**Information Security Plan**
**Allegato sulla Regolamentazione UE**

Il presente Allegato descrive gli impegni di Infor in relazione ai requisiti specifici previsti dalle direttive, dai regolamenti e dalle leggi nazionali di attuazione della normativa UE applicabili in materia di cybersecurity e data governance ("***Leggi Applicabili in Materia di Cybersecurity e Data Governance***") ed è incorporato, ove applicabile al Cliente (come disciplinato di seguito), negli accordi stipulati dal Cliente con Infor (collettivamente, gli "***Accordi***"). In caso di conflitto o incoerenza tra i termini del presente Allegato e qualsiasi altro termine degli Accordi, prevarrà il presente Allegato.

## I. DISPOSIZIONI GENERALI

### 1. DEFINIZIONI

1.1 I termini indicati con la lettera maiuscola, ma non definiti nel presente Allegato, hanno il significato ad essi attribuito nell'Information Security Plan, disponibile al seguente link: www.infor.com/security-plan (l'"ISP"). I termini "Processo TIC", "Prodotto TIC", "Servizio TIC", "Incidente", "Sistema Informativo e di Rete", "Rischio", e "Minaccia Informatica Significativa" avranno il significato ad essi attribuito dalle Leggi Applicabili in Materia di Cybersecurity e Data Governance.

### 2. RISPETTO DELLE LEGGI E COOPERAZIONE

2.1 Infor rispetterà le Leggi Applicabili in Materia di Cybersecurity e Data Governance applicabili al proprio business e, previa ragionevole richiesta, coopererà con tutte le rilevanti autorità competenti e/o con il Cliente in merito al rispetto da parte di Infor delle obbligazioni previste nell'Accordo ai sensi delle Leggi Applicabili in Materia di Cybersecurity e Data Governance. Infor e il Cliente si impegnano a informarsi reciprocamente nel caso di qualsiasi modifica significativa o evento, difficoltà, rischio o informazione che potrebbe avere un effetto avverso sui Servizi TIC o sull'esecuzione dell'Accordo (a meno che la condivisione di tali informazioni non sia vietata dalla Legge Applicabile).

### 3. DATA DI EFFICACIA

3.1 I termini del presente Allegato saranno efficaci a partire dalla data di entrata in vigore delle Leggi Applicabili in Materia di Cybersecurity e Data Governance.

### 4. AGGIORNAMENTI

4.1 Il Cliente riconosce che le misure di sicurezza tecnica e organizzativa descritte nel presente Allegato sono soggette ad aggiornamento dei requisiti previsti ai sensi delle Leggi Applicabili in Materia di Cybersecurity e Data Governance, nonché al progresso e allo sviluppo tecnico, e che Infor potrà aggiornare o modificare tali misure nel tempo, purché tali aggiornamenti e modifiche non risultino in un peggioramento della sicurezza complessiva dei servizi forniti al Cliente.

### 5. LEGGE APPLICABILE

5.1 Il presente Allegato è governato ed eseguito ai sensi della legge applicabile prevista dall'Accordo, a meno che le Leggi Applicabili in Materia di Cybersecurity e Data Governance non prevedano l'applicabilità di una legge differente, in tal caso, ai fini del presente Allegato, la legge applicabile ai sensi delle Leggi Applicabili in Materia di Cybersecurity e Data Governance prevarrà rispetto alla legge individuata nell'Accordo.

### 6. RESPONSABILITÀ

6.1 Infor e il Cliente concordano che la responsabilità massima di ciascuna parte e delle rispettive Affiliate (come definite nell'Accordo) derivante da o in connessione con il presente Allegato, sia per violazione contrattuale, illecito civile o altro, è soggetta, tra le parti (incluse le Affiliate), alle disposizioni applicabili sulla limitazione della responsabilità contenute nell'Accordo. Inoltre, Infor non sarà responsabile per eventuali violazioni da parte del Cliente delle Leggi Applicabili in Materia di Cybersecurity e Data Governance o per il mancato rispetto da parte del Cliente dei requisiti previsti dall'autorità competente.

## II. DIRETTIVA NIS 2

### 1. AMBITO DI APPLICAZIONE E DEFINIZIONI

1.1 I termini e le condizioni previsti dalla Sezione II del presente Allegato si applicano esclusivamente ai Clienti UE che soddisfino i criteri e le soglie per essere qualificati come enti "importanti" o "essenziali" ai sensi della Direttiva NIS2. A meri fini di chiarezza, la Sezione I si ritiene incorporata nella Sezione II.

