Accordo sull'affidamento del trattamento dei dati a un responsabile

in relazione all'amministrazione fiduciaria di cartelle ipotecarie registrali (Nominee) e della liquidità in cambio di garanzie ipotecarie (LCGI)

per Credit Servicer

tra

_____ (di seguito «**partecipante**»)

_____

_____

(IDI: CHE-_____)

e

SIX SIS SA (di seguito «**SIX SIS**»)
Baslerstrasse 100
4601 Olten
(IDI: CHE-106.842.854)

e

SIX Terravis SA (di seguito «**SIX Terravis**»)
Hardturmstrasse 201
8005 Zurigo
(IDI: CHE-114.332.360)

(SIX SIS e SIX Terravis, qui di seguito denominate congiuntamente «**SIX**»)
(congiuntamente le «**parti**»)

1. Dichiarazione

Le parti riconoscono reciprocamente il loro interesse e la capacità giuridica necessaria per concludere il presente accordo. Dichiarano inoltre che

- il partecipante ha incaricato SIX della fornitura dei servizi Terravis-Nominee ai sensi del «Contratto di partecipazione concernente l'amministrazione fiduciaria di cartelle ipotecarie registrali per Credit Servicer» **(contratto di partecipazione Nominee**); e Terravis-LCGI ai sensi del «Contratto di partecipazione Terravis-LCGI» **(contratto di partecipazione LCGI**, congiuntamente i **contratti di partecipazione**) (Terravis-Nominee e Terravis-LCGI), congiuntamente i **servizi**;

- al fine di fornire i servizi sono trattati dati personali, di cui il partecipante è responsabile;

- gli obblighi delle parti in materia di protezione dei dati devono essere regolati sulla base delle seguenti leggi:

    - 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 **(GDPR**);
    - Legge federale sulla protezione dei dati (**LPD**);
    - Ordinanza svizzera sulla legge federale sulla protezione dei dati **(OPDa**).

- Sulla base di quanto sopra, le parti stipulano il presente accordo sull'affidamento del trattamento dei dati a un responsabile **(accordo**). Esso disciplina il trattamento dei dati personali da parte di SIX in relazione ai contratti di partecipazione.

Ai sensi dell'art. 28 GDPR e dell'art. 9 LPD, si applicano le seguenti disposizioni.

2. Scopo dell'accordo

Il presente accordo ha lo scopo di disciplinare la protezione dei dati personali di cui il partecipante è responsabile **(dati personali**) e, in particolare, il loro trattamento da parte di SIX ai sensi dell'Allegato 1 nell'ambito dei contratti di partecipazione.

3. Obblighi di SIX

SIX dichiara e garantisce in qualità di responsabile del trattamento dei dati ai sensi dell'art. 28 GDPR e dell'art. 9 LPD

- di aver attuato le misure organizzative, tecniche e di sicurezza specificate nell'Allegato 2.

- di utilizzare i dati personali esclusivamente in relazione ai contratti di partecipazione e, in nessun caso, per scopi propri. SIX tratterà i dati personali in conformità alle istruzioni del partecipante; SIX è inoltre tenuta a informare il partecipante se ritiene che un'istruzione violi la legge sulla protezione dei dati o altre norme giuridiche applicabili. SIX non si assume alcuna responsabilità

per le istruzioni impartite dal partecipante che violano la legge sulla protezione dei dati o altre norme giuridiche applicabili. SIX informerà il partecipante se l'osservanza di un'istruzione potrebbe impedire od ostacolare la fornitura di servizi, attualmente o in futuro.

- di non trasmettere o divulgare i dati personali a terzi e di non consentire a terzi l'accesso agli stessi.

- di non trasferire i dati personali in Paesi con un livello di protezione dei dati inadeguato. Fanno eccezione i casi in cui vi sia il previo consenso scritto del partecipante o la trasmissione sia debitamente autorizzata.

- di informare per iscritto il partecipante immediatamente dopo essere venuta a conoscenza di una violazione dei dati personali. Se possibile, questa notifica contenere le seguenti informazioni:

  (i) descrizione della natura e della portata dell'incidente, compresa la categoria e il numero approssimativo di persone e dati interessati.

  (ii) nome e dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto da cui è possibile ottenere ulteriori informazioni.

  (iii) possibili conseguenze dannose di un accesso non autorizzato.

  (iv) Descrizione delle misure adottate da SIX per attenuare potenziali conseguenze negative.

  Se SIX non è in grado di trasmettere queste informazioni contemporaneamente, le renderà disponibili gradualmente e nel più breve tempo possibile.

