CONDIZIONI GENERALI

DEFINIZIONI

Le presenti condizioni generali (di seguito definite le "Condizioni Generali") disciplinano i termini e condizioni della licenza d'uso di software concessa al cliente (il "Cliente") dal Fornitore, come di seguito definito, nonché la fornitura al Cliente dei Software, servizi di aggiornamento, assistenza e manutenzione su installazioni *on premises* o Cloud come descritto nell'Allegato commerciale (i "Servizi"). Per "Fornitore" si intende, alternativamente, uno dei seguenti soggetti:

(i) Sigma Sistemi Srl, con sede legale in Bari (BA), via Don Guanella 15-B, codice fiscale e partita IVA n. 03925490728 ("SigmaSistemi"); oppure
(ii) la società appartenente al gruppo facente capo a SigmaSistemi e indicata nell'Ordine; oppure
(iii) il distributore ufficiale SigmaSistemi indicato nell'Ordine.

Nelle presenti condizioni generali di contratto (le "**Condizioni Generali**"), i termini e le espressioni di seguito elencati, quando riportati con iniziale maiuscola, devono intendersi con il significato ad essi attribuito nel presente paragrafo.
I termini indicati al singolare si intendono anche al plurale e viceversa.

Aggiornamenti e Sviluppi: significa tutti gli aggiornamenti, supplementi, adattamenti, sviluppi, migliorie e modifiche in genere apportate da SigmaSistemi e/o da terzi titolari ai Software. Gli Aggiornamenti e Sviluppi non comprendono quelli resi necessari dalla modifica, integrazione, abrogazione o emissione di leggi, decreti, regolamenti, direttive, ordini o decisioni, italiani, comunitari o stranieri che, a insindacabile giudizio del produttore, abbiano un impatto significativo sull'operatività e/o sui costi e/o sulla struttura dei Software o apportino modifiche sostanziali o strutturali alla normativa in vigore alla data del Contratto.
Assistenza: significa il servizio di supporto tecnico volto a suggerire al Cliente, su richiesta di quest'ultimo e laddove possibile, soluzioni tecniche per assicurare la corretta fruizione dei Servizi Cloud.
Cliente: significa la persona fisica o giuridica indicata nell'Ordine.
Codice Etico: significa il codice etico adottato da SigmaSistemi e consultabile al sito http://www.sigmasistemi.com/s.php/2/Azienda.html
Comunicazione di Ritiro: ha il significato di cui al paragrafo 12.1(b).
Condizioni Integrative: significa le autonome condizioni contrattuali disciplinanti la fornitura, da parte di SigmaSistemi, di determinati specifici Servizi Cloud le quali prevarranno sulle Condizioni Generali.
Connettività: significa la connessione al Data Center effettuata dal Cliente mediante collegamento a una rete di telecomunicazioni o a internet.
Contratto: significa le presenti Condizioni Generali, i relativi allegati, le Condizioni Integrative, l'Ordine, la documentazione tecnica eventualmente consegnata al Cliente, gli eventuali moduli di sottoscrizione e le eventuali istruzioni *online* per l'utilizzo dei Software.
Controllate: significa le società direttamente o indirettamente controllate dal Cliente ai sensi dell'art. 2359, primo comma, numeri 1 e 2, c.c. eventualmente elencate nell'Ordine.
Corrispettivi: significa le somme, indicate nell'Ordine, che il Cliente corrisponderà a SigmaSistemi o, se diversamente indicato nell'Ordine, al Distributore TS, in ragione della fornitura dei Servizi Cloud.
Credenziali di Accesso: significa il sistema di autenticazione attraverso il quale è possibile accedere e utilizzare il Software per fruire dei Servizi Cloud, inclusi i codici di identificazione e le chiavi di accesso forniti da SigmaSistemi al Cliente ed associati a ciascun Utente e gli eventuali *token*.
Data Center: significa i centri servizi che ospitano i *server* interconnessi, di proprietà di SigmaSistemi o di terzi, sui quali risiede l'Infrastruttura Cloud.
Distributore: significa il soggetto che, in virtù di un valido contratto sottoscritto con SigmaSistemi, ha il diritto di commercializzare i Servizi Cloud.
GDPR: indica il Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679.
Gruppo SigmaSistemi: indica SigmaSistemi Srl (con C.F. e P. IVA n. 03925490728) e tutte le società direttamente o indirettamente controllate da, o collegate a, SigmaSistemi ai sensi dell'art. 2359 c.c.
Legislazione in materia di Protezione dei Dati Personali: indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove mantengano la propria efficacia vincolante successivamente al 25 maggio 2018).
Infrastruttura Cloud: significa il sistema *cloud* di titolarità di SigmaSistemi e/o di terzi che ospita i Software.
Licenza: ha il significato di cui al paragrafo 10.2.
DPA: indica l'Accordo Principale per il Trattamento dei Dati Personali e il documento DPA – Condizioni Speciali applicabile, allegati al presente Contratto.
Nuovo Prodotto: ha il significato di cui al paragrafo 12.1(b).
Ordine: significa Modulo di sottoscrizione, Allegato Commerciale, Offerta / Ordine, o *coupon*, in formato elettronico o cartaceo, compilato e accettato (anche on-line) dal Cliente e contenente alcuni termini e le condizioni specificamente applicabili ai Servizi Cloud indicati nell'Ordine medesimo. Resta inteso che in caso di discordanza tra i termini e le condizioni indicate nell'Ordine e le disposizioni delle Condizioni Generali e/o delle Condizioni Integrative, prevarranno le disposizioni dell'Ordine.
Parti: significa, congiuntamente, SigmaSistemi e il Cliente.
Partner: significa il/i soggetto/i individuato/i da SigmaSistemi, Consulenti, Distributori, Fornitori che collabora/no allo scopo di fornire al Cliente i Servizi Cloud e/o l'Assistenza.
PEC: significa posta elettronica certificata.
Prodotti: significa Software, Servizi Professionali, Cloud, Prodotti Informatici.
Prodotto Obsoleto: ha il significato di cui al paragrafo 12.1(a).
Proprietà Intellettuale: significa ogni diritto di proprietà intellettuale e/o industriale, registrato o non registrato, in tutto o in parte, ovunque nel mondo, quali - a titolo esemplificativo e non esaustivo - marchi, brevetti, modelli di utilità, disegni e modelli, nomi a dominio, know-how, opere coperte dal diritto d'autore, database e software (ivi inclusi, ma non limitatamente a, le sue derivazioni, il codice sorgente, il codice oggetto e le interfacce).
Saas: significa *software-as-a-service*.
Servizi Cloud: significa i servizi forniti da SigmaSistemi al Cliente attraverso l'accesso e l'utilizzo, da parte di quest'ultimo, dei Software, e di quanto riportato nell'Ordine.
Software: significa i prodotti software di titolarità di SigmaSistemi o di una delle società parte del Gruppo SigmaSistemi o di Terzi, specificamente individuati nelle Condizioni Integrative e ospitati sull'Infrastruttura Cloud, eventualmente aggiornati e/o modificati a seguito degli Aggiornamenti e Sviluppi.
Sub-Licenza – Licenza Service: ha il significato di cui al paragrafo 10.3.
SigmaSistemi: significa la società SigmaSistemi Srl (C.F. e P. IVA n. 03925490728), con sede in via Don Guanella 15-B, 70124 Bari, ovvero la diversa società del Gruppo SigmaSistemi indicata nell'Ordine.
Utente: significa ciascun dipendente e/o collaboratore del Cliente, da quest'ultimo autorizzato ad utilizzare le Credenziali di Accesso per accedere e utilizzare i Software su installazioni *on premises* o Cloud.

1. Ambito di applicazione delle Condizioni Generali

1.1. Le presenti Condizioni Generali si applicano all'utilizzo, da parte del Cliente, dei Software e alla fornitura, da parte di SigmaSistemi, di Prodotti Software, Servizi Professionali e Cloud specificamente indicati nell'Ordine, attraverso l'accesso e l'utilizzo, da parte del Cliente, di ciascuno dei Software indicati nell'Ordine. Le presenti Condizioni Generali si applicano, inoltre, a tutti gli Aggiornamenti e Sviluppi, salvo essi siano regolati da separate e autonome Condizioni Integrative.

2. Prodotti Software Servizi Professionali e Cloud

2.1. Con il Contratto, a fronte del puntuale pagamento dei Corrispettivi, SigmaSistemi fornirà al Cliente, che accetta, i Prodotti Software Servizi Professionali e Cloud indicati nell'Ordine e altri Allegati commerciali, che sono destinati nel loro insieme a soddisfare gli scopi del Cliente, compreso le componenti acquistate successivamente ad integrazione del presente accordo.
2.2. Il Cliente potrà fruire dei Servizi Cloud esclusivamente attraverso l'accesso e l'utilizzo in modalità Saas dei relativi Software.
2.3. Fermo restando quanto previsto al paragrafo 10.3, a fronte della corresponsione degli eventuali Corrispettivi aggiuntivi specificamente indicati nell'Ordine ovvero determinati in base a separati accordi scritti, SigmaSistemi si impegna a fornire i Servizi Cloud indicati nell'Ordine anche in favore delle Controllate. Ciascuna Controllata potrà fruire dei Prodotti e Servizi Cloud esclusivamente attraverso l'accesso e l'utilizzo in modalità Saas dei relativi Software.

3. Obblighi del Cliente

3.1. Con il Contratto, il Cliente si impegna a:
(a) corrispondere a SigmaSistemi o, se diversamente indicato nell'Ordine, al Distributore i Corrispettivi dovuti ai sensi dell'articolo 7;
(b) dotarsi autonomamente di materiale *hardware* e *software*, nonché di una Connettività adeguata al fine di poter accedere al Data Center e utilizzare i Software per fruire dei Servizi Cloud;
(c) adeguare autonomamente le caratteristiche dei propri sistemi informatici e della Connettività alle modifiche, alle sostituzioni e ai correttivi eventualmente apportati ai Software e ai Servizi Cloud successivamente alla conclusione del Contratto;
(d) usare i Software e/o i Servizi Cloud in maniera conforme alla Licenza ed esclusivamente per gli scopi cui essi sono destinati;
(e) fornire a SigmaSistemi tutte le informazioni necessarie per consentire a SigmaSistemi un corretto e completo adempimento delle obbligazioni assunte ai sensi del presente Contratto, nonché a comunicare immediatamente le eventuali relative variazioni, ivi inclusa qualsiasi variazione relativa agli Utenti e/o alle Controllate;
(f) fare prendere visione a ciascun Utente delle presenti Condizioni Generali;
(g) fare prendere visione e accettare a ciascuna Controllata le presenti Condizioni Generali.

4. Credenziali di Accesso

4.1. Il Cliente e/o ciascun Utente e/o ciascuna Controllata potranno utilizzare il Software e fruire dei Servizi Cloud attivati mediante le Credenziali di Accesso che verranno fornite da SigmaSistemi.
4.2. Il Cliente è consapevole del fatto che la conoscenza delle Credenziali di Accesso da parte di soggetti terzi consentirebbe a questi ultimi l'utilizzo non autorizzato del Software, la fruizione non autorizzata dei Servizi Cloud e l'accesso alle eventuali informazioni ivi memorizzate. Il Cliente sarà in ogni caso ritenuto esclusivo responsabile per ogni utilizzo, autorizzato o meno, del Software mediante le Credenziali di Accesso.
4.3. Il Cliente è tenuto a custodire e a far sì che ciascun Utente e/o Controllata custodisca le Credenziali di Accesso con la massima riservatezza e con la massima diligenza, obbligandosi a non cederle né a consentirne l'uso a terzi non espressamente autorizzati.
4.4. SigmaSistemi e/o gli eventuali Partner commerciali non potranno in alcun caso essere ritenuti responsabili di qualsiasi danno, diretto e/o indiretto, che dovesse derivare al Cliente, a ciascun Utente e/o a terzi in conseguenza della mancata osservanza da parte del Cliente e/o di ciascun Utente delle previsioni di cui al presente articolo 4.

