CONTRATTO DI CONTITOLARITÀ DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ARTICOLO 26, REGOLAMENTO UE 2016/679

Sottoscritto in Milano in data 7 Febbraio 2022

da e tra

GS1 ITALY con sede legale in Via Paleocapa n. 7, 20121 Milano, Codice Fiscale 80140330152, P. IVA 06758670969, in persona del legale rappresentante *pro tempore*, munito degli occorrenti poteri ("**GS1 Italy**")

E

GS1 ITALY SERVIZI S.r.l. con sede legale in Via Paleocapa, 7, 20121 Milano, Codice Fiscale e Partita IVA 06166030962, in persona del legale rappresentante *pro tempore*, munito degli occorrenti poteri ("**GS1 Italy Servizi**")

GS1 Italy e GS1 Italy Servizi di seguito congiuntamente indicate come le "**Parti**" e individualmente come la "**Parte**"

PREMESSO CHE

(i) GS1 Italy è una associazione senza scopo di lucro e rappresenta in Italia GS1, organismo internazionale che amministra e coordina la corretta implementazione del sistema "GS1" per la codifica dei prodotti nel settore del largo consumo (in precedenza denominato "EAN/UCC"), nonché il sistema "ECR" relativo all'interfacciamento strategico ed operativo tra industria e distribuzione e fra questi soggetti ed il consumatore finale;

(ii) GS1 Italy è socio unico di GS1 Italy Servizi;

(iii) a propria volta GS1 Italy Servizi presta servizi e assistenza alle imprese, in particolare in ambito di realizzazione e diffusione di tecniche, soluzioni operative, standard e strumenti atti ad ottimizzarne l'efficienza dei processi relativi al sistema produttivo e distributivo, e, dunque, è società statutariamente deputata alla prestazione, soprattutto a favore delle imprese associate a GS1 Italy, di servizi volti a facilitare a queste ultime la concreta implementazione di regole, standard e specifiche tecniche elaborate in seno a GS1 Italy stessa;

(iv) sussiste, dunque, tra GS1 Italy e GS1 Italy Servizi, giuridicamente e di fatto, uno stretto legame funzionale ed organizzativo, tanto che entrambe hanno in comune e condividono, in senso lato, scopi ed obiettivi, nonché strumenti e risorse necessari od utili a perseguirli, anche nell'ambito del trattamento dei dati personali;

(v) ai sensi dell'articolo 4 n. 7) del Regolamento UE 2016/679, *Regolamento Generale sulla Protezione dei Dati Personali*, il "titolare del trattamento" è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*";

(vi) stanti le ragioni di sinergia e di condivisione di risorse sopra sinteticamente esposte, le Parti ritengono coerente ed opportuno gestire il trattamento di taluni dati personali, come *infra* meglio indicati, in regime di contitolarità;

(vii) ai sensi dell'articolo 26 del Regolamento UE 2016/679, *Regolamento Generale sulla Protezione dei Dati Personali*, i contitolari del trattamento "(...) *determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13*

e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti";

(viii) come anche evidenziato dal Gruppo di Lavoro ex Articolo 29 (oggi Comitato Europeo per la Protezione dei Dati) nel parere 1/2010, si è in presenza di una situazione di contitolarità "(...) *quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti che caratterizzano il responsabile del trattamento* (...) *la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale. In effetti, quando vi è una pluralità di attori, questi possono avere una relazione molto stretta (condividendo, ad esempio, tutte le finalità e tutti gli strumenti di un trattamento) o più distante (condividendo ad esempio solo le finalità o i mezzi, o una parte di essi)*";

(ix) alla luce di quanto precede ed in conformità a quanto indicato dall'articolo 26 del Regolamento UE 2016/679, *Regolamento Generale sulla Protezione dei Dati Personali*, le Parti intendono con il presente contratto disciplinare, come in effetti disciplinano, i rispettivi compiti, ruoli e responsabilità nonché perimetro di azione per quanto concerne il trattamento e la gestione di dati personali;

TUTTO CIÒ PREMESSO
LE PARTI STIPULANO E CONVENGONO QUANTO SEGUE

1. PREMESSE ED ALLEGATI

1.1 Le premesse e gli allegati al presente contratto di contitolarità ("**Contratto**") ne costituiscono parte integrante e sostanziale.

1.2 In caso di contrasto e/o incongruenze tra quanto previsto dal presente Contratto e quanto indicato nei relativi allegati prevarrà il presente Contratto.

1.3 Le Parti sin da ora concordano che gli Allegati al presente Contratto potranno essere, di tempo in tempo, rivisti, modificati e/o aggiornati e che ciascuna nuova versione degli Allegati, accettata e sottoscritta da entrambe le Parti, andrà a sostituire la precedente ed a formare parte integrante e sostanziale del Contratto in luogo di quest'ultima.

2. DEFINIZIONI

2.1 Salvo ove diversamente previsto dal presente Contratto, i seguenti termini ed espressioni con iniziale maiuscola avranno il significato indicato di seguito:

"**Archivio/i**":	si intendono, congiuntamente e/o singolarmente, gli archivi, i database, i software e, in generale, la strumentazione, cartacea/fisica e/o informatica o telematica, utilizzata sia da GS1 Italy sia da GS1 Italy Servizi ai fini del trattamento dei Dati Personali e così come indicata nell'**Allegato 1-*bis*** al presente Contratto e come potrà essere, di tempo in tempo, eventualmente aggiornata;
"**Codice Privacy**":	indica la normativa italiana in materia di protezione dei dati personali di cui al D.Lgs. n. 196/2003 (e relativi allegati) e sue successive modifiche ed integrazioni (quali, in particolare, apportate con D.Lgs. n. 101/2018);
"**Contitolare/i**":	ha il significato ad esso attribuito dal combinato disposto degli articoli 4 n. 7 e 26 del Regolamento UE 2016/679. Ai fini del presente Contratto, per Contitolare/i devono intendersi, rispettivamente e congiuntamente, a seconda dei casi, GS1 Italy e GS1 Italy Servizi;
"**Contratto**":	indica il presente Contratto redatto ai sensi dell'articolo 26, Regolamento UE 2016/679, in uno con i rispettivi Allegati, come di tempo in tempo, modificati, integrati, aggiornati e sostituiti;

"Dati Personali" o **"Dati"**:	indica qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compresi, a titolo meramente esemplificativo, un numero di identificazione, dati relativi all'ubicazione, un identificativo online. Nell'ambito del presente Contratto si intenderanno, in particolare, per "Dati Personali" quelli riferibili agli Interessati di cui *infra,* oggetto del Trattamento Condiviso e raccolti, trattati, elaborati tramite gli Archivi;
"Garante":	si intende il Garante per la Protezione dei Dati Personali, ossia l'autorità di controllo italiana per la protezione dei dati personali come definita dagli articoli 51 e seguenti del Regolamento UE 2016/679;
"Interessato/i":	si intende la/e persona/e fisiche cui si riferiscono i Dati Personali;
"Leggi sulla Protezione dei Dati":	indica tutte le leggi e i regolamenti, inclusi ma non limitati al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e al Codice Privacy, come sopra definito, nonché provvedimenti di volta in volta in vigore che sono applicabili al trattamento dei dati personali effettuato in forza di questo Contratto;
"Regolamento" o **"RGPD"**:	si intende il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (*Regolamento Generale sulla Protezione dei Dati*);
"Titolare/i":	si intende il soggetto al quale, ai sensi dell'articolo 4, punto 7), GDPR "(…) *singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali*". Ai fini del presente Contratto per Titolare/i si intende ciascuna Parte in relazione ad un Trattamento Esclusivo, di cui *infra*;
"Trattamento":	si intende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di Dati;
"Trattamento/i Condiviso":	indica, singolarmente e congiuntamente, il Trattamento e i Trattamenti di Dati Personali condiviso tra i Contitolari e meglio descritto *sub* articolo 4 che segue;
"Trattamento Esclusivo":	indica il Trattamento di dati personali che ciascuna Parte svolge per il perseguimento di proprie finalità esclusive e non condivise con l'altra Parte e, dunque, diverse da quelle indicate nel presente Contratto, come precisato all'articolo 4.2 che segue.

3. OGGETTO DEL CONTRATTO

3.1 Le Parti concordano che oggetto di Trattamento Condiviso in forza del presente Contratto saranno i Dati Personali riferibili agli Interessati, come indicato al successivo articolo 4 e come meglio dettagliato nell'**Allegato 1** al presente Contratto, come, di tempo in tempo, eventualmente aggiornato e/o integrato.

3.2 Con la sottoscrizione del presente Contratto, le Parti intendono, dunque, definire e/o disciplinare, in relazione al Trattamento Condiviso, ai sensi e per gli effetti di cui all'articolo 26, Regolamento, i ruoli e le responsabilità di ciascuna Parte in relazione al Trattamento Condiviso.
3.3 Fermo restando quant'altro meglio previsto da questo Contratto, ciascun Contitolare garantisce all'altro Contitolare che tratterà i Dati Personali in conformità alle Leggi sulla Protezione dei Dati, esclusivamente per le finalità e secondo i termini di questo Contratto.

4. TRATTAMENTO CONDIVISO DEI DATI PERSONALI

4.1 Le Parti concordano di assumere il ruolo di Contitolari, ai sensi del Regolamento, rispetto al Trattamento dei Dati Personali degli Interessati che vengono raccolti secondo una o più delle modalità di seguito riportate:

- in occasione di contatti stabiliti direttamente e di persona con gli Interessati, verbalmente o tramite utilizzo di moduli o formulari cartacei; e/o
- on-line tramite compilazione di moduli e *form* elettronici pubblicati sui siti web (ivi espressamente incluse pagine su social network e/o applicazioni mobile) di uno o di entrambi i Contitolari ovvero tramite altri strumenti elettronici o telematici (anche di tracciamento, quali i cookie);
- attraverso acquisizione dei dati da soggetti terzi, nel rispetto dei requisiti di cui al GDPR,

e che sono già presenti negli Archivi alla data di sottoscrizione di questo Contratto, e/o che saranno - successivamente e nel corso della durata del Contratto stesso - inseriti e trattati tramite gli Archivi, il tutto secondo quanto meglio riportato nell'Allegato 1 al presente Contratto.
4.2 In aggiunta a quanto poc'anzi esposto, i Titolari, disgiuntamente tra loro, individuano specifiche finalità e/o mezzi di Trattamento strettamente legati alle rispettive attività, diversi e/o ulteriori rispetto a quelli di cui al paragrafo 4.1 che precede, e quali derivanti dal perseguimento dei rispettivi oggetti sociali e/o dall'adempimento di obblighi di legge su ciascuna di esse singolarmente gravanti.
4.3 Fermo restando quanto indicato al successivo articolo 5, le Parti, per quanto di rispettiva competenza, si impegnano a rispettare, applicare, a far applicare ed a far rispettare, anche ai sensi e per gli effetti di cui all'articolo 1381, codice civile, al proprio personale, dipendente e non, e collaboratori o fornitori esterni appositamente autorizzati al trattamento ai termini di legge, secondo quanto indicato al successivo articolo 8.1, le disposizioni del presente Contratto e quelle di cui alle Leggi sulla Protezione dei Dati e ad adottare misure di sicurezza adeguate a salvaguardare i Dati Personali contro i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta secondo quanto *infra* meglio indicato.

5. OBBLIGHI DI INFORMATIVA E DIRITTI DEGLI INTERESSATI

5.1 In relazione agli obblighi di informativa di cui agli articoli 13 e 14 del Regolamento, i Contitolari si obbligano, in relazione al Trattamento Condiviso, a fornire agli Interessati l'informativa e/o ad integrare la propria informativa secondo il modello che sarà tra le Parti condiviso, in ogni caso provvedendo a portare a conoscenza degli Interessati l'informativa così aggiornata o modificata ed avendo cura di documentare tale adempimento. Resta espressamente inteso che l'onere e la responsabilità di porre in essere e dare attuazione concreta a tale adempimento grava in misura uguale su ciascun Contitolare in relazione alla modulistica ed ai canali di contatto con gli Interessati da ciascuno di essi concretamente adottati.
5.2 Per quanto riguarda il Trattamento Condiviso, gli interessati sono informati dei diritti loro riconosciuti dagli articoli 15 - 22 del Regolamento mediante il modello di informativa sopra citato.
5.3 Allo scopo di consentire agli Interessati il concreto ed effettivo esercizio dei rispettivi diritti, le Parti hanno individuato l'indirizzo email privacy@gs1it.org dal quale sarà fornito riscontro alle richieste degli Interessati stessi.
5.4 Per gli scopi sopra descritti ed in conformità alle disposizioni dell'articolo 26, 2° comma, del Regolamento, i Contitolari si impegnano a mettere a disposizione degli Interessati, anche tramite pubblicazione on-line sui propri rispettivi siti web istituzionali, un estratto del presente Contratto, nel formato che sarà condiviso tra le Parti.

6. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

6.1 I Dati Personali oggetto di Trattamento Condiviso saranno conservati per il periodo di tempo condiviso tra le Parti e che sarà indicato in un documento conforme, nella sostanza, al modello che costituisce **Allegato 2** al presente Contratto, e limitatamente al Trattamento Condiviso.
6.2 La proroga e l'allungamento del periodo di conservazione di cui all'Allegato 2 da parte di uno od entrambi i Contitolari è da considerarsi escluso, salvo che i Contitolari congiuntamente individuino i motivi di liceità, necessità e finalità che possano giustificare un'estensione temporale della conservazione e ne diano atto in un documento scritto e sottoscritto da entrambe le Parti.
6.3 Al di fuori dei casi sopra indicati, in relazione a particolari esigenze derivanti da specifiche circostanze (quali, a mero titolo esemplificativo, la necessità di produrre nei confronti di un'autorità competente, ivi espressamente incluso il Garante, i Dati Personali) o da specifici incombenti, di legge o di contratto, che riguardino o gravino su di una sola delle Parti, i Contitolari si impegnano sin da ora a portare all'attenzione dei rispettivi Referenti le circostanze del caso ed a definire in buona fede e nel rispetto delle disposizioni del Regolamento applicabili quali azioni sia lecito e possibile intraprendere.

7. MISURE DI SICUREZZA E GESTIONE DI *DATA BREACHES*

7.1 Ciascun Contitolare, per quanto di rispettiva competenza, si impegna a collaborare nella individuazione e pianificazione, ad adottare e a dare concreta attuazione a misure tecniche ed organizzative che, tenuto conto delle attuali conoscenze in materia e dei costi di applicazione e di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento Condiviso, come anche della probabilità e gravità di eventuali rischi per i diritti e le libertà delle persone fisiche derivanti dal Trattamento Condiviso, garantiscano un livello di sicurezza adeguato rispetto a tali rischi. Ciascun Contitolare, in particolare, si impegna a dare attuazione alle misure *sub* **Allegato 3** al presente Contratto, per quanto di propria competenza, ferma la possibilità per ciascun Contitolare di elaborare, proporre e sottoporre all'attenzione ed all'approvazione dell'altro misure diverse ed integrative rispetto a quelle di cui al citato Allegato 3.
7.2 Eventuali incidenti di sicurezza, violazioni o cosiddetti "*data breaches*" su Dati oggetto di Trattamento Condiviso, quali disciplinati dagli articoli 33 e 34 del Regolamento, dovranno essere gestite ed elaborate secondo la procedura stabilita dalle Parti che, per comodità di riferimento, viene riprodotta quale **Allegato 4** al presente Contratto.
7.3 Nel caso in cui l'effettuazione del Trattamento Condiviso dovesse richiedere la conduzione preliminare di una valutazione di impatto ai sensi dell'articolo 35 del Regolamento, le Parti concorderanno separatamente ed in buona fede i rispettivi ruoli e responsabilità in relazione a tale adempimento allo scopo di garantire, anche sotto tale aspetto, il costante rispetto di quanto previsto dal Regolamento.

8. ISTRUZIONI SUL TRATTAMENTO DEI DATI E NOMINA DI RESPONSABILI ESTERNI

8.1 Ciascun Contitolare si impegna a porre in essere, all'interno della propria organizzazione imprenditoriale, di propria iniziativa ed a proprio onere e spese, tutti gli adempimenti disciplinati dal Regolamento anche in relazione al Trattamento Condiviso e, in particolare, oltre a quanto precisato all'articolo 4.3 che precede, a:

- non svolgere alcuna operazione di Trattamento Condiviso dei Dati - compresa la comunicazione e la diffusione a soggetti terzi - diversa da quelle indicate nell'informativa consegnata agli Interessati e per cui sia stato rilasciato il consenso, ove necessario ai sensi di legge e/o previsto dal modello organizzativo adottato, implementando tutte le misure idonee ad evitare che ciò succeda;
- individuare nell'ambito della propria struttura imprenditoriale i soggetti autorizzati al Trattamento Condiviso, ai sensi dell'articolo 29 del Regolamento, impartendo loro le necessarie istruzioni per un corretto adempimento delle disposizioni di legge e del presente Contratto. Sarà onere di ciascun Contitolare aggiornare, ove necessario, le lettere di incarico e autorizzazione al trattamento già consegnate e vigilare sull'operato dei propri incaricati o soggetti autorizzati al trattamento, provvedendo ad istruirli e formarli. Programmi specifici di formazione relativi al Trattamento Condiviso potranno essere, di tempo in tempo, valutati ed organizzati da parte dei Contitolari, previa condivisione e accordo in merito a proposte formative, date, luoghi, relatori e costi.