- di tenere un registro del trattamento dei dati effettuato per conto del partecipante, contenente le informazioni di cui all'art. 30 cpv. 2 GDPR e all'art. 12 LPD.

- al ricevimento di una richiesta da parte di terzi per (i) l'accesso, (ii) la rettifica, (iii) la cancellazione, (iv) la trasmissione e/o (v) l'opposizione al trattamento dei dati personali, o (vi) la limitazione del trattamento,

- di inoltrare senza indugio la richiesta al partecipante affinché questi possa rispondere entro i termini di legge.

- di disporre di un responsabile della protezione dei dati ai sensi del GDPR o di un consulente per la protezione dei dati ai sensi della LPD, i cui dati di contatto sono riportati nell'Allegato 3 del presente accordo.

- di supportare il partecipante in modo appropriato con valutazioni sulle conseguenze e analisi dei rischi derivanti dal trattamento dei dati.

- di sostenere il partecipante in modo appropriato e, se necessario, anche nella consultazione delle autorità di vigilanza.

- di fornire al partecipante la prova dell'adempimento dei suoi obblighi ai sensi del presente accordo.

- di assistere adeguatamente il partecipante nella gestione e nella risposta alle richieste di esercizio del diritto di accesso, rettifica, cancellazione, opposizione, limitazione del trattamento e/o portabilità dei dati che SIX può ricevere da persone interessate, entro termini ragionevoli e con un preavviso sufficiente a consentire al partecipante di rispettare i termini legalmente applicabili in relazione ai suddetti diritti.

- di garantire che le persone che hanno accesso ai dati personali ricevano una formazione adeguata sulla protezione di tali dati.

4. Regola di conflitto di leggi

Il presente accordo integra i contratti dei partecipanti.

Le parti concordano il seguente chiarimento e la seguente regola di conflitto di leggi:

le disposizioni del presente accordo prevalgono su qualsiasi disposizione dei contratti dei partecipanti in materia di affidamento del trattamento dei dati a un responsabile.

5. Audit

Il partecipante monitora il trattamento dei dati personali e può effettuare audit o ispezioni a proprie spese, rimborsando a SIX i costi che ne derivano.

SIX consente audit e ispezioni da parte del partecipante e vi partecipa attivamente nell'ambito delle consuete possibilità operative, di personale e di altri aspetti operativi.

Gli audit e le ispezioni vengono effettuati da SIX, che raccoglie le informazioni e le mette a disposizione del partecipante, sempre a spese di quest'ultimo.

Il partecipante si impegna a dare un preavviso di almeno 20 giorni lavorativi in caso di audit o ispezione. Garantisce inoltre che questi saranno eseguiti in conformità agli standard, ai protocolli e alle procedure di lavoro di SIX.

6. Rapporti di subappalto

SIX può esternalizzare l'elaborazione dei dati a società del Gruppo SIX e a terzi. A tal fine, obbliga tali società a rispettare le disposizioni del presente accordo in relazione al trattamento dei dati personali.

Se è necessario subappaltare parti della fornitura di servizi a terzi, SIX ne informa preventivamente il partecipante per iscritto. La comunicazione deve includere i settori subappaltati e le informazioni sul subincaricato (società e dati di contatto). Ciò non pregiudica i servizi accessori che SIX SIS e/o SIX Terravis possono subappaltare indipendentemente dai servizi per le operazioni regolari.

Il partecipante può rifiutare il ricorso a un subappalto entro 5 giorni lavorativi **(rifiuto**). Se il partecipante non lo rifiuta entro tale termine, il subappalto si considera approvato. Il partecipante è tenuto a giustificare il rifiuto, per cui può rifiutare i subappalti solo per motivi importanti. In caso di rifiuto, SIX ha il diritto di disdire i contratti di partecipazione, compreso il presente accordo, con un preavviso di 60 giorni di calendario per la fine di un mese civile.

Nei confronti del partecipante, SIX è inoltre tenuta a rispettare le disposizioni del presente accordo qualora il suo subincaricato non le rispetti.

Con la presente, il partecipante concede a SIX un'autorizzazione generale scritta a ricorrere ai subincaricati elencati nell'allegato 4 (elenco dei subincaricati).

7. Riservatezza e sicurezza dei dati personali

SIX si impegna a trattare con riservatezza tutti i dati personali raccolti nell'ambito dei servizi e a rispettare l'obbligo di riservatezza.

