ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

Grandi Giochi S.r.l. (di seguito, "GP") e la controparte ("**Fornitore**" o "**Responsabile**"), che accetta l'accordo che segue nonché tutti gli Allegati (sia quelli resi disponibili da GP online sul proprio sito o che quelli sottoposti al Fornitore durante la fase di contrattualizzazione), hanno stipulato un contratto per la fornitura dei Servizi del Responsabile o comunque un altro atto giuridico volto a disciplinare i rapporti tra le Parti, o, ancora, hanno posto in essere un comportamento concludente volto alla conclusione di un contratto che implica attività di trattamento di Dati Personali (di seguito, come di volta in volta modificato o aggiornato, solo il "**Contratto**").

Il presente accordo per il trattamento dei dati (compresi i suoi allegati, "**Accordo per il Trattamento dei Dati**" o "**DPA**") contiene le previsioni dell'art. 28 GDPR come interpretate dal Comitato Europeo per la protezione dei dati personali nell'Opinione 14/2019.

L'Accordo per il Trattamento dei Dati è concluso tra GP e il Fornitore ed è parte integrante del Contratto. L'Accordo per il Trattamento dei Dati (compresi i suoi allegati resi disponibili online sul sito di GP o direttamente sottoposti al Fornitore in fase di contrattualizzazione) sarà efficace, e sostituirà qualsiasi altro accordo tra le parti precedentemente applicabile in relazione allo stesso oggetto (comprese eventuali modifiche o addendum al trattamento dei dati relativi ai Servizi del Responsabile) a partire dalla Data di Entrata in Vigore e per tutto il Periodo.

Il soggetto che sottoscrive il presente Accordo per il Trattamento dei Dati per conto del Fornitore garantisce che: (a) ha il potere di rappresentanza per vincolare il Fornitore al presente Accordo per il Trattamento dei Dati; e (b) sottoscrive, per conto del Fornitore, il presente Accordo per il Trattamento dei Dati o i suoi Allegati. Qualora non disponga del potere di rappresentanza per vincolare il Fornitore, la preghiamo di non sottoscrivere il presente Accordo per il Trattamento dei Dati o i suoi Allegati, come richiesto da GP, e di trasmetterlo al soggetto debitamente autorizzato a tali attività e in possesso del potere di firma e rappresentanza del Fornitore.

Questo DPA riflette le intese intercorse tra le Parti rispetto al trattamento dei Dati Personali di GP come disciplinato dalla Legislazione Applicabile in Materia di Protezione dei Dati e può sempre essere consultato anche online sul sito di GP.

Di conseguenza
le Parti convengono e stipulano quanto segue:

1. Definizioni

1.1. Le parole con una lettera iniziale maiuscola hanno il significato indicato nell'introduzione e qui di seguito:

"**Autorità di Controllo**" si intende una "autorità di controllo" come definita nel GDPR e ai fini di questo DPA è quella indicata nell'Allegato I ;

"**Categorie Particolari di Dati Personali**" si intende qualsiasi informazione personale che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale di un Interessato, così come il trattamento di dati genetici, dati biometrici destinati a identificare in modo univoco un Interessato, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di un Interessato, o dati relativi a condanne penali e reati o alle correlate misure di sicurezza relative ad un Interessato;

"Clausole Contrattuali Standard" indica le Clausole Contrattuali Standard per i trasferimenti di dati personali verso Paesi terzi secondo l'articolo 28(7) del Regolamento (EU) 2016/679 approvate dal Parlamento Europeo e dal Consiglio disponibili qui: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en%20;

"**Contitolari**" o "**Contitolare del Trattamento**" si intende qualsiasi Titolare che determina, congiuntamente ad un altro Titolare le Attività di Trattamento e le Misure di Sicurezza applicabili al Trattamento dei Dati di GP;

"**Data di Entrata in Vigore**" indica la data in cui le Parti hanno firmato, accettato o altrimenti concordato l'entrata in vigore di questo DPA;

"**Dati Personali di GP** si intendono i Dati Personali che vengono Trattati dal Fornitore per conto di GP nella fornitura dei Servizi del Responsabile;

"**Diritti dell'Interessato**" si intendono i diritti spettanti agli Interessati ai sensi del Regolamento, qualora non siano esclusi dalla Legislazione Applicabile in Materia di Protezione dei Dati. A fini di chiarezza, questi includono almeno il diritto di richiedere l'accesso, la rettifica o la cancellazione dei dati personali, nonché di opporsi al trattamento dei dati di GP.

"Documentazione di Sicurezza" indica qualsiasi certificazione di sicurezza o documentazione (es. misure organizzative e tecniche di sicurezza, piani di disaster recovery e business continuity, ecc.) che dimostri la conformità al presente DPA e/o alla Legislazione Applicabile in Materia di Protezione dei Dati per quanto riguarda il Trattamento dei Dati di GP;

"**Fornitore**" indica ogni società indicata nell'Allegato I di questo DPA (esclusa GP) che, nell'ambito della fornitura dei propri servizi a GP, assume il ruolo di Responsabile del Trattamento;

"**Incidente**" si intende una distruzione, perdita, alterazione, divulgazione non autorizzata o accesso accidentale o illegale ai Dati di GP sui sistemi gestiti o comunque sotto la responsabilità del Responsabile. Ai fini del presente DPA, gli incidenti saranno considerati come "violazioni dei dati personali", come definito nell'art. 4(12) del Regolamento;

"**Indirizzo E-mail di Notifica**" si intende privacy@giochipreziosi.it o gli eventuali altri dati di contatto di GP elencati nell'Allegato I del presente DPA;

"**Interessato**": qualsiasi persona fisica o, se possibile ai sensi della Legislazione Applicabile in Materia di Protezione dei Dati, persona giuridica, che può essere identificata o identificabile, ciò mediante il il richiamo a qualsiasi elemento identificativo come il nome, il numero di identificazione, dati di localizzazione, un identificativo online o a uno o più elementi relativi all'identità fisica, psichica, fisiologica, genetica, economica, culturale o sociale di tale persona fisica, opinioni politiche, le sue comunicazioni private o confidenziali;

"**Legislazione Applicabile in Materia di Protezione dei Dati**" indica la Legislazione Locale in Materia di Protezione dei Dati applicabile al trattamento dei Dati di GP.