8.2 La predisposizione di eventuali documenti contrattuali di nomina di responsabili del trattamento dei Dati oggetto di Trattamento Condiviso ai sensi dell'articolo 28 del Regolamento, così come l'autorizzazione, generale e/o specifica, alla nomina di (sub) responsabili del Trattamento Condiviso dovranno essere condivise

dai Contitolari e comunque sottoscritte ed eseguite da entrambi, pena la relativa inefficacia e/o invalidità e la responsabilità esclusiva per eventuali violazioni, di legge o di contratto, relative al Trattamento Condiviso (o di porzione di esso) oggetto di esternalizzazione, in capo alla Parte che abbia violato la presente clausola. Le Parti si riservano sin da ora di valutare gli eventuali interventi da apportare alle nomine a responsabile del trattamento in corso alla data di sottoscrizione di questo Contratto e che abbiano un impatto sul Trattamento Condiviso.
Senza pregiudizio per quanto precede, le Parti sin da ora concordano che, ferme le necessarie personalizzazioni da condursi caso per caso, il contratto di designazione di eventuali responsabili esterni dovrà essere conforme, nella sostanza, all'**Allegato 5** al presente Contratto.

9. DURATA

9.1 Il presente Contratto avrà decorrenza dalla data di relativa sottoscrizione ed avrà durata indeterminata, salvo quanto di seguito indicato.
9.2 Le Parti si danno reciprocamente atto e concordano che il presente Contratto si risolverà e cesserà automaticamente in caso di cessazione, per qualsivoglia ragione e/o causa, del Trattamento Condiviso.

10. RESPONSABILITÀ

10.1 Alla luce di quanto previsto agli articoli che precedono, ciascun Contitolare riconosce, dichiara ed accetta di essere responsabile congiuntamente con l'altro Contitolare sia nei confronti degli Interessati sia nei confronti del Garante in relazione al Trattamento Condiviso dei Dati Personali posto in essere ai sensi del presente Contratto.
10.2 Senza pregiudizio per quanto precede, ciascun Contitolare si impegna a manlevare e mantenere indenne (ove del caso, comparendo in giudizio e consentendone l'estromissione ex art. 108 c.p.c.) l'altro Contitolare da ogni eventuale responsabilità, danno, azione, reclamo - sia degli Interessati sia del Garante o di altra Autorità di Controllo competente -, pregiudizio, costo, onere o spesa (ivi incluse eventuali e ragionevoli spese legali) che dovessero derivare all'altro Contitolare dal mancato rispetto e/o violazione da parte propria, di propri dipendenti, collaboratori, incaricati delle disposizioni di cui al presente Contratto, del Regolamento e/o della normativa, di tempo in tempo, vigente ed applicabile al Trattamento Condiviso, con il conseguente obbligo di risarcire tutti gli eventuali danni che potrebbero derivarne al Contitolare adempiente.
10.3 Resta espressamente inteso tra le Parti che gli articoli 10.1 e 10.2 non si applicano al Trattamento Esclusivo.

11. FORO COMPETENTE

11.1 Il presente Contratto è disciplinato dalla legge sostanziale e processuale italiana e dovrà essere interpretato in conformità a quest'ultima.
11.2 Tutte le controversie derivanti da questo Contratto, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, saranno devolute alla competenza esclusiva del Tribunale di Milano.

12. COMUNICAZIONI

12.1 Eventuali comunicazioni dovute in forza del presente Contratto dovranno essere trasmesse agli indirizzi delle Parti indicati nell'epigrafe di questo Contratto o all'eventuale diverso indirizzo (anche email) che ciascuna Parte potrà provvedere a comunicare all'altra mediante comunicazione inoltrata secondo le modalità sopra descritte.
12.2 Ciascuna Parte si riserva, ove ritenuto necessario, di comunicare all'altra Parte l'eventuale nominativo e/o i dati di contatto di un proprio referente (di seguito "**Referente/i**") con la funzione di monitorare l'esecuzione del Contratto nell'ambito della disciplina qui prevista, di supportare il *Data Protection Officer*, ove presente e nominato, limitatamente al Trattamento Condiviso oggetto di Contratto, con esclusione di qualsiasi potere inerente alla modificazione della medesima disciplina contrattuale.

13. CONTRATTO INTEGRALE E MODIFICHE

13.1 Il presente Contratto, unitamente alle relative Premesse ed Allegati che ne formano parte integrante e sostanziale, costituisce l'unico ed integrale contratto tra le Parti in relazione alla materia che ne è oggetto e sostituisce ogni altro contratto, accordo o impegno, scritto o orale, che le Parti possano aver precedentemente assunto in relazione a tale materia.

13.2 Nessuna modifica od integrazione del presente Contratto o ad alcuno dei relativi Allegati sarà vincolante per le Parti se non concordata per iscritto tra le Parti medesime e sottoscritta dai rispettivi rappresentanti autorizzati.

14. CLAUSOLE FINALI

14.1 Le Parti concordano e danno reciprocamente atto che la stipulazione e l'esecuzione del presente Contratto risponde ad un obbligo previsto dal Regolamento e comunque ad esigenze di trasparenza dei rapporti e dei ruoli dei Contitolari e che, pertanto, nessun compenso e/o corrispettivo è dovuto da una Parte nei confronti dell'altra in relazione all'esecuzione delle attività qui disciplinate.

14.2 Salvo quanto previsto in materia di cessione di azienda o ramo di azienda, il presente Contratto non potrà essere ceduto, in qualsiasi forma e anche parzialmente, da una delle Parti senza il preventivo consenso scritto dell'altra Parte; in caso contrario, la Parte non informata potrà risolvere il presente Contratto senza preavviso, fatto salvo l'eventuale maggior danno.

14.3 Il presente Contratto costituisce manifestazione integrale della volontà negoziale delle Parti che, avendo avuto occasione di negoziare e negoziato il contenuto di tutte le relative clausole, dichiarano, quindi, di approvare specificamente, singolarmente e nel loro insieme, con conseguente inapplicabilità degli articoli 1341 e 1342 del codice civile.

14.4 La numerazione e titolazione degli articoli del presente Contratto hanno sole finalità di chiarezza espositiva e non potranno influenzare l'interpretazione del Contratto, che dovrà essere effettuata, nel rispetto dei criteri ermeneutici previsti dalla legge applicabile, avendo primario riguardo alle finalità perseguite dalle Parti, ai contenuti complessivi dell'accordo negoziale ed al tenore letterale del Contratto.

14.5 Per tutto quanto non espressamente previsto nel presente Contratto troveranno integrale applicazione le disposizioni del Codice Privacy, del Regolamento e di eventuali altre fonti, ivi inclusi eventuali provvedimenti del Garante in relazione alla materia del Trattamento e della protezione dei dati personali.

*

In fede di quanto precede, le Parti hanno sottoscritto il presente contratto in n. 2 esemplari nella data e nel luogo in epigrafe indicati

GS1 Italy
Il legale rappresentante

GS1 Italy Servizi S.r.l.
Il legale rappresentante

Elenco Allegati:

Allegato 1 – Descrizione dei Trattamenti Congiunti
Allegato 1bis - Descrizione degli Archivi
Allegato 2 – Policy sulla conservazione dei Dati Personali - *Data Retention Policy*
Allegato 3 – Misure di sicurezza
Allegato 4 – Procedura di gestione dei *data breaches*
Allegato 5 – Documento di designazione di responsabile in relazione al Trattamento Condiviso

ALLEGATO 1

DESCRIZIONE DEI TRATTAMENTI CONGIUNTI

Il presente Allegato riporta le informazioni relative al/ai Trattamento/i Congiunto/i dei dati personali oggetto del Contratto.

Tipologie di Dati Personali oggetto di trattamento

- dati personali identificativi, comprensivi di nome, cognome, codice fiscale, azienda di appartenenza, ruolo ricoperto (*job description*) presso l'azienda;
- dati di contatto: indirizzo dell'azienda di appartenenza, email aziendale, telefono (fisso e mobile) aziendale;
- dati e informazioni relativi a servizi, eventi, attività proposti dai Contitolari ed ai quali l'Interessato abbia aderito e/o richiesto informazioni e/o rispetto ai quali abbia manifestato interesse;
- dati acquisiti tramite sistemi di tracciamento online (tipicamente cookie);
- log e dati personali associati, ivi incluse le credenziali di accesso a prodotti e/o servizi "GS1";
- dati aggregati e/o anonimizzati derivanti da elaborazioni interne.

Categorie di interessati a cui fanno riferimento i Dati Personali

- associati "GS1", associati IBC, associati ADM;
- associati "prospect" (*i.e.* soggetti che hanno manifestato interesse ad associarsi ed a fruire dei servizi "GS1");
- utenti ECR;
- clienti (*i.e.* soggetti che abbiano richiesto e/o acquistato uno specifico servizio) e clienti *prospect*;
- utenti web/social (i) che si siano registrati ai siti web e/o (ii) che abbiano visitato e interagito con le pagine web, e/o (iii) che abbiano formulato richieste di informazioni e/o di servizi compilando *form* elettronici di registrazione presenti sui siti web gestiti dai Contitolari, ivi espressamente inclusi gli utenti "Interno1".

Natura e finalità del Trattamento Condiviso dei Dati Personali

Per le finalità del Contratto il Trattamento Condiviso include qualsivoglia operazione o complesso di operazioni di trattamento così come disciplinata dal Regolamento *(i.e.* la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati personali) finalizzata:

- a individuare, definire e pianificare strategie e politiche congiunte di realizzazione dei sistemi standard GS1, dei processi condivisi ECR e dei servizi a questi complementari e/o con questi ultimi connessi;
- a individuare, elaborare, pianificare, realizzare e veicolare un'efficace strategia di comunicazione e le connesse attività ed iniziative verso gli Interessati aventi ad oggetto l'offerta di prodotti e di servizi di entrambe le Parti, anche in una logica di completezza del servizio e di allargamento dell'offerta per il destinatario finale;
- ad analizzare ed elaborare informazioni aggregate, all'interno del "gruppo imprenditoriale", in merito agli Interessati per finalità di ottimizzazione e migliore gestione dell'attività delle Parti ed in funzione dell'elaborazione delle politiche condivise sopra menzionate.

*

Le Parti concordano che il presente Allegato potrà essere rivisto e/o integrato in caso di mutamenti sostanziali in uno o più degli elementi del Trattamento Condiviso, come sopra descritto.

ALLEGATO 1-*BIS*

DESCRIZIONE DEGLI ARCHIVI

I dati personali oggetto del Contratto e dei Trattamenti Condivisi sono, alla data di sottoscrizione del presente Contratto, gestiti ed archiviati tramite un sistema gestionale che sarà dismesso e sostituito nel corso dell'anno 2022.

Il sistema gestionale attuale sarà sostituto con i seguenti sistemi gestionali, che saranno, tra l'altro, utilizzati per la gestione ed il trattamento dei dati personali oggetto dei Trattamenti Condivisi:

- il sistema gestionale ERP SAP Business One;
- il sistema gestionale CRM SAP Customer Cloud CX.

I dati personali oggetto del Contratto potranno, inoltre, essere archiviati e trattati tramite i sistemi di posta elettronica di ciascuna delle Parti.

In via meramente residuale tali dati potranno essere oggetto di trattamento e/o archiviazione cartacea, ove necessario per le finalità per i quali sono trattati.

ALLEGATO 2

POLICY SULLA CONSERVAZIONE DEI DATI PERSONALI
DATA RETENTION POLICY

VERSION	DATA	AUTORE	NOTE
1.0	Gennaio 2022	GS1 Italy – GS1 Italy Servizi S.r.l.	Versione iniziale

INDICE

1. PREMESSA

Uno dei principi generali sanciti dal Regolamento (UE) 2016/679, *Regolamento Generale sulla Protezione dei Dati Personali* (**"Regolamento"**) prevede che la conservazione dei dati personali debba essere temporalmente e funzionalmente limitata al perseguimento degli scopi (legittimi) per i quali i dati sono stati raccolti e vengono trattati: si tratta del principio di "limitazione della conservazione".

In, particolare, l'art. 5, comma 1, lett. e), Regolamento, stabilisce che "(…) *i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)".*

In aggiunta, il Considerando n. 39 del Regolamento prescrive che i Dati personali non siano conservati per un periodo più esteso rispetto al necessario e, pertanto, pone a carico del titolare del trattamento l'obbligo di stabilire un termine per la cancellazione dei dati personali oggetto di operazioni di trattamento.

In ragione di quanto precede, le organizzazioni hanno ritenuto necessario adottare la presente policy sulla conservazione dei dati personali.

Il presente documento ha, infatti, lo scopo di fungere da supporto nelle decisioni relative alla conservazione o all'eliminazione di dati personali trattati da GS1 Italy e da GS1 Italy Servizi S.r.l. (di seguito congiuntamente "**Organizzazioni**" e individualmente "**Organizzazione**") ed è redatta in conformità alle disposizioni del Regolamento.

Questo documento si rivolge a tutti i dipendenti e collaboratori delle Organizzazioni (qualunque sia il relativo inquadramento e mansione) e costituisce una guida agli adeguati periodi di conservazione dei dati personali trattati dalle Organizzazioni stesse.

Il presente documento si applica a tutti i tipi di dati personali creati, ricevuti o trasmessi durante le attività interne e commerciali delle Organizzazioni, ad esempio dati identificativi, recapiti, identificatori personali (quali codice fiscale e partita IVA), informazioni lavorative, esperienza professionale, formazione e competenze, viaggi e spese, informazioni relative all'account dell'utente, informazioni di navigazione, il tutto come di seguito meglio precisato.

2. DEFINIZIONI

Allo scopo di facilitare la lettura e la comprensione di quanto indicato nel prosieguo si riportano di seguito alcune delle principali definizioni di cui alla norma poc'anzi menzionata.