5. Assistenza

5.1. A fronte del puntuale pagamento dei Corrispettivi, SigmaSistemi si impegna a mettere a disposizione del Cliente un servizio di Assistenza, in conformità alle modalità indicate nella comunicazione di "Benvenuto".
5.2. Il Cliente prende atto ed accetta che il servizio di Assistenza verrà erogato esclusivamente da remoto, rimanendo espressamente escluso qualsiasi intervento diretto sui sistemi informatici del Cliente e/o delle Controllate.

6. Aggiornamenti e Sviluppi

6.1. Il Cliente prende atto e accetta che, laddove ritenuto opportuno a insindacabile giudizio di SigmaSistemi e/o terzi proprietari, gli Aggiornamenti e Sviluppi potranno: (i) determinare la modifica o l'eliminazione di alcune funzionalità dei Software; oppure (ii) consistere in sostituzioni o migrazioni (anche parziali) dei Software e dei relativi Servizi Cloud.
6.2. Il Cliente esonera SigmaSistemi da qualsivoglia responsabilità connessa ad eventuali danni derivanti da potenziali Aggiornamenti e Sviluppi, salvo tali danni derivino da dolo o colpa grave di SigmaSistemi.
6.3. Gli Aggiornamenti e Sviluppi non comprendono gli aggiornamenti, supplementi, adattamenti, sviluppi, migliorie e modifiche in genere resi necessari dalla modifica, integrazione, abrogazione o emissione di leggi, decreti, regolamenti, direttive, ordini o decisioni, italiani, comunitari o stranieri che, a insindacabile giudizio di SigmaSistemi e/o terzi proprietari, abbiano un impatto significativo sull'operatività e/o sui costi di SigmaSistemi e/o terzi proprietari, sulla struttura dei Software o apportino modifiche sostanziali o strutturali alla normativa in vigore alla data del Contratto.

7. Corrispettivi

7.1. A fronte della fornitura dei Servizi Cloud, il Cliente si impegna a corrispondere a SigmaSistemi o, se diversamente indicato nell'Ordine, al Distributore SS i Corrispettivi indicati nell'Ordine, secondo le modalità e le tempistiche ivi previste. In mancanza di espressa previsione nell'Ordine, i Corrispettivi dovranno essere corrisposti entro trenta giorni dal ricevimento di regolare fattura emessa da SigmaSistemi o, se diversamente indicato nell'Ordine, dal Distributore SS.
7.2. Tutti i Corrispettivi devono intendersi al netto di I.V.A. e degli eventuali altri oneri di legge.
7.3. Il Cliente prende atto e accetta espressamente che i Corrispettivi sono soggetti ad aggiornamento annuale nella misura del 100% della variazione in aumento dell'indice ISTAT dei prezzi della produzione dei servizi, calcolato come media degli ultimi dodici mesi.
7.4. Il Cliente prende atto che i Software e i relativi Servizi Cloud sono soggetti, per loro stessa natura, ad una costante evoluzione tecnologica e normativa che richiede continue e onerose attività di aggiornamento, sviluppo e, in alcuni casi, di sostituzione, necessarie al fine di garantire la loro funzionalità. In ragione di quanto precede, SigmaSistemi avrà il diritto di modificare i Corrispettivi anche in misura superiore all'indice ISTAT con le modalità di cui all'articolo 15.
7.5. Fermo restando quanto previsto al paragrafo 7.4 che precede, qualora, durante l'esecuzione del Contratto, dovessero verificarsi circostanze imprevedibili tali da rendere maggiormente onerosa l'erogazione dei Servizi Cloud da parte di SigmaSistemi, quest'ultima avrà diritto di percepire un equo compenso *una tantum* ovvero di modificare unilateralmente i Corrispettivi.
7.6. In caso di mancato o ritardato pagamento di una qualsiasi somma dovuta ai sensi del Contratto, il Cliente decadrà automaticamente dal beneficio del termine e sulle somme dovute matureranno interessi di mora nella misura prevista dal d.lgs. 231/2002.
7.7. Il Cliente rinuncia a proporre eccezioni senza avere preventivamente adempiuto alle proprie obbligazioni di pagamento ai sensi del presente articolo 7.
7.8. Il Cliente accetta che il rapporto contrattuale intercorrente tra SigmaSistemi e i propri distributori o fornitori avente ad oggetto la commercializzazione dei Servizi Cloud potrebbe cessare nel corso della durata del presente Contratto e che, in tal caso:
(a) SigmaSistemi comunicherà al Cliente la cessazione del rapporto contrattuale intercorrente tra la medesima SigmaSistemi e il Distributore o Fornitore;
(b) ogni contratto intercorrente con il Cliente con riferimento ai Servizi Cloud sarà ceduto ad altro Partner, ai sensi e per gli effetti dell'art. 1406 c.c.;
(c) il Cliente presta sin da ora, ai sensi e per gli effetti dell'art. 1407 c.c., il proprio consenso alla cessione di cui alla lettera (b) che precede.

8. Riservatezza

8.1. È tassativamente vietata alle Parti ogni forma di comunicazione e/o divulgazione o comunque di utilizzazione, anche per interposta persona e/o ente, di qualsiasi notizia, informazione e documentazione comunque appresa e ottenuta in occasione dell'esecuzione del Contratto e che SigmaSistemi abbia classificato come "*riservata*" o "*confidenziale*", anche ove non si tratti di veri e propri segreti industriali, tanto se attinente alle Parti, quanto se riguardante imprese loro clienti e/o fornitrici, salvo:
(a) quanto espressamente richiesto dall'esecuzione del Contratto;
(b) espressa autorizzazione scritta dell'altra Parte;
(c) quando le Parti siano a ciò obbligate per legge e/o per provvedimento dell'autorità amministrativa e/o giudiziaria.
8.2. Fatto salvo il caso in cui le informazioni e/o documenti di cui al paragrafo 8.1 costituiscano informazioni segrete ai sensi dell'articolo 98 del D.Lgs. n. 30/2005, il divieto di cui al precedente paragrafo resterà incondizionatamente fermo anche dopo la cessazione del Contratto, per qualsiasi causa intervenuta, per il successivo periodo di 3 (tre) anni, ritenuto congruo da entrambe le Parti, fatta salva la caduta in pubblico dominio dell'informazione che non sia imputabile alle Parti.

9. Partner

9.1. SigmaSistemi, nell'adempiere alle proprie obbligazioni di cui al Contratto, potrà avvalersi, a propria insindacabile discrezione, della cooperazione tecnica, organizzativa, di propri Partner commerciali, ai quali potrà affidare la prestazione di alcune o tutte le attività elencate nelle presenti Condizioni Generali e/o nell'Ordine.

10. Proprietà Intellettuale

10.1. Tutti i diritti di Proprietà Intellettuale indicati nell'Ordine, ivi inclusi i relativi diritti di sfruttamento economico, sull'Infrastruttura Cloud, sul Software, sui Servizi Cloud, sulla documentazione, sugli Aggiornamenti e Sviluppi e sui lavori derivati sono e rimangono, in tutto e in parte e ovunque nel mondo, di esclusiva titolarità di SigmaSistemi, e/o, se del caso, ai terzi proprietari, nelle Condizioni Integrative o nella documentazione tecnica di supporto.

10.2. Al solo scopo di permettere al Cliente di fruire dei Servizi Cloud indicati nell'Ordine, SigmaSistemi concede al Cliente, che accetta, una licenza d'uso del Software non esclusiva, non cedibile, temporanea e limitata al numero massimo di Utenti indicati nell'Ordine ("**Licenza**").
10.3. A parziale deroga di quanto previsto al paragrafo 10.2 che precede, a fronte della corresponsione degli eventuali Corrispettivi aggiuntivi di cui al paragrafo 2.2, al Cliente è concessa la facoltà di concedere alle Controllate una sub-licenza d'uso del Software ("**Sub-Licenza**"), fermo restando che, in ogni caso, il Cliente non potrà concedere Sub-Licenze per un numero di Utenti superiore a quanto espressamente indicato nell'Ordine. Sarà consentito al Cliente la condivisione degli archivi informatici e alcune funzionalità operative e collaborative con altri soggetti, quali ad esempio: Studio consulente e suo cliente assistito. Il servizio è attivabile su richiesta previo l'acquisto della specifica ("**Licenza Service**") e servizi correlati. Le Licenze d'uso di tutti i Prodotti Software e componenti correlati sono regolate dalle politiche commerciali dei rispettivi produttori o distributori, le quali si danno per conosciute e integralmente richiamate nel presente contratto, nonché alla Legge DPR 518 del 29 dicembre 1992 e successive modifiche, sulla tutela del Software.
10.4. Il Cliente si impegna, anche ai sensi dell'art. 1381 c.c. per ciascun Utente e per le Controllate, ad utilizzare i Software e gli Aggiornamenti e Sviluppi negli stretti limiti della Licenza (o della Sub-Licenza, o Licenza Service) e nel rispetto dei diritti di Proprietà Intellettuale di SigmaSistemi o di terzi. Pertanto, a titolo esemplificativo e non esaustivo e fatti in ogni caso salvi gli inderogabili limiti di Legge, il Cliente non potrà:
(a) aggirare le limitazioni tecniche e le misure tecnologiche di protezione presenti nel Software e/o negli Aggiornamenti e Sviluppi, ivi incluso il sistema di autenticazione;
(b) decodificare, decompilare o disassemblare il Software e/o gli Aggiornamenti e Sviluppi;
(c) eseguire o far eseguire copie del Software e/o degli Aggiornamenti e Sviluppi;
(d) pubblicare o far pubblicare il Software e/o gli Aggiornamenti e Sviluppi;
(e) utilizzare il Software e/o gli Aggiornamenti e Sviluppi al di fuori dell'Infrastruttura Cloud;
(f) commercializzare a qualsivoglia titolo il Software e/o gli Aggiornamenti e Sviluppi.
10.5. Restano altresì in capo a SigmaSistemi (e/o, se del caso, ai terzi proprietari di cui al precedente paragrafo 10.1) o a terzi tutti i diritti sui marchi, loghi, nomi, nomi a dominio e altri segni distintivi comunque associati all'Infrastruttura Cloud, al Software, agli Aggiornamenti e Sviluppi e/o ai Servizi Cloud, con la conseguenza che il Cliente non potrà in alcun modo utilizzarli senza la preventiva autorizzazione scritta di SigmaSistemi (e/o del terzo titolare). I Prodotti Software e ogni componente del Servizio, con esclusione dei prodotti fisici eventualmente acquistati, vengono concessi al Cliente Finale con lo schema contrattuale della locazione di cose, ovvero della Licenza d'uso temporanea non esclusiva; per cui il Cliente non acquisirà in nessun caso la proprietà.