"Legislazione Europea" indica, collettivamente, il Regolamento, la Direttiva ePrivacy, tutti gli orientamenti, le raccomandazioni, i pareri, le decisioni vincolanti e altri documenti pubblici pertinenti dell'EDPB (il Comitato Europeo per la Protezione dei Dati), nonché la legislazione nazionale sulla protezione dei dati di qualsiasi Stato membro del SEE applicabile a una Parte;

"**Legislazione Locale in Materia di Protezione dei Dati**" indica, collettivamente, le leggi in materia di privacy/protezione dei dati applicabili alle Parti o applicabili nei confronti delle Parti da parte degli Interessati di GP, relativamente al trattamento dei dati di GP ai sensi del presente DPA. Per le Parti stabilite nell'Unione Europea, che offrono beni/servizi a Interessati di GP situati nell'Unione Europea, o che controllano il comportamento degli Interessati di GP all'interno

dell'Unione Europea, la Legislazione Locale in Materia di Protezione dei Dati include la Legislazione Europea;

"Meccanismo di Trasferimento" si intende una decisione vincolante emessa dalla Commissione Europea che permette il Trasferimento di dati personali dallo SEE verso un Paese terzo il cui l'ordinamento interno fornisca un adeguato livello di tutela in materia di protezione dei dati personali. In tale definizione si intendono ricomprese le Clausole Contrattuali Standard nonché le norme vincolanti di impresa (BCRs);

"**Misure tecniche e organizzative**" o "**TOM**" si riferisce alle misure descritte nell'Allegato II di questo DPA;

"**Parti**" indica, collettivamente, GP e il Responsabile. GP e il Responsabile possono essere indicati singolarmente come "**Parte**";

"**Periodo**" indica il periodo dalla Data di Entrata in Vigore fino alla cessazione del Trattamento dei Dati GP da parte del Fornitore ai sensi del DPA;

"Regolamento" indica il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

"**Responsabile del Trattamento**" o "**Responsabile**" indica qualsiasi persona fisica o giuridica, autorità pubblica, organismo o altro ente che elabora i Dati di GP per conto di un Titolare del trattamento.

"**SEE**" significa Spazio Economico Europeo;

"**Servizi del Responsabile**" indica, collettivamente, le attività assegnate da GP al Fornitore, comprese quelle sub-appaltate ai Sub-responsabili, come descritto negli Allegati I e III del presente DPA;

"**Soggetti Interessati di GP**" indica tutte le persone fisiche e giuridiche che rientrano nelle categorie elencate nell'allegato I del presente DPA. Ai fini del presente DPA, i Soggetti Interessati di GP sono considerati come Interessati;

"**Sub-responsabili**" indica i terzi autorizzati ed elencati nell'Allegato III del presente DPA a Trattare i Dati Personali di GP al fine di fornire parte dei Servizi del Responsabile e/o qualsiasi supporto tecnico correlato;

"**Trasferimento Transfrontaliero**" indica qualsiasi trasferimento di Dati GP da una Parte a un'altra Parte situata al di fuori della sua giurisdizione;

"**Titolare del Trattamento**" o "**Titolare**" indica qualsiasi Parte che determina le attività di Trattamento e le Misure di Sicurezza applicabili al Trattamento dei Dati Personali di GP;

"**Trattamento**" (così come "**Trattamenti**", "**Trattati**" e altre varianti) significa qualsiasi operazione o insieme di operazioni eseguite su Dati Personali o insiemi di Dati Personali, con o senza mezzi automatici, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione o altrimenti messa a disposizione, il raffronto o la combinazione, la restrizione, la cancellazione o la distruzione. Ai fini del presente DPA, i Trasferimenti Transfrontalieri sono considerati una forma di Trattamento;

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

1.2. Qualsiasi definizione specifica stabilita dalla Legislazione Locale in Materia di Protezione dei Dati sarà considerata equivalente alle definizioni di cui sopra, quando il loro significato è il medesimo.

1.3. I termini "includere" e "incluso" significano "incluso ma non limitato a". Tutti gli esempi nel DPA sono illustrativi e non sono gli unici esempi espressione di un particolare concetto.

1.4. Se questo DPA è tradotto in un'altra lingua e c'è una discrepanza tra il testo italiano e il testo tradotto, il testo italiano prevale.

2. Trattamento dei Dati Personali

2.1. Ruoli, responsabilità e istruzioni

2.1.1. Le Parti riconoscono e concordano che, per quanto riguarda il Trattamento dei Dati Personali relativi alle Parti e ai firmatari del presente DPA o ai loro rappresentanti/persone di contatto, ai fini della gestione del rapporto ai sensi del presente DPA, ciascuna Parte agirà in qualità di Titolare del Trattamento.