Fermo quant'altro previsto dal presente documento, i termini con iniziale maiuscola avranno il significato di seguito meglio precisato:

"Base giuridica"	si intende una delle condizioni di liceità del trattamento di cui all'articolo 6 del Regolamento;
"Cancellazione dei dati"	indica la distruzione definitiva – fisica o tecnica – idonea a rendere non più recuperabili mediante gli ordinari mezzi disponibili in commercio le informazioni contenute in un supporto elettronico e/o cartaceo;

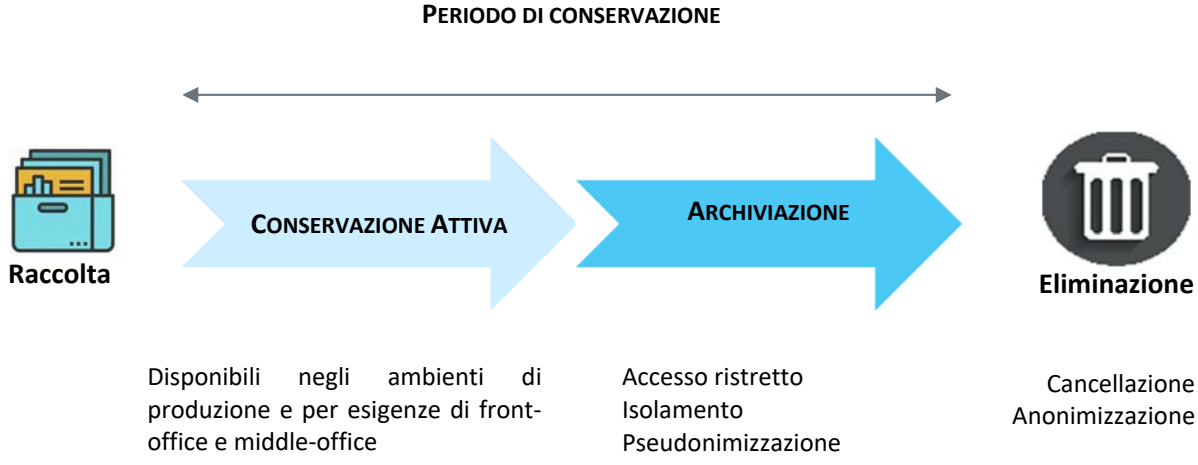
"Codice"	indica il D.Lgs. n. 196/2003, *Codice in materia di protezione dei dati personali*, e successive modifiche ed integrazioni (ivi incluse, in particolare, quelle di cui al D.Lgs. n. 101/2018);
"Contitolari"	indica i due o più titolari che, ai sensi dell'articolo 26, Regolamento, determinano congiuntamente le finalità e i mezzi del trattamento. Ai fini della presente policy il termine "Contitolari" indica GS1 Italy e GS1 Italy Servizi S.r.l., quando agiscono rispetto ai trattamenti condivisi oggetto dell'accordo di contitolarità in essere tra le citate parti;
"Dati personali" o "Dati"	si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, 1° comma, n. 2, Regolamento);
"Destinatari"	indica gli amministratori, i dirigenti, i dipendenti, i collaboratori, i Responsabili del trattamento, i fornitori e i soggetti terzi che effettuano operazioni di trattamento dei dati di cui le Organizzazioni sono Titolari (o Contitolari) e nei confronti dei quali trova applicazione la presente policy;
"Garante"	indica l'Autorità di Controllo italiana ossia il Garante per la Protezione dei Dati personali;
"Informativa"	indica l'informativa sul trattamento dei dati personali da rendere all'Interessato ai sensi degli artt. 13 e 14 del Regolamento;
"Interessato"	è la persona fisica (identificata o identificabile) cui si riferiscono i dati personali;
"Leggi sulla protezione dei dati"	indica tutte le leggi e i regolamenti, inclusi ma non limitati al Regolamento (UE) 2016/679 in materia di protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione dei dati (RGPD) e al Codice, nonché provvedimenti, autorizzazioni e/o raccomandazioni, di tempo in tempo in vigore ed applicabili al Trattamento dei Dati personali;
"Policy"	indica la presente policy sulla conservazione dei dati personali;
"Responsabile del trattamento" o "Responsabile"	si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare (o dei contitolari) del trattamento (articolo 4, 1° comma, n. 8, GDPR);
"Referente" o "Referente Privacy"	indica il soggetto, persona fisica o ufficio, (eventualmente) designato dal Titolare o a cui siano stati delegati i poteri o i compiti per l'implementazione delle disposizioni del Regolamento all'interno di una o entrambe le Organizzazioni e della gestione delle tematiche associate alla tutela dei dati personali all'interno dell'organizzazione aziendale e/o nei confronti dei terzi. I dettagli del Referente sono opportunamente resi noti da parte delle Organizzazioni a tutti i dipendenti e collaboratori;

"Regolamento"	indica il Regolamento (UE) 2016/679, Regolamento Generale sulla protezione dei dati;
"Soggetti Autorizzati"	indica i dipendenti e/o i collaboratori delle Organizzazioni autorizzati da queste ultime a compiere operazioni di Trattamento di Dati personali nell'esercizio delle mansioni e delle funzioni agli stessi affidate;
"Titolare del trattamento" o "Titolare"	si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (articolo 4, 1° comma, n. 7, Regolamento). Ai fini della presente Policy Titolare è, a seconda dei casi, GS1 Italy o GS1 Italy Servizi S.r.l. ciascuna per i Trattamenti di Dati di propria rispettiva competenza;
"Trattamento/i"	indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, 1° comma, n. 2, Regolamento).

3. CONSERVAZIONE DEI DATI PERSONALI: NOZIONI GENERALI

3.1 Un ciclo di vita applicabile a tutti i dati personali

I Dati devono essere gestiti in modo adeguato durante tutto il loro ciclo di vita, ossia dal momento della relativa raccolta, nel corso del periodo di utilizzo ed elaborazione e sino alla relativa eliminazione.
Il periodo di conservazione si identifica con il periodo nel corso del quale i Dati personali sono effettivamente utilizzati per raggiungere lo scopo del trattamento per cui sono stati raccolti, e con il momento della relativa archiviazione, generalmente richiesta dalle disposizioni di legge applicabili (segnatamente in materia contrattuale e fiscale/tributaria).
La conformità alla presente Policy garantisce che i Dati personali siano mantenuti per un periodo di conservazione fisso e che i Dati personali obsoleti siano eliminati in modo sistematico, controllato e sicuro.



LEGENDA

Raccolta
La raccolta dei dati personali, nella maggior parte dei casi direttamente dalla persona fisica, è il punto di partenza del periodo di conservazione.

Periodo di conservazione attiva
In questa fase, i dati personali vengono messi a disposizione ed elaborati per le esigenze operative delle Organizzazioni (commerciali, risorse umane, ecc.).

Periodo di archiviazione
Quando i dati personali non sono più necessari per le esigenze aziendali, potrebbe esserci ancora l'esigenza di tenerli per un dato periodo di tempo per adempiere ad obblighi di legge (anche in ambito fiscale o tributario).
Le Organizzazioni garantiscono che non venga eliminato alcun documento prima del termine del periodo di conservazione previsto dalla legge.
Tra tutti i dati personali raccolti, dovrebbe essere effettuata una selezione per la sola archiviazione dei dati necessari. Alla scadenza del periodo di conservazione, i dati devono essere distrutti (secondo la strategia di eliminazione).

Eliminazione
In questa fase, i dati non sono più necessari né per le attività commerciali, né per esigenze legali o normative. I dati devono pertanto essere eliminati, o, in alcune circostanze, anonimizzati.

3.2 Un periodo connesso a ciascun trattamento
Il periodo di ciascun Trattamento dei dati personali è strettamente legato alle rispettive finalità e base giuridica.

Per la determinazione del periodo di conservazione, le Organizzazioni hanno l'obbligo di:
- ✓ verificare i dati personali in possesso del proprio staff e personale;
- ✓ identificare lo scopo del trattamento per cui sono stati raccolti;
- ✓ fare riferimento al programma di conservazione dei dati (di cui all'Allegato 1 alla presente Policy) o usare i criteri dettagliati nel successivo paragrafo 5.

4. SCOPO E AMBITO DI APPLICAZIONE

La presente Policy individua i ruoli e le responsabilità di ciascun soggetto coinvolto nel Trattamento dei Dati personali effettuato dalle Organizzazioni, affinché siano individuati i soggetti deputati al monitoraggio e alla supervisione della corretta applicazione del principio di "limitazione della conservazione".
La presente Policy si applica a tutti i Dati personali oggetto di Trattamento da parte del Titolare, dei Contitolari e/o dei Responsabili del trattamento, conservate e memorizzate mediante supporti cartacei e/o informatici.
Gli Interessati a cui i Dati personali afferiscono possono essere a titolo indicativo e non esaustivo:
- associati e clienti;
- ex associati e clienti;
- potenziali associati e clienti;
- utenti web e/o di piattaforme gestite dalle Organizzazioni;
- dipendenti;
- ex dipendenti;
- candidati;
- fornitori e consulenti.

Dal punto di vista oggettivo, la presente Policy si applica a tutti i supporti, siano essi cartacei e/o informatici, contenenti Dati personali. A titolo meramente esemplificativo, si riportano nel seguito alcuni esempi di supporti che potrebbero contenere Dati personali:

- sistemi informatici quali il sistema gestionale e/o sistemi di "*customer relationship management*";
- file e cartelle di archiviazione presenti su personal computer e/o dispositivi mobile;
- messaggi di posta elettronica;
- documenti cartacei;
- documenti digitali;
- fotografie, video e audio;
- dati generati dai sistemi di controllo degli accessi fisici.

La presente Policy si applica, anche dove di seguito non espressamente indicato, sia ai Dati personali trattati da ciascuna Organizzazione in qualità di Titolare autonomo del trattamento sia rispetto ai Dati personali oggetto di trattamenti condivisi tra le Organizzazioni e rispetto ai quali queste ultime assumono il ruolo di Contitolari del trattamento, secondo quanto indicato nell'accordo di contitolarità tra le stesse stipulando e/o in essere.

5. PRINCIPI – GUIDA NELLA DETERMINAZIONE DEI PERIODI DI CONSERVAZIONE

Ferme restando le indicazioni di cui all'Allegato 1 che segue, si riportano i principi che dovranno fungere da criterio nell'individuazione del periodo di conservazione, di volta in volta, applicabile.

5.1 Principio di necessità

I Dati personali sono trattati e conservati nella misura in cui il Trattamento sia necessario per il perseguimento dello scopo per il quale gli stessi sono stati raccolti.

A tale riguardo, è necessario che il Titolare (o Contitolari) conservi i Dati personali solo se indispensabili per il raggiungimento delle finalità consentite, e non anche quando i medesimi obiettivi possano essere raggiunti mediante l'utilizzo di dati anonimi o che comunque consentano una più circoscritta identificazione degli Interessati.

ESEMPIO: La conservazione dei CV dei candidati non selezionati dovrà avvenire per il periodo necessario ai fini della gestione del processo di selezione e di eventuali ulteriori contatti immediatamente successivi al completamento della selezione.
Nota: la conservazione dei CV per un periodo successivo alla conclusione del processo di selezione comporterebbe per il Titolare il rischio di trattare dati non più aggiornati e non più pertinenti.

ESEMPIO: La conservazione dei Dati personali trattati ai fini della gestione di una richiesta di informazioni formulata dall'interessato dovrà essere limitata al periodo necessario all'evasione della richiesta da parte dell'Organizzazione e/o al fine di consentire alla stessa di dimostrare di aver adempiuto alla richiesta.
Nota: la conservazione dei Dati personali relativi al soggetto richiedente per un periodo successivo all'evasione della richiesta e/o per il periodo utile a dimostrare il corretto adempimento da parte dell'Organizzazione non è più necessaria essendo stato raggiunto lo scopo per cui i Dati personali sono stati raccolti dall'Organizzazione stessa.

5.2 Obblighi di legge e/o contrattuali

I Dati personali sono conservati nel rispetto dei termini sanciti dalla normativa vigente ed applicabile in materia fiscale, giuslavoristica, civile, ecc., nonché nel pieno rispetto di eventuali termini negozialmente concordati dalle parti contrattuali.
A titolo meramente esemplificativo e non esaustivo, si vedano, nel seguito, alcuni esempi di termini di conservazione sanciti dalla normativa vigente:

Riferimento normativo	Contenuto	Possibili ambiti di applicazione
Art. 2220 cod. civ.	Comma 1: *Le scritture devono essere conservate per **dieci anni dalla data dell'ultima registrazione**.* Comma 2: *Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti.* Comma 3: *Le scritture e i documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti.*	• Documenti contabili delle Organizzazioni, ivi inclusi i libri contabili e le registrazioni contabili; • Bilancio di esercizio, conto economico, relazione dei revisori contabili etc.; • Documentazione comprensiva di libri, registri e altri supporti di dati dai quali il contribuente può sempre mostrare i propri diritti e obblighi nell'interesse di imporre tasse. • Lettere e telegrammi.
Art. 43 D.P.R. 600/1973	Comma 1: *Gli avvisi di accertamento devono essere notificati, a pena di decadenza, **entro il 31 dicembre del quinto anno successivo a quello in cui è stata presentata la dichiarazione**.* Comma 2: *Nei casi di omessa presentazione della dichiarazione o di presentazione di dichiarazione nulla l'avviso di accertamento può essere notificato **entro il 31 dicembre del settimo anno successivo a quello in cui la dichiarazione avrebbe dovuto essere presentata.***	• Tutte le informazioni che potrebbero essere pertinenti alla posizione fiscale, inclusi tutti i libri e i registri.
Art. 2946 c.c.	Comma 1: *Salvi i casi in cui la legge dispone diversamente, i diritti si estinguono per **prescrizione con il decorso di dieci anni.***	• Tutte le informazioni che potrebbero essere necessarie al fine di garantire l'esercizio dei diritti dell'Organizzazione.
Art. 2496 c.c.	Comma 1: *Compiuta la liquidazione, la distribuzione dell'attivo o il deposito indicato nell'articolo 2494, i libri della società devono essere depositati e conservati per dieci anni presso l'ufficio del registro delle imprese; chiunque può esaminarli, anticipando le spese.*	• Documenti e registri dell'entità giuridica sciolta e/o posta in liquidazione.
Art. 2948 comma 1 n. 5 c.c.	*Si prescrivono in cinque anni […] le indennità spettanti per la cessazione del rapporto di lavoro.*	• Documentazione relativa ai salari, compresi i rimborsi esentasse.

5.3 Opportunità

I Dati personali sono conservati per il periodo stabilito dal Titolare (o dai Contitolari) in base a motivate e ragionevoli scelte di opportunità.

A titolo esemplificativo, il Titolare (o i Contitolari) conserva i Dati personali per finalità legate alla difesa in giudizio da azioni di natura contrattuale, sicché sono conservati i Dati personali necessari al fine di dimostrare di aver correttamente adempiuto alle obbligazioni derivanti dall'esecuzione del rapporto contrattuale.

Inoltre, il Titolare (o i Contitolari) conserva i Dati personali per finalità legate alla difesa in giudizio da azioni di natura extracontrattuale, sicché sono conservati i Dati personali per un periodo pari a 5 anni dalla cessazione del rapporto contrattuale.

6. CONDIZIONI DI CONSERVAZIONE APPLICABILI

6.1 Durante la fase di conservazione attiva

Durante la conservazione attiva, i Dati personali devono rimanere disponibili per raggiungere lo scopo per cui sono stati raccolti.
Durante tale periodo, devono essere conservati in un luogo protetto, sicuro e accessibile in modo da poter implementare tecnicamente i diritti dei soggetti interessati.

6.2 Durante la fase di archiviazione

Durante il periodo di archiviazione, i dati personali devono essere protetti e tenuti al di fuori dagli ambienti produttivi e non possono essere eliminati. I Dati personali devono essere resi disponibili solo a un numero ristretto di persone (solitamente solo alle persone con responsabilità legali, normative o di revisione).

I dati possono essere archiviati:

- in una banca dati specifica, separati da altre banche dati attive, con accesso ristretto alle persone che hanno interesse ed esigenza di accedere a tali dati per assolvere alle proprie funzioni (ad es. amministratori);

- nella banca dati attiva, a condizione che i dati archiviati siano segregati rispetto agli altri con mezzi di separazione logica (gestione dei diritti e autorizzazioni di accesso) che li rendano inaccessibili a persone che non abbiano interesse nel trattamento degli stessi.

6.3 Anonimizzazione ed eliminazione

Quando la conservazione o archiviazione dei Dati personali non sia più richiesta e si possa (o si debba) procedere all'eliminazione, la cancellazione diventa una necessità fondamentale e obbligatoria (sia dal punto di vista di un sistema informatico sia ai sensi delle disposizioni di legge in materia di protezione dei dati).

6.4 Metodo

Dovranno essere implementati meccanismi di eliminazione (manuale o automatica) per permettere l'eliminazione (inclusa l'anonimizzazione) dei vari gruppi di Dati.

Il metodo di eliminazione deve garantire la cancellazione dei Dati da tutti i dispositivi di archiviazione.

La cancellazione dei Dati personali deve essere permanente e irreversibile. Pertanto nessun recupero deve essere possibile utilizzando software di terzi.

In alternativa all'eliminazione è possibile procedere all'anonimizzazione dei dati personali. L'anonimizzazione dei dati personali deve rendere impossibile l'identificazione di uno specifico soggetto interessato, dev'essere permanente e irrevocabile, ossia deve essere impossibile stabilire (anche con un'operazione inversa o a ritroso) l'identità di qualsiasi persona fisica tramite utilizzo di una informazione esistente.

Tutte le misure tecniche e organizzative necessarie devono essere adottate per garantire una cancellazione o anonimizzazione sicura.

Si devono considerare tutte le copie e i duplicati per le operazioni di eliminazione.

Resta salvo quanto indicato al successivo paragrafo 6.6.

6.5 Registrazione dell'eliminazione

Il Titolare (o i Contitolari), con l'ausilio del Referente, ove nominato, è responsabile del processo continuo di identificazione dei documenti che hanno raggiunto il periodo di conservazione stabilito e di supervisionare la loro distruzione.

Dev'essere impostato un meccanismo di registrazione per permettere la tracciatura delle operazioni di Cancellazione. In altri termini, l'eliminazione dev'essere registrata dal Titolare (o i Contitolari) per ciascuna area di operatività al fine di dimostrare la conformità con la presente Policy. Devono essere descritti i documenti eliminati, la data, il nome del Soggetto Autorizzato che ha richiesto l'eliminazione dei documenti e la ragione dell'eliminazione.

Se il trattamento dei Dati coinvolge terzi, quali i Responsabili del trattamento, questi devono fornire prova della distruzione (ad es. esibendo un certificato o una attestazione di distruzione).

6.6 Avviso prima dell'eliminazione: conservazione a fini legali

Tutti i dipendenti e i collaboratori, a qualunque titolo, delle Organizzazioni devono essere portati a conoscenza di quanto segue.