11. Responsabilità e dichiarazioni del Cliente

11.1. Con l'accettazione delle presenti Condizioni Generali, il Cliente dichiara di (*i*) avere tutti i diritti e poteri necessari per concludere e dare esecuzione piena ed efficace al Contratto e di (*ii*) voler utilizzare i Software (ivi inclusi gli eventuali Aggiornamenti e Sviluppi) e i Servizi Cloud nell'ambito della propria attività imprenditoriale, artigianale, commerciale o professionale e che, pertanto, non si applicano nei suoi confronti le disposizioni del D.Lgs. 206/2005 a protezione dei consumatori.
11.2. Il Cliente si impegna a far sì che le disposizioni del Contratto siano rispettate da ciascun Utente e da ciascuna Controllata, ivi inclusi i rispettivi dipendenti e/o collaboratori. Anche ai sensi dell'art. 1381 c.c., il Cliente è considerato esclusivo responsabile dell'operato di tali soggetti e garantisce altresì il rispetto di tutte le normative applicabili, ivi incluse quelle in materia fiscale e civile.
11.3. È fatto divieto di utilizzare i Software, i Servizi Cloud e/o gli Aggiornamenti e Sviluppi al fine di depositare, conservare, inviare, pubblicare, trasmettere e/o condividere dati, applicazioni o documenti informatici che:
(a) siano in contrasto o violino i diritti di Proprietà Intellettuale di titolarità di SigmaSistemi e/o di terzi proprietari;
(b) abbiano contenuti discriminatori, diffamatori, calunniosi o minacciosi;
(c) contengano materiali pornografico, pedopornografico, osceno o comunque contrario alla pubblica morale;
(d) contengano virus, *worm*, *trojan horse* o, comunque, altri elementi informatici di contaminazione o distruzione;
(e) costituiscano attività di *spamming*, *phishing* e/o simili;
(f) siano in ogni caso in contrasto con le disposizioni normative e/o regolamentari applicabili.
11.4. SigmaSistemi si riserva il diritto di sospendere la fornitura dei Servizi Cloud e l'accesso ai Software al Cliente, a ciascun Utente e/o a ciascuna Controllata, ovvero di impedire l'accesso ai dati ivi memorizzati, qualora venga a conoscenza di una violazione di quanto previsto nel presente articolo e/o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo in base alle norme vigenti. In tal caso, SigmaSistemi provvederà a comunicare al Cliente le motivazioni dell'adozione della sospensione all'accesso, salva la facoltà di risolvere il Contratto ai sensi del successivo articolo 19.
11.5. Il Cliente prende atto che i Software, gli Aggiornamenti e Sviluppi e/o i Servizi Cloud possono contenere e/o necessitare l'uso di software cosiddetti *open source* e si impegna, anche ai sensi dell'art. 1381 c.c. per ciascun Utente e per ciascuna Controllata, ad osservare i termini e le condizioni ad essi specificamente applicabili. Ove necessario, tali condizioni verranno rese idoneamente conoscibili al Cliente da parte di SigmaSistemi.

12. Ritiro dal mercato e sostituzione

12.1. Il Cliente prende atto che i Software, i Servizi Cloud e gli ambienti nei quali essi operano sono soggetti, per loro natura, ad una costante evoluzione tecnologica che può determinare la loro obsolescenza e, in alcuni casi, l'opportunità di un ritiro dal mercato e, eventualmente, di una sostituzione con nuove soluzioni tecnologiche. Pertanto, SigmaSistemi e/o terzo proprietario, potrebbe decidere, a suo insindacabile giudizio, nel corso della durata del presente Contratto, di ritirare dal mercato i Servizi Cloud e/o i relativi Software (eventualmente sostituendoli con nuove soluzioni tecnologiche). In tal caso:
(a) SigmaSistemi comunicherà per iscritto (anche a mezzo email) al Cliente, con un preavviso di almeno sei mesi, che intende ritirare dal mercato uno o più Servizi Cloud e/o i relativi Software (ciascuno di essi il "**Prodotto Obsoleto**");
(b) la comunicazione di cui al punto (a) che precede ("**Comunicazione di Ritiro**") conterrà una descrizione dell'eventuale nuovo Servizio Cloud e/o Software (il "**Nuovo Prodotto**") che sostituirà ciascun Prodotto Obsoleto, restando inteso che il Nuovo Prodotto potrà basarsi su tecnologie diverse rispetto a quelle del Prodotto Obsoleto;
(c) laddove il Prodotto Obsoleto non fosse sostituito da alcun Nuovo Prodotto, il Contratto cesserà di produrre effetti con riferimento al Prodotto Obsoleto nella data che sarà indicata da SigmaSistemi e/o terzi proprietari nella Comunicazione di Ritiro (comunque non precedente all'ultimo giorno del sesto mese successivo alla data della Comunicazione di Ritiro); a partire da tale data, il Prodotto Obsoleto cesserà di essere fornito e il Cliente avrà diritto alla restituzione della quota dei Corrispettivi eventualmente già pagata per il periodo in cui non potrà godere del Prodotto Obsoleto;
(d) laddove il Prodotto Obsoleto fosse sostituito con un Nuovo Prodotto, il Cliente avrà il diritto, esercitabile entro 15 giorni dalla data della Comunicazione di Ritiro, di recedere dal Contratto con riferimento al solo Prodotto Obsoleto con efficacia dall'ultimo giorno del sesto mese successivo alla data della Comunicazione di Ritiro (data dalla quale il Prodotto Obsoleto cesserà di essere fornito) restando inteso che, in caso contrario, il Contratto continuerà ad esplicare i propri effetti (fatta espressa eccezione per quanto specificatamente indicato nella Comunicazione di Ritiro) con riferimento al Nuovo Prodotto e ogni riferimento al Prodotto Obsoleto dovrà intendersi riferito al Nuovo Prodotto.

13. Manleva

13.1. Il Cliente si impegna a manlevare e tenere indenne SigmaSistemi da qualsiasi danno, pretesa, responsabilità e/o onere, diretti o indiretti e comprese le ragionevoli spese legali, che SigmaSistemi dovesse subire o sopportare in conseguenza dell'inadempimento da parte del Cliente e/o di ciascun Utente e/o di ciascuna Controllata di ciascuno degli obblighi previsti dal Contratto e, in particolare, di quanto previsto dagli articoli 3 (Obblighi del Cliente), 4 (Credenziali di Accesso), 8 (Riservatezza), 10 (Proprietà Intellettuale), 11 (Responsabilità e dichiarazioni del Cliente), 12 (Ritiro dal mercato e sostituzione dei prodotti), 21 (Codice Etico, Codice di Condotta Anti-Corruzione e Modello Organizzativo) e 24 (Cessione del contratto e autorizzazione preventiva ex art. 1407 c.c.).

14. Responsabilità di SigmaSistemi

14.1. SigmaSistemi non rilascia dichiarazioni e garanzie espresse o implicite sul fatto che i Servizi Cloud, il Software e/o gli Aggiornamenti e Sviluppi siano adatti a soddisfare le specifiche esigenze del Cliente, che siano esenti da errori o che abbiano funzionalità non previste nelle specifiche tecniche e nella documentazione relativa.
14.2. SigmaSistemi non potrà essere ritenuta responsabile per danni, diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Cliente e/o a ciascun Utente e/o alle Controllate e/o a terzi in conseguenza dell'uso dei Servizi Cloud, dei Software e/o degli Aggiornamenti e Sviluppi in maniera non conforme a quanto previsto dal Contratto e/o dalle leggi vigenti.
14.3. SigmaSistemi non sarà in alcun modo responsabile di eventuali malfunzionamenti e/o mancata fruizione dei Servizi Cloud, dei Software e/o degli Aggiornamenti e Sviluppi che derivino da una Connettività inadeguata rispetto alle relative caratteristiche tecniche.

14.4. In nessun caso SigmaSistemi potrà essere ritenuta responsabile per eventuali danni o perdite, di qualunque natura o entità, derivanti dalle elaborazioni effettuate dal Cliente e/o da ciascun Utente e/o da ciascuna Controllata mediante i Servizi Cloud, i Software e/o gli Aggiornamenti e Sviluppi, essendo in ogni caso il Cliente e/o l'Utente e/o la Controllata tenuto a verificare la correttezza di tali elaborazioni.
14.5. Salvo che ciò sia necessario per adempiere a disposizioni di legge e/o a richieste dell'autorità giudiziaria, SigmaSistemi non è tenuta in alcun modo alla verifica dei dati e dei contenuti immessi dal Cliente e/o da ciascun Utente e/o da ciascuna Controllata nell'Infrastruttura Cloud attraverso i Servizi Cloud e, pertanto, non potrà in alcun modo essere ritenuta responsabile per danni e/o perdite, diretti o indiretti e di qualsiasi natura, derivanti da errori e/o omissioni di tali dati o connessi alla loro natura e/o caratteristiche.
14.6. SigmaSistemi, fatti salvi gli inderogabili limiti di legge, non potrà in nessun caso essere ritenuta responsabile per qualsiasi danno (diretto o indiretto), costo, perdita e/o spesa che il Cliente e/o terzi dovessero subire in conseguenza di attacchi informatici, attività di *hacking* e, in generale, accessi abusivi e non autorizzati da parte di terzi al Data Center, all'Infrastruttura Cloud, ai Software e, in generale, ai sistemi informatici del Cliente e/o di SigmaSistemi e/o di terzi, dai quali possano derivare, senza pretesa di esaustività, le seguenti conseguenze: (i) mancata fruizione dei Servizi Cloud; (ii) perdite di dati di titolarità o comunque nella disponibilità del Cliente; e (iii) danneggiamento dei sistemi hardware e/o software e/o alla Connettività del Cliente.
14.7. Salvo il caso di dolo o colpa grave, la responsabilità di SigmaSistemi non potrà mai eccedere l'ammontare del Corrispettivo annuale pagato dal Cliente ai sensi del presente Contratto. SigmaSistemi non potrà essere ritenuta responsabile per eventuali danni da lucro cessante, mancato guadagno o danni indiretti, perdita o danneggiamento di dati, fermo fabbrica, perdita di opportunità commerciali o di benefici di altro genere, pagamento di penali, ritardi o altre responsabilità del Cliente e/o delle Controllate verso terzi.

15. Modifiche Unilaterali

15.1. Il Contratto potrà essere modificato da SigmaSistemi in qualsiasi momento, dandone semplice comunicazione scritta (anche via *e-mail* o con l'ausilio di programmi informatici) al Cliente.
15.2. In tal caso, il Cliente avrà la facoltà di recedere dal Contratto con comunicazione scritta inviata a SigmaSistemi a mezzo raccomandata con ricevuta di ricevimento nel termine di 15 giorni dal ricevimento della comunicazione scritta da parte di SigmaSistemi di cui al paragrafo che precede.
15.3. In mancanza di esercizio della facoltà di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al Contratto si intenderanno da quest'ultimo definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

16. Sospensione e interruzione

16.1. SigmaSistemi compirà ogni ragionevole sforzo per garantire la massima disponibilità dei Servizi Cloud. Il Cliente, tuttavia, prende atto ed accetta che SigmaSistemi potrà sospendere e/o interrompere la fornitura dei Servizi Cloud, previa comunicazione scritta al Cliente, qualora si dovessero rendere necessari interventi di manutenzione ordinaria o straordinaria al Data Center e/o all'Infrastruttura Cloud e/o ai Software e Servizi. In tali casi, SigmaSistemi si impegna a ripristinare la disponibilità dei Servizi Cloud nel minor tempo possibile.
16.2. Fatto salvo quanto previsto ai paragrafi 11.4 e 19.2, SigmaSistemi si riserva altresì la facoltà di sospendere o interrompere la fornitura dei Servizi Cloud:
(a) in caso di mancato o ritardato pagamento, totale o parziale, dei Corrispettivi;
(b) qualora ricorrano ragioni di sicurezza e/o riservatezza;
(c) in caso di violazione, da parte del Cliente e/o di ciascun Utente e/o di ciascuna Controllata, agli obblighi di legge in materia di utilizzo dei servizi informatici e della rete internet;
(d) nel caso in cui si verifichino problematiche al Data Center e/o all'Infrastruttura Cloud e/o ai Software che non siano rimediabili senza sospendere il relativo accesso, ivi inclusa l'ipotesi di relativa sostituzione e/o migrazione anche parziale, in ogni caso previo avviso scritto al Cliente circa le ragioni della sospensione e le tempistiche di intervento previste.

17. Durata

17.1. Fatto salvo quanto eventualmente e diversamente previsto nelle Condizioni Integrative o nell'Ordine, il Contratto rimarrà efficace tra le Parti fino al 31 dicembre dell'anno di sottoscrizione e si intenderà automaticamente rinnovato alla scadenza per successivi periodi di un anno ciascuno, salvo disdetta da inviarsi con le modalità tecniche tempo per tempo indicate da SigmaSistemi oppure, in mancanza di diversa indicazione, a mezzo raccomandata A/R e/o PEC, almeno 4 (quattro) mesi prima della scadenza.

