e in ogni caso siano adeguatamente protette sia all'interno che all'esterno del loro luogo di riferimento;

b) le informazioni siano distrutte prima di procedere allo smaltimento o al riciclo dei dispositivi sui cui erano conservate;

c) le apparecchiature non protette siano rese sicure e sia previsto un apposito spazio ed una chiara Policy di verifica.

2.2.8 Operazioni di sicurezza

Procedure e responsabilità operative

Il Responsabile ed i Sub-Responsabili si impegnano: a documentare le procedure e le responsabilità operanti per l'area IT; a controllare i cambiamenti alle infrastrutture ed ai sistemi IT; a gestire i singoli poteri e le relative prestazioni; a separare i sistemi di sviluppo, quelli di verifica e quelli operativi.

Protezione da malware

Il Responsabile ed i Sub-Responsabili si impegnano a garantire il controllo dei malware, comprensivo di un'idonea consapevolezza sul punto da parte degli utenti.

Backup

Il Responsabile ed i Sub-Responsabili si impegnano ad eseguire Idonei backup e a custodirli coerentemente ad una Policy per i backup.

Autenticazione e monitoraggio

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le attività, le eccezioni, gli errori e gli eventi relativi alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avvengano previo inserimento delle credenziali di autenticazione adeguatamente protette. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire che gli orologi siano sincronizzati.

Controllo di software operativi

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'installazione di software sui sistemi operativi sia controllata.

Gestione delle vulnerabilità tecniche

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le vulnerabilità tecniche siano corrette con idonee patch e che siano previste regole per l'installazione dei software da parte degli utenti.

Considerazioni sull'audit per le informazioni di sistema

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'audit per l'area IT sia programmato e controllato per minimizzare l'effetto avverso sui sistemi di produzione o l'accesso abusivo ai dati.

2.2.9 Sicurezza delle comunicazioni

Gestione della sicurezza della rete

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le reti e i servizi in rete siano resi sicuri, ad esempio attraverso la loro separazione.

Trasferimento delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a definire policy, procedure ed accordi (ad es. accordi di riservatezza) relativi al trasferimento delle informazioni verso/da terze parti, compresi i messaggi elettronici.

2.2.10 Acquisizione, sviluppo e manutenzione del sistema

Requisiti di sicurezza dei sistemi di informazione

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i requisiti per il controllo di sicurezza siano analizzati e specificati, comprese le applicazioni web e le transazioni.

Sicurezza nello sviluppo e processi di supporto

Il Responsabile ed i Sub-Responsabili si impegnano: a definire in una Policy le regole che governano la sicurezza dello sviluppo dei software/sistemi; a garantire che siano controllate le modifiche al sistema (sia per le applicazioni che per i sistemi operativi); a garantire che i pacchetti software non siano teoricamente modificati e che siano osservati i principi di sicurezza ingegneristica; a rendere sicuro l'ambiente di sviluppo e controllare lo sviluppo esternalizzato; a garantire che la sicurezza del sistema sia testata e che siano definiti criteri di ammissibilità che includano gli aspetti di sicurezza.

Test di verifica dei dati

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i test di verifica dei dati siano accuratamente selezionati/generati e controllati.

2.2.11 Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori

Il Responsabile ed i Sub-Responsabili si impegnano a definire policy, procedure, sistemi di consapevolezza volti a proteggere le informazioni dell'organizzazione che siano accessibili ai soggetti esterni operanti nell'area IT e ad altri fornitori esterni per l'intera catena di fornitura, concordata nei contratti o negli accordi.

Gestione dei servizi resi dal fornitore

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'erogazione dei servizi resi dal fornitore sia monitorata e rivista/verificata in relazione al contratto/accordo e che le modifiche al servizio siano controllate.

2.2.12 Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti alle informazioni di sicurezza e miglioramenti

Dovrebbero essere previste responsabilità e procedure (report, valutazioni, rispondere a e imparare da) volte a gestire in modo coerente ed efficace gli eventi, gli incidenti e le debolezze relative alle informazioni di sicurezza, anche al fine di conservare prove valide in eventuali giudizi.

2.2.13 Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Continuità della sicurezza delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che la continuità della sicurezza delle informazioni sia pianificata, implementata e revisionata come parte integrante del sistema organizzativo di continuità aziendale.

Ridondanze

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che le strutture IT siano sufficientemente ridondanti per soddisfare i requisiti di disponibilità.

2.2.14 Conformità

Conformità ai requisiti legali e contrattuali

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che l'organizzazione identifichi e documenti i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.

Revisione della sicurezza delle informazioni

Il Responsabile ed i Sub-Responsabili si impegnano a garantire che i progetti dell'organizzazione relativamente alla sicurezza delle informazioni siano revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. Il Responsabile ed i Sub-Responsabili si impegnano altresì a garantire che i manager revisionino periodicamente la conformità dei dipendenti e dei sistemi alle policy di sicurezza, alle procedure, ecc., e promuovano azioni correttive ove necessario.

APPENDICE 3

(Elenco dei Sub-Responsabili)

La tabella dei Sub-Responsabili deve essere compilata di volta in volta dal Responsabile e trasmessa al Titolare in modo che il Titolare possa opporsi all'impiego di nuovi Sub-Responsabili ai sensi dell'art. 28 del Regolamento.

Sub-Responsabili (indicare: luogo di stabilimento e dettagli di contatto) *Ad es., Nome della società, Indirizzo, soggetto responsabile in materia di protezione dei Dati Personali e dettagli di contatto*	**Paese/i in cui i Dati Personali sono trattati e finalità** *Ad es., Italia per hosting e Francia per backup*
…	…
…	…
…	…
…	…
…	…
…	…
…	…