1.2 "**NIS 2 Directive**" significa la Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

### 2. GOVERNANCE

2.1 Infor dispone di organi direttivi all'interno del proprio *security office* che approvano, supervisionano e sono responsabili dell'attuazione delle misure di gestione del rischio di cybersecurity di Infor, incluso il programma di sicurezza informatica.

### 3. PROGRAMMA DI SICUREZZA INFORMATICA

3.1 Infor ha implementato e manterrà un programma di sicurezza informatica che: (A) sia disegnato per: (1) garantire la sicurezza e la confidenzialità dei Sistemi Informativi e di Rete di Infor; (2) proteggere da ogni possibile minaccia o rischio per la sicurezza e la confidenzialità dei Sistemi Informativi e di Rete di Infor; e (3) proteggere da accessi non autorizzati ai, o usi dei, Sistemi Informativi e di Rete di Infor; and (B) stabilisca la policy di Infor per rispondere ad ogni Incidente.

3.2 Il programma di sicurezza informatica è disponibile al seguente link: www.infor.com/security-plan.

### 4. MISURE DI GESTIONE DEL RISCHIO CYBERSECURITY

4.1 Infor ha implementato e manterrà misure di gestione del rischio cybersecurity che:

(A) siano proporzionate ai rischi a cui sono esposti i Sistemi Informativi e di Rete di Infor tenuto conto dello stato dell'arte e, dove applicabili, degli standard internazionali ed europei, e del costo della loro implementazione;

(B) siano basati su un approccio "*all-hazards*", che ambisca a proteggere da Incidenti i Sistemi Informativi e di Rete di Infor e l'ambiente fisico di tali sistemi; e

(C) includano almeno (a) *policy* relative all'analisi del rischio e della sicurezza dei sistemi informativi; (b) misure volte ad identificare ogni rischio di Incidenti, incluse le procedure di gestione degli incidenti; (c) continuità operativa, quali la gestione dei backup e il *disaster recovery*, nonché la gestione delle crisi; (d) sicurezza della *supply chain*, inclusi gli aspetti in materia di sicurezza concernenti le relazioni tra Infor e i suoi fornitori diretti o appaltatori; (e) sicurezza nell'acquisizione, sviluppo e manutenzione dei Sistemi Informativi e di Rete, inclusa la gestione e divulgazione delle vulnerabilità; (f) *policy* e procedure volte a valutare l'efficacia delle misure di gestione del rischio cybersecurity adottate da Infor; (g) pratiche di base di pulizia informatica, come principi *zero-trust*, aggiornamenti software, configurazione dei dispositivi, segmentazione della rete, gestione delle identità e degli accessi o consapevolezza degli utenti, formazione sulla cybersicurezza per il personale con cadenza regolare e finalizzata ad aumentare la consapevolezza riguardo alle minacce informatiche, phishing o tecniche di ingegneria sociale; (h) *policy* e procedure relative all'uso della crittografia e della cifratura; (i) sicurezza delle risorse umane, protocolli di controllo degli accessi e gestione degli *assets*; e (j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, comunicazioni vocali, video e testuali sicure e sistemi di comunicazione d'emergenza sicuri internamente ad Infor.

### 5. SUPPLY CHAIN

5.1 Infor dichiara e garantisce che i sistemi di sicurezza della *supply chain* implementati da Infor terranno conto dei seguenti criteri: (a) le vulnerabilità specifiche di ognuno dei propri fornitori e appaltatori; (b) la qualità complessiva dei prodotti e delle pratiche di cybersecurity dei propri fornitori e appaltatori, incluse le loro procedure di sviluppo sicuro; e, ove applicabile, (c) i risultati di qualsiasi valutazione coordinata del rischio di

sicurezza delle specifiche catene di fornitura di Servizi TIC, Prodotti TIC o Processi TIC critici, effettuata dagli Stati Membri dell'UE e da qualsiasi autorità competente.

5.2 Infor effettua una due diligence sui propri fornitori di servizi terzi per valutare le loro misure di gestione del rischio di cybersecurity e stipula accordi con tali fornitori di servizi terzi che contengono requisiti di cybersecurity e data governance sostanzialmente simili a quelli del presente Allegato.

5.3 A seguito della richiesta del Cliente, Infor fornirà prova ragionevole di tali misure di sicurezza applicate alla propria supply chain entro un periodo di tempo ragionevole.