18. Recesso

18.1. SigmaSistemi si riserva il diritto di recedere dal presente Contratto in ogni momento, con comunicazione a mezzo raccomandata A/R e/o PEC da inviarsi al Cliente con almeno 4 (quattro) mesi di preavviso.
18.2. Nel caso in cui SigmaSistemi eserciti il proprio diritto di recesso per motivi diversi rispetto a quelli di cui al paragrafo 18.3 che segue, il Cliente avrà diritto alla restituzione della quota di corrispettivo per il periodo di mancata fruizione dei Servizi Cloud, qualora essa sia già stata versata.
18.3. SigmaSistemi si riserva altresì il diritto di recedere dal Contratto anche nell'ipotesi in cui il Cliente sia gravemente inadempiente con riferimento ad uno qualsiasi degli eventuali ulteriori contratti conclusi tra il medesimo Cliente e SigmaSistemi, ovvero tra il Cliente e una delle società controllate, direttamente o indirettamente, ai sensi dell'art. 2359, primo comma, c.c., da SigmaSistemi.

19. Clausola risolutiva espressa e interdizione dall'Infrastruttura Cloud

19.1. Fatto salvo il risarcimento del danno, SigmaSistemi si riserva il diritto di risolvere il Contratto ai sensi dell'art. 1456 c.c. a seguito di invio di semplice comunicazione scritta a mezzo PEC ovvero lettera raccomandata A/R in caso di mancato adempimento da parte del Cliente e/o di ciascun Utente anche di una sola delle previsioni: 3 (Obblighi del Cliente), 4.3 (Credenziali di Accesso), 7.1-7.5 (Corrispettivi), 8 (Riservatezza), 10 (Proprietà Intellettuale), 11.1-11.2-11.3 (Responsabilità e dichiarazioni del Cliente), 12 (Ritiro dal mercato e sostituzione dei prodotti), 13 (Manleva), 21 (Codice Etico) e 24 (Cessione del contratto e autorizzazione preventiva ex. art. 1407 c.c.).
19.2. Fermo restando l'obbligo per il Cliente di versare i Corrispettivi di cui all'articolo 7, SigmaSistemi, in caso di inadempimento del Cliente e/o di ciascun Utente e/o di ciascuna Controllata ad una delle obbligazioni di cui al paragrafo 19.1, si riserva altresì la facoltà di interrompere in ogni momento la fornitura dei Servizi Cloud in favore del Cliente e/o di ciascuna Controllata. In tale ipotesi, SigmaSistemi comunicherà al Cliente l'intenzione di interrompere la fornitura dei Servizi Cloud, invitando il Cliente, ove possibile, a porre rimedio all'inadempimento entro un determinato termine. Il Cliente rimane in ogni caso obbligato a versare quanto dovuto anche in caso di interruzione della fornitura dei Servizi Cloud.

20. Effetti della cessazione del Contratto e restituzione

20.1. In caso di cessazione del Contratto per qualsiasi causa intervenuta, SigmaSistemi cesserà la fornitura dei Servizi Cloud al Cliente e a ciascuna Controllata.
20.2. Fermo restando quanto previsto al paragrafo 20.1, a seguito della cessazione del Contratto, per qualsiasi ragione intervenuta, il Cliente e/o ciascuna Controllata avrà la facoltà di effettuare il download dei propri dati, documenti e/o contenuti con le modalità e nei termini previsti dall'Accordo Principale per il Trattamento di Dati Personali di cui all'art. 28.
20.3. Fatti salvi diversi accordi fra le Parti e gli inderogabili limiti di legge, laddove il Cliente e/o le eventuali Controllate non abbiano scaricato o richiesto la restituzione dei dati, documenti e/o contenuti nel termine di cui al paragrafo 20.2, SigmaSistemi avrà la facoltà di cancellarli in maniera permanente.
20.4. Resta in ogni caso inteso che le seguenti previsioni sopravvivranno alla cessazione del Contratto, per qualsiasi causa intervenuta: 1 (Ambito di applicazione delle Condizioni Generali), 7 (Corrispettivi), 8 (Riservatezza), 10 (Proprietà Intellettuale), 11 (Responsabilità e dichiarazioni del Cliente), 12 (Ritiro dal mercato e sostituzione dei prodotti), 13 (Manleva), 14 (Responsabilità di SigmaSistemi), 21 (Codice Etico), 22 (Comunicazioni), 23 (Legge applicabile e foro esclusivo), 25 (Effetto novativo), 26 (Tolleranza), 27 (Invalidità e inefficacia parziale).

21. Codice Etico SigmaSistemi

21.1. Il Cliente dichiara di essere a conoscenza delle disposizioni di cui al Decreto Legislativo 8 giugno 2001 n. 231, e successive integrazioni in materia di responsabilità amministrativa degli enti, nonché delle norme del Codice Etico adottato da SigmaSistemi disponibile sul sito https://www.sigmasistemi.com/s.php/2/Azienda.html e si impegna a rispettarne i contenuti, per quanto applicabili alla propria attività, e ad astenersi da comportamenti ad essi contrari. L'inosservanza da parte del Cliente dell'obbligo assunto ai sensi del presente articolo 21, ovvero la non correttezza o veridicità delle dichiarazioni ivi contenute, determinano un inadempimento grave, in presenza del quale SigmaSistemi avrà il diritto di risolvere il presente Contratto ai sensi dell'art. 1456 c.c.

22. Comunicazioni

22.1. Tutte le comunicazioni al Cliente inerenti al Contratto potranno essere effettuate all'indirizzo *email* comunicato dal Cliente medesimo nell'Ordine. Resta inteso che sarà cura e responsabilità del Cliente comunicare ogni variazione in relazione all'indirizzo *email* identificato dal Cliente per tutte le comunicazioni.

23. Legge applicabile e foro esclusivo

23.1. Il presente contratto è regolato e deve essere interpretato in conformità alla legge italiana.

23.2. Per tutte le controversie che dovessero insorgere tra le Parti in base al presente contratto, sarà competente a giudicare in via esclusiva, derogata ogni diversa norma di competenza territoriale, l'Autorità Giudiziaria di Bari.

24. Cessione del contratto e autorizzazione preventiva ex. art. 1407 c.c.

24.1. Salva preventiva autorizzazione scritta di SigmaSistemi, è fatto divieto al Cliente di cedere, in tutto o in parte, il Contratto.

24.2. Il Cliente acconsente sin da ora, ai sensi e per gli effetti dell'art. 1407 c.c., alla cessione da SigmaSistemi ad altro Partner commerciale, del contratto avente ad oggetto i Servizi Cloud, in caso di cessazione o impossibilità di adempimento per qualsivoglia motivo.

25. Effetto novativo

25.1. È escluso qualsiasi rilievo di eventuali precedenti accordi individuali tra le Parti, che si intendono assorbiti ed esaustivamente superati dalla disciplina del Contratto.

26. Tolleranza

26.1. L'eventuale omissione di far valere uno o più dei diritti previsti dal Contratto non potrà comunque essere intesa come definitiva rinuncia a tali diritti e non impedirà, quindi, di esigerne in qualsiasi altro momento il puntuale e rigoroso adempimento.

27. Invalidità ed inefficacia parziale

27.1. L'eventuale invalidità o inefficacia di una qualsiasi delle pattuizioni del Contratto lascerà intatte le altre pattuizioni giuridicamente e funzionalmente indipendenti, salvo quanto previsto dall'art. 1419, primo comma, c.c.

28. Trattamento dati personali

28.1. Con riferimento al trattamento dei dati personali di soggetti terzi immessi o comunque trattati dal Cliente attraverso il Software ("**Dati Personali di Terzi**"), ai sensi del GDPR, le Parti si danno atto e accettano di conformarsi a quanto previsto nell'Accordo Principale per il Trattamento di Dati Personali ("**DPA**") accluso al presente Contratto sub Allegato A. PDA

28.2. Il Cliente dovrà manlevare e tenere indenne SigmaSistemi da qualunque pregiudizio, onere, sanzione o pretesa che SigmaSistemi dovesse subire o ricevere in ragione della violazione da parte del Cliente degli obblighi stabiliti dal DPA (ivi incluso per ciò che attiene ad eventuali pretese o richieste degli interessati o di terzi ed i relativi costi legali di difesa). SigmaSistemi, in ogni caso, non potrà essere ritenuta responsabile per l'eventuale carenza, lacunosità o non correttezza delle istruzioni impartite dal Cliente in merito al trattamento dei Dati Personali di Terzi o per la mancata adozione di misure di sicurezza tecnico-organizzative relative al proprio personale.

28.3. I dati personali del Cliente, o del personale del Cliente raccolti ed elaborati da SigmaSistemi per finalità e con modalità proprie e del cui trattamento, pertanto, SigmaSistemi è Titolare ai sensi del GDPR ("**Dati Personali del Cliente**"), saranno trattati da SigmaSistemi in conformità a quanto riportato nell'informativa rilasciata ai sensi dell'articolo 13 del GDPR.

28.4. Le Parti convengono che SigmaSistemi potrà procedere all'elaborazione e utilizzo di informazioni puramente statistiche, su base aggregata, raccolte in relazione all'utilizzo dei Servizi Cloud da parte del Cliente, ivi incluse informazioni relative ai meta-dati associati ai documenti, a fini di studio e statistici. Il Cliente concede a tal fine a SigmaSistemi una licenza non esclusiva, perpetua, irrevocabile, valida in tutto il mondo e a titolo gratuito, ad utilizzare tali informazioni per dette finalità.

28.5. Le Parti riconoscono che l'esecuzione dei Servizi Cloud può comportare il trattamento da parte di SigmaSistemi di dati personali di titolarità del Cliente o di cui il Cliente è stato nominato, a propria volta, responsabile del trattamento dal legittimo titolare ("**Terzo Beneficiario**"). Al riguardo, le Parti riconoscono che SigmaSistemi agirà in relazione a tali trattamenti, nel rispetto delle previsioni di cui al DPA, in qualità di Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del GDPR nonché della Legislazione in materia di Protezione dei Dati Personali.

ALLEGATO A

SERVIZI DI AGGIORNAMENTO, ASSISTENZA TECNICA E MANUTENZIONE

SERVIZI COMPRESI

Aggiornamenti e Sviluppi resi necessari dalla modifica, integrazione o emissione leggi, decreti, regolamenti, direttive, ordini o decisioni, italiani, comunitari o stranieri che, a insindacabile giudizio del Fornitore o, Produttore del Software non abbiano un impatto significativo sull'operatività e costi;

Aggiornamenti e Sviluppi derivanti da nuove versioni (c.d. "Release") del Software;

Assistenza tecnica tramite IVR (o tramite ulteriori eventuali sistemi che saranno tempo per tempo sviluppati e implementati) entro il numero massimo di ticket eventualmente indicato nell'Ordine;

Teleassistenza con dispositivi Sw;

Monitorare sulla corretta fruizione dei sistemi Cloud.

SERVIZI NON COMPRESI

Ore di viaggio per interventi di assistenza tecnica;

Ripristino delle normali condizioni operative a seguito dell'uso di accessori non forniti dal Fornitore ovvero a seguito di negligenza, incuria, dolo o eventuali tentativi da parte del cliente di effettuare modifiche;

Ripristino delle normali condizioni operative a seguito di cambio dell'hardware;

Ripristino delle normali condizioni operative a seguito di alluvioni, incendi manomissione dolosa, atti di teppismo, danneggiamenti in seguito a furti o tentativo di furto e altri eventi di forza maggiore;

Fornitura di supporti (dischi, toner, etc.);

Aggiornamenti, sviluppi o attività in genere resi necessari dalla modifica, integrazione o emissione leggi, decreti, regolamenti, direttive, ordini o decisioni, italiani, comunitari o stranieri che, a insindacabile giudizio del Fornitore, abbiano un impatto significativo sull'operatività e/o sui costi del Fornitore;

Rimozione VIRUS e assistenza helpdesk su gestione di package software non inclusi nell'ordine;

Personalizzazioni su programmi e stampe standard (da analizzare preventivamente);

Interventi di assistenza o manutenzione che siano resi necessari a causa di

(i) manomissioni o interventi di manutenzione e/o assistenza eseguiti da parte di personale non incaricato dal Fornitore,

(ii) incidenti provocati da eventi politici, atti vandalici o comunque dal fatto doloso di dipendenti del cliente o di terzi;

(iii) negligenza, incuria, impiego non corretto o non conforme alle eventuali istruzioni del Fornitore o di TeamSystem;

(iv) interruzioni o fluttuazioni dell'energia elettrica;

(v) allagamenti, incendi, fenomeni atmosferici, calamità naturali o altre cause accidentali;

(vi) ogni altra attività non espressamente compresa nei Servizi.