Se le Organizzazioni ritengono o comunicano, tramite la direzione aziendale, che i Dati personali sono rilevanti per un contenzioso potenziale o attuale (o altra controversia che potrebbe portare a un contenzioso), indagine, revisione o altro evento, la conservazione dev'essere protratta e i Dati personali coinvolti non devono essere eliminati né i documenti o archivi che contengono i Dati devono essere modificati o altrimenti alterati, ivi incluse le e-mail, fino a quando la direzione aziendale non avrà determinato che tali documenti non sono più necessari.

In caso di dubbi sull'applicabilità di tale "conservazione a fini legali", contattare la direzione aziendale.

Potrebbe anche essere richiesta la sospensione di qualsiasi procedura routinaria di eliminazione dei documenti in connessione ad altri eventi specifici, quali la fusione dell'Organizzazione con un'altra organizzazione o la sostituzione del sistema informatico/informativo.

In tal caso, i Dati personali verranno protetti in un ambiente di archiviazione.

7. IMPLEMENTAZIONE DELLA POLICY

7.1 Garantire che i sistemi implementino i meccanismi di cancellazione o anonimizzazione fin dalla progettazione *(by design)*

Il ciclo di vita dei Dati dovrebbe essere parte dell'approccio alla riservatezza dei dati fin dalla progettazione, quindi dalla progettazione al ritiro dei prodotti/sistemi.

Prima che sia implementato un sistema, le capacità di gestire la conservazione in base a questa Policy deve essere specificata (definizione dei periodi di conservazione, documentazione sui requisiti di legge, ruoli aziendali e criteri da usare per l'applicazione dei periodi di conservazione).

I progetti verranno validati come parte di un formale processo di approvazione per garantire che i requisiti di conservazione dei dati siano definiti e implementati.

Con l'evoluzione dei periodi di conservazione e delle regole, l'esigenza di implementare un approccio flessibile alla gestione della conservazione dei dati nei sistemi è un requisito importante. Il sistema, al momento della progettazione, dovrà essere costruito in modo da minimizzare lo sforzo per l'implementazione di possibili cambiamenti.

7.2 Garantire che i sistemi esistenti implementino i meccanismi di cancellazione o anonimizzazione *(by default)*

Per i sistemi esistenti, dovrebbe essere determinato un periodo di conservazione secondo le fasi elencate nel paragrafo che precede.

Dovranno essere implementati meccanismi di eliminazione (manuali o automatici) o anonimizzazione per permettere l'eliminazione dei vari gruppi di dati in base alle regole definite nel Programma di conservazione dei dati.

Dovrà inoltre essere previsto un meccanismo di registrazione per permettere la rendicontazione sui Dati eliminati per dimostrare la conformità. Dovrà inoltre essere predisposto e mantenuto un registro dei documenti eliminati.

7.3 Garantire la conformità in caso di Trattamento dei Dati da parte di terzi

Qualora il trattamento dei Dati personali venga eseguito per conto dell'Organizzazione, anche il Responsabile del trattamento dei dati dovrà osservare i requisiti della presente Policy. Le Organizzazioni dovranno documentare il processo di selezione del responsabile, come parte dei principi di responsabilità e di riservatezza fin dalla progettazione.

7.4 Riesaminare regolarmente la presente Policy

Come conseguenza dei cambiamenti nei regolamenti, nella giurisprudenza, nelle raccomandazioni del Garante o per l'evoluzione delle esigenze aziendali, la presente Policy dovrà essere periodicamente riesaminata.

8. RUOLI E RESPONSABILITÀ

8.1 Titolare / Contitolari

Il Titolare (o i Contitolari) avvalendosi della collaborazione del Referente, ove nominato, e di Soggetti Autorizzati definisce le tempistiche di conservazione dei Dati personali Trattati.

8.2 Soggetti Autorizzati

I Soggetti Autorizzati, anche sulla base delle loro specifiche competenze, hanno il compito di assistere il Titolare (o i Contitolari) e il Referente (se nominato) nell'individuare, in relazione ai Trattamenti di propria competenza, i criteri da applicare al fine di consentire al Titolare di definire le tempistiche di conservazione.

ESEMPIO: i dipendenti della funzione o ufficio Finance o Amministrativo, nella loro qualità di Soggetti Autorizzati, comunicano al Titolare la sussistenza di obblighi di legge e/o contrattuali che richiedono la conservazione dei Dati personali per specifici periodi di tempo, nonché l'opportunità e/o la necessità di conservare tali dati per un periodo ulteriore (ragionevole) rispetto ai termini fissati per legge. In tal caso il Referente assiste la Funzione Finance nel definire eventualmente i periodi ulteriori di conservazione rispetto a quelli previsti dagli obblighi di legge e/o contrattuali.

8.3 Referente Privacy

Il Referente Privacy, se nominato, ha il compito di assistere il Titolare (o i Contitolari) nell'individuare i criteri da applicare al fine di consentire al Titolare (o ai Contitolari) di definire le tempistiche di conservazione.

Il Referente Privacy ha il compito, *inter alia*, di monitorare la corretta implementazione della presente Policy da parte dei Destinatari, nonché di effettuare controlli e revisioni periodiche al fine di verificare che siano rispettati i macro-criteri per la determinazione dei termini di conservazione dei Dati personali.

8.4 Funzione IT

La Funzione IT, su istruzione del Titolare (o dei Contitolari), è tenuta a supportare quest'ultimo nell'espletamento delle attività connesse alla Cancellazione dei Dati personali presenti su ogni dispositivo e/o banca dati e/o *directories* e/o sistema e/o qualsivoglia supporto informatico contenente Dati personali.

9. AZIONI / RACCOMANDAZIONI SULLA CONSERVAZIONE DEI DATI PERSONALI

AZIONI OBBLIGATORIE

- Assicurarsi che le attività di trattamento svolte siano conformi a questa Policy
- Definire un periodo di conservazione per qualsiasi nuova attività di Trattamento
- Garantire la cancellazione dei Dati alla fine del periodo di conservazione
- Limitare l'accesso ai Dati personali non più necessari per le attività operative

AZIONI VIETATE

- Mantenere dati personali più a lungo di quanto previsto in questa Policy o in altri documenti adottati in materia dall'Organizzazione
- Rendere disponibili a chiunque i documenti contenenti Dati personali

IN CASO DI DUBBI

In caso di dubbi in merito alla possibile "conservazione a fini legali" dei Dati, contattare la direzione aziendale o il Referente (se nominato).

10. INOSSERVANZA DELLA POLICY

Si porta a conoscenza di tutti i Destinatari che le linee guida contenute nella presente Policy hanno carattere vincolante.

Eventuali violazioni della presente Policy possono avere gravi ripercussioni sulle Organizzazioni e comportare, nei confronti del dipendente inadempiente, l'applicazione di provvedimenti disciplinari, in conformità alle disposizioni di legge e del CCNL applicabile e nei confronti degli altri Destinatari anche la cessazione del rapporto contrattuale.

I comportamenti che costituiscono violazione della presente Policy possono violare, nel contempo, anche disposizioni di legge tali da comportare per l'utilizzatore inadempiente conseguenze di natura civile e penale.

Anche l'Organizzazione può essere perseguita e sanzionata in conseguenza della condotta dei Destinatari. Agli stessi potrà dunque venire richiesto di risarcire i danni derivati dalle violazioni della presente Policy.

ALLEGATO I: PERIODI DI CONSERVAZIONE DEI DATI

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
RISORSE UMANE	**Candidati**	Dati personali comuni, Categorie particolari di dati, eventuali dati giudiziari (se previsto dalla legge o dal CCNL applicabile)	**Documenti di selezione del personale** (*e.g. curricula vitarum*, schede di valutazione)	Massimo 3 mesi dal colloquio o dall'ultimo contatto con il candidato (fatta eccezione per figure e/o esigenze specifiche).	Si tratta di una raccomandazione.
	Dipendenti	Dati personali comuni, Categorie particolari di dati, eventuali dati giudiziari (se previsto dalla legge o dal CCNL applicabile)	**Gestione del personale (ivi inclusa la gestione della cartella del dipendente)**	Massimo 10 anni dalla data di cessazione del contratto di lavoro dipendente. In presenza di uno storico di richieste di prova di periodi contributivi da parte del dipendente: per un periodo di 2 anni dalla data presunta di pensionamento dell'ex dipendente. Restano salve diverse disposizioni di legge o del CCNL applicabile. Libro Unico del Lavoro: 5 anni dalla data dell'ultima registrazione Registro infortuni: 4 anni dall'ultima registrazione. Eventuali termini superiori di conservazione saranno applicabili ed applicati se previsti dalla normativa, nazionale e/o comunitaria, e/o dal CCNL. In	In conservazione attiva durante l'intera durata del rapporto contrattuale con il dipendente. Nell'archivio intermedio dal momento della cessazione del contratto di lavoro.

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
				particolare, a mero titolo di esempio, nel caso di esposizione ad agenti cancerogeni o mutageni nel corso della durata del rapporto di lavoro, i dati (limitatamente alle annotazioni del registro di esposizione e alle cartelle sanitarie e di rischio) saranno conservati, tramite il medico competente, fino a cessazione del rapporto di lavoro e, successivamente, fino al termine ulteriore prescritto ai sensi di legge.	
			Gestione paghe	Come sopra	Come sopra
	Collaboratori	Dati personali comuni, Categorie particolari di dati	**Gestione dei collaboratori (adempimenti contrattuali, fiscali e di legge)**	Massimo 10 anni dalla data di cessazione del contratto di collaborazione.	
	Dipendenti	Dati personali comuni	**Gestione orari di lavoro e accessi**	Massimo 10 anni dalla data di cessazione del contratto di lavoro dipendente salvo diverse disposizioni di legge o del CCNL di tempo in tempo applicabili.	Il periodo necessario a raggiungere lo scopo
	Dipendenti		**Sanzioni disciplinari**	Massimo 2 anni (dall'ultima contestazione / sanzione disciplinare), salvo diverse disposizioni di legge o del CCNL	

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
				di tempo in tempo applicabili.	
	Personale (generale)	Utenze telefoniche, credenziali accesso a siti e sistemi, account di posta elettronica, registrazione di contenuti/eventi informatici	**Gestione dei sistemi informatici/informativi e degli strumenti di lavoro**	I dati saranno cancellati conformemente alle procedure in vigore. Per quanto riguarda l'account di posta elettronica del personale cessato, il sistema di inoltro avrà una durata compresa tra i 6 ed i 12 mesi dalla cessazione del rapporto; per quanto riguarda i log di accesso, verranno cancellati dopo 12 mesi ovvero nei diversi termini a seconda degli automatismi previsti dalla relativa piattaforma.	
RAPPORTI CONTRATTUALI (E PRE-CONTRATTUALI) CON ASSOCIATI / CLIENTI / UTENTI	**Associati e clienti (*i.e.* referenti contrattuali, persone fisiche)**	Dati personali comuni	**Gestione contatti, trattative e contratti (ivi espressamente inclusi i contratti di associazione) con associati e clienti (ivi inclusi fatturazione, relativi aspetti contabili ed amministrativi)**	Per tutta la durata del rapporto associativo / contrattuale / commerciale e, successivamente, per almeno 10 anni decorrenti dalla cessazione del contratto.	Fino alla scadenza del periodo di prescrizione
			Archiviazione in risposta all'obbligo di mantenere i dati contabili	Fino alla scadenza degli obblighi legali (anche in materia di prescrizione e decadenza).	Archiviazione in conformità all'obbligo di mantenere i dati contabili.

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
			Archiviazione in caso di azione legale	Fino alla fine del periodo di prescrizione / decadenza o fino alla scadenza dei diritti di impugnativa.	Archiviazione in caso di azione legale.
		Dati personali comuni (legati all'individuo e/o all'ente di appartenenza)	**Trasmissione di comunicazioni istituzionali dell'Organizzazione**	In quanto legate al rapporto contrattuale od associativo (e costituente parte del servizio erogato), per tutta la durata del corrispondente rapporto, salvo richiesta dell'interessato di non riceverle.	
		Dati personali comuni (legati all'individuo e/o all'ente di appartenenza)	**Marketing (e.g. invio di comunicazioni di marketing, inviti a corsi od eventi, invio di questionari di gradimento o survey**, non ricadenti nel punto che precede**)**	A seconda dei casi, fino a revoca del consenso da parte dell'interessato o, in caso di legittimo interesse, fino ad opposizione da parte dell'interessato.	
		Dati personali comuni (legati all'individuo e/o all'ente di appartenenza), nonché dati ed informazioni in merito a prodotti /servizi acquistati ed eventi cui l'interessato ha aderito o rispetto a cui	**Profilazione** (finalizzata ad invio di comunicazioni, come indicato al punto che precede)	Fino a revoca del consenso da parte dell'interessato.	

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
		ha manifestato interesse			
	Utenti web o di piattaforme delle Organizzazioni (ivi inclusi utenti di servizi di formazione)	Dati personali comuni	**Gestione contatti, iscrizioni, registrazioni e contratti e prestazione dei servizi richiesti e/o risposta a eventuali richieste**	Per tutta la durata del rapporto contrattuale / commerciale e/o di prestazione del servizio, successivamente, per almeno 10 anni decorrenti dalla cessazione del contratto.	Fino alla scadenza del periodo di prescrizione
RAPPORTI CONTRATTUALI (E PRE-CONTRATTUALI) CON I FORNITORI	**Fornitori (i.e. referenti contrattuali, persone fisiche)**	Dati personali comuni	**Gestione contatti, trattative e contratti con i clienti (ivi inclusi gestione ed evasione dell'ordine, fatturazione, relativi aspetti contabili ed amministrativi)**	Per tutta la durata del rapporto contrattuale / commerciale e, successivamente, per almeno 10 anni decorrenti dalla cessazione del contratto o dall'ultimo contatto commerciale.	
			Archiviazione in caso di azione legale	Fino alla fine del periodo di prescrizione / decadenza o fino alla scadenza dei diritti di impugnativa.	Archiviazione in caso di azione legale.
			Archiviazione in risposta all'obbligo di mantenere i dati contabili	Fino alla scadenza degli obblighi legali (anche in materia di prescrizione e decadenza).	Archiviazione in conformità all'obbligo di mantenere i dati contabili.

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
RAPPORTI CON ORGANISMI SOCIALI	**Soci, consiglieri, sindaci e componenti dell'Organismo di Vigilanza**	Dati personali comuni	**Instaurazione ed esecuzione del rapporto contrattuale**	Per tutta la durata del rapporto associativo / contrattuale / commerciale	Fino alla scadenza del periodo di prescrizione
			Archiviazione in caso di azione legale	Fino alla fine del periodo di prescrizione / decadenza o fino alla scadenza dei diritti di impugnativa.	Archiviazione in caso di azione legale.
RAPPORTI CON UNIVERSITÀ	**Studenti universitari**	Dati personali comuni	**Gestione dell'attribuzione e di borse di studio e facilitazioni secondo gli accordi in essere con le Università, nonché gestione dell'iscrizione e della partecipazione a corsi e master organizzati e/o sponsorizzati da GS1 Italy**	Per tutta la durata del rapporto contrattuale / sino a conclusione della borsa di studio / servizio offerto dall'Organizzazione e, successivamente, fino al termine del periodo di prescrizione / decadenza.	
SISTEMI DI ACCESSO ALLA SEDE	**Ospiti e visitatori**	Dati personali comuni	**Gestione registrazione di ospiti e visitatori presso la sede delle Organizzazioni**	Per tutta la durata della visita e, successivamente, in coerenza con gli standard di qualità ISO e/o con altre normative applicabili al Titolare.	
VIDEOSORVEGLIANZA	**Personale, ospiti e visitatori**	Immagini video	**Sicurezza della sede**	24 ore (a eccezione di speciali esigenze di ulteriore	Nel rispetto di quanto previsto dalla Linee Guida

AREA	SOGGETTI INTERESSATI	NATURA DEI DATI	FINALITÀ DEL TRATTTAMENTO	PERIODO DI CONSERVAZIONE	ALTRE INDICAZIONI
				conservazione in relazione a festività o chiusura degli uffici – per il cui caso è possibile una più lunga conservazione di 48 ore – nonché nel caso di specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria), salvo ove diversamente indicato in un documento da redigersi da parte delle Organizzazioni a giustificazione della scelta di conservazione per un periodo maggiore ed a bilanciamento degli interessi coinvolti (purché nel rispetto delle disposizioni di legge in materia di tutela del lavoratore, ove applicabili) .	del Comitato Europeo per la Protezione dei Dati n. 3/2019 e di quanto indicato dal Provvedimento Generale del Garante per la Protezione dei Dati Personali dell'8 aprile 2010 e successive modifiche ed integrazioni (ove applicabile), nonché dalla legge locale di tempo in tempo vigente o di autorizzazioni rilasciate dalle autorità competenti (es. Ispettorato Territoriale del Lavoro). Resta salvo quanto indicato nella colonna a fianco.