## 6. RISPOSTA AGLI INCIDENTI

6.1 Infor monitorerà che non vi siano accessi non autorizzati ai propri Sistemi Informativi e di Rete e implementerà una *policy* di risposta agli Incidenti che specifichi le azioni da intraprendere nel caso in cui Infor riscontri o venga a conoscenza di un Incidente.

6.2 Nel caso in cui Infor venisse a conoscenza di un Incidente Significativo che abbia un impatto sul Cliente, Infor dovrà:

(A) Notificare il Cliente come segue:

(1) Prontamente e senza ingiustificato ritardo (ed, in ogni caso, entro 24 ore dal momento in cui è venuto a conoscenza di tale Incidente Significativo): (a) informare il Cliente del verificarsi di tale Incidente Significativo; e (b) fornire al Cliente informazioni dettagliate in merito all'Incidente Significativo, incluse le seguenti: (i) se si sospetta che l'Incidente Significativo sia stato causato da azioni illegali o maligne o possa avere un impatto transfrontaliero; (ii) ogni informazione volta a determinare un eventuale impatto transfrontaliero dell'Incidente Significativo; e (iii) una valutazione iniziale dell'Incidente Significativo, incluso in termini di severità e impatto, nonché, quando disponibile, gli indicatori di compromesso;

(2) Prontamente e senza ingiustificato ritardo, fornire al Cliente le seguenti informazioni ulteriori in merito all'Incidente Significativo: (a) una descrizione dettagliata dell'Incidente Significativo, inclusa la sua severità e il suo impatto; (b) il tipo di minaccia o la causa principale che è probabile che abbia scatenato l'Incidente Significativo; (c) le misure di mitigazione applicate e in corso; e (d) ove applicabile, l'impatto transfrontaliero dell'Incidente Significativo.

(B) Investigare e condurre una ragionevole analisi della causa (o delle cause) di tale Incidente Significativo;

(C) Fornire al Cliente aggiornamenti periodici relativi a ogni investigazione in corso;

(D) Sviluppare e implementare un piano appropriato per mitigare la, e porre rimedio alla, causa di tale Incidente Significativo, nel limite in cui tale causa fosse sotto il controllo di Infor; e

(E) Collaborare, se ragionevole, con l'indagine del Cliente e con gli sforzi del Cliente per conformarsi a qualsiasi notifica relativa a tale Incidente Significativo, inclusa l'assistenza nella redazione di eventuali report sull'Incidente Significativo per le autorità competenti.

6.3 Se Infor dovesse venire a conoscenza di una Minaccia Informatica Significativa che abbia un impatto sul Cliente (incuse le vulnerabilità delle applicazioni Infor che rientrino nella definizione di Minaccia Informatica Significativa), Infor dovrà:

(A) Prontamente e senza indugio informare il Cliente di tale Minaccia Informatica Significativa;

(B) Fornire al Cliente informazioni dettagliate in merito all'impatto della Minaccia Informatica Significativa rispetto al Cliente, per quanto note ad Infor;

(C) Investigare e condurre una ragionevole analisi della causa (o delle cause) di tale Minaccia Informatica Significativa;

(D) Sviluppare e implementare un piano appropriato per mitigare la, e porre rimedio alla, causa di tale Minaccia Informatica Significativa, nel limite in cui tale Minaccia Informatica Significativa si avveri e la causa fosse sotto il controllo di Infor; e

(E) Conformarsi alle richieste ragionevoli del Cliente di fornire informazioni sulla Minaccia Informatica Significativa che il Cliente deve includere nelle notifiche obbligatorie a terzi relative alla Minaccia Informatica Significativa, nel caso in cui fossero richieste ai sensi delle Leggi Applicabili in Materia di Cybersecurity e Data Governance.

## 7. AUDIT

7.1 Infor dovrà acquisire e mantenere almeno una delle seguenti certificazioni e attestazioni relative ai suoi Servizi Cloud (se applicabile) e, su richiesta scritta del Cliente, dovrà fornire al Cliente prova di tali certificazioni e/o attestazioni:

(1) SSAE SOC 2 Type 2 (anche conosciuta come AICPA TSC 2014 Type 2)
(2) ISO 27001:2022
(3) FedRAMP

Infor dovrà assicurarsi che i propri fornitori di servizi terzi acquisiscano o mantengano almeno una delle suddette certificazioni e attestazioni relative ai servizi che tali fornitori terzi forniscono ad Infor e/o ai suoi clienti, o fornire un'alternativa soddisfacente che dimostri le misure di gestione del rischio di cybersecurity intraprese in relazione alla natura dei servizi forniti.