2.1.2. Per quanto riguarda il Trattamento dei Dati Personali di GP, le Parti riconoscono e convengono che: (a) GP agisce in qualità di Titolare del Trattamento o di Contitolare del Trattamento, come specificato nell'Allegato I del DPA; (b) il Fornitore agisce in qualità di Responsabile del Trattamento; (c) l'Allegato I del DPA descrive l'oggetto e i dettagli del Trattamento; (d) ciascuna Parte rispetterà gli obblighi ad essa applicabili ai sensi della Legislazione Applicabile in Materia di Protezione dei Dati relativamente ai Dati Personali di GP.

2.1.3. Le Parti riconoscono e accettano che la regolamentazione di tutte le attività di Trattamento dei Dati Personali di GP che non rientrano nell'ambito dei Servizi del Responsabile, o che sono ulteriormente determinate autonomamente da ogni singola Parte, sono escluse dall'ambito del presente DPA.

2.2. **Istruzioni di GP.** Con la sottoscrizione del presente DPA, GP incarica il Fornitore di Trattare i Dati Personali di GP: (a) solo in conformità con la Legislazione Applicabile in Materia di Protezione dei Dati; (b) solo per fornire i Servizi del Responsabile e qualsiasi supporto tecnico correlato; (c) come ulteriormente specificato/indicato da GP attraverso l'utilizzo dei Servizi del Responsabile (comprese le modifiche alle impostazioni e/o funzionalità dei Servizi del Responsabile) e qualsiasi supporto tecnico correlato; (d) come documentato nel Contratto, e nel presente DPA; e (e) come ulteriormente documentato in qualsiasi istruzione scritta, fornita da GP al Fornitore come ulteriore istruzione ai fini del presente DPA. Ad eccezione di quanto previsto alla Sezione 2.3, nel caso in cui il Fornitore violi quanto previsto dal presente articolo e/o comunque proceda a determinare le finalità e i mezzi del trattamento rispetto ai Dati Personali di GP, sarà considerato un autonomo Titolare del Trattamento.

2.3. **Rispetto delle istruzioni da parte del Fornitore**. Il Fornitore si atterrà alle istruzioni descritte nella Clausola 2.2 (istruzioni di GP), a meno che la Legislazione Locale in Materia di Protezione dei Dati a cui il Fornitore è soggetto non richieda al Fornitore di effettuare un diverso o ulteriore trattamento dei Dati Personali di GP, nel qual caso il Fornitore informerà prontamente GP all'Indirizzo E-mail di Notifica prima che il Trattamento abbia inizio o immediatamente appena possibile. A meno che tale Legislazione non vieti al Fornitore di farlo per inderogabili motivi di interesse pubblico, le ragioni di un diverso o ulteriore Trattamento dei Dati Personali di GP saranno documentate come Documentazione di Sicurezza.

3. Cancellazione ed esportazione dei Dati di GP

3.1. Cancellazione ed esportazione per il Periodo

3.1.1. **Servizi del Responsabile con funzionalità di esportazione**. Qualora i Servizi del Responsabile includano la possibilità per GP di esportare i Dati Personali di GP autonomamente ed in formato interoperabile, il Fornitore assicurerà che tale operazione sia garantita per l'intero Periodo e fino a 90 giorni successivi allo stesso.

3.1.2. **Servizi di elaborazione con funzionalità di cancellazione**. Se i Servizi del Responsabile includono la possibilità per GP di cancellare autonomamente i Dati Personali di GP, il Fornitore garantirà che tale cancellazione dai propri sistemi sia effettuata non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la Legislazione Locale in Materia di Protezione dei Dati cui il Fornitore è soggetto non richieda la conservazione. In quest'ultimo caso, il Fornitore tratterà i Dati Personali di GP solo per le finalità e il periodo definiti da tale Legislazione. Tale ulteriore trattamento dei Dati Personali di GP sarà documentato come Documentazione di Sicurezza.

3.1.3. **Servizi del Responsabile senza funzionalità di cancellazione o estrazione**. Durante il Periodo, qualora i Servizi del Responsabile non includano la possibilità di estrarre e/o cancellare autonomamente i Dati Personali di GP, il Fornitore si conformerà a qualsiasi richiesta di GP di facilitare tale operazione con le stesse modalità e tempistiche indicate nella Clausola 3.1.1 (Servizi del Responsabile con funzionalità di esportazione) e nella Clausola 3.1.2 (Servizi del Responsabile con funzionalità di cancellazione).

3.2 Cancellazione alla scadenza del Periodo. Fatte salve le disposizioni della Clausola 3.1.1 (Servizi del Responsabile con funzionalità di esportazione), alla scadenza del Periodo, GP ordina al Fornitore di cancellare tutti i Dati Personali di GP (comprese le copie esistenti) dai sistemi del Fornitore in conformità con la Legislazione Applicabile in Materia di Protezione dei Dati. Il Fornitore eseguirà questa istruzione non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, dandone conferma all'Indirizzo E-mail di Notifica, a meno che la Legislazione Locale in Materia di Protezione Dei Dati a cui il Fornitore è soggetto non richieda la conservazione. In quest'ultimo caso, il Fornitore tratterà i Dati Personali di GP solo per le finalità e il Periodo definiti da tale Legislazione. Tale ulteriore trattamento dei Dati Personali di GP sarà documentato come Documentazione di Sicurezza.