SIX SIS e SIX Terravis autorizzano al trattamento dei dati personali solo i collaboratori che si sono espressamente impegnati per iscritto a mantenere la riservatezza e a rispettare le relative misure di sicurezza.

8. Durata

Il presente accordo ha la stessa durata degli accordi dei partecipanti e dei relativi allegati e accordi integrativi.

Al termine del presente accordo, SIX si impegna a distruggere i dati personali a cui ha avuto accesso, nonché i documenti o i supporti di dati in cui tali dati possono essere contenuti, oppure li restituirà al partecipante. In particolare, SIX è tenuta a restituire o distruggere:

(i) dati contenuti nei file di cui il partecipante è responsabile in relazione ai servizi;

(ii) dati appartenenti al partecipante e che SIX può aver generato nell'ambito del trattamento dei dati e

(iii) tutti i supporti o documenti in cui sono salvati questi dati.

I dati non saranno distrutti se esiste un obbligo legale di conservazione; in questo caso SIX restituirà i dati personali secondo le indicazioni del partecipante. I dati relativi a situazioni di emergenza vengono inoltre archiviati in conformità al contratto di partecipazione Terravis-LCGI.

Su richiesta del partecipante, SIX rilascia un certificato che conferma la corretta e completa distruzione dei dati personali.

9. Informazioni sulla protezione dei dati

Le parti si tengono reciprocamente informate sul trattamento dei dati personali dei firmatari del presente accordo, delle persone di contatto e di altre parti coinvolte (**dati personali**), i cui dati sono necessari per la corretta erogazione del servizio.

Lo scopo del trattamento è quello di gestire e mantenere il rapporto tra le parti fintantoché il trattamento dei dati personali è necessario per l'esecuzione del presente accordo.

I dati personali vengono conservati per la durata del rapporto contrattuale e, successivamente, per i periodi in cui è possibile far valere una responsabilità legale.

I dati personali non saranno trasmessi a terzi e non saranno oggetto di trasferimento all'estero, a meno che non vi sia un obbligo legale in tal senso o ciò si renda necessario per l'adempimento del presente accordo. Questa disposizione non si applica alla trasmissione dei dati personali alla Banca nazionale svizzera (BNS) in conformità con il contratto di partecipazione Nominee-LCGI.

Nonostante quanto sopra esposto, le parti potranno, sulla base del legittimo interesse e ai fini della corretta gestione e del mantenimento del rapporto contrattuale, trasmettere i dati personali alle società dei rispettivi gruppi. Se la comunicazione di questi dati personali implica un trasferimento all'estero di dati, le parti contraenti si impegnano a rispettare le condizioni previste dalle leggi e dalle disposizioni applicabili al fine di garantire la corretta protezione dei dati.

Le persone interessate possono esercitare i propri diritti di accesso, rettifica, cancellazione, portabilità e limitazione del trattamento contattando il responsabile della protezione dei dati dell'altra parte (dati di contatto nell'Allegato 3).

Le parti si impegnano a rendere disponibili le informazioni contenute nella presente clausola a tutti i dipendenti o alle persone di contatto della propria impresa i cui dati personali vengono comunicati all'altra parte nell'ambito della fornitura del servizio.

10. Foro competente e diritto applicabile

Il presente accordo è assoggettato al diritto svizzero. Il foro competente è Zurigo.

Le persone aventi dritto di firma delle parti hanno debitamente sottoscritto il presente accordo con i relativi allegati e le appendici.

_____

_____

_____ _____

Olten,
SIX SIS SA

_____ _____

Zurigo,
SIX Terravis SA

_____ _____

Walter Berli
Direttore

Raphael Fuchs
Membro della Direzione

ALLEGATO 1

DETTAGLI SULL'AFFIDAMENTO DEL TRATTAMENTO DEI DATI A UN RESPONSABILE

A. Parti e ruoli

Responsabile:

Nome:	
Indirizzo:	
Nome, funzione e dati di contatto della persona di riferimento:	

Responsabile del trattamento dei dati:

Nome:	SIX SIS SA
Indirizzo:	Baslerstrasse 100, 4601 Olten
Nome, funzione e dati di contatto della persona di riferimento:	Raphael Fuchs, vicedirettore generale di SIX Terravis SA raphael.fuchs2@six-group.com