7.2 In aggiunta ai report di audit descritti nella Sezione 7.1. di cui sopra, se richiesto dal Cliente e nel rispetto degli obblighi di confidenzialità previsti nell'Accordo, non più di una volta all'anno, a meno che il Cliente non agisca in virtù di una richiesta dell'autorità competente (in tal caso, non troveranno applicazione i limiti annuali), Infor fornirà prontamente risposta scritta a ogni ragionevole domanda o questionario del Cliente (e/o dei suoi rappresentanti) relativi al contenuto del programma di sicurezza di Infor e fornirà ragionevole prova della loro conformità ai requisiti del presente Allegato, incluse copie generalmente disponibili di dati, documenti e informazioni relative ai Servizi necessari per supportare il Cliente nel rispettare qualsiasi richiesta vincolante o ordine ricevuto da un'autorità competente. Infor fornirà le informazioni pertinenti senza indebito ritardo (e, in ogni caso, entro il termine previsto nella richiesta vincolante o nell'ordine ricevuto dal Cliente dall'autorità competente).

7.3 Il Cliente può, una volta all'anno, verificare la conformità di Infor ai propri obblighi previsti da questo Allegato, inclusa la verifica delle pratiche di sicurezza IT di Infor e degli ambienti di controllo applicabili, in conformità con il processo descritto nella Sezione 7, solo se:

(A) Infor non abbia fornito prova sufficiente del proprio rispetto delle misure di gestione del rischio di cybersecurity descritte nel presente Allegato tramite i report e la documentazione di cui alla precedente Sezione 7.2, o, ove applicabile, ogni altro report di audit o altra informazione che Infor renda generalmente disponibile ai propri clienti;

(B) Abbia avuto luogo un Incidente Significativo;

(C) Infor abbia informato il Cliente di essere soggetta a una richiesta di accesso da parte di un'autorità relativa ai Dati del Cliente;

(D) Un audit sia stato formalmente richiesto da un'autorità competente con giurisdizione sul Cliente; oppure

(E) Una delle Leggi Applicabili in Materia di Cybersecurity e Data Governance non derogabili abbia conferito al Cliente un diritto diretto di audit.

7.4 Prima dell'inizio di un audit, il Cliente e Infor ne concorderanno l'ambito, le tempistiche, la durata, il controllo e i requisiti di prova. Il Cliente potrà utilizzare una società di audit indipendente accreditata per eseguire l'audit per suo conto, a condizione che l'auditor di terza parte sia concordato dalle parti (e che non sia un concorrente di Infor o non sia adeguatamente qualificato o indipendente). Il Cliente accetta che l'audit venga condotto senza interferire in modo irragionevole con le attività aziendali di Infor (o dei suoi subappaltatori), durante l'orario lavorativo regolare e con ragionevole preavviso, e nel rispetto delle politiche di sicurezza e delle procedure di riservatezza applicabili di Infor (o dei suoi subappaltatori). Qualora non fosse consentito effettuare audit *in loco* di data center, sistemi o strutture fisiche, Infor lavorerà con il Cliente (e i suoi subappaltatori, se applicabile) per raggiungere una soluzione reciprocamente accettabile, sufficiente a fornire le informazioni necessarie affinché il Cliente possa ottemperare ai requisiti dell'audit previsti dalle Leggi Applicabili in Materia di Cybersecurity e Data Governance. Né il Cliente né l'auditor avranno accesso ai dati degli altri clienti di Infor o ai sistemi o alle strutture di Infor non coinvolti nei Servizi forniti al Cliente. Il Cliente fornirà i risultati di qualsiasi audit ad Infor. Le parti si

accorderanno su eventuali rapporti o azioni correttive. Infor si impegna a fare sforzi commercialmente ragionevoli per approntare le azioni correttive concordate.

7.5 Il Cliente è responsabile di ogni costo e spesa relativa all'audit, inclusi tutti i costi e le spese ragionevolmente sostenute da Infor in relazione all'audit ed ogni costo e spesa sostenuta da Infor per qualsiasi subappaltatore qualora l'audit coinvolga un subappaltatore, salvo che tale audit non rilevi una violazione sostanziale da parte di Infor del presente Allegato, in tal caso Infor sopporterà le proprie spese relative alla parte dell'audit connessa alla violazione.