4. Sicurezza dei Dati Personali

4.1 TOM e assistenza da parte del Fornitore

4.1.1. **TOM sui sistemi del Fornitore**. Il Fornitore adotterà e manterrà misure tecniche e organizzative per proteggere i Dati Personali di GP da distruzione, perdita, alterazione, divulgazione o accesso accidentali o illegali, come descritto nell'Allegato II del presente DPA. Tenendo conto dello stato dell'arte e dei costi di implementazione, nonché della natura, della portata, del contesto e della finalità del Trattamento effettuato tramite i Servizi del Responsabile, nonché del rischio di probabilità e gravità per i diritti e le libertà dei Soggetti Interessati; in ogni caso l'Allegato II includerà sempre misure di sicurezza (a) per criptare i Dati Personali di GP; (b) per contribuire a garantire la costante riservatezza, integrità, disponibilità e resilienza dei sistemi e dei Servizi del Fornitore; (c) per contribuire al ripristino tempestivo dei Dati Personali di GP a seguito di un Incidente; e (d) per verificarne periodicamente l'efficacia. Il Fornitore ha il diritto di aggiornare o modificare i TOM di volta in volta, a condizione che tali aggiornamenti e modifiche non comportino un peggioramento della sicurezza complessiva dei Servizi del Responsabile. Ogni modifica dovrà essere condivisa con GP tramite l'Indirizzo E-mail di Notifica ed espressamente acconsentita da quest'ultima.

4.1.2. **Misure di sicurezza per il personale del Fornitore.** Il Fornitore adotterà misure appropriate per garantire il rispetto dei TOM da parte di tutti coloro che operano sotto la sua autorità, compresi i suoi dipendenti, agenti, appaltatori e subappaltatori, nella misura applicabile al loro ambito di pertinenza, assicurando anche che tutte le persone autorizzate a trattare i Dati Personali di GP si siano impegnate alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza in conformità alla Legislazione Applicabile in Materia di Protezione dei Dati.

4.1.3. **Assistenza del Fornitore in materia di sicurezza.** Il Fornitore assisterà GP nell'assicurare il rispetto di tutti gli obblighi di GP in materia di sicurezza dei Dati Personali e dagli Incidenti di GP, inclusi (se applicabili) gli obblighi di GP ai sensi della Legislazione Applicabile sulla Protezione dei Dati, attraverso: (a) l'implementazione e la manutenzione dei TOM in conformità alla clausola 4.1.1. (TOM sui sistemi del Fornitore); (b) l'attuazione delle disposizioni della Clausola 4.2 (Incidenti); e (c) la fornitura a GP della Documentazione di Sicurezza in conformità alla Clausola 4.5.1 (Revisione della Documentazione di Sicurezza) e le informazioni previste nel presente DPA.

4.2. Incidenti

4.2.1. **Diligenza professionale.** Il Fornitore adotta la diligenza professionale nel controllare la sicurezza dei Dati Personali di GP Trattati nella fornitura dei Servizi del Responsabile.

4.2.2. **Notifica dell'Incidente.** Se il Fornitore viene a conoscenza di un Incidente, il Fornitore dovrà (a) informare GP tempestivamente e in ogni caso entro 24 ore; e (b) adottare misure ragionevoli per ridurre al minimo il danno e mettere al sicuro i Dati Personali di GP in modo tempestivo (c) collaborare con GP al fine di indagare sulle cause e sulla gravità dell'Incidente.

4.2.3. **Dettagli dell'Incidente**. Le notifiche effettuate ai sensi della clausola 4.2.2 (Notifica dell'Incidente) descriveranno nel modo più accurato possibile (anche tramite notifiche supplementari) i dettagli dell'Incidente, comprese le categorie e il numero approssimativo di Soggetti Interessati di GP coinvolti e il numero dei Dati Personali dei Soggetti Interessati coinvolti, i rischi potenziali per i Soggetti Interessati e le misure che il Fornitore ha adottato o raccomanda a GP di adottare per affrontare l'Incidente e mitigarne gli effetti.

4.2.4. **Comunicazione della notifica dell'Incidente**. Il Fornitore invierà comunicazione di qualsiasi Incidente all'Indirizzo E-Mail di Notifica pertinente e, se richiesto da GP, mediante altre comunicazioni dirette (ad esempio, mediante chiamata telefonica o incontro faccia a faccia).

4.2.5. **Valore della notifica**. La notifica del Fornitore di un Incidente ai sensi della presente Clausola 4.2 (Incidenti) sarà costruita come una dichiarazione proveniente da chi ha l'autorità di rappresentare il Fornitore nei confronti di GP rispetto all'Incidente.

4.3. Responsabilità e valutazione della sicurezza di GP

4.3.1. **Responsabilità di GP in materia di sicurezza**. Fatti salvi gli obblighi del Fornitore ai sensi delle clausole 4.1 (TOM e assistenza da parte del Fornitore) e 4.2 (Incidenti), GP accetta di essere l'unica responsabile dell'utilizzo dei Servizi del Responsabile, compresa la protezione delle credenziali di autenticazione, dei sistemi e dei dispositivi da essa utilizzati per accedere ai Servizi del Responsabile.

4.3.2. **Valutazione della sicurezza di GP**. Il Fornitore riconosce e concorda che GP ha il diritto di richiedere un aggiornamento delle misure di sicurezza attuate e mantenute dal Fornitore come indicato nella Clausola 4.1.1. (TOM sui sistemi del Fornitore) qualora - per la natura, portata, contesto e finalità del Trattamento o per le evidenze emerse a seguito di controlli e audit - esse non forniscano un livello di sicurezza adeguato al rischio derivante dal Trattamento dei Dati Personali di GP.