B. Descrizione del trattamento dei dati

Categorie di persone interessate:	Persone fisiche e giuridiche (proprietari di fondi, debitori ipotecari).
Categorie di dati personali:	Nome, sesso, indirizzo, data di nascita, luogo di origine/cittadinanza, forma societaria, sede legale, IDI.
Dati personali sensibili trattati (se applicabile) e applicazione di restrizioni o garanzie che tengano pienamente conto della natura dei dati e dei rischi connessi, come ad esempio una rigorosa limitazione delle finalità, le restrizioni di accesso (compreso l'accesso solo al	Non vengono trattati dati personali particolarmente sensibili. Restrizione dell'accesso elettronico, attribuzione dei diritti secondo il principio «need to know» a collaboratori appositamente formati.

personale che ha seguito una formazione specifica), la tenuta di un registro d'accesso ai dati, le restrizioni applicabili ai trasferimenti successivi o le misure di sicurezza aggiuntive.	
Frequenza del trattamento dei dati (una volta, più volte nel corso della durata del contratto, regolarmente).	Più volte nel corso della durata del contratto.
Natura del trattamento dei dati.	Raggruppamento dei dati contenuti in ordini, contratti di pegno, cambio di creditori o promesse di pagamento nell'ambito di transazioni notarili o del registro fondiario o di trasferimenti ipotecari. Allestimento delle dichiarazioni di cessione e retrocessione e degli elenchi di portafoglio all'attenzione della BNS nell'ambito dei pool ipotecari LCGI.
Finalità del trattamento dei dati, eventuali ulteriori trattamenti dei dati:	Adempimento dei contratti di partecipazione.
Periodo di conservazione o, se non può essere determinato in anticipo, criteri per determinare il periodo di conservazione.	20 anni
Per il trattamento dei dati da parte di subincaricati: oggetto, natura e durata del trattamento dei dati.	In modo analogo all'elaborazione dei dati da parte del responsabile del trattamento dei dati.

ALLEGATO 2

MISURE ORGANIZZATIVE E TECNICHE PER GARANTIRE LA SICUREZZA DEI DATI

SIX attuerà misure atte a:

a) assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione;
b) ripristinare rapidamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
c) verificare, analizzare e valutare regolarmente l'efficacia delle misure tecniche e organizzative implementate per garantire la sicurezza del trattamento dei dati;
d) pseudonomizzare e criptare i dati personali, se necessario.

Le parti convengono che le misure previste dal presente allegato garantiscono un livello di sicurezza adeguato al rischio esistente.

1	**Riservatezza (articolo 32 GDPR / articolo 3.1 LPD)**
1.1	**Misure per prevenire l'accesso fisico non autorizzato**
☒	Strutture, edifici e locali sono protetti dall'accesso non autorizzato mediante barriere, pareti antieffrazione, finestre inferriate o simili.
☒	Le strutture e gli edifici sono monitorati tramite videosorveglianza, bande magnetiche di sicurezza, sensori antieffrazione o altre misure tecniche od organizzative.
☒	I documenti di identità vengono controllati dal personale di sicurezza.
☒	L'accesso fisico è consentito solo alle persone autorizzate, previa verifica della loro identità. Il controllo dei documenti di identità, delle schede d'accesso personalizzate e delle presenze registrate con un lettore di carta chip avviene in modo automatizzato.
☒	L'accesso viene registrato automaticamente.
☒	L'accesso fisico è concesso sulla base di una procedura di autorizzazione.
☒	L'hardware, il server e i componenti dei sistemi di elaborazione dati sono collocati in locali separati dai normali uffici.
☒	L'hardware, il server e i componenti dei sistemi di elaborazione dati sono situati in locali separati dai normali uffici e sono protetti in modo speciale contro l'accesso fisico non autorizzato.
1.2	**Misure di controllo dell'accesso logico**
☒	L'autorizzazione all'accesso logico viene concessa sulla base di una procedura di autorizzazione (attribuzione del nome utente e della password iniziale).
☒	L'accesso logico viene concesso dopo il login, compresa l'autenticazione (nome utente, password o dispositivo token).