ALLEGATO B

DPA

ACCORDO PRINCIPALE PER IL TRATTAMENTO DI DATI PERSONALI – MASTER DATA PROCESSING AGREEMENT
(ex art. 28 del Regolamento UE 2016/679)

TRA

Il presente accordo per la protezione di dati personali è concluso tra il Fornitore, come di seguito definito, e il cliente che accetta il presente accordo. Per "**Fornitore**" si intende uno o più dei seguenti soggetti:

(i) SigmaSistemi Srl, con sede legale in Bari, via Don Guanella 15 B, codice fiscale e partita IVA n. 03925490728; e/o
(ii) la società appartenente al gruppo facente capo a SigmaSistemi e indicata nel Contratto;

E

il soggetto indicato nel Contratto quale cliente (di seguito il "**Cliente**"),
di seguito, congiuntamente, le "**Parti**" o disgiuntamente la "**Parte**"

PREMESSO CHE

a) il Cliente ha sottoscritto uno o più contratti con il Fornitore (di seguito il "**Contratto**");
b) le Parti intendono disciplinare nel presente "*accordo principale per il trattamento dei dati personali – Master Data Processing Agreement*" (nel seguito "**DPA**" o "**Accordo**") le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi e le responsabilità connesse al trattamento medesimo, ivi incluso l'impegno assunto dal Fornitore quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679 (nel seguito "**GDPR**");
c) le caratteristiche specifiche del trattamento dei Dati Personali sono descritte, con riferimento a ciascun Servizio, nelle "*condizioni speciali di trattamento dei Dati Personali" disponibili sul sito:* https://www.sigmasistemi.com/p.php/7702/informativa-sul-trattamento-dei-dati-personali.html *(di seguito "DPA* **- Condizioni Speciali**") le quali costituiscono parte integrante ed essenziale del presente Accordo.

Tutto quanto sopra premesso le Parti convengono quanto segue:

1. DEFINIZIONI E INTERPRETAZIONE

1.1. Le premesse costituiscono parte integrante del presente Accordo. Nell'Accordo i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:
"Data di Decorrenza dell'Accordo" indica la data in cui il Cliente sottoscrive o accetta il presente Accordo;
"Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente, o dall'Utente Finale in relazione alla fruizione dei Servizi, nella misura in cui siano oggetto di trattamento da parte del Fornitore, sulla base del Contratto. Un elenco delle categorie di Dati Personali è riportata nei DPA – Condizioni Speciali;
"Decisione di Adeguatezza" indica una decisione della Commissione Europea sulla base dell'Articolo 45(3) del GDPR in merito al fatto che le leggi di un certo paese garantiscano un adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali;
"Giorni Lavorativi" indica ciascun giorno di calendario, a eccezione del sabato, della domenica e dei giorni nei quali le banche di credito ordinarie non sono di regola aperte sulla piazza di Milano, per l'esercizio della loro attività;
"Email di notifica" si intende l'indirizzo (o gli indirizzi) email fornito/i dal Cliente, all'atto della sottoscrizione del Servizio o fornito tramite altro canale ufficiale al Fornitore, a cui il Cliente intende ricevere le notifiche da parte del Fornitore;
"Istruzioni" indica le istruzioni scritte impartite dal Titolare nel presente Accordo (inclusivo dei relativi DPA – Condizioni Speciali) e, eventualmente, nel Contratto;
"Legislazione in materia di Protezione dei Dati Personali" indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia in materia di protezione dei Dati Personali, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia di protezione dei Dati Personali (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove mantengano la propria efficacia vincolante successivamente al 25 maggio 2018).
"Personale del Fornitore" indica i dirigenti, dipendenti consulenti, e altro personale del Fornitore, con esclusione del personale dei Responsabili Ulteriori del Trattamento;
"Richiesta" indica una richiesta di accesso di un Interessato, una richiesta di cancellazione o correzione dei Dati Personali, o una richiesta di esercizio di uno degli altri diritti previsti dal GDPR;
"Responsabile Ulteriore del Trattamento" indica qualunque subappaltatore cui il Fornitore abbia subappaltato uno qualsiasi degli obblighi assunti contrattualmente e che, nell'adempiere tali obblighi, potrebbe dover raccogliere, accedere, ricevere, conservare o altrimenti trattare Dati Personali;
"Servizio/i" indica il servizio o i servizi oggetto dei Contratti sottoscritti tempo per tempo tra il Cliente e il Fornitore;
"**Utente Finale**" si intende l'eventuale fruitore finale del Servizio, Titolare del Trattamento; e "**Violazione della Sicurezza 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 occorsa su sistemi gestiti dal Fornitore o comunque sui quali il Fornitore abbia un controllo.
1.2. I termini "ivi compreso/a/i/e" e "incluso/a/i/e" saranno interpretati come se fossero seguiti dall'espressione "a titolo puramente esemplificativo", così da fornire un elenco non esaustivo di esempi.
1.3. Per le finalità del presente Accordo, i termini "Interessato", "Trattamento", "Titolare del trattamento", "Responsabile del trattamento", "Trasferimento" e "Misure tecnico-organizzative adeguate" saranno interpretati in conformità alla Legislazione in materia di Protezione dei Dati Personali applicabile.

2. RUOLO DELLE PARTI

2.1. Le Parti riconoscono e convengono che il Fornitore agisce quale Responsabile del trattamento in relazione ai Dati Personali e il Cliente agisce di regola quale Titolare del trattamento dei Dati Personali.
2.2. Qualora il Cliente svolga operazioni di trattamento per conto di altro Titolare, il Cliente potrà agire come Responsabile del trattamento. In tal caso, il Cliente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Cliente, del Fornitore quale ulteriore Responsabile del trattamento derivante dalla stipulazione del presente Accordo è stata autorizzata dal relativo Titolare del trattamento e si impegna ad esibire al Fornitore, dietro sua semplice richiesta scritta, la documentazione attestante quanto sopra.
2.3. Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.
2.4. Il Fornitore ha nominato un Responsabile della protezione dei dati, domiciliato presso la sede di SigmaSistemi Srl via Don Guanella 15 B - Bari, che può essere contattato al seguente indirizzo: privacy@sigmasistemi.com o al numero telefonico 080/5025466

3. TRATTAMENTO DEI DATI PERSONALI

3.1. Con la stipulazione del presente Accordo (inclusivo di ciascun DPA - Condizioni Speciali applicabile), il Cliente affida al Fornitore l'incarico di trattare i Dati Personali ai fini della prestazione dei Servizi, così come meglio dettagliato nel Contratto e nei DPA – Condizioni Speciali; i DPA – Condizioni Speciali sono disponibili tramite link al seguente indirizzo https://www.sigmasistemi.com/p.php/7702/informativa-sul-trattamento-dei-dati-personali.html
3.2. Il Fornitore si impegna a conformarsi alle Istruzioni, fermo restando che, qualora il Cliente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Cliente le predette variazioni ed i costi connessi.
3.3. Nei casi di cui all'art. 3.2 e in caso di richieste del Cliente che comportino il trattamento di Dati Personali che siano, ad avviso del Fornitore, in violazione della Legislazione in materia di Protezione dei Dati Personali, il Fornitore è autorizzato ad astenersi dall'eseguire tali Istruzioni e ne informerà prontamente il Cliente. In tali casi il Cliente potrà valutare eventuali variazioni alle Istruzioni impartite o contattare l'Autorità di controllo per verificare la liceità delle richieste avanzate.

4. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

4.1. Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi, il Fornitore si impegna a eseguire il trattamento dei Dati Personali:
4.1.1. Soltanto nella misura e con le modalità necessarie per erogare i Servizi o per adempiere opportunamente i propri obblighi, previsti dal Contratto e dal presente Accordo ovvero imposti dalla legge o da un organo di vigilanza o controllo competente. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all'Email di notifica;
4.1.2. In conformità alle Istruzioni del Cliente;
4.2 Il personale del Fornitore che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al trattamento dei dati personali. Tale personale è altresì vincolato da obblighi di riservatezza e dal Codice Etico aziendale e deve attenersi alle policy di riservatezza e di protezione dei dati personali adottate dal Fornitore.

5. AFFIDAMENTO A TERZI

5.1. In relazione all'affidamento a Responsabili Ulteriori del Trattamento di operazioni di trattamento di Dati Personali, le Parti convengono quanto segue:
5.1.1. Il Cliente acconsente espressamente che alcune operazioni di trattamento di Dati Personali siano affidate dal Fornitore ad altre società del gruppo SigmaSistemi e/o a soggetti terzi individuati nei DPA – Condizioni Speciali;
5.1.2. Il Cliente acconsente altresì all'affidamento di operazioni di Trattamento dei Dati Personali a ulteriori soggetti terzi secondo le modalità previste al successivo articolo 5.1.4.;
5.1.3. Resta inteso che la sottoscrizione delle Clausole Contrattuali Tipo (prevista dal successivo punto 7 in caso di trasferimento all'estero dei Dati Personali) da parte del Cliente con un Responsabile Ulteriore del trattamento deve intendersi quale consenso all'affidamento al terzo delle operazioni di trattamento.
5.1.4. Nei casi in cui il Fornitore ricorra a Responsabili Ulteriori del Trattamento per l'esecuzione di specifiche attività di trattamento dei Dati Personali, il Fornitore:
5.1.4.1. Si impegna ad avvalersi di Responsabili Ulteriori del Trattamento che garantiscono misure tecniche e organizzative adeguate e garantisce che l'accesso ai Dati Personali, e il relativo trattamento, sarà effettuato esclusivamente nei limiti di quanto necessario per l'erogazione dei servizi subappaltati;
5.1.4.2. Almeno 15 (quindici) giorni prima della data di avvio delle operazioni di trattamento dei Dati Personali da parte del Responsabile Ulteriore del Trattamento informa il Cliente dell'affidamento al terzo (nonché dei dati identificativi del terzo, della sua ubicazione – ed eventualmente, dell'ubicazione dei server sui quali saranno conservati i dati, se applicabile - e delle attività affidate) mediante invio di Email di notifica o altro mezzo ritenuto idoneo dal Fornitore. Il Cliente potrà recedere dal Contratto entro 15 (quindici) giorni dal ricevimento della comunicazione, fermo restando l'obbligo di corrispondere al Fornitore gli importi dovuti alla data di cessazione del Contratto;
5.1.5. Eventuali informazioni aggiuntive sull'elenco dei Responsabili Ulteriori del Trattamento, dei trattamenti loro affidati e della loro ubicazione, sono contenuti nei DPA - Condizioni Speciali relativi ai Servizi attivati dal Cliente.