ALLEGATO 3

MISURE DI SICUREZZA

Gli Archivi oggetto del Trattamento Condiviso sono protetti dalle seguenti misure di sicurezza:

MISURE DI SICUREZZA TECNICO-INFORMATICHE	DESCRIZIONE (SINTESI)
CRITTOGRAFIA DEI DATI	Il sistema di cifratura è applicato ai dati personali oggetto del Contratto.
CONTROLLO ACCESSO LOGICO	Solo il personale autorizzato ha accesso logico agli ambienti (virtuali e non) in cui sono ospitati gli Archivi, tramite l'utilizzo di credenziali di autenticazione gestite da parte del Dipartimento Sistemi Informativi. Le password di accesso devono essere cambiate periodicamente dall'operatore autorizzato e devono rispondere a requisiti minimi di lunghezza e complessità. L'accesso al sistema gestionale effettuato al di fuori dei locali aziendali è soggetto ad autenticazione a due fattori, con riferimento tanto agli accessi da personal computer quanto a quelli effettuati da dispositivi mobile. È in corso di valutazione l'estensione dell'autenticazione a due fattori anche agli altri sistemi.
LOG-FILE	Tutti i sistemi che concorrono alla fornitura dei Servizi, compresi firewall, apparati di rete, Sistemi Operativi ed applicazioni, registrano log sui loro rispettivi sistemi di gestione dei log, i quali sono registrati e conservati per consentire revisioni di sicurezza e attività di diagnostica per un tempo comunque coerente con le previsioni di legge applicabili.
SISTEMI DI CONSERVAZIONE CLOUD/BACK UP E SISTEMI DI RIDONDANZA	Tutti i sistemi che concorrono alla fornitura dei Servizi - con la sola eccezione del sistema di archiviazione documentale - sono fruibili in cloud. Sistemi di back-up sono disponibili per ciascuno dei sistemi utilizzati.
DISASTER RECOVERY PLAN	Processi di disaster e recovery plan sono applicati dai Contitolari con riguardo ai server dell'infrastruttura in cui sono ospitati gli Archivi.
PRESIDI CONTRO MALWARE E VIRUS INFORMATICI	Tutti i server dell'infrastruttura in cui sono ospitati gli Archivi e tutte le postazioni di lavoro tramite le quali gli operatori autorizzati possono accedere ai server sono equipaggiati con idoneo software di Antivirus ed Antimalware conforme agli ultimi standard del settore e tenuto regolarmente aggiornato a livello centrale.
FIREWALL E CONTROLLO DELL'ACCESSO ALLE RETI	L'accesso alla rete di utenti e dispositivi non autorizzati è impedito tramite sistemi di firewall e controllo dell'accesso alle reti.

MISURE ORGANIZZATIVE	DESCRIZIONE
NOMINA DELL'AMMINISTRATORE DI SISTEMA	In conformità a quanto previsto dal Provvedimento del Garante del 27 novembre 2008, si è provveduto ad individuare e nominare gli amministratori di sistema. Gli amministratori di sistema sono stati individuati in dipendenti di GS1 Italy che forniscono idonee garanzie di rispetto dei requisiti previsti dal citato Provvedimento.
POLITICHE E PROCEDURE A TUTELA DEI DATI	I Contitolari adottano apposite procedure a tutela dei dati personali oggetto dei Trattamenti Condivisi, tra le quali una politica di *data retention* ed una procedura per la gestione delle violazioni di dati (*data breach*) che costituiscono allegati al presente Contratto.
ORGANIZZAZIONE DELLE RISORSE UMANE E "DATA PROTECTION AWARENESS"	Dipendenti e collaboratori che hanno accesso ai Dati Personali sono stati incaricati e/o autorizzati per iscritto ad eseguire le operazioni di trattamento dati. Eventuali aggiornamenti alle istruzioni sono apportati se necessari in funzione del Trattamento Condiviso.
REGISTRO DEI TRATTAMENTI	Viene redatto un Registro del Trattamento Condiviso ai sensi dell'articolo 30 del GDPR o, in alternativa, i registri tenuti singolarmente dalle Parti sono aggiornati di conseguenza.

ALLEGATO 4

PROCEDURA PER LA GESTIONE DI UNA VIOLAZIONE DI DATI PERSONALI
(*DATA BREACH POLICY*)

VERSION	DATA	AUTORE	NOTE
1.0	Gennaio 2022	GS1 Italy – GS1 Italy Servizi	Versione iniziale

INDICE

1. PREMESSA E DEFINIZIONI

Il Regolamento (UE) 2016/679, Regolamento Generale sulla protezione dei dati (di seguito il "**Regolamento**" o "**GDPR**"), pone particolare attenzione al caso di violazione dei dati personali, prevedendo altresì specifici adempimenti carico del titolare e/o del responsabile del trattamento.

In ragione delle operazioni di trattamento di dati personali effettuate, **GS1 Italy e GS1 Italy Servizi S.r.l.** (di seguito congiuntamente "**Organizzazioni**" e individualmente "**Organizzazione**") hanno ritenuto necessario adottare la presente procedura al fine di indicare ai destinatari le azioni da compiere in caso di violazione dei dati personali e così garantire l'osservanza delle relative previsioni da parte delle Organizzazioni.

Allo scopo di facilitare la lettura e la comprensione di quanto indicato nel prosieguo, si riportano di seguito alcune delle principali definizioni di cui alla norma poc'anzi menzionata.

Fermo quant'altro previsto dal presente documento, i termini con iniziale maiuscola avranno il significato di seguito meglio precisato:

"Contitolari"	indica i due o più titolari che, ai sensi dell'articolo 26, Regolamento, determinano congiuntamente le finalità e i mezzi del trattamento. Ai fini della presente policy il termine "Contitolari" indica GS1 Italy e GS1 Italy Servizi S.r.l., quando agiscono rispetto ai trattamenti condivisi oggetto dell'accordo di contitolarità in essere tra le citate parti;
"Dati personali" o "Dati"	si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, 1° comma, n. 2, Regolamento);
"Garante"	indica l'Autorità di Controllo italiana ossia il Garante per la Protezione dei Dati personali;
"Interessato"	è la persona fisica (identificata o identificabile) cui si riferiscono i dati personali;
"Procedura" o "Policy"	indica, salvo ove diversamente previsto, il presente documento;
"Referente Privacy"	indica il soggetto, persona fisica o ufficio, eventualmente designato dal Titolare ai fini dell'implementazione delle disposizioni del Regolamento all'interno delle Organizzazioni e della gestione delle tematiche associate alla tutela dei dati personali all'interno dell'organizzazione aziendale e/o nei confronti dei terzi. Il nominativo del Referente Privacy viene opportunamente reso noto da parte delle Organizzazioni a tutti i dipendenti e collaboratori;
"DPO"	indica il responsabile della protezione dei Dati, soggetto (eventualmente) designato dal Titolare ai sensi e per gli effetti di cui all'articolo 37 del Regolamento e con funzioni di informazione, consulenza, sorveglianza del rispetto delle disposizioni normative e di contatto con l'Autorità di Controllo e gli Interessati;

"Responsabile del trattamento" o "Responsabile"	si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (articolo 4, 1° comma, n. 8, GDPR);
"Titolare del trattamento" o "Titolare"	si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (articolo 4, 1° comma, n. 7, Regolamento). Ai fini della presente Policy Titolare è, a seconda dei casi, GS1 Italy o GS1 Italy Servizi S.r.l. ciascuna per i Trattamenti di Dati di propria rispettiva competenza e "Titolari" indica entrambe le Organizzazioni;
"Violazione", "Violazione di Dati" o "Data Breach"	si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (articolo 4, 1° comma, n. 12, Regolamento).

2. CAMPO DI APPLICAZIONE

2.1 Il Regolamento ha introdotto in capo ai soggetti che trattano Dati Personali, ivi incluse, dunque, le Organizzazioni, l'obbligo di notificare al Garante eventuali Violazioni di Dati trattati, a meno che il Titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la Violazione dei Dati Personali presenti un rischio per i diritti e le libertà fondamentali delle persone fisiche. Qualora da tale Violazione derivino rischi elevati per le persone fisiche, l'obbligo di comunicazione si estende anche ai singoli Interessati coinvolti.
In ragione delle attività di trattamento di Dati personali svolte, le Organizzazioni hanno ritenuto necessario adottare la presente Policy al fine di disciplinare le opportune modalità di gestione delle Violazioni di dati, individuando le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di trattamento di Dati rispetto a cui ciascuna Organizzazione è Titolare (o Contitolare, a seconda dei casi) e in relazione a quei Trattamenti di Dati per quali le Organizzazioni agiscono come Contitolari.
2.2 Tutti i soggetti, sia interni sia esterni all'organizzazione imprenditoriale delle Organizzazioni, che trattino Dati personali su autorizzazione o per conto di quest'ultimo sono tenuti a conoscere e rispettare questa Procedura in caso di Violazione dei Dati personali.

3. IDENTIFICAZIONE DI UNA VIOLAZIONE DI DATI

3.1 Ai sensi del Regolamento, una Violazione di Dati include qualunque situazione in cui la sicurezza dei dati personali è stata o potrebbe essere compromessa da un evento avente un impatto sulla riservatezza, integrità o disponibilità dei Dati. Questo genere di evento, che pone a rischio la sicurezza sui dati, può consistere, a titolo di esempio, nella divulgazione, copia, trasmissione, accesso, rimozione, distruzione, furto o uso, sia accidentali sia intenzionali, dei dati personali da parte di soggetti non autorizzati.
3.2 Esistono diverse tipologie di Violazione dei Dati quali, a solo titolo di esempio:

- **violazione della riservatezza**, che si verifica quando i Dati personali sono compromessi tramite un accesso non autorizzato che comporta la fuoriuscita dei Dati stessi dall'ambito controllato in cui si trovano;
- **violazione dell'integrità**, che si verifica in caso di modifica non desiderata dei Dati personali che determina errori o malfunzionamenti nel trattamento originale;
- **violazione della disponibilità**, che si ha quando i Dati personali sono stati persi o non sono più accessibili.

3.3 I seguenti incidenti di sicurezza potrebbero causare una Violazione di Dati (si noti che il presente elenco non è esaustivo):

- perdita o furto di dispositivi portatili o di apparecchiature che possono contenere Dati personali (ad esempio computer, chiavi USB, telefoni cellulari, computer portatili, dischi, ecc.);
- perdita o furto di documenti cartacei che possono contenere Dati personali;
- accesso non autorizzato ai sistemi informatici (ad esempio *hacking*);
- violazioni della sicurezza fisica (ad esempio lasciare Dati personali in aree accessibili e non sotto chiave);
- smaltimento non sicuro di documenti riservati su supporto cartaceo;
- abbandono di apparecchiature informatiche incustodite dopo aver inserito le credenziali di accesso a un account senza aver bloccato lo schermo per evitare l'accesso alle informazioni da parte di terzi;
- divulgazione di Dati confidenziali a persone fisiche non autorizzate;
- controlli dell'accesso inappropriati che permettono l'uso non autorizzato dei Dati personali;
- alterazione o cancellazione di documenti contenenti Dati personali;
- pubblicazione di dati riservati su internet e divulgazione accidentale delle password;
- virus o altri attacchi alla sicurezza dei sistemi informatici o delle reti sempre che riguardino i Dati personali;
- e-mail o altra corrispondenza contenente Dati personali e che sia trasmessa a soggetti terzi non autorizzati o a questi ultimi altrimenti deviata;
- screenshot di una schermata del computer o registrazione di una conversazione telefonica.

4. GESTIONE DI UNA VIOLAZIONE DEI DATI

Ai sensi degli articoli 33 e 34 del GDPR, nel caso in cui una Violazione dei Dati possa portare a un rischio per i diritti e le libertà degli Interessati, essa dovrà essere:

- notificata al Garante entro 72 ore (si veda il riquadro qui sotto in merito alla decorrenza di tale termine); e
- comunicata agli Interessati senza ingiustificato ritardo (solo in caso di "rischio elevato").

Per consentire ai Titolari (o Contitolari, a seconda dei casi) di rispettare queste scadenze, è assolutamente necessario che:

- dipendenti e collaboratori delle Organizzazioni, nello svolgimento delle attività di propria competenza, provvedano alla tempestiva comunicazione di una Violazione, potenziale o attuale, o anche in caso di sospetto di tale Violazione, al Referente Privacy (se nominato) o, in alternativa, alla Dirigenza e prestino tutta la necessaria collaborazione ai fini della verifica, dell'indagine e della risposta alla Violazione dei Dati;
- i responsabili del trattamento comunichino tempestivamente al Titolare/i (o Contitolari) una Violazione, potenziale o attuale, o anche il sospetto di tale Violazione;
- il Referente Privacy, se nominato, quale punto di riferimento all'interno delle Organizzazioni per la corretta applicazione delle disposizioni del Regolamento, verifichi costantemente la corretta applicazione delle norme di condotta definite dalla presente Procedura, conduca e sovrintenda le attività di indagine necessarie ad accertare l'eventuale Data Breach, assista le Organizzazioni nell'effettuazione delle segnalazioni al Garante e/o nelle comunicazioni agli Interessati nonché a manutenere il registro delle violazioni segnalate, il tutto in collaborazione con il DPO, se nominato.

ATTENZIONE

Il termine di 72 ore per la notifica della Violazione dei Dati al Garante decorre:

- ✓ dal momento in cui la Violazione viene portata all'attenzione del Titolare/i (o Contitolari);
- ✓ dal momento in cui il Titolare/i (o Contitolari) si rende conto della Violazione (con ragionevole grado di certezza)

4.1 FASE 0: verificarsi di un incidente di sicurezza

Un incidente di sicurezza si verifica quando il patrimonio di informazioni e di Dati delle Organizzazioni è compromesso e viene scoperto da un dipendente/collaboratore/agente/fornitore o da altre terze parti.

4.2 Fase 1: comunicazione al Referente Privacy della risposta alla Violazione dei Dati

La persona che ha scoperto l'incidente, sia esso potenziale o confermato, deve immediatamente avvisare il Referente Privacy, se nominato, e comunque inviare una e-mail al seguente indirizzo con una breve descrizione della violazione e degli elementi noti fino a quel momento: privacy@gs1it.org.
In particolare, la segnalazione dovrà riportare in oggetto la dicitura "SEGNALAZIONE DI VIOLAZIONE DI DATI" (o similare) e indicare almeno i seguenti elementi:

- una breve descrizione dell'evento / incidente di sicurezza alla base della Violazione;
- le categorie di dati coinvolti (dati personali / categorie particolari di dati) ed il relativo numero (in termini di massima);
- le categorie (ad esempio: dipendenti, clienti, utenti web) di Interessati coinvolti ed il numero approssimativo degli stessi;
- l'indicazione delle misure adottate per minimizzare le conseguenze derivanti dalla Violazione.

4.3 Fase 2: identificazione dei collaboratori per le indagini

Il Referente Privacy, se nominato, o la dirigenza, presa in carico la segnalazione di Violazione, è tenuto, nel più breve tempo possibile, ad informare il DPO, se nominato, e ad identificare i dipendenti/collaboratori delle Organizzazioni da coinvolgere nelle indagini relative alla Violazione, a seconda dei ruoli all'interno delle Organizzazioni stesse. Potranno dunque essere coinvolti, di tempo in tempo ed a mero titolo di esempio, i seguenti uffici/funzioni: risorse umane, servizi generali, amministrazione, comunicazione / marketing, IT / sistemi informativi.

Tali collaboratori sono identificati caso per caso, in base al "luogo" o "strumento" in cui si è verificata la Violazione e alle persone che potrebbero aver avuto un ruolo nella stessa e si estende anche ai fornitori esterni nell'ipotesi in cui la Violazione sia avvenuta nei sistemi nella disponibilità o gestiti da questi ultimi ma abbia compromesso Dati personali di pertinenza delle Organizzazioni.

Di seguito il Referente Privacy unitamente ai dipendenti / collaboratori individuati sarà definito quale "**Team**".

4.4 Fase 3: analisi preliminare

Una volta identificati i soggetti da coinvolgere e definito il Team, il Referente Privacy, se nominato, o la dirigenza dovrà procedere, con il supporto del DPO (se designato) o comunque, se ritenuto, di un consulente (anche esterno), all'analisi preliminare dell'incidente al fine di verificarne il perimetro:

- **Caso 1a: la violazione non ha interessato Dati personali ed è di tipo informatico**
  La violazione verrà gestita come qualsiasi altra violazione della sicurezza, e verrà osservato quanto previsto dal programma di risposta agli incidenti ("Incident Response Plan" – "IRP"), ove adottato, o altra procedura in uso presso le Organizzazioni, senza che sia necessario passare alle fasi di seguito indicate.