☒	L’accesso ai sistemi di elaborazione delle informazioni, ai PC e alle postazioni di lavoro sul posto di lavoro viene documentato (ad es. file di log).
☒	Gli utenti possono bloccare la propria sessione per evitare un uso non autorizzato utilizzando un salvaschermo protetto da password. Le sessioni possono essere temporaneamente sospese.
☒	Le sessioni inattive vengono interrotte automaticamente dopo un determinato periodo di attesa.
☒	Le sessioni attive sono protette contro l’appropriazione indebita da parte di altri utenti.
☒	I tentativi di accesso non autorizzati vengono rilevati (intrusion detection) e provocano una reazione.
☒	Prima del lancio, i sistemi vengono rafforzati secondo le procedure definite.
☒	Esistono misure di sicurezza per le password (cambio regolare delle password, cronologia delle password, divieto di password banali e di archiviazione scritta delle password).
1.3	**Misure di controllo dell’accesso ai dati**
☒	Le autorizzazioni di accesso vengono concesse agli utenti in base ai principi «need to know» e «need to do», secondo una procedura di autorizzazione (ad esempio, i diritti di accesso definiti vengono assegnati separatamente).
☒	Gli utenti possono utilizzare solo i dati personali per i quali possiedono un’autorizzazione di accesso (in base all’attribuzione dei ruoli, utenti funzionali, ecc.)
☒	I tentativi di accesso da parte di persone non autorizzate vengono rilevati (ad es. registro di utilizzo del sistema) e valutati di conseguenza.
2.	**Integrità (articolo 32 GDPR / articolo 3.2 LPD)**
2.1	**Misure di controllo della trasmissione dei dati**
☒	I dati vengono criptati durante la trasmissione elettronica.
☒	I dati vengono trasmessi attraverso reti protette. Le reti esterne sono utilizzate esclusivamente con misure di sicurezza (VPN, linee dedicate).
☒	Il meccanismo di filtraggio impedisce l’accumulo di connessioni da e verso sistemi non autorizzati o indesiderati (tramite firewall).
☒	I supporti con i dati personali sono protetti durante il trasporto per evitare accessi non autorizzati, danni o perdite.
☒	I dati personali vengono memorizzati in forma criptata sui supporti di dati (chiavette o nastri USB).
☒	I supporti con i dati vengono smaltiti nel rispetto delle norme sulla protezione dei dati.
☒	I supporti con i dati vengono smaltiti in conformità alle norme sulla protezione dei dati o vengono smaltiti professionalmente da una società di smaltimento specializzata.
☒	I documenti cartacei vengono smaltiti tramite un distruggidocumenti o una società di smaltimento specializzata.
2.2	**Misure per il controllo dell’inserimento dati**
☒	L’inserimento, la modifica o la cancellazione dei dati vengono registrati in modo tale da poter identificare l’ora, l’autore e il contenuto della modifica.

☒	Le attività rilevanti dell'utente vengono registrate (login, orario e modifica del contenuto).
☒	I sistemi di gestione dei log analizzano i dati registrati.
3.	**Disponibilità (articolo 32 GDPR / articolo 3.2 LPD)**
☒	I componenti hardware del sistema sono protetti contro la rimozione fisica non autorizzata (furto).
☒	I dati vengono smaltiti solo dopo i periodi di conservazione predefiniti.
☒	Vengono create copie di sicurezza che possono essere utilizzate in caso di perdita dei dati originali.
☒	La capacità di ripristinare i dati originali viene verificata regolarmente.
☒	Le copie di sicurezza vengono archiviate separatamente dai dati originali.
☒	La sicurezza contro i guasti è garantita dall'uso di tecnologie RAID (p.es. duplicazione dei dischi rigidi).
☒	Un gruppo di continuità (UPS) garantisce il mantenimento delle operazioni in qualsiasi momento in caso di interruzioni temporanee di corrente.
☒	In caso di emergenza, l'hardware e il software necessari sono disponibili e pronti all'uso, in modo che i dati originali possano essere ripristinati utilizzando le apparecchiature di back-up.
4.	**Misure per la revisione e la verifica periodiche (art. 32 GDPR / art. 3.2 LPD)**
☒	Gestione della protezione dei dati
☒	Gestione delle risposte agli incidenti di sicurezza
☒	Protezione dei dati attraverso la tecnologia e impostazioni predefinite per la protezione dei dati personali
☒	Verifica dell'ordine o del contratto

ALLEGATO 3

Dati di contatto dei responsabili della protezione dei dati delle parti

Per la persona responsabile:

Per il responsabile del trattamento dei dati:

SIX Group Services Ltd.,
Data Protection Officer,
Hardturmstrasse 201,
8005 Zurich, Switzerland,
E-mail: dataprotection@six-group.com

ALLEGATO 4

ELENCO DEI SUBINCARICATI AUTORIZZATI

Subincaricato ulteriore	**Servizio fornito**	**Sede del subincaricato ulteriore**
SIX Group Services SA	Infrastruttura tecnica di base	Zurigo
InnoQ AG	Sviluppo software (in body leasing presso SIX Terravis con postazioni di lavoro SIX)	Cham