## III. DORA

### 1. AMBITO DI APPLICAZIONE E DEFINIZIONI

1.1 I termini e le condizioni previsti nella Sezione III del presente Allegato si applicano esclusivamente ai Clienti UE che soddisfano i criteri e le soglie per le entità finanziarie regolamentate dal DORA. A meri fini di chiarezza, la Sezione I si ritiene incorporata nella Sezione III; inoltre, nel caso in cui ne venga fatto esplicito riferimento, si applicheranno anche specifici paragrafi contenuti nella Sezione II.

1.2 "**DORA**" significa il Digital Operational Resilience Act (Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022).

### 2. SERVIZI

2.1 I Servizi TIC forniti da Infor al Cliente sono descritti nell'Accordo.

### 3. LOCATION

3.1 A meri fini di chiarezza, i dati di produzione del Cliente sono archiviati nella località di installazione selezionata e Infor non sposterà nessuno dei dati di produzione del Cliente al di fuori di questa località senza il previo consenso scritto e indicazione del Cliente. Su indicazione del Cliente, una quantità limitata di dati personali potrà essere accessibile a distanza al di fuori della località di installazione selezionata per fornire supporto e servizi al Cliente. Infor dovrà informare il Cliente in anticipo se prevede di modificare le località (cioè le regioni o i paesi) in cui i Servizi saranno forniti e in cui i Dati del Cliente saranno archiviati e trattati, come previsto nell'Accordo.

### 4. PROGRAMMA DI SICUREZZA E SLA

4.1 Si applicano le misure di gestione del rischio di *cybersecurity* di cui alle precedenti Sezioni II.3 e II.4. Troveranno inoltre applicazione gli impegni assunti da Infor in materia di risposta agli incidenti. A meri fini di chiarezza, il caso di messa in liquidazione di Infor è una delle cause che obbligano Infor a restituire al Cliente i Dati del Cliente ai sensi del programma di sicurezza informatica.

4.2 Gli impegni di disponibilità del livello di servizio di Infor sono descritti Service Level Agreement disponibile al seguente link: https://www.infor.com/service-level-description ("SLA"). Gli impegni di supporto specifici per ciascun prodotto sono descritti nel Modulo d'Ordine, se applicabile.

### 5. *ICT SECURITY TRAINING* E PROGRAMMI DI AWARENESS

5.1 Nel caso in cui Infor acceda ai sistemi informatici di rete *on-premise* del Cliente come parte dei Servizi, il Cliente può richiedere, previo ragionevole preavviso, ad Infor di partecipare a qualsiasi programma di sensibilizzazione alla sicurezza ICT e/o formazione sulla resilienza operativa digitale che il Cliente fornisce o gestisce in relazione alla propria attività ("Training"). A tal proposito, le parti concordano che:

(A) La frequenza, le tempistiche e la durata di tale Training saranno concordati anticipatamente tra le parti; e

(B) Infor si riserva il diritto di richiedere al Cliente il rimborso delle spese ragionevoli e correttamente sostenute; e

(C) La partecipazione di Infor a tali Training non richiederà a Infor di compiere alcuna azione che possa interferire, prevenire o ostacolare Infor nel fornire i Servizi TIC o nell'adempiere alle sue obbligazioni ai sensi dell'Accordo.

## 6. RISOLUZIONE

6.1 In aggiunta alle ipotesi di risoluzione dell'Accordo ivi previste o disciplinati altrove nei presenti termini e condizioni, come previsto dall'Art. 28 Sezione 7 DORA e ferma restando la procedura prevista nell'Accordo per il caso di cessazione degli effetti dell'Accordo, il Cliente può risolvere l'Accordo, in tutto o in parte, esclusivamente nei seguenti casi: (i) Infor non abbia sanato una violazione significativa delle Leggi Applicabili in Materia di Cybersecurity e Data Governance o di questo Allegato, (ii) il Cliente identifichi circostanze che si ritengono capaci di alterare l'esecuzione dei Servizi TIC da parte di Infor, inclusi cambiamenti sostanziali che incidono sull'Accordo o sullo status di Infor come fornitore, (iii) vengano riscontrate debolezze relative alla gestione complessiva del rischio ICT di Infor e in particolare nel modo in cui Infor garantisce la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, sia che si tratti di dati personali o di altri dati sensibili, o di dati non personali, oppure (iv) se l'autorità competente non possa più supervisionare efficacemente il Cliente a causa delle condizioni o delle circostanze relative a Infor o all'Accordo.

## 7. RAPPORTI CON LE AUTORITÀ COMPENTENTI

7.1 Infor garantisce piena collaborazione con le autorità competenti e le autorità di risoluzione delle crisi del Cliente, inclusi le persone da esse nominati.