- **Caso 1b: se la violazione non ha interessato Dati personali e non è di tipo informatico** (ma riguarda, ad esempio, archivi logici o materiale stampato)
  La Violazione verrà segnalata al consulente legale o fiscale, per valutarne eventuali ripercussioni sotto questi profili, senza che sia necessario passare alle fasi elencate di seguito.

- **Caso 2: la Violazione ha interessato Dati personali e può essere qualificata come un Data Breach**, come definito all'articolo 3 che precede.
  In tal caso, le fasi descritte in seguito dovranno essere seguite in modo appropriato. Si noti che se un Responsabile del trattamento (ad esempio un fornitore) è coinvolto nella Violazione dei Dati, ad esempio perché la violazione è avvenuta all'interno dei suoi sistemi informatici, dovrà essere, a sua volta, coinvolto nelle fasi di cui al paragrafo 4.5 che segue.

4.5 Fase 4a: contenimento e recupero

Una volta stabilito che (i) si è verificata una Violazione dei Dati e che (ii) essa ha ad oggetto Dati personali, il Team deve definire un piano di azione, comunicandolo anche al DPO (o al consulente nominato) per sua valutazione.

In base alla natura della Violazione dei Dati, il Team deve quindi lavorare con il relativo dipartimento (Informatico, Servizi generali, ecc.) al fine di:

- ✓ isolare l'incidente (ad es. mettendo in quarantena i dispositivi interessati, sospendendo le caselle e-mail coinvolte, ecc.);
- ✓ adottare le misure necessarie per recuperare eventuali perdite e mitigare i rischi (ad es. trovare un dispositivo perso, cambiare i codici di accesso alle porte, ecc.);
- ✓ recuperare o ripristinare i Dati compromessi;
- ✓ raccomandare la comunicazione alle forze dell'ordine nei casi di furto o altra attività criminale;
- ✓ raccomandare azioni specifiche al dipartimento coinvolto per mitigare le conseguenze della violazione.

Se la Violazione dei Dati è imputabile ad un comportamento, doloso o colposo, di un dipendente, sarà necessario informare la funzione Risorse Umane.

4.6 Fase 4b: valutazione del rischio

Durante la valutazione del rischio derivante da una Violazione di Dati, il Referente Privacy o la dirigenza considererà, con il supporto del DPO, se nominato (o il consulente eventualmente incaricato), la natura e l'entità dei Dati personali coinvolti, la natura e l'entità degli Interessati e il danno potenziale agli stessi.

Per supportare nella valutazione del rischio della Violazione di Dati, è stata redatta una metodologia che viene dettagliata nell'**Allegato 1**. La metodologia indica i diversi elementi da prendere in considerazione per la valutazione del rischio: l'impatto della violazione sugli Interessati (fisico, morale e finanziario/materiale), il numero degli Interessati e alcuni fattori di aumento e diminuzione del rischio.

Se gli elementi raccolti in fase di analisi suggeriscono che la Violazione di Dati ha una portata più estesa di quanto inizialmente previsto, si prega di tornare alla fase 3 e, con il supporto del Team, approfondire il perimetro della Violazione.

4.7 Fase 5: risultati della Violazione dei Dati

I risultati delle fasi 4a e 4b della Violazione saranno riassunti nella Scheda di Violazione dei Dati di cui all'**Allegato 3**.

Il responsabile del Team in cui si è verificata la Violazione di Dati confermerà i tempi stimati per l'avvio e la conclusione degli interventi raccomandati ai fini della mitigazione e/o eliminazione del rischio.

Se, secondo la valutazione, la Violazione di Dati è destinata a causare:

- un rischio per i diritti e le libertà degli Interessati, il Garante verrà informato dal Titolare/i (o Contitolari);
- un rischio **elevato** per i diritti e le libertà degli Interessati, sia il Garante sia gli Interessati coinvolti verranno informati dal Titolare/i (o Contitolari).

Anche se la Violazione di Dati non è destinata a causare un rischio per i diritti e le libertà degli Interessati, la Scheda di Violazione dei Dati deve comunque essere completata e inserita nel Registro delle Violazioni dei Dati, annotando che la Violazione di Dati non è stata notificata.

In base al risultato della valutazione del rischio, le Organizzazioni potranno quindi determinare se la Violazione dei Dati deve essere annotata internamente (si veda la fase 6), notificata al Garante (si veda la fase 7.1) e/o comunicata agli Interessati (si veda la fase 7.2).

		Garante	Soggetti interessati

4	Impatto molto elevato	Notifica obbligatoria	Comunicazione obbligatoria
3	Impatto elevato	Notifica obbligatoria	Comunicazione fortemente raccomandata
2	Impatto limitato	Notifica raccomandata	Comunicazione raccomandata
1	Trascurabile	Notifica non necessaria	Comunicazione non necessaria

Si rinvia a quanto previsto più nel dettaglio dall'Allegato 1.

4.8 Fase 6: annotazione interna di Violazione dei Dati

Quando si verifica una Violazione di Dati, il Referente Privacy o la dirigenza deve redigere un riassunto dell'incidente che includa i seguenti elementi:

- descrizione di alto livello della Violazione di Dati;
- impatto sull'Organizzazione;
- azioni correttive intraprese per prevenire che l'evento si ripeta;
- raccomandazioni per ulteriori azioni;
- requisiti di notifica verso l'esterno della Violazione.

4.9 Fase 7: comunicazione verso l'esterno della Violazione

In base ai risultati della valutazione del rischio, il Titolare/i (o Contitolari) valuta e decide se notificare la Violazione di Dati al Garante e/o comunicarla agli Interessati, secondo quanto di seguito precisato:

4.9.1 Notifica al Garante

La notifica al Garante è prevista solo se la Violazione di Dati può determinare un rischio per i diritti e le libertà degli Interessati.
Le Organizzazioni sono tenute ad informare il Garante entro 72 ore dalla scoperta della Violazione di Dati.
Se la notifica non avviene entro il predetto termine, sarà necessario includere nella comunicazione tardiva al Garante le ragioni che giustificano tale ritardo.
La notifica è una responsabilità delle Organizzazioni e dovrà effettuarsi secondo il modello di cui all'**Allegato 2**.
La notifica deve includere almeno le seguenti informazioni:

- una descrizione della Violazione di Dati (natura, modo e tempo in cui si è verificata, categorie e numero approssimativo di Interessati in questione, nonché categorie e numero approssimativo di registrazioni dei Dati personali in questione);
- gli impatti potenziali della Violazione di Dati;
- le misure e le azioni adottate o suggerite per rispondere ai rischi e porre rimedio alla Violazione di Dati e anche, se del caso, per attenuarne i possibili effetti negativi.

DEROGA

L'obbligo di notifica al Garante non sussiste se l'Organizzazione è in grado di provare che la Violazione di Dati che si è verificata non danneggerà gli Interessati in alcun modo.
Tale valutazione deve essere condotta caso per caso in funzione delle circostanze della fattispecie concreta in cui si è verificata la Violazione di Dati.
La valutazione e successiva decisione di non notificare al Garante una Violazione di Dati devono essere documentate e incluse nella Scheda di Violazione dei dati (Allegato 3) e nel Registro delle Violazioni (Allegato 4).

4.9.2 Comunicazione agli Interessati

La comunicazione agli Interessati è prevista unicamente per l'ipotesi in cui la Violazione di Dati può determinare un **rischio elevato** per i diritti e le libertà delle persone.
La comunicazione della Violazione agli Interessati i cui Dati siano stati compromessi deve essere effettuata non appena possibile e senza ingiustificato ritardo.
Si noti che, anche quando la Violazione di Dati riguarda un solo Interessato, qualora l'Organizzazione, su suggerimento del DPO, se nominato, (o del consulente eventualmente incaricato) consideri il rischio sufficientemente elevato e quindi necessaria la notifica, l'Interessato verrà informato.

In qualsiasi caso, la comunicazione è una responsabilità dell'Organizzazione.

La comunicazione agli Interessati deve avvenire mediante il canale di volta in volta ritenuto più idoneo e deve essere effettuata con un linguaggio semplice e chiaro.

La comunicazione agli Interessati deve contenere almeno le seguenti informazioni:
- la natura della Violazione;
- il nome e i dati di contatto del DPO, se nominato, o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze della Violazione di Dati;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare (o dai Contitolari) per porre rimedio alla Violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

DEROGA

La comunicazione agli Interessati non è dovuta se l'Organizzazione:
(i) ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati personali oggetto della Violazione, in particolare quelle destinate a rendere i Dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
(ii) ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
(iii) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

5. CONSAPEVOLEZZA IN CASO DI VIOLAZIONE DEI DATI

COSA FARE

- comunicare la violazione non appena possibile al Referente Privacy, se nominato, o alla direzione aziendale;

- rendersi disponibili in caso di domande da parte del Referente Privacy, della dirigenza aziendale e/o del Team responsabile della risposta alla Violazione di Dati e/o del DPO (quest'ultimo, se nominato) o del consulente eventualmente incaricato in luogo del DPO;

- documentare qualsiasi azione per la comunicazione al Team responsabile della risposta alla Violazione di Dati, incluse date e ore;

- discutere la Violazione esclusivamente con il Referente Privacy, se nominato, o con la direzione aziendale, il Team o il DPO (quest'ultimo, se nominato) o del consulente eventualmente incaricato

in luogo del DPO.

COSA NON FARE

- ignorare o cercare di nascondere la Violazione;
- diffondere di propria iniziativa la notizia/il contenuto della violazione all'esterno dell'organizzazione (si ricorda che è onere dell'Organizzazione procedere alle comunicazioni dovute per legge).

In caso di dubbio, contattare il Referente Privacy / la direzione aziendale e il DPO (quest'ultimo, se nominato, e, se non nominato, il consulente eventualmente incaricato).

ALLEGATO 1

VALUTAZIONE DEL RISCHIO DELLA VIOLAZIONE DEI DATI

1 – Individuazione del livello di impatto

L'individuazione del livello di impatto della Violazione di Dati, intesa come la stima del potenziale danno agli individui che possa derivare dalla Violazione stessa, deve essere effettuata sulla base dei criteri che seguono:

- *Contesto del trattamento dei dati personali (CTD)*: indica il tipo di Dato violato, unitamente ad una serie di fattori collegati al contesto generale del trattamento.
- *Facilità di identificazione dell'interessato (FI)*: indica quanto agevolmente può essere dedotta l'identità del soggetto interessato dai Dati oggetto della Violazione.
- *Circostanze della violazione (CV)*: indica le specifiche circostanze della Violazione, ossia il tipo di Violazione (alterazione, perdita, divulgazione non autorizzata). L'impatto può infatti essere diverso se la Violazione consiste in una divulgazione al pubblico o in una sottrazione o perdita. A mero titolo di esempio, se i Dati concernenti la busta paga di un dipendente sono divulgati pubblicamente questo potrebbe avere un impatto morale sull'Interessato, ma solo se sono alterati o persi l'impatto potrebbe essere di tipo economico.

2 – Calcolo della gravità della Violazione

Sulla base dei criteri indicati al paragrafo precedente:

- **CTD** rappresenta il fulcro dell'individuazione della criticità di una determinata categoria di Dati nell'ambito di una specifica attività di trattamento.

    1. Al fine della sua quantificazione è dunque necessario individuare a quale categoria i Dati violati appartengono, classificandoli almeno in una delle seguenti categorie e attribuendo loro il relativo valore numerico:

Dati comuni	1
Dati relativi a preferenze, abitudini e comportamento	2
Dati finanziari	3
Dati appartenenti a categorie particolari	4

    2. È poi opportuno aggiustare tale valore, in aumento o in diminuzione, a seconda che su di esso incidano fattori relativi al contesto dell'attività di trattamento quali, a titolo esemplificativo, il volume dei dati, le particolari caratteristiche del Titolare o dei soggetti interessati, l'erroneità/inaccuratezza dei Dati, la pubblica disponibilità dei Dati precedentemente alla Violazione, la natura dei Dati. A seguito dell'aumento o della diminuzione del valore iniziale, il CTD verrà quantificato in una misura variabile tra 1 e 4. Qualora più fattori concorressero all'aumento o alla diminuzione, questi andrebbero considerati cumulativamente. Ove il Titolare ritenesse di modificare il risultato di tale operazione in quanto esso non corrisponda al valora ragionevolmente attribuibile, potrà farlo motivando espressamente tale decisione.

- **FI** è un fattore correttivo del CTD. La criticità complessiva di un'attività di trattamento dei dati può infatti essere mitigata dal valore relativo alla facilità di identificazione dell'Interessato per mezzo dei Dati oggetto di Violazione. In altre parole, minore è la possibilità che il soggetto interessato venga identificato associando ad esso i Dati violati, minore risulterà il valore relativo alla gravità complessiva della Violazione.

Allo scopo di quantificare tale valore, sono state individuate quattro categorie alle quali la FI può essere ricondotta, ossia: *trascurabile*, *limitata*, *significativa*, *massima*. A tali categorie verranno rispettivamente associati valori numerici da 1 a 4.
In fase di attribuzione di tale valore, dovrà essere tenuto in considerazione il fatto che l'identificazione del soggetto Interessato tramite i Dati violati può essere diretta (*e.g.* sulla base di un nome o un cognome), ovvero indiretta (*e.g.* sulla base del numero del documento d'identità). Il valore di FI potrà variare a seconda delle circostanze stesse della Violazione.

A titolo esemplificativo, si riportano alcuni casi di Dati identificativi e i relativi valori di FI associati:

Dato violato: nominativo (nome e cognome)		
FI = 0,25	*trascurabile*	Identificazione del soggetto interessato attraverso il nominativo ove tale nominativo è molto comune nel Paese di residenza
FI = 0,5	*limitata*	Identificazione del soggetto interessato attraverso il nominativo ove tale nominativo non è molto comune nel Paese di residenza
FI = 0,75	*significativa*	Identificazione del soggetto interessato attraverso il nominativo nell'ambito di una piccola città ove pochi individui o addirittura nessuno ha il medesimo nominativo
FI = 1	*massima*	Identificazione del soggetto interessato nell'ambito del Paese di residenza tramite associazione di data di nascita e indirizzo email

Dato violato: numero telefonico/ indirizzo		
FI = 0,25	*trascurabile*	Identificazione del soggetto interessato attraverso il numero telefonico nell'ambito di un Paese ove il numero o indirizzo non siano inseriti in un registro pubblico
FI = 0,5	*limitata*	Identificazione del soggetto interessato attraverso il numero telefonico nell'ambito di una piccola città ove il numero o indirizzo non siano inseriti in un registro pubblico
FI = 1	*massima*	Identificazione del soggetto interessato attraverso il numero telefonico nell'ambito di un Paese ove il numero o indirizzo siano inseriti in un registro pubblico

- **CV** quantifica le specifiche circostanze della Violazione riscontrabili o meno in una determinata situazione. Ove presente, tale valore modifica la gravità complessiva della Violazione, contribuendo ad aumentare la quantificazione generale del rischio.
I fattori che integrano le CV sono individuati come segue:
  i. ***Perdita di riservatezza***: si verifica quando alle informazioni accedono soggetti che non sono a ciò autorizzati e non vi è alcuna legittima finalità che giustifichi tale accesso. La misura di tale valore varia a seconda dell'ambito della divulgazione, ossia del potenziale numero e tipologia di soggetti che possono avere illegittimamente avuto accesso alle informazioni.
  ESEMPI:

0	esempi di Dati esposti a rischi relativi alla perdita di riservatezza senza che vi sia evidenza di alcuna illegittima attività di trattamento	Documento cartaceo o pc portatile perduto durante il transito
		Smaltimento delle attrezzature senza distruzione dei Dati personali
+ 0,25	esempi di Dati comunicati ad un numero di destinatari conosciuti	Email contenente Dati personali erroneamente inviata ad un numero di destinatari conosciuti
		Accessibilità da parte di alcuni clienti di account appartenenti ad altri clienti nell'ambito di un servizio online
+ 0,5	esempi di Dati comunicati ad un numero non identificato di destinatari	Dati pubblicati in una bacheca online
		Vendita da parte di un dipendente di un supporto elettronico contenente Dati di clienti

ii. ***Perdita di integrità***: si verifica quando le informazioni originarie vengono alterate e la sostituzione dei Dati può essere pregiudizievole per l'individuo.
ESEMPI:

0	esempi di Dati alterati in assenza di alcuna identificazione di un loro utilizzo scorretto o illegale	Registro contenente dati personali è stato erroneamente aggiornato ma ne era stata estratta copia precedentemente all'aggiornamento
+ 0,25	esempi di Dati alterati e plausibilmente utilizzati in modo scorretto o illegale, con possibilità di recupero	Registro necessario per la fornitura di un servizio online è stato modificato, il soggetto dovrà pertanto accedere al servizio in modalità offline
		Registro rilevante in relazione all'accuratezza della documentazione medica dell'individuo nell'ambito di un servizio online è stato modificato
+ 0,5	esempi di Dati comunicati ad un numero non identificato di destinatari	Valgono esempi precedenti con, in aggiunta, l'impossibilità di recuperare copia originale dei Dati

iii. ***Perdita di disponibilità***: si verifica quando non è possibile accedere ai Dati originari in caso di necessità. La perdita di disponibilità può essere temporanea (quando i Dati sono recuperabili ma per procedere a tale recupero occorre del tempo e ciò può essere pregiudizievole per l'individuo) o permanente (quando i Dati non possono essere recuperati).
ESEMPI:

0	esempi di Dati recuperabili senza alcuna difficoltà	Una copia dei documenti è perduta ma altre copie sono disponibili
		Un database è compromesso ma può essere agevolmente ricostruito utilizzando altri database
+ 0,25	esempi di temporanea indisponibilità	Un database è compromesso ma può essere ricostruito attraverso altri database, pur implicando una certa lavorazione
		Un documento è perduto ma le informazioni possono essere nuovamente fornite dall'individuo
+ 0,5	esempi di indisponibilità (i Dati non possono essere recuperati né dal titolare né dal soggetto interessato)	Un documento è perduto/ un database è compromesso, non vi è alcuna copia back-up delle informazioni in esso contenute e tali informazioni non possono essere nuovamente fornite dall'individuo

iv. ***Volontarietà della violazione***: tale elemento dipende dal fatto che la Violazione sia avvenuta per errore, sia esso tecnico o umano, ovvero tramite azione volontaria. Le Violazioni involontarie includono i casi di perdita accidentale, utilizzo inadeguato, errore umano o errore nella configurazione o nel funzionamento del software. Violazioni volontarie includono i casi di *hacking* finalizzato al danneggiamento degli individui, di trasferimento di Dati personali a terzi per fini di profitto, di azioni volte a danneggiare il Titolare del trattamento.
ESEMPI:

+ 0,5	La Violazione è stata posta in essere volontariamente, con l'intento, ad esempio, di recare pregiudizio al titolare e/o danno ai soggetti interessati	Un dipendente di una società intenzionalmente condivide Dati personali di clienti attraverso social media
		Un dipendente di una società vende Dati personali di clienti ad altra società
		Un membro di un social network intenzionalmente invia informazioni relative ad altri membri alle loro famiglie, con il fine di danneggiarli

Le circostanze così individuate possono peraltro cumularsi, contribuendo a modificare in aumento o in diminuzione la valutazione finale della gravità della Violazione.

Alla luce di tali specificazioni, il risultato finale dell'individuazione della gravità della Violazione dei Dati (GR) verrà calcolato utilizzando la formula GR = CTD x FI + CV

Il risultato di tale operazione verrà poi valutato sulla base di una tabella di rischio ove sono individuati quattro livelli: *non significativo*, *limitato*, *elevato* e *molto elevato*.

È peraltro necessario specificare come tale individuazione del livello di rischio non implichi conseguenze dal punto di vista legale ma si limiti a fornire una rappresentazione volta ad una puntuale notificazione alle Autorità competenti.

	Livello di rischio	Valore	Descrizione
N	**Non significativo**	GR < 2	I soggetti coinvolti non sono toccati dalla Violazione o comunque rischiano di dover affrontare piccoli inconvenienti come conseguenze della stessa, superabili senza alcun particolare problema (quale potrebbe essere la perdita di tempo relativa al re-inserimento delle informazioni, il fastidio, l'irritazione, ecc.)
L	**Limitato**	2 ≤ GR < 3	I soggetti coinvolti potrebbero affrontare inconvenienti significativi, che saranno in grado di affrontare nonostante alcune difficoltà (costi aggiuntivi, diniego di accesso a servizi commerciali, timore, stress, danno fisico di lieve entità, ecc.)
E	**Elevato**	3 ≤ GR < 4	I soggetti coinvolti potrebbero affrontare conseguenze significative, che saranno in grado di superare con serie difficoltà (appropriazione indebita di fondi, inserimento in *black-list* da parte di istituti bancari, danni alla proprietà, perdita dell'impiego, azione legale, peggioramento delle condizioni fisiche, ecc.)
M	**Molto elevato**	4 ≤ GR	I soggetti coinvolti potrebbero affrontare conseguenze significative o addirittura irreversibili (stress finanziario come debiti considerevoli o inabilità al lavoro, disturbi fisici o psicologici a lungo termine, morte, ecc.)

In caso di dubbio, assumere il livello di impatto più elevato.

3 - Numero dei soggetti interessati

Una volta stabilito il livello di impatto, deve essere considerato il numero degli Interessati coinvolti nella Violazione di Dati.

	Descrizione
A	Oltre 10.000 Soggetti interessati coinvolti
B	Da 1.001 a 10.000 Soggetti interessati coinvolti
C	Da 101 a 1.000 Soggetti interessati coinvolti
D	Da 0 a 100 Soggetti interessati coinvolti

4 - Valutazione iniziale del rischio

Una volta confrontati i criteri di cui ai paragrafi 1 e 2 che precedono, si determina il livello di rischio compreso tra 1 e 4:

	M	E	L	N
A	4	4	3	3
B	4	4	2	2
C	4	3	2	1
D	4	3	1	1

5 – Decisione per la notifica in base all'impatto

All'esito della valutazione effettuata sulla base dei criteri sopra indicati sarà possibile identificare l'impatto:

		Garante	Soggetti interessati
4	Impatto molto elevato	Notifica obbligatoria	Comunicazione obbligatoria
3	Impatto elevato	Notifica obbligatoria	Comunicazione fortemente raccomandata
2	Impatto limitato	Notifica raccomandata	Comunicazione raccomandata
1	Trascurabile	Notifica non necessaria	Comunicazione non necessaria

ALLEGATO 2

MODELLO PER LA NOTIFICA DELLE VIOLAZIONI DEI DATI

1. Titolare del trattamento dei dati	
Denominazione sociale	**GS1 Italy / GS1 Italy Servizi S.r.l.**
Indirizzo	Via Paleocapa, 7 - Milano
Partita IVA / Codice Fiscale	
Numero di telefono	
E-mail e PEC	

2. Violazione dei dati	
2.1 Data e ora	
Data della violazione	
Ora della violazione	
Data di scoperta della violazione	
Ora di scoperta della violazione	

Se la Violazione dei dati è stata notificata da un Responsabile del trattamento:

Data di scoperta della Violazione da parte del Responsabile del trattamento	
Ora di scoperta della Violazione da parte del Responsabile del trattamento	

2.2 Descrizione della Violazione	
Tipo di Violazione	☐ Violazione della riservatezza – i Dati personali sono stati compromessi tramite accesso non autorizzato ☐ Perdita di integrità – modifica non desiderata dei Dati personali ☐ Perdita della disponibilità – i Dati personali sono persi/inaccessibili ☐ Altro – specificare:

Categorie di Dati personali coinvolti

☐ Stato civile (ad es. nome, sesso, data di nascita, età)

☐ Recapiti (ad es. indirizzo postale o e-mail, numero di telefono)

☐ Identificazione e accesso ai dati (ad es. credenziali di accesso, numero cliente)

☐ Informazioni di carattere economico (ad es. numero di carta di credito, dati bancari, stipendio)

☐ Categorie particolari di Dati personali (ad es. dati medici, dettagli sull'origine etnica o razziale, opinioni politiche, credo religioso)

☐ Altro – specificare:

Luogo della violazione
Strumenti per la conservazione dei Dati personali coinvolti

☐ Server interno

☐ Computer fisso

☐ Computer portatile

☐ Hard-drive esterno

☐ Documenti fisici

☐ Altro – specificare:

Descrizione generale della Violazione

Prime azioni di risposta intraprese per mitigare il rischio

3. Soggetti interessati

3.1 Soggetti interessati coinvolti dalla violazione

Categorie di soggetti interessati coinvolti

☐ Dipendenti o agenti (persone fisiche)

☐ Appaltatori, fornitori o partner commerciali (persone fisiche)

☐ Clienti o utenti

☐ Altro – specificare:

Numero di soggetti interessati coinvolti

Luogo in cui si trovano i soggetti interessati coinvolti ☐

3.2 Comunicazione ai soggetti interessati

Decisione riguardante la comunicazione

☐ Abbiamo provveduto a informare i soggetti interessati il:

☐ Abbiamo pianificato di informare i soggetti interessati il:

☐ Non informeremo i soggetti interessati perché:

- ☐ Potrebbe compromettere le indagini
- ☐ Possiamo fornire prova del fatto che la violazione non causerà un rischio elevato per i soggetti interessati
- ☐ Abbiamo adottato misure appropriate prima della violazione (ad es. criptaggio, pseudonimizzazione)
- ☐ Abbiamo adottato le conseguenti misure per prevenire la materializzazione dei rischi
- ☐ Non siamo in grado di identificarli ma faremo una comunicazione sui media nazionali/locali o sul sito web della Società

Strumenti di comunicazione

☐ via posta

☐ via e-mail

☐ Altro – specificare:

Numero di soggetti interessati informati

4. Impatto della violazione

4.1 Conseguenze potenziali

In caso di violazione della riservatezza

☐ I Dati possono essere diffusi più di quanto previsto dall'Interessato (ad es. divulgazione di fotografie/informazioni sui social media)

☐ I Dati possono essere collegati ad altre informazioni relative ai soggetti interessati (ad es. geolocalizzazione connesse al luogo di residenza)

☐ I Dati possono essere elaborati in modo illegale (ad es. scopi commerciali, furto di identità)

In caso di perdita di integrità

☐ I Dati possono essere modificati e invalidati, causando potenzialmente errori o malfunzionamenti di elaborazione, alterando il servizio fornito all'Interessato

☐ I Dati possono essere modificati in dati validi diversi, alterando il trattamento originale

In caso di perdita della disponibilità

☐ I Dati possono non essere disponibili per il trattamento e il titolare del trattamento non può fornire i servizi previsti all'Interessato

☐ I Dati possono non essere disponibili per il trattamento e causare errori, malfunzionamenti o alterazioni del servizio fornito all'Interessato (ad es. dati mancanti nella banca dati relativa ai pagamenti del dipendente che causano errori nell'elaborazione del pagamento)

Altro danno potenziale all'Interessato

4.2 Valutazione del rischio

Livello	Descrizione del livello	Danni potenziali
Basso	Nessun impatto sui soggetti interessati o disagio trascurabile	Leggero ritardo delle procedure amministrative, inconveniente di minore importanza
Medio	Disagio importante per l'Interessato, superabile con qualche difficoltà	Aumento del costo del servizio, tariffe, negazione del servizio, sofferenza fisica o psicologica trascurabile
Elevato	Conseguenze importanti per l'Interessato, superabili ma con molta difficoltà	Sottrazione di denaro, conto bancario congelato, deterioramento di beni, perdita del lavoro, azione legale, importante sofferenza fisica o psicologica

Molto elevato	Conseguenze importanti per l'Interessato, superabili ma con molta difficoltà	Sottrazione di denaro, conto bancario congelato, deterioramento di beni, perdita del lavoro, azione legale, importante sofferenza fisica o psicologica

In base alla precedente tabella, spuntare le caselle per indicare il livello di rischio:

Tipo di rischio	Basso	Medio	Elevato	Molto elevato
☐ **Furto di identità**	☐	☐	☐	☐
☐ **Danno di reputazione**	☐	☐	☐	☐
☐ **Danno emotivo**	☐	☐	☐	☐
☐ **Danno economico**	☐	☐	☐	☐
☐ **Pericolo fisico**	☐	☐	☐	☐
☐ **Pericolo di vita**	☐	☐	☐	☐
☐ **Altro – specificare:**	☐	☐	☐	☐

5. Misure di sicurezza

Misure preventive messe in atto <u>prima</u> della Violazione

☐ **Criptaggio**

☐ **Funzioni hash**

☐ **Pseudonimizzazione/anonimizzazione**

☐ **Limitazione dell'accesso**

☐ **Altro – specificare:**

Misure successive o di riparazione messe in atto <u>dopo</u> la Violazione

Raccomandazioni ai soggetti interessati per minimizzare il rischio

Piano d'azione per prevenire un'altra violazione

6. Osservazioni aggiuntive

ALLEGATO 3

SCHEDA DI VIOLAZIONE DEI DATI

Rif.

Parte 1 - I tuoi dati

Cognome	Nome
Titolo	Ufficio/funzione
Data	

Parte 2 - Dettagli della violazione dei dati

Violazione avvenuta	Violazione scoperta

Descrizione della violazione:

Causa della violazione:

Parte 3 - Dati interessati

Specificare quali tipologie di dati sono stati compromessi:

☐ Nome	☐ Dati personali	☐ Stile di vita e sociale
☐ Recapiti	☐ Dati famigliari	☐ Risposte ai sondaggi
☐ Dati finanziari	☐ Competenze professionali e formazione	
☐ Appartenenza ad associazioni sindacali	☐ Prodotti e servizi forniti	☐ Fotografie, videosorveglianza
☐ Dati di posizione (ad es. GPS)	☐ Opinioni politiche	☐ Etnia
☐ Credo religioso	☐ Reati (inclusi presunti tali)	☐ Orientamento sessuale /
☐ Dettagli dei reclami, lamentele	☐ Procedimenti civili o penali	
☐ Altro (specificare):		

Elencare le misure preventive in essere per prevedere simili incidenti:

(ad es. crittografia, protezione di documento tramite password, armadietti chiusi a chiave, ecc.)

Parte 4 - Persone fisiche interessate

Descrivere le categorie di persone fisiche interessate dalla violazione:

☐ Clienti / Associati	☐ Dipendenti	☐ Studenti
☐ Fornitori	☐ Visitatori	☐ Consulenti/esperti
☐ Agenti	☐ Persone fisiche catturate da immagini videosorveglianza	☐ Soggetti che hanno risposto a sondaggi
☐ Utenti web	☐ Altro (specificare)	

Numero di persone interessate		
Persone che sono a conoscenza	☐ Sì	☐ No

della violazione La persona fisica ha presentato un reclamo	☐ Sì ☐ No *In caso positivo, specificare come:*

Parte 5 - Contenimento e recupero

Descrizione delle azioni immediate intraprese per contenere la violazione dei dati:

I dati a rischio sono stati recuperati?

☐ Sì ☐ No

In caso positivo, specificare come e quando:

Parte 6 - Rischi associati

Potenziali conseguenze avverse della violazione dei dati sulle persone interessate:

ad es. furto di identità, frode di carta di credito, danno di reputazione, ecc.

Quanto sono gravi tali conseguenze?

☐ Non gravi ☐ Gravi ☐ Molto gravi

Quale probabilità anno di materializzarsi?