6. DISPOSIZIONI IN MATERIA DI SICUREZZA

6.1. *MISURE DI SICUREZZA DEL FORNITORE* – Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi il Fornitore si impegna ad adottare misure tecnico-organizzative adeguate per evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata di, o l'accesso ai, Dati Personali, come descritte nell'Allegato 1 al presente Accordo ("**Misure di Sicurezza**").
6.1.1. L'Allegato 1 all'Accordo contiene misure di protezione degli archivi dati commisurate al livello dei rischi presenti con riferimento ai Dati Personali per consentire la riservatezza, integrità, disponibilità e la resilienza dei sistemi e dei Servizi del Fornitore, nonché misure per consentire il tempestivo ripristino degli accessi ai Dati Personali in caso di Violazione della Sicurezza dei Dati Personali, e misure per testare l'efficacia nel tempo di dette misure. Il Cliente dà atto ed accetta che, tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento dei Dati Personali, le procedure e i criteri di sicurezza implementati dal Fornitore garantiscono un livello di protezione adeguato al rischio per quanto riguarda i suoi Dati Personali.
6.1.2. Il Fornitore potrà aggiornare e modificare nel tempo le Misure di Sicurezza sopra indicate, fermo restando che tali aggiornamenti e modifiche non potranno comportare una riduzione del livello di sicurezza complessivo dei Servizi. Di tali aggiornamenti e modifiche sarà fornita notifica al Cliente mediante invio di comunicazione all'Email di notifica.
6.1.3. Qualora il Cliente richieda di adottare misure di sicurezza aggiuntive rispetto alle Misure di Sicurezza, il Fornitore si riserva il diritto di valutarne la fattibilità e potrà applicare costi aggiuntivi a carico del Cliente per tale implementazione.
6.1.4. Il Cliente riconosce e accetta che il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni disponibili al Fornitore stesso secondo quanto specificamente riportato nei relativi DPA – Condizioni Particolari, presterà assistenza al Cliente nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32-34 del GDPR nei modi seguenti:
6.1.4.1. Implementando e mantenendo aggiornate le Misure di Sicurezza secondo quanto previsto ai precedenti punti 6.1.1, 6.1.2, 6.1.3;
6.1.4.2. Conformandosi agli obblighi di cui al punto 6.3.
6.1.5. Resta inteso che, nei Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente (installazioni *on premises)*, le Misure di Sicurezza sopra indicate troveranno applicazione esclusivamente in relazione ai Servizi che prevedono il Trattamento dei Dati Personali da parte del Fornitore o di suoi affidatari (es. supporto e assistenza da remoto, servizi di migrazione).
6.1.6. Qualora il prodotto consenta l'integrazione con applicativi di terze parti, il Fornitore non sarà responsabile dell'applicazione delle Misure di Sicurezza relative alle componenti delle terze parti o delle modalità di funzionamento del prodotto derivanti dall'integrazione effettuata dalle terze parti.
6.2. *MISURE DI SICUREZZA DEL CLIENTE* – Fermi restando gli obblighi di cui al precedente punto 6.1 in capo al Fornitore, il Cliente riconosce e accetta che, nella fruizione dei Servizi, rimane responsabilità esclusiva del Cliente l'adozione di adeguate misure di sicurezza in relazione alla fruizione dei Servizi da parte del proprio personale e di coloro che sono autorizzati ad accedere a detti Servizi.
6.2.1. A tal fine il Cliente si impegna ad utilizzare i Servizi e le funzionalità di trattamento dei Dati Personali in modo da garantire un livello di protezione adeguato al rischio effettivo.
6.2.2. Il Cliente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Cliente o dai fruitori presso l'Utente Finale per accedere ai Servizi, e per effettuare i salvataggi e backup dei Dati Personali al fine di garantire il ripristino dei Dati Personali nel rispetto delle norme di legge.
6.2.3. Resta escluso qualsiasi obbligo o responsabilità in capo al Fornitore circa la protezione dei Dati Personali che il Cliente o l'Utente Finale, se applicabile, conservino o trasferiscano fuori dai sistemi utilizzati dal Fornitore e dai suoi Responsabili Ulteriori del Trattamento (ad esempio, in archivi cartacei, o presso propri data center, come nel caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso altri fornitori del Cliente).
6.3. *VIOLAZIONI DI SICUREZZA* – Fatta eccezione per il caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente per i quali non trova applicazione il presente punto 6.3, qualora il Fornitore venga a conoscenza di una Violazione di Sicurezza dei Dati Personali, lo stesso:
6.3.1. Informerà senza ingiustificato ritardo il Cliente mediante comunicazione inoltrata all'Email di notifica;
6.3.2. Adotterà misure ragionevoli per limitare i possibili danni e la sicurezza dei Dati Personali;
6.3.3. Fornirà al Cliente, per quanto possibile, una descrizione della Violazione della Sicurezza dei Dati Personali ivi incluse le misure adottate per evitare o mitigare i potenziali rischi e le attività raccomandate dal Fornitore al Cliente per la gestione della Violazione di Sicurezza;
6.3.4. Considererà informazioni confidenziali ai sensi di quanto previsto nel Contratto, le informazioni attinenti alle eventuali Violazioni della Sicurezza, i relativi documenti, comunicati e avvisi e non comunicherà a terzi dati informazioni, fuori dai casi strettamente necessari all'assolvimento degli obblighi del Cliente derivanti dalla Legislazione in materia di Protezione dei Dati Personali senza il previo consenso scritto del Titolare del Trattamento.
6.4. Nei casi di cui al precedente punto 6.3, è responsabilità esclusiva del Cliente adempiere, nei casi previsti dalla Legislazione in materia di Trattamento di Dati Personali, agli obblighi di notificazione della Violazione di Sicurezza ai terzi (all'Utente Finale qualora il Cliente sia un Responsabile del Trattamento) e, se il Cliente è Titolare del Trattamento, all'Autorità di controllo e agli interessati.
6.5. Resta inteso che la notificazione di una Violazione di Sicurezza o l'adozione di misure volte a gestire una Violazione di Sicurezza non costituisce riconoscimento di inadempimento o di responsabilità da parte del Fornitore in relazione a detta Violazione di Sicurezza.
6.6. Il Cliente dovrà comunicare tempestivamente al Fornitore eventuali utilizzi impropri degli account o delle credenziali di autenticazione oppure eventuali Violazioni di Sicurezza di cui abbia avuto conoscenza riguardanti i Servizi.

7. LIMITAZIONI AL TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

7.1. Il Fornitore non trasferirà i Dati Personali al di fuori dello SEE se non in accordo con il Cliente.
7.2. Se, ai fini della conservazione o del trattamento dei Dati Personali da parte di un Responsabile Ulteriore del trattamento, è necessario effettuare il trasferimento dei Dati Personali fuori dallo SEE in un paese che non gode di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, il Fornitore:

7.2.1. Farà in modo che il Responsabile Ulteriore del trattamento stipuli le clausole contrattuali tipo previste nella Decisione della Commissione europea 2010/87/UE, del 5 febbraio 2010, per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi (le "**Clausole Contrattuali Tipo**"), o loro equivalente, se modificate nel tempo. Copia delle Clausole Contrattuali Tipo sottoscritte dal Fornitore per conto del Cliente saranno rese disponibili al Cliente;
7.2.2. Potrà proporre al Cliente altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali (es. Privacy Shield in caso di Responsabili Ulteriori del trattamento situati negli Stati Uniti e per cui sia verificabile l'aderenza tramite i canali e registri ufficiali, o trasferimenti infragruppo del Responsabile Ulteriore del Trattamento che sia parte di un gruppo societario che ha ottenuto l'approvazione delle BCR per i Responsabili del trattamento).
7.3. Nei casi di cui al precedente punto 7.2.1 con il presente Accordo il Cliente conferisce espressamente mandato al Fornitore a sottoscrivere le Clausole Contrattuali Tipo con i Responsabili Ulteriori del Trattamento riportati nei relativi DPA – Condizioni Particolari. Qualora Titolare del trattamento sia l'Utente Finale, il Cliente si impegna a informare l'Utente Finale di tale trasferimento e dichiara che l'autorizzazione ad avvalersi del Responsabile Ulteriore del Trattamento situato fuori dallo SEE equivale al mandato di cui sopra.

8. VERIFICHE E CONTROLLI

8.1. Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o *best practice*, i cui esiti saranno riportati in specifici report ("**Report**"). Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.
8.2. Nei casi previsti dall'art. 8.1, il Cliente concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report messi a disposizione dal Fornitore.
8.3. Il Fornitore riconosce il diritto del Cliente, con le modalità e nei limiti di seguito indicati, ad effettuare audit indipendenti per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo e nei rispettivi DPA – Condizioni Speciali, e di quanto previsto dalla normativa. Il Cliente potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.
8.4. Nel caso di cui al precedente punto 8.2, il Cliente dovrà previamente inviare richiesta scritta all'indirizzo di posta privacy@sigmasistemi.com successivamente alla richiesta di audit o ispezione il Fornitore e il Cliente concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il Cliente e coloro che effettuano le verifiche e i costi che il Fornitore potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.
8.5. Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che siano, ad insindacabile giudizio del Fornitore, non adeguatamente qualificati o indipendenti, siano concorrenti del Fornitore o che siano evidentemente inadeguati. In tali circostanze il Cliente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.
8.6. Il Cliente si impegna a corrispondere al Fornitore gli eventuali costi calcolati dal Fornitore e comunicati al Cliente nella fase di cui al precedente punto 8.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.
8.7. *Resta* fermo quanto previsto in relazione ai diritti di ispezione del Titolare del trattamento e delle autorità nelle Clausole Contrattuali Tipo eventualmente sottoscritte ai sensi del precedente punto 7, che non potranno considerarsi modificate da alcuna delle previsioni contenute nel presente Accordo o nei relativi DPA – Condizioni Speciali.
8.8. Il presente punto 8 non è applicabile ai Contratti aventi ad oggetto prodotti installati presso il Cliente o *presso* fornitori del Cliente.
8.9. Le attività di verifica che interessino eventuali Responsabili Ulteriori dovranno essere svolte nel rispetto *delle* regole di accesso e delle politiche di sicurezza dei Responsabili Ulteriori.

9. ASSISTENZA A FINI DI CONFORMITÀ

9.1. Il *Fornitore* presterà assistenza al Cliente e coopererà nei modi di seguito indicati al fine di consentire al Cliente il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.
9.2. Qualora il Fornitore riceva Richieste o reclami da un Interessato in relazione ai Dati Personali, il Fornitore raccomanderà all'Interessato di rivolgersi al Cliente o all'Utente Finale, nel caso in cui quest'ultimo sia il *Titolare* del Trattamento. In tali casi il Fornitore informerà tempestivamente il Cliente del ricevimento della Richiesta mediante invio di Email di notifica e fornirà al Cliente le informazioni ad esso disponibili unitamente a copia della Richiesta o del reclamo. Resta inteso che tale attività di cooperazione sarà svolta in via eccezionale, in quanto la gestione dei rapporti con gli Interessati resta esclusa dai Servizi ed è responsabilità del Cliente gestire eventuali reclami in via diretta e garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il Cliente stesso, o l'Utente Finale se Titolare del Trattamento. Sarà responsabilità del Cliente, o dell'Utente Finale qualora questi sia Titolare del Trattamento, provvedere a dar seguito a tali Richieste o reclami.
9.3. Il Fornitore provvederà a informare tempestivamente il Cliente, salvo il caso in cui ciò sia vietato dalla legge, con avviso all'Email di notifica di eventuali ispezioni o richieste di informazioni presentate da autorità di controllo e forze di polizia rispetto a profili che riguardano il trattamento dei Dati Personali.
9.4. Qualora, ai fini dell'evasione delle Richieste di cui ai precedenti punti, il Cliente abbia necessità di ricevere informazioni dal Fornitore circa il trattamento dei Dati Personali, il Fornitore presterà la necessaria assistenza nei limiti di quanto ragionevolmente possibile, a condizione che tali richieste siano presentate con congruo preavviso.
9.5. Il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili, fornirà ragionevole assistenza al Cliente nel rendere disponibili informazioni utili per consentire al Cliente l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali nei casi previsti dalla legge. In tal caso il Fornitore renderà disponibili informazioni di carattere generale in base al Servizio, quali le informazioni contenute nel Contratto, nel presente Accordo e nei DPA - Condizioni Particolari relativi ai Servizi interessati. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del Cliente. Resta inteso che è responsabilità e onere esclusivo del Cliente, o dell'Utente Finale se Titolare del trattamento, procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei Dati Personali dallo stesso posto in essere nel contesto dei Sevizi.
9.6. Il Fornitore si impegna a rendere Servizi improntati ai principi di minimizzazione del trattamento (*privacy by design & by default*), fermo restando che è responsabilità esclusiva del Cliente, o dell'Utente Finale, se Titolare del Trattamento, assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi e verificare che le misure tecniche e organizzative di un Servizio soddisfano i requisiti di conformità della Società, ivi inclusi i requisiti previsti dalla Legislazione in materia di protezione dei dati personali.
9.7. Il Cliente prende atto che, in caso di Richieste di portabilità dei Dati Personali avanzate dai rispettivi Interessati, e solo in relazione ai Servizi che generano Dati Personali rilevanti a tal fine, il Fornitore presterà assistenza al Cliente mettendo a disposizione le informazioni necessarie per estrarre i dati richiesti in formato conforme a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.
9.8. I precedenti punti 9.5 e 9.7 non sono applicabili in caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente.