4.4. **Certificazione di sicurezza**. Per valutare e contribuire a garantire la continua efficacia dei TOM, il Fornitore può, a sua esclusiva discrezione, integrare i TOM e la Documentazione di Sicurezza implementando certificazioni (ad esempio, ISO27001), codici di condotta e/o meccanismi di certificazione.

4.5. Controlli e audit

4.5.1. **Revisione della Documentazione di Sicurezza**. Al fine di dimostrare il rispetto da parte del Fornitore dei suoi obblighi ai sensi del presente DPA, il Fornitore renderà la Documentazione di Sicurezza disponibile a GP per sua valutazione.

4.5.2. **Diritti di audit di GP**. Le Parti convengono che: (a) il Fornitore consentirà a GP, o a un revisore terzo nominato da GP, di effettuare audit (comprese le ispezioni) per verificare il rispetto da parte del Fornitore degli obblighi derivanti dal presente DPA in conformità alla Clausola 4.5.3 (Condizioni aggiuntive per gli audit) e agli standard internazionali ISO19011. Il Fornitore contribuirà a tali audit in conformità con la presente Clausola 4.5 (Controlli e Audit); (b) GP può anche condurre un audit per verificare l'osservanza da parte del

Fornitore dei suoi obblighi ai sensi del presente DPA esaminando i certificati emessi ai sensi della Clausola 4.4 (Certificazione di sicurezza), a condizione che essi riflettano il risultato di un audit condotto da un revisore terzo.

4.5.3. **Condizioni aggiuntive per gli audit.** Per quanto riguarda l'audit, le Parti concordano che:

(a) GP invierà al Fornitore qualsiasi richiesta di audit in conformità alla Clausola 4.5.2(a) come descritto nella Clausola 9.1 (Contatti del Fornitore);

(b) al ricevimento da parte del Fornitore di una richiesta ai sensi della clausola 4.5.3(a), GP e il Fornitore si impegnano a discutere e concordare in anticipo la data di inizio, l'ambito e la durata, i controlli di sicurezza e riservatezza applicabili a qualsiasi verifica ai sensi della clausola 4.5.2(a);

(c) il Fornitore può addebitare una commissione (basata su costi ragionevoli) per qualsiasi audit di cui alla Clausola 4.5.2(a) nel caso in cui sia già stato garantito l'esercizio del diritto di audit senza alcun costo per GP nell'arco dei 12 mesi precedenti alla nuova richiesta; oltre ad un audit annuale, resta altresì fermo il diritto di GP (e/o di terze parti da essa incaricate) a svolgere senza alcun costo eventuali audit in caso di Incidenti e/o violazioni da parte del Fornitore degli obblighi di cui al presente DPA. Al di fuori di queste ipotesi, il Fornitore fornirà in anticipo a GP i dettagli di ogni costo applicabile e la base di calcolo. GP sarà responsabile di eventuali commissioni addebitate da terzi incaricati da GP di effettuare tali audit;

(d) il Fornitore può opporsi a qualsiasi revisore terzo nominato da GP per effettuare le verifiche ai sensi della clausola 4.5.2(a) se fornisce prove scritte che: (i) il revisore terzo non è adeguatamente qualificato o indipendente; (ii) il revisore terzo è un concorrente del Fornitore. Qualsiasi obiezione dimostrata o dimostrabile di questo tipo da parte del Fornitore imporrà a GP di nominare un altro revisore o di condurre direttamente l'audit;

(e) nessuna disposizione del presente DPA imporrà al Fornitore di rivelare o concedere l'accesso a GP o al revisore terzo a:

(i) qualsiasi dato di qualsiasi altro cliente del Fornitore, a meno che non si tratti di Dati Personali di GP;

(ii) qualsiasi informazione contabile o finanziaria interna del Fornitore;

(iii) qualsiasi segreto commerciale e know-how del Fornitore;

(iv) qualsiasi informazione che potrebbe compromettere la sicurezza dei sistemi o dei locali del Fornitore; o far sì che il Fornitore violi i suoi obblighi ai sensi della Legislazione Applicabile sulla Protezione dei Dati o i suoi obblighi di sicurezza nei confronti di GP o di terzi; o

(v) qualsiasi informazione a cui GP o il revisore terzo cerchino di accedere per ragioni diverse dall'adempimento in buona fede degli obblighi di GP ai sensi della Legislazione Applicabile in Materia di Protezione dei Dati;

(f) l'esecuzione degli audit è soggetta a un accordo specifico di riservatezza tra tutte le Parti coinvolte e/o uno specifico accordo che contenga ulteriori legittime istruzioni da parte di GP.

5. Valutazioni d'impatto sulla protezione dei dati e consultazione preventiva

5.1. Il Fornitore si impegna (tenendo conto della natura del Trattamento e delle informazioni a disposizione del Fornitore) ad assistere GP nel garantire il rispetto di qualsiasi obbligo di GP in materia di valutazioni d'impatto sulla protezione dei dati e di consultazione preventiva, se così richiesto dalla Legislazione Applicabile in Materia di Protezione dei Dati, mediante: (a) la condivisione della Documentazione di Sicurezza in conformità alla Clausola 4.5.1 (Revisione della Documentazione di Sicurezza); (b) la condivisione delle informazioni contenute nel presente DPA; e (c) l'invio o la messa a disposizione di altri materiali relativi ai Servizi del Responsabile e/o relativi al Trattamento dei Dati Personali di GP (ad esempio, materiali di supporto).