☐ Improbabile ☐ Probabile ☐ Molto probabile

Parte 6 - Rischi associati (continuazione)

I rischi sopra indicati sono stati gestiti correttamente? ☐ Sì ☐ No

In caso negativo, specificare perché:

Parte 7 - Notifica

Persone fisiche	☐ Sì	☐ No	Data
Garante	☐ Sì	☐ No	Data
Forze dell'ordine	☐ Sì	☐ No	Data

Ragione dell'eventuale ritardo nell'invio della notifica:

Parte 8 - Risultati e raccomandazioni

Azioni intraprese per risolvere la violazione

Conseguenze potenziali non realizzate della violazione

Azioni raccomandate per prevenire la ripetizione dell'incidente

Firmato da	Data

ALLEGATO 4
REGISTRO DELLE VIOLAZIONI DEI DATI

REGISTRO INTERNO DELLE VIOLAZIONI DEI DATI PERSONALI										
Rif.	**Data**	**Tipo di violazione**	**Data e ora di scoperta della violazione**	**Descrizione della violazione**	**Luogo della violazione**	**Risultato della valutazione del rischio**	**Azione correttiva**	**Comunicazione agli Interessati (sì/no) e dettagli**	**Notifica al Garante (sì/no) e dettagli**	**Altre informazioni**

ALLEGATO 5

CONTRATTO PER IL TRATTAMENTO DI DATI PERSONALI E NOMINA DEL RESPONSABILE ESTERNO [*BOZZA STANDARD*]

Sottoscritto in [●] il [●]

da e tra

GS1 Italy con sede legale in Milano, Via Paleocapa 7, Codice Fiscale n. 80140330152 in persona del legale rappresentante *pro-tempore* (di seguito anche "**GS1 Italy**")

E

GS1 Italy Servizi S.r.l., con sede in Milano, Via Paleocapa 7, Codice Fiscale n. 06166030962 in persona del legale rappresentante *pro-tempore* (di seguito anche "**GS1 Italy Servizi**")

- da un lato -

E

[●], con sede legale in [●], Via [●], Codice Fiscale e Partita IVA n. [●], in persona del legale rappresentante pro-tempore, munito degli occorrenti poteri (di seguito "**Fornitore**")

- dall'altro lato -

GS1 Italy, GS1 Italy Servizi S.r.l. e Fornitore di seguito congiuntamente indicati come "**Parti**" e individualmente come la "**Parte**"

PREMESSO CHE

(i) GS1 Italy e GS1 Italy Servizi hanno in comune e condividono scopi ed obiettivi, nonché strumenti e risorse necessari od utili a perseguirli, anche nell'ambito del trattamento dei dati personali ed hanno a tale scopo sottoscritto un accordo di contitolarità, ai sensi e per gli effetti di cui all'articolo 26 del Regolamento UE 2016/679, *Regolamento Generale sulla Protezione dei Dati Personali*, in relazione a taluni trattamenti di dati personali tra di loro condivisi (di seguito "**Accordo di Contitolarità**" o solo "**Contitolarità**");

(ii) le Parti hanno sottoscritto un accordo in forza del quale [*DA COMPLETARE*] (di seguito "**Accordo**");

(iii) in occasione ed in funzione dello svolgimento delle attività e dei servizi di cui all'Accordo, il Fornitore può, dunque, venire a conoscenza e raccogliere dati personali rispetto a cui GS1 Italy e GS1 Italy Servizi sono contitolari (di seguito "**Contitolari**") e che ricadono nell'ambito di operatività dell'Accordo di Contitolarità;

(iv) in ragione di quanto indicato ai punti che precedono i Contitolari ravvisano quindi la necessità di nominare il Fornitore, nella persona del suo legale rappresentante, responsabile esterno del trattamento dei dati personali di cui venga a conoscenza in esecuzione dell'Accordo, in maniera tale da garantire che il trattamento dei dati in questione avvenga nel pieno rispetto delle disposizioni del Regolamento UE 2016/679, cosiddetto "*General Data Protection Regulation*";

(v) il Fornitore ha manifestato la propria disponibilità ad assolvere l'incarico di responsabile esterno del trattamento dei dati personali ed ha, a tale scopo, confermato di possedere i requisiti di cui all'articolo 28 del citato Regolamento UE 2016/679 e di offrire garanzie sufficienti per mettere in atto tutte misure

adeguate affinché il trattamento dei dati personali sia conforme alle disposizioni di legge in vigore in materia di protezione di dati personali e garantisca la tutela dei diritti dell'interessato.

TUTTO CIÒ PREMESSO
LE PARTI CONVENGONO E STIPULANO QUANTO SEGUE

1. Premesse, Allegati e Definizioni

1.1 Le Premesse e gli allegati ("**Allegati**") costituiscono parte integrante e sostanziale del presente contratto ("**Contratto**").

1.2 Salvo quant'altro specificato nel presente Contratto, i termini identificati con lettera maiuscola hanno il significato di seguito precisato (le parole al singolare includono il plurale e viceversa):

1.2.1 **"Accordo"** indica l'accordo di collaborazione in essere tra il Fornitore e uno o entrambi i Contitolari di cui al punto (i) delle premesse che precedono;

1.2.2 **"Contitolare/i"** indica, a seconda dei casi, GS1 Italy e/o GS1 Italy Servizi, come indicato alla premessa (i) che precede;

1.2.3 **"Dati Personali"** o **"Dati"** indica qualsiasi informazione relativa a un individuo identificato o identificabile oggetto di Contitolarità e che deve essere trattata dal Fornitore in funzione dei Servizi oggetto di Accordo ed in forza del presente Contratto;

1.2.4 **"Leggi sulla Protezione dei Dati"** indica tutte le leggi e i regolamenti, inclusi ma non limitati al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e al D.lgs. n. 196/2003, *Codice in materia di protezione dei dati personali*, e successive modifiche e integrazioni (ivi incluse in particolare quelle di cui al D.Lgs. n. 101/2018), nonché provvedimenti di volta in volta in vigore che sono applicabili al trattamento dei dati personali effettuato in forza di questo Contratto;

1.2.5 **"MTO"** indica le misure tecniche e organizzative richieste ai sensi dell'articolo 32 del Regolamento;

1.2.6 **"Nomina"** o **"Contratto"** indica il presente accordo di nomina del Responsabile del Trattamento dei Dati Personali ai sensi dell'art. 28 del Regolamento, compresi i relativi allegati, come di tempo in tempo eventualmente integrati od aggiornati;

1.2.7 **"Regolamento"** indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 in materia di protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione dei dati, e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);

1.2.8 **"Responsabile"** o **"Responsabile del Trattamento"** indica il Fornitore che tratta Dati Personali per conto dei Contitolari ai sensi dell'Art. 28 del Regolamento;

1.2.9 **"Richiesta dell'Interessato"** indica la richiesta presentata dall'interessato al Contitolare o al Responsabile mediante la quale l'individuo esercita i diritti riconosciuti dal Regolamento o da altre Leggi in materia di Protezione dei Dati Personali. Ai sensi del Regolamento sono riconosciuti a tutela degli interessati i seguenti diritti: il diritto di informazione, il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione, il diritto di limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione e i diritti in relazione al processo decisionale e alla profilazione automatizzati;

1.2.10 **"RPD"** o "**DPO**" indica il responsabile della protezione dei dati, una persona fisica che sovrintende alla conformità della protezione dei dati di un'organizzazione;

1.2.11 **"Servizi"** indica i servizi che devono essere eseguiti dal Fornitore come indicato nelle premesse che precedono;

1.2.12 **"Sub-responsabile"** indica il soggetto, persona fisica o giuridica od ente, nominato dal Responsabile del Trattamento, che tratta Dati Personali per conto dei Contitolari;

1.2.13 **"Trattamento"** o **"Trattare"** indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, il blocco, la cancellazione o la distruzione;

1.2.14 **"Violazione dei Dati Personali"** indica una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o trattati in altro modo.

2. Oggetto

2.1 Ai termini ed alle condizioni di cui al presente Contratto, i Contitolari designano il Fornitore Fornitore, che, a propria volta, accetta, quale *Responsabile esterno del trattamento dei dati personali* in relazione ai Dati Personali ed ai Trattamenti da condursi su tali Dati necessari, funzionali e/o utili all'esecuzione e gestione dei Servizi, il tutto come meglio specificato nell'**Allegato 1** al presente Contratto.

2.2 Nell'ambito dei reciproci rapporti contrattuali, le Parti si impegnano a rispettare le Leggi sulla Protezione dei Dati.

3. Obblighi del Responsabile del Trattamento

3.1 Con la sottoscrizione del presente Contratto, il Responsabile del Trattamento si impegna a:

3.1.1 trattare i Dati Personali esclusivamente per gli scopi che sono oggetto della presente Nomina secondo quanto riportato nell'Allegato 1;

3.1.2 trattare i Dati Personali in conformità e nel rispetto delle istruzioni documentate provenienti dal Titolare del Trattamento;

3.1.3 informare i Contitolari qualora ritenga che un'istruzione impartita da questi ultimi costituisca una violazione delle Leggi sulla Protezione dei Dati;

3.1.4 garantire la riservatezza dei Dati Personali trattati nell'ambito dell'Accordo;

3.1.5 assicurare che le persone autorizzate a trattare i Dati Personali nell'ambito dell'Accordo e della presente Nomina, ivi inclusi propri dipendenti e collaboratori:

- si siano impegnate a rispettare la riservatezza sui Dati, anche tramite sottoscrizione di apposito impegno scritto, e siano tenute all'obbligo legale di riservatezza;
- abbiano ricevuto istruzioni dettagliate e adeguata formazione in merito alla protezione dei Dati Personali;

3.1.6 tenere in considerazione ed applicare, per quanto riguarda l'utilizzo di strumenti, prodotti, applicazioni o servizi impiegati nel trattamento dei Dati Personali, i principi previsti dalle Leggi sulla Protezione dei Dati;

3.1.7 informare - tempestivamente e comunque senza ritardo – i Contitolari di ogni Violazione dei Dati Personali al seguente indirizzo e-mail: privacy@gs1it.org;

3.1.8 provvedere alla individuazione ed alla nomina del/degli amministratore/i di sistema ai sensi del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 recante "*Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" e ss.mm.ii.;

3.1.9 fornire, limitatamente ai trattamenti di cui all'Accordo, assistenza ai Contitolari affinché possano adempiere agli obblighi cui sono soggetti ai sensi Leggi sulla Protezione dei Dati;

3.1.10 mantenere un registro delle attività di Trattamento svolte per conto dei Contitolari;

3.1.11 attuare MTO necessarie a garantire un livello di sicurezza adeguato al rischio;

3.1.12 non trasferirei i Dati Personali al di fuori del territorio dell'Unione Europea o dello Spazio Economico Europeo (ivi incluso tramite applicativi o piattaforme che facciano uso di soluzioni *cloud*) senza la preventiva autorizzazione scritta da parte dei Contitolari che non sarà irragionevolmente negata e, anche in caso di autorizzazione, garantire che il trasferimento internazionale sia fondato su di una condizione di adeguatezza, come prevista dalle Leggi sulla Protezione dei Dati.

4. Sub-responsabili

4.1 Qualora, in funzione della concreta esecuzione dell'Accordo, si renda necessario affidare a soggetti terzi, diversi dal Responsabile, l'effettuazione di operazioni che comportino il Trattamento, anche parziale, dei Dati Personali, il Responsabile si impegna a non delegare né affidare, in qualsivoglia modo ed a qualunque titolo, una o più operazioni di Trattamento dei Dati Personali e, quindi, a non ricorrere ad un altro responsabile o Sub-responsabile del trattamento senza aver previamente ottenuto autorizzazione scritta specifica dei Contitolari, che non potrà essere irragionevolmente negata o ritardata. La presente clausola si applica anche qualora il Responsabile intenda sostituire il (sub)responsabile originariamente individuato (e autorizzato).

4.2 È sin da ora espressamente concordato che, qualora il Responsabile ricorra, previa autorizzazione, ad un altro Sub-responsabile del trattamento per l'esecuzione di specifiche attività per conto dei Contitolari, sarà tenuto ad imporre a tale altro Sub-responsabile, mediante contratto scritto, obblighi in materia di protezione dei Dati che siano coerenti, nella sostanza, con quelli di cui a questo Contratto. Il Responsabile dovrà, inoltre, fornire, su richiesta, copia di tali accordi ai Contitolari.

5. Rapporti con gli interessati

È onere dei Contitolari, al momento della raccolta dei Dati Personali, fornire adeguate informazioni agli Interessati circa le operazioni di Trattamento effettuate da parte del Responsabile del Trattamento. Il Responsabile del Trattamento si impegna ad assistere i Contitolari nel fornire riscontro alle Richieste degli Interessati e nell'adempimento degli obblighi derivanti dalle stesse.

6. Durata – Effetti della cessazione

6.1 Il presente Contratto entra in vigore a far data dall'inizio dell'esecuzione dei Servizi di cui all'Accordo e, in ogni caso, dall'avvio della collaborazione tra le Parti e termina alla data di scadenza, anche prorogata, o alla cessazione, per qualsivoglia causa intervenuta, di tale collaborazione, fermo ed impregiudicato quanto di seguito previsto.

6.2 Alla cessazione dell'Accordo per qualsivoglia causa intervenuta, il Responsabile del Trattamento si impegna, su richiesta scritta dei Contitolari, a restituire tutti i Dati Personali. La restituzione sarà, ove richiesto, accompagnata dalla distruzione delle copie esistenti nei sistemi informativi del Responsabile del Trattamento e da attestazione scritta di avvenuta distruzione, il tutto senza oneri aggiuntivi a carico dei Contitolari.

6.3 Resta ferma la facoltà del Responsabile del Trattamento di conservare copia dei Dati Personali per i fini e secondo le modalità e tempistiche previste dalle Leggi sulla Protezione dei Dati per l'esercizio dei propri diritti in caso di contestazioni e/o reclami proposti da terzi, nel rispetto dei termini prescrizionali e/o decadenziali di legge.

7. Controlli

7.1 Il Responsabile si rende disponibile a fornire, per tutta la durata del Contratto e dell'Accordo, ai Contitolari o a loro incaricati l'accesso ad archivi/documenti, informatici e non, secondo quanto ragionevolmente necessario in funzione delle esigenze dei Contitolari e laddove ciò sia necessario ai sensi di legge e comunque ai fini del controllo del puntuale rispetto degli impegni assunti dal Responsabile ai sensi del presente Contratto e/o in adempimento di un obbligo di legge.

8. Disposizioni finali

8.1 Ulteriori e più specifiche istruzioni e/o indicazioni potranno essere fornite dai Contitolari nel corso della durata del presente Contratto.

8.2 Resta salva la possibilità per i Contitolari di avvalersi di altri soggetti qualificati e nominati come responsabili del trattamento in relazione ai Dati e/o ad attività di trattamento su questi ultimi analoghe a quelle necessarie al fine dell'esecuzione dei Servizi.

8.3 Le Parti si impegnano sin da ora reciprocamente a rivedere e/o aggiornare il presente Contratto, laddove ciò dovesse rendersi necessario o comunque utile sulla base delle indicazioni che potranno essere, di tempo in tempo, successivamente alla data di sottoscrizione del presente documento, fornite dal legislatore, nazionale o comunitario, o dall'Autorità di Controllo o dalle autorità competenti.

8.4 Il presente Contratto integra, limitatamente alla materia che ne forma oggetto, i contenuti dell'Accordo e, in generale, le condizioni della collaborazione tra le Parti in merito all'esecuzione dei Servizi. In caso di contrasto e/o incongruenze prevarrà, limitatamente alla materia del trattamento dei dati personali, quanto previsto da questo Contratto.

8.5 Le Parti devolvono la risoluzione di eventuali controversie che dovessero sorgere dal presente Contratto, ivi incluso in relazione alla sua interpretazione, validità e cessazione alla competenza esclusiva del Foro di Milano.

In fede di quanto precede, il presente accordo viene sottoscritto in n. 2 esemplari nel luogo e nella data in epigrafe indicati.

GS1 Italy

Nome e Cognome del firmatario: _____

Ruolo: _____

Firma: _____

GS1 Italy Servizi S.r.l.
Nome e Cognome del firmatario: _____
Ruolo: _____
Firma: _____

Fornitore
Nome e Cognome del firmatario: _____
Ruolo: _____
Firma: _____

Allegato 1: Dettagli in merito al trattamento dei dati affidato al Responsabile

ALLEGATO 1

TRATTAMENTO DEI DATI PERSONALI AFFIDATO AL RESPONSABILE

Il presente Allegato comprende le informazioni relative al trattamento dei dati personali richieste dall'articolo 28 (3) del Regolamento UE 2016/679.

Oggetto e durata del Trattamento dei Dati Personali
L'oggetto e la durata del trattamento dei dati personali da parte del nominato Responsabile esterno sono individuati nell'accordo sul trattamento dei dati e nomina a responsabile e/o nell'accordo di collaborazione in essere tra le parti.

Natura e finalità del Trattamento dei Dati Personali
- ☐ Prestazione di servizi di ……[*Specificare*]
- ☐ Altro …….[*Specificare*]

Tipologie di Dati Personali oggetto di trattamento
[Selezionare la voce corrispondente e/o precisare meglio alla voce in bianco]
- ☐ dati anagrafici
- ☐ indirizzo postale
- ☐ recapiti telefonici
- ☐ documenti di identità (carta di identità e codice fiscale principalmente)
- ☐ dati bancari
- ☐ indirizzi email
- ☐ dati carta di credito
- ☐ immagini (foto o video)
- ☐ ubicazione e/o spostamenti
- ☐ log e dati personali associati
- ☐ traffico telematico
- ☐ categorie particolari di dati personali (intendendosi per tali i dati personali idonei a rivelare "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale*", nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona), ossia i seguenti: ……..……..……[*Specificare*]
- ☐ altro ……..…..……[*Specificare*]

Categorie di interessati a cui fanno riferimento i Dati personali
[Selezionare la voce corrispondente e/o precisare meglio alla voce in bianco]
- ☐ Clienti / associati
- ☐ Potenziali clienti / associati
- ☐ Fornitori di ……..……...…[*Verificare e specificare*]
- ☐ Partner contrattuali di …….…….[*Verificare e specificare*]
- ☐ Utenti del/dei sito/i web……..…….……...……[*Verificare e specificare*]

Da siglare a cura delle parti