10. OBBLIGHI DEL CLIENTE E LIMITAZIONI

10.1. Il Cliente si impegna a impartire Istruzioni conformi alla normativa e a utilizzare i Servizi in modo conforme alla Legislazione in materia di Protezione dei Dati Personali e solo per trattare Dati Personali che siano stati raccolti in conformità alla Legislazione in materia di Protezione dei Dati Personali.
10.2. L'eventuale trattamento di Dati Personali di cui agli artt. 9 e 10 del GDPR sarà consentito solo ove espressamente previsto nel DPA - Condizioni Particolari; fuori da tali casi, l'eventuale trattamento di tali Dati Personali sarà consentito solo previo accordo scritto tra le Parti ai sensi di quanto previsto al punto 3.2.
10.3. Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento (e, nei casi in cui tali obblighi sono in capo all'Utente Finale, garantisce che analoghi obblighi sono imposti a carico dell'Utente Finale) dalla Legislazione in materia di Protezione dei Dati Personali, ivi inclusi gli obblighi di informativa nei confronti degli Interessati. Il Cliente si impegna inoltre a garantire che il trattamento dei Dati Personali effettuato mediante l'utilizzo dei Servizi avvenga solo in presenza di idonea base giuridica.
10.4. Qualora il rilascio dell'informativa e l'ottenimento del consenso debbano avvenire per il tramite del prodotto oggetto del Contratto, il Cliente dichiara di aver valutato il prodotto e che esso risponde alle esigenze del Cliente. Resta altresì a carico del Cliente valutare se l'eventuale modulistica resa disponibile dal Fornitore per agevolare l'assolvimento degli obblighi di informativa e consenso (es. modello di privacy policy per App o informative presenti negli applicativi), quando disponibile, sia conforme alla Legislazione in materia di Protezione dei Dati Personali e adattare la stessa ove ritenuto opportuno.
10.5. E' altresì onere esclusivo del Cliente provvedere alla gestione dei Dati Personali in conformità alle Richieste avanzate dagli Interessati, e pertanto provvedere ad esempio agli eventuali aggiornamenti, integrazioni, rettifiche e cancellazioni dei Dati Personali.
10.6. E' onere del Cliente mantenere l'account collegato all'Email di notifica attivo ed aggiornato.
10.7. Il Cliente prende atto che, ai sensi dell'art. 30 del GDPR, il Fornitore è tenuto a mantenere un registro delle attività di trattamento eseguite per conto dei Titolari (o Responsabili) del Trattamento e a raccogliere a tal fine i dati identificativi e di contatto di ciascun Titolare (e/o Responsabile) del Trattamento per conto del quale il Fornitore agisce e che tali informazioni devono essere rese disponibili all'autorità competente, su richiesta. Pertanto, quando richiesto, il Cliente si impegna a dare al Fornitore i dati identificativi e di contatto sopra indicati con le modalità individuate dal Fornitore nel tempo e a mantenere aggiornate tali informazioni tramite i medesimi canali.

10.8. Il Cliente dichiara pertanto che le attività di trattamento dei Dati Personali, come descritte nei Contratti, nel presente Accordo e nei relativi DPA – Condizioni Particolari, sono lecite.

11. DURATA

11.1. Il presente Accordo avrà efficacia a decorrere dalla Data di Decorrenza dell'Accordo e cesserà automaticamente, alla data di cancellazione di tutti i Dati Personali da parte del Fornitore, come previsto nel presente Accordo e, se previsto, nei relativi DPA – Condizioni Particolari.

12. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONEDEI DATI PERSONALI

12.1. Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore cesserà ogni trattamento dei Dati Personali, e

12.1.1 provvederà alla cancellazione dei Dati Personali (ivi incluse eventuali copie) dai sistemi del Fornitore o da quelli su cui lo stesso abbia controllo entro il termine previsto nel Contratto, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria al fine di assolvere ad una disposizione di legge italiana o europea;

12.1.2. distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria ai fini del rispetto di norme di legge italiane o europee; e

12.1.3. manterrà a disposizione del Cliente i Dati Personali per l'estrazione per il periodo di 12 (dodici) mesi successivi alla cessazione del Contratto. Durante tale periodo, il trattamento sarà limitato alla sola conservazione finalizzata a mantenere i Dati Personali a disposizione del Cliente per l'estrazione di cui al punto 12.2.

12.2. Fermo restando quanto altrimenti previsto nel presente Accordo, il Cliente riconosce di poter estrarre i Dati Personali, alla cessazione del Servizio, nei modi convenuti nel Contratto e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto 12.1.3.

12.3. Resta inteso che quanto previsto ai punti 12.1e 12.2 non si applica ai Contratti aventi ad oggetto prodotti installati presso il Cliente o presso altri fornitori del Cliente. In tali casi, è responsabilità del Cliente estrarre, entro e non oltre 30 (trenta) giorni dal termine della Durata del Contratto, i Dati Personali che ritenga utile conservare; il Cliente riconosce che successivamente al predetto termine i Dati Personali potrebbero non essere più accessibili. Nei casi di cui al presente punto 12.3 resta altresì responsabilità del Cliente provvedere alla cancellazione dei Dati Personali nel rispetto delle norme di legge.

12.4. Restano ferme eventuali ulteriori o diverse disposizioni circa la cancellazione dei Dati Personali previste nei rispettivi DPA – Condizioni Speciali.

13. RESPONSABILITA'

13.1. Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente Accordo e dai relativi DPA – Condizioni Particolari e dalla Legislazione in materia di protezione dei Dati Personali.

13.2. Fatti salvi i limiti inderogabili di legge, il Fornitore sarà tenuto a risarcire il Cliente in caso di violazione del presente Accordo e/o dei relativi DPA – Condizioni Particolari entro i limiti massimi convenuti nel Contratto.

14. DISPOSIZIONI VARIE

14.1. Il presente Accordo sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsivoglia istruzione fornita in qualsiasi forma dal Cliente al Fornitore precedentemente alla data del presente Accordo in merito ai Dati Personali trattati nell'ambito dell'esecuzione del Contratto.

14.2. Il presente Accordo potrà essere modificato dal Fornitore dandone comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Cliente. In tal caso, il Cliente avrà il diritto di recedere dal Contratto con comunicazione scritta inviata al Fornitore a mezzo raccomandata con ricevuta di ricevimento nel termine di 15 giorni dal ricevimento della comunicazione del Fornitore. In mancanza di esercizio del diritto di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al presente Accordo si intenderanno da questi definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

14.3. In caso di conflitto tra le previsioni del presente Accordo e quanto previsto nel Contratto per la prestazione dei Servizi, o in documenti del Cliente non espressamente accettati dal Fornitore in deroga al presente Accordo e/ ai rispettivi DPA – Condizioni Speciali, prevarrà quanto previsto nel presente Accordo e nelle clausole dei relativi DPA – Condizioni Speciali.

ALLEGATO 1

Misure di sicurezza tecniche e organizzative

In aggiunta alle misure di sicurezza previste nel Contratto e nel DPA il Responsabile del Trattamento applica le seguenti misure di sicurezza tecniche e organizzative a seconda della tipologia di Servizio con cui vengono erogati o licenziati i Prodotti:

A – Cloud SaaS
B – Servizi Iaas
C – BPO (Business Process Outsourcing)
D – BPI (Business Process Insourcing)
E – On premises

A – CLOUD SaaS

Misure di sicurezza organizzative

Policy e Disciplinari utenti – Il Fornitore applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.

Autorizzazione accessi logici – il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.

Gestione interventi di assistenza – Gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale.

Valutazione d'impatto sulla protezione dei dati (DPA) – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento.

Incident Management – Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.

Data Breach – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.

È comunque demandata al Titolare del trattamento la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto e per i 60 giorni successivi al termine dello stesso.

Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.

Misure di sicurezza tecniche

Firewall, IDPS - I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi di Intrusion Detection & Prevention, mantenuti aggiornati in relazione alle migliori tecnologie disponibili.

Sicurezza linee di comunicazione - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.
Credenziali di autenticazione – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave.
Parola chiave – Relativamente alle caratteristiche di base ovvero obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.
Logging – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.
Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici.
Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery; essi garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.
Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.
Data center – L'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in un data center sito in Italia la cui gestione è demandata ad un fornitore certificato ISO 27001. In particolare le misure di sicurezza fisica poste a protezione del Data Center sono di seguito elencate:
• Perimetro di sicurezza esterno con accesso fisico limitato ai soli soggetti autorizzati;
• Recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento;
• Le aree esterne sono monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza;
• Accesso pedonale selettivo/singolo;
• Accesso veicolare selettivo;
• Perimetro di sicurezza interno;
• Presidio di vigilanza per controlli aree interne ed esterne, supervisione, Ronda armata;
• Allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i Data Center;
• Presidio di reception per la gestione degli accessi;
• Tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception;
• Perimetro di massima sicurezza interno;
• Varco di accesso sala sistemi dotato di protezione passiva interbloccato;
• Sistema di controllo accessi con gestione delle liste ABILITATI;
• Sensori magnetici stato porta in grado di rilevare lo stato della porta;
• Uscite d'emergenza dotate di sensori stato porta.
Tutti gli allarmi sono remotizzati al presidio di vigilanza.
Per il dettaglio delle misure di sicurezza adottate con riferimento ai servizi di data center erogati dai Responsabili Ulteriori del Trattamento, individuati nei DPA Condizioni Speciali, si fa rinvio alle misure di sicurezza indicate descritte dai medesimi Responsabili Ulteriori e rese disponibili nei relativi siti istituzionali ai seguenti indirizzi (o a quelli che saranno successivamente resi disponibili dai Responsabili Ulteriori):
Per i servizi di Data Center erogati da Telecom Italia: https://www.telecomitalia.com/tit/it/sustainability/reports-results/certifications.html/
Per i servizi di Data Center erogati da Amazon Web Services: https://aws.amazon.com/it/compliance/data-center/controls/

B – Servizi Iaas

Misure di sicurezza organizzative

Autorizzazione accessi logici – Il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
Utenze – Le utenze del servizio si scindono in utenze amministrative dell'infrastruttura di virtualizzazione e utenze amministrative della console di gestione dell'infrastruttura Cloud SigmaSistemi.
Le VM sono configurate con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione.
Sicurezza linee di comunicazione - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione.
Change Management – Il Fornitore ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa.
Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.
Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale).
Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. Ove previsto dagli accordi contrattuali, sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.
È comunque demandata al Titolare del trattamento la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto e per i 60 giorni successivi al termine dello stesso.

Misure di sicurezza tecniche

Logging – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.
Firewall, IDS/IPS – I sistemi anti-intrusione, quali Firewall e IDS/IPS, sono posizionati all'interno del segmento di rete che collega l'infrastruttura Cloud con Internet, al fine di intercettare ogni eventuale azione malevola volta a degradare, parzialmente o totalmente, l'erogazione del servizio. Nello specifico gli apparati adottati sono del tipo UTM SourceFire (Cisco), che includono sia la componente Firewall sia la componente IDS/IPS.
Incident Management– Il Fornitore ha in essere una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.
Alta affidabilità – il Fornitore garantisce l'alta affidabilità nei seguenti termini:
• L'architettura Server è basata sull'utilizzo della soluzione di virtualizzazione VMWare applicata mediante duplicazione fisica e virtuale dei singoli sistemi, al fine di garantire la tolleranza ai guasti e l'eliminazione dei single point of failure. In particolare in caso di failure di un sistema, il software di gestione dell'ambiente virtuale è in grado di ridistribuire le attività in corso verso gli altri sistemi (high availabilty e load balancing), riducendo al minimo i disservizi e garantendo la persistenza delle connessioni esistenti.
• Ciascun Server è attestato su una SAN mediante connessione fibra ottica ad alta velocità.
• Tutte le componenti dell'infrastruttura, tra i quali server, apparati di rete e sicurezza, sistemi Storage ed infrastruttura SAN, sono completamente ridondate per eliminare ogni single point of failure.
• L'architettura di rete è progettata per proteggere i sistemi di front-end da Internet e dalle reti interne mediante l'utilizzo di una DMZ protetta da due livelli di firewalling distinti (defense-in-depth): un firewall di frontiera connesso ad Internet ed un secondo firewall, che integra anche funzionalità di Intrusion Prevention, di proprietà dell'organizzazione, è messo a protezione della DMZ e dei sistemi di backend.