6. Diritti degli Interessati

6.1. **Risposte alle richieste dei Soggetti Interessati di GP**. Qualora il Fornitore riceva una richiesta da parte di un Soggetto Interessato in relazione ai Dati Personali di GP, il Fornitore risponderà prontamente e in ogni caso entro 3 giorni dalla richiesta invitandolo a presentare la sua richiesta all'Indirizzo E-mail di Notifica pertinente, in modo che GP possa fornire una risposta alla richiesta del Soggetto Interessato.

6.2. **Assistenza del Fornitore in materia di esercizio dei diritti degli Interessati**. Il Fornitore si impegna (tenendo conto della natura del Trattamento dei Dati Personali di GP) ad assistere GP nell'adempimento di qualsiasi obbligo delle medesime in relazione ai Diritti degli Interessati, mediante: (a) se applicabile, la fornitura di specifiche funzionalità nei Servizi del Responsabile; (b) il rispetto degli impegni di cui alla Clausola 6.1 (Risposte alle richieste degli Interessati di GP).

7. Sub-responsabili

7.1. **Autorizzazione all'impiego di Sub-responsabili**. GP conferisce un'autorizzazione generale per l'impiego di Sub-responsabili per la fornitura dei Servizi del Responsabile.

7.2. **Informazioni sui Sub-responsabili**. Il Fornitore si impegna a compilare l'elenco e le rispettive informazioni sui Sub-responsabilii nell'Allegato III del presente DPA.

7.3. **Requisiti per l'impiego dei Sub-responsabili**. Nell'impiego di un Sub-responsabile, il Fornitore garantirà che:

(i) il Sub-responsabile può accedere e utilizzare i Dati Personali di GP solo nella misura strettamente necessaria all'esecuzione degli obblighi che gli sono stati conferiti in conformità al Contratto e al DPA, e – ove applicabile - con i Meccanismi di Trasferimento;

(ii) al Sub-responsabile si applicheranno gli stessi obblighi previsti per il Responsabile dal presente DPA nonché dall'articolo 28(3) del Regolamento;

(iii) GP può, a propria discrezione, subentrare nella posizione contrattuale del Fornitore con il Sub-responsabile se il primo è effettivamente venuto meno, ha cessato legalmente di esistere o è diventato insolvente, e nessun altro soggetto giuridico ha assunto, per contratto o per legge, tutti gli obblighi del Fornitore (cosiddetta clausola del terzo beneficiario);

(iv) il Fornitore rimane pienamente responsabile per tutti gli obblighi subappaltati nonché per tutti gli atti e le omissioni del Sub-responsabile.

7.4. **Possibilità di opporsi alle modifiche dei Sub-responsabili**. Le Parti concordano che:

(a) durante il Periodo, il Fornitore comunicherà all'Indirizzo E-mail di Notifica la sua intenzione di assumere nuovi (o rimuovere) Sub-responsabili per il Trattamento dei Dati Personali di GP almeno 30 giorni prima dell'inizio del subappalto. Tale comunicazione includerà tutte le informazioni richieste nell'Allegato III del presente DPA;

(b) GP potrà opporsi all'impiego di uno qualsiasi dei nuovi Sub-responsabili: i) richiedendo di non impiegare i nuovi Sub-responsabili che non siano stati ritenuti idonei al Trattamento dei Dati Personali di GP entro 30 giorni dalla comunicazione del Fornitore rispetto ai nuovi Sub-responsabili; ii) risolvendo il Contratto previa comunicazione scritta al Fornitore, a condizione che GP effettui tale comunicazione entro 30 giorni dalla comunicazione dell'ingaggio dei nuovi Sub-responsabili come descritto nella Clausola 7.4(a);

(c) se GP non si è opposta come indicato nella clausola 7.4(b), il Fornitore accetta di inviare all'Indirizzo E-mail di Notifica l'allegato III del presente DPA aggiornato il quale sarà considerato parte integrante di questo DPA.

8. **Esclusione di Trasferimenti Transfrontalieri**

8.1. Le Parti riconoscono e accettano che non sono autorizzati né saranno effettuati Trasferimenti Transfrontalieri per svolgere i Servizi del Responsabile, neanche tramite l'impiego di Sub-responsabili.

9. **Dettagli dei contatti delle Parti e Registri del Trattamento**

9.1. **Dettagli dei contatti del Fornitore**. Le Parti accettano di utilizzare l'Indirizzo E-mail di Notifica in relazione a tutto quanto contenuto nel presente DPA. Nel caso in cui l'Indirizzo E-mail di Notifica non sia funzionante, le Parti sono autorizzate ad utilizzare, in successione alternativa, gli indirizzi e-mail/di posta elettronica certificata: a) del Data Protection Officer del Fornitore (se nominato); b) l'indirizzo e-mail indicato dal Fornitore nell'Accordo; c) qualsiasi altro indirizzo e-mail utilizzato dal Fornitore durante la fornitura dei Servizi del Responsabile per ricevere determinate notifiche in relazione al DPA.

9.2. **Registri del Trattamento.** Il Fornitore prende atto che, ai sensi del Regolamento, GP è tenuta a: (a) raccogliere e conservare determinate informazioni, tra cui il nome e i dati di contatto di ciascun Responsabile del Trattamento e Sub-responsabile coinvolto nel Trattamento dei Dati di GP e (se nominato) del delegato e del DPO; e (b) rendere tali informazioni disponibili a qualsiasi Autorità di Controllo. Di conseguenza, il Fornitore fornirà tali informazioni a GP attraverso l'Indirizzo E-mail di Notifica come da Documentazione di Sicurezza e si impegna a garantire che tutte le informazioni fornite siano sempre accurate e aggiornate.

10. **Conflitti**

10.1. **Conflitti tra gli accordi delle Parti**. In caso di conflitto o incoerenza tra le disposizioni del Contratto e del DPA, si applicherà il seguente ordine di prevalenza: (a) le disposizioni del DPA; e (b) le restanti disposizioni del Contratto. Fatti salvi eventuali emendamenti al DPA, il Contratto rimane pienamente valido ed efficace.

10.2. **Violazioni di leggi o regolamenti**. Qualsiasi disposizione del DPA che sia contraria alla Legislazione Applicabile in Materia di Protezione dei Dati sarà considerata come non riprodotta nel presente documento e sarà sostituita nella sua interezza dalla disposizione che è stata violata se non può essere derogata da un accordo tra le Parti.

11. **Modifiche**

11.1. **Modifiche agli Allegati**. Di tanto in tanto, il Fornitore può modificare il contenuto degli Allegati se espressamente consentito dal DPA. Il Fornitore può modificare l'elenco dei Servizi del Responsabile nell'Allegato I solo: a) per riflettere un cambiamento nel nome di un servizio; b) per aggiungere un nuovo servizio; o c) per eliminare un servizio se: (i) tutti i contratti per la fornitura di tale servizio siano terminati; o (ii) il Fornitore abbia ricevuto il consenso da GP.

11.2. **Modifiche al DPA**. GP può modificare il DPA se la modifica: (a) è espressamente consentita dalla Legislazione Applicabile in Materia di Protezione dei Dati; (b) è obbligatoria per conformarsi alla Legislazione Applicabile in Materia di Protezione dei Dati, a una sentenza o altra ordinanza di un tribunale o alle linee guida emesse da un'Autorità di Controllo o da un'autorità governativa.

11.3. **Notifica delle modifiche**. Salvo il caso indicato alla clausola 11.2(b) in cui la modifica è immediatamente efficace tra le Parti, se GP intende modificare il presente DPA ai sensi della clausola 11.2, GP informerà il Fornitore almeno 30 giorni prima che la modifica diventi efficace, inviando una e-mail all'indirizzo indicato nella clausola 9.1. Se il Fornitore si oppone a tali modifiche, potrà recedere dal Contratto dandone comunicazione scritta a GP entro 30 giorni dalla comunicazione della modifica da parte di GP; se il Fornitore non esercita il diritto di recesso entro il suddetto termine, la modifica è vincolante tra le Parti a tutti gli effetti legali e contrattuali.

12. **Obbligo di riferire e cooperare**

12.1. Le Parti, nell'ambito del Trattamento dei Dati Personali di GP che effettuano ai sensi del presente DPA, coopereranno in buona fede per garantire il rispetto degli obblighi assunti ai sensi del presente DPA. In particolare, ciascuna Parte condividerà la documentazione di conformità con l'altra Parte su richiesta.

12.2. Qualsiasi Parte che riceva una richiesta di chiarimento o di ispezione da parte di un'Autorità di Controllo in merito al Trattamento dei Dati Personali di GP ai sensi del presente DPA riferirà tale richiesta senza indebito ritardo alle altre Parti interessate, offrendo supporto su richieste semplici nella misura in cui la Parte sia coinvolta.

12.3. Il DPA è da intendersi come Documentazione di Sicurezza da mostrare all'Autorità di Controllo e agli Interessati di GP, se richiesto dalla Legislazione sulla Protezione dei Dati Personali.

13. Risoluzione dell'Accordo

13.1. **Clausola risolutiva espressa**. Ferme restando le disposizioni contenute nel Contratto e ad integrazione delle stesse, le Parti convengono che GP potrà risolvere il Contratto per uno o più dei Servizi del Responsabile secondo le modalità indicate nello stesso al semplice verificarsi di uno di tali eventi:

(a) una violazione degli obblighi contenuti nella Clausola 2.3 (Conformità del Fornitore alle istruzioni); 3.1 (Cancellazione ed esportazione per il Periodo); 4.1.3 (Assistenza alla sicurezza del Fornitore); 4.2.2 (Notifica degli Incidenti); 4.5.2 (Diritti di audit di GP; 5 (Valutazioni di impatto sulla protezione dei dati e consultazione preventiva); 6 (Diritti degli Interessati); 7.3 (Requisiti di impegno dei Sub-responsabili); 8 (Esclusione di Trasferimenti Transfrontalieri);

(b) la cooperazione tra le Parti è diventata impossibile:

(i) a causa di sanzioni o rischio di sanzioni, anche amministrative, emesse dall'Autorità di Controllo o da altri organi giudiziari nei confronti del Fornitore, che minerebbero la fiducia di GP in relazione all'affidabilità e professionalità del Fornitore nel Trattamento dei Dati Personali di GP;

(ii) a causa di Incidenti del Fornitore relativi ai Servizi del Responsabile.

13.2. **Prestazione residua del Fornitore.** La risoluzione del Contratto ai sensi della clausola 13.1 non pregiudica gli obblighi ai sensi della clausola 3.2. (Cancellazione alla scadenza del Periodo).