Data Center – L'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in un data center sito in Italia la cui gestione è demandata ad un fornitore certificato ISO 27001. In particolare le misure di sicurezza fisica poste a protezione del Data Center sono di seguito elencate:
• Perimetro di sicurezza esterno:
recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento;
le aree esterne sono monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza;
accesso pedonale selettivo/singolo;
accesso veicolare selettivo;
ronda armata.
• Perimetro di sicurezza interno:
presidio di vigilanza per controlli aree interne ed esterne, supervisione;
allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i Data Center;
presidio di reception per la gestione degli accessi;
tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception.
• Perimetro di massima sicurezza interno:
varco di accesso sala sistemi dotato di protezione passiva interbloccato;
sistema di controllo accessi con gestione delle liste ABILITATI;
sensori magnetici stato porta in grado di rilevare lo stato della porta;
uscite d'emergenza dotate di sensori stato porta.
Tutti gli allarmi sono remotizzati al presidio di vigilanza.

C – BUSINESS PROCESS OUTSOURCING (BPO)

Misure di sicurezza organizzative

Certificazioni – Il Fornitore si avvale di Data Center certificati:
Per le certificazioni Telecom Italia conseguite in ambito security e processi:
https://www.telecomitalia.com/tit/it/sustainability/reports-results/certifications.html/
Policy e Disciplinari utenti – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.
Autorizzazione accessi logici – Il Fornitore definisce i profili di accesso nel rispetto del least privilege necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
Gestione interventi di assistenza – Il Fornitore regolamenta la gestione degli interventi di assistenza allo scopo di garantire l'esecuzione delle sole attività disciplinate contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale.
Change Management – Il Fornitore ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa.
Valutazione d'impatto sulla protezione dei dati (DPA) – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento.
Incident Management – Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.
Data Breach – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.
Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento, corsi di formazione sulla corretta gestione dei dati personali.

Misure di sicurezza tecniche

Alta affidabilità – Il Fornitore garantisce l'alta affidabilità nei seguenti termini:
• L'architettura Server è completamente basata sull'utilizzo della soluzione di virtualizzazione VMWare applicata mediante duplicazione fisica e virtuale dei singoli sistemi, al fine di garantire la tolleranza ai guasti e l'eliminazione dei single point of failure. In particolare in caso di failure di un sistema, il software di gestione dell'ambiente virtuale è in grado di ridistribuire le attività in corso verso gli altri sistemi (high availabilty e load balancing), riducendo al minimo i disservizi e garantendo la persistenza delle connessioni esistenti.
• Ciascun Server è attestato su una SAN mediante connessione fibra ottica ad alta velocità.
• Tutte le componenti dell'infrastruttura, tra i quali server, apparati di rete e sicurezza, sistemi Storage ed infrastruttura SAN, sono completamente ridondate per eliminare ogni single point of failure.
• L'architettura di rete è progettata per proteggere i sistemi di front-end da Internet e dalle reti interne mediante l'utilizzo di una DMZ protetta da due livelli di firewalling distinti (defense-in-depth): un firewall di frontiera connesso ad Internet ed un secondo firewall, che integra anche funzionalità di Intrusion Prevention, di proprietà dell'organizzazione, è messo a protezione della DMZ e dei sistemi di backend.
Hardening – Sono in essere apposite attività di hardening finalizzate a prevenire il verificarsi di incidenti di sicurezza minimizzando le debolezze architetturali dei sistemi operativi, delle applicazioni e degli apparati di rete considerando - in particolare – le diminuzione dei rischi connessi alle vulnerabilità di sistema, la diminuzione dei rischi connessi al contesto applicativo presente sui sistemi e l'aumento dei livelli di protezione dei servizi erogati dai sistemi stessi.
Firewall, IDS/IPS – I sistemi anti-intrusione, quali Firewall e IDS/IPS, sono posizionati all'interno del segmento di rete che collega l'infrastruttura cloud con Internet, al fine di intercettare ogni eventuale azione malevola volta a degradare, parzialmente o totalmente, l'erogazione del servizio. Nello specifico gli apparati adottati sono del tipo UTM SourceFire (Cisco), che includono sia la componente Firewall sia la componente IDS/IPS.
Sicurezza linee di comunicazione - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.
Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale).
Credenziali di autenticazione – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave.
Parola chiave – Relativamente alle caratteristiche di base ovvero, obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.
Logging – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.
Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.
È comunque demandata al Titolare la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto e per i 60 giorni successivi al termine dello stesso.
Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery i quali garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

Vulnerability Assessment & Penetration Test – Il Fornitore effettua periodicamente attività di analisi delle vulnerabilità finalizzata a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo.
Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni / sistemi / reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica / logica ed avere accesso agli stessi.
I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto.
Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.
Data Center – L'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in un data center sito in Italia la cui gestione è demandata ad un fornitore certificato ISO 27001. In particolare le misure di sicurezza fisica poste a protezione del Data Center sono di seguito elencate:
• Perimetro di sicurezza esterno:
recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento;
le aree esterne sono monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza;
accesso pedonale selettivo/singolo;
accesso veicolare selettivo;
ronda armata.
• Perimetro di sicurezza interno:
presidio di vigilanza per controlli aree interne ed esterne, supervisione;
allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i Data Center;
presidio di reception per la gestione degli accessi;
tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception.
• Perimetro di massima sicurezza interno:
varco di accesso sala sistemi dotato di protezione passiva interbloccato;
sistema di controllo accessi con gestione delle liste ABILITATI;
sensori magnetici stato porta in grado di rilevare lo stato della porta;
uscite d'emergenza dotate di sensori stato porta.
Tutti gli allarmi sono remotizzati al presidio di vigilanza.

D - BPI – BUSINESS PROCESS INSOURCING

Misure di sicurezza organizzative

Policy e Disciplinari utenti – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.
Autorizzazione accessi logici – Il Fornitore definisce i profili di accesso e rispetto del *least privilege* necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
Data Breach – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.
Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.

Misure di sicurezza tecniche

Sicurezza linee di comunicazione - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione.
Backup & Restore – Ove previsto dagli accordi contrattuali, sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.

E – ON PREMISES

Misure di sicurezza organizzative

Policy e Disciplinari utenti – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare, in fase di assistenza tecnica, il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.
Autorizzazione accessi logici – Il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
Gestione interventi di assistenza – Il Fornitore regolamenta la gestione degli interventi di assistenza allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è rivestita dal Cliente.
Incident Management & Data Breach – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.
Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.

Misure di sicurezza tecniche

Sicurezza linee di comunicazione - Per quanto di propria competenza, in fase di gestione di interventi di assistenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.
Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale).
Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

NEXT CLOUD

CONDIZIONI INTEGRATIVE

Le presenti condizioni integrative ("Condizioni Integrative") modificano e/o integrano le Condizioni Generali Cloud di SigmaSistemi ("Condizioni Cloud") allo scopo di disciplinare i termini e le condizioni di utilizzo del software per la gestione della contabilità aziendale ("Software").

Resta inteso che, ove non diversamente disciplinato nelle presenti Condizioni Integrative, trovano applicazione le Condizioni Cloud. Ove non specificamente definiti nelle presenti Condizioni Integrative, i termini qui indicati con lettera maiuscola devono intendersi con il significato ad essi attribuito nelle Condizioni Cloud.

1. Moduli. Utilizzando il software in Cloud, il Cliente ha la possibilità di fruire di determinati Servizi Cloud associati a ciascuno dei moduli ("Moduli") dei quali il gestionale si compone, così come specificamente individuati nell'Ordine.

2. Licenza. Con la sottoscrizione del Contratto, incluse le presenti Condizioni Integrative, SigmaSistemi concede al Cliente, che accetta, una Licenza del Software limitata ai Moduli attivati e per il numero di Utenti specificato nell'Ordine, restando inteso che il Cliente potrà fruire del Software in modalità Saas attraverso le Credenziali di Accesso fornite al Cliente da SigmaSistemi.

3. Operazioni. A seconda dei Moduli prescelti, il numero di operazioni effettuabili attraverso il Software ("Operazioni") potrebbe essere limitato. Eventuali Operazioni, eccedenti il numero massimo eventualmente consentito, comporteranno il pagamento di Corrispettivi aggiuntivi.

4. Corrispettivi. A parziale deroga di quanto previsto al paragrafo 7.1 delle Condizioni Cloud e ferme restando le ulteriori previsioni di cui all'articolo 7, il Cliente, salvo diversamente indicato nell'Ordine, si impegna a versare i Corrispettivi dovuti entro 30 (trenta) giorni dal ricevimento di regolare fattura emessa da SigmaSistemi o, se diversamente indicato nell'Ordine. I Corrispettivi, salvo che sia diversamente indicato nell'Ordine, verranno fatturati da SigmaSistemi con cadenza annuale. Inoltre, sempre fatto salvo quanto diversamente stabilito nell'Ordine, in relazione ad alcuni predeterminati Moduli, il Corrispettivo potrebbe variare a seconda del numero di Utenti (a titolo puramente esemplificativo, da 1 a 10 Utenti potrebbe essere stabilito un Corrispettivo; da 11 a 20, un diverso e maggiore Corrispettivo; da 21 a 30, un diverso ed ancor maggior Corrispettivo; e così oltre).

5. API. Il Software Cloud è dotato di specifiche API che permettono lo scambio di dati e informazioni tra il Software e applicativi terzi ("Software Connessi"). Ferme restando le limitazioni di responsabilità a favore di SigmaSistemi di cui all'articolo 14 delle Condizioni Cloud, SigmaSistemi, negli inderogabili limiti di legge, non potrà in alcun modo essere ritenuta responsabile per danni diretti o indiretti e/o perdite, di qualunque natura o entità, che il Cliente o terzi dovessero subire in conseguenza di malfunzionamenti e/o elaborazioni errate del Software Cloud che siano conseguenza di (i) errori e/o malfunzionamenti nell'elaborazione e/o nella trasmissione di dati e informazioni imputabili a ciascuno dei Software Connessi e/o (ii) di uno scorretto utilizzo dell'API da parte del Cliente.

6. Terzi Autorizzati. Il Cliente, tramite apposita funzionalità del Software, ha il diritto di permettere a soggetti terzi che siano già a loro volta utenti di Software Cloud ("Terzi Autorizzati") di accedere al profilo del Cliente al fine di consultare i dati e i documenti ivi memorizzati e/o di utilizzare il Software in suo nome e per suo conto. Il Cliente riconosce e dichiara di essere esclusivo responsabile dell'autorizzazione concessa ai Terzi Autorizzati per utilizzare il Software Cloud in suo nome e per suo conto. Pertanto, ferme restando le limitazioni di responsabilità a favore di SigmaSistemi di cui all'articolo 14 delle Condizioni Cloud, SigmaSistemi, negli inderogabili limiti di legge, non potrà in alcun modo essere ritenuta responsabile per danni diretti o indiretti e/o perdite, di qualunque natura o entità, che il Cliente o terzi dovessero subire in conseguenza dell'uso o del non uso del Software Cloud da parte dei Terzi Autorizzati in maniera non conforme al Contratto, alle leggi vigenti e/o alle istruzioni impartite dal Cliente.