13.3. **Non acquiescenza**. La mancata applicazione della clausola 13, dei diritti derivanti dalla Legislazione Applicabile in Materia di Protezione dei Dati, del Contratto o del DPA non impedisce a GP di avvalersene successivamente per proteggere i loro diritti e interessi legittimi.

14. Responsabilità e risarcimento

14.1. **Perimetro del danno**. Le Parti riconoscono e accettano che qualora un Soggetto Interessato di GP lamenti ("**Reclamante**"), nei confronti delle Parti, di aver subito un danno - materiale o immateriale - causato da una violazione del Regolamento:

(a) il Fornitore, ai sensi dell'art. 82(2) del Regolamento, sarà pienamente responsabile dei danni materiali o immateriali causati all'Interessato di GP, dichiarando sin d'ora di manlevare e tenere indenne GP, qualora non abbia rispettato gli obblighi del Regolamento specificamente rivolti ai Responsabili del Trattamento, o qualora abbia agito in modo difforme o contrario alle istruzioni di GP fornite attraverso il presente DPA;

(b) nel caso in cui il Fornitore e GP siano coinvolti nello stesso Trattamento e siano entrambi responsabili del danno causato al Reclamante, ai sensi dei commi 2 e 3 dell'Art. 82 del Regolamento, ciascuno dei due sarà responsabile in solido per l'intero ammontare del danno, fermo restando, per entrambi, il diritto di rivalsa nei confronti dell'altro per la quota di risarcimento spettante al medesimo soggetto in base al danno causato;
(c) se il danno causato al Reclamante è dovuto alla violazione delle disposizioni del presente DPA o della Legislazione Europea e Nazionale ed è interamente imputabile al Fornitore, il Fornitore è tenuto a risarcire integralmente GP se quest'ultima ha provveduto a risarcire il Reclamante in tutto o in parte;
(d) ogni Parte indennizzerà o risarcirà l'altra Parte se e nella misura in cui ha contribuito al danno reclamato dal Reclamante o non ha adottato misure di mitigazione adeguate, o ha violato le disposizioni del presente DPA o della Legislazione Europea e Nazionale.

15. Allegati

15.1 I seguenti allegati sono parte integrante del DPA:

- Allegato I - Parti e descrizione del Trattamento
- Allegato II - TOM (rinvenibile anche online sul sito di GP)
- Allegato III - Elenco dei Sub-responsabili.

Ultimo aggiornamento 13 gennaio 2023

Allegato II: TOM

L'Allegato relativo alle misure di sicurezza ("TOMs") può essere consultato anche online sul sito https://giochipreziosi.it/

A partire dalla Data di Entrata in Vigore, il Fornitore implementa e mantiene le Misure di Sicurezza di cui al presente Allegato II. Periodicamente, il Fornitore può aggiornare o modificare tali Misure di Sicurezza, a condizione che tali aggiornamenti e modifiche non comportino il deterioramento della sicurezza complessiva dei Servizi del Responsabile o comunque una diminuzione del livello di sicurezza concordato di seguito. Ogni modifica va comunicata al Titolare come indicato nel DPA.

Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile ed i Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

Informazioni sulle misure di sicurezza

Gestione della sicurezza delle informazioni

La Direzione definisce una serie di politiche e misure per chiarire gli obiettivi al fine di supportare la sicurezza delle informazioni. A livello apicale, è prevista una "Policy per la sicurezza delle informazioni" di carattere generale, come specificato nella sezione 5.2 della ISO/IEC27001.

Organizzazione della sicurezza delle informazioni

Organizzazione interna

L'organizzazione definisce i ruoli e le responsabilità per la sicurezza delle informazioni e assegnarli singolarmente a soggetti determinati. Ove necessario, i compiti sono separati per ruoli e persone al fine di evitare conflitti di interesse e prevenire attività inappropriate.

Dispositivi mobili e telelavoro

È prevista una Policy di sicurezza e adeguati controlli per i dispositivi mobili (come laptop, tablet, PC, dispositivi indossabili, smartphone, strumenti USB e altri) e per il telelavoro (come coloro che lavorano da casa, quelli che viaggiano assiduamente e le postazioni di lavoro da remoto/virtuali).

Sicurezza delle risorse umane

Prima dell'instaurazione del rapporto di lavoro

Le responsabilità della sicurezza delle informazioni sono prese in considerazione durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e inserite all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

Durante il rapporto di lavoro

I manager si assicurano che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni. È necessario formalizzare un procedimento disciplinare per gestire gli incidenti relativi alla sicurezza delle informazioni presumibilmente causati dai lavoratori.

Conclusione o modifiche al rapporto di lavoro

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

Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale

Tutte le informazioni relative alle risorse del patrimonio aziendale sono inventariate ed i relativi soggetti di riferimento identificati al fine di individuare le responsabilità per la loro sicurezza. È necessario definire una Policy per un "uso corretto" delle stesse e le risorse dovranno rientrare all'interno dell'organizzazione al momento dell'uscita dei soggetti coinvolti.

Classificazione delle informazioni

Le informazioni sono classificate e catalogate dai rispettivi soggetti di riferimento in linea con quanto previsto dalle esigenze di sicurezza, nonché trattate in modo appropriato.

Gestione dei media

Le informazioni conservate sui media sono gestite, controllate, modificate ed utilizzate in modo tale da non comprometterne il loro contenuto.

Controllo degli accessi

Requisiti aziendali per il controllo degli accessi

I requisiti previsti dall'organizzazione per controllare l'accesso alle informazioni relative al patrimonio aziendale sono chiaramente documentati in una Policy per il controllo degli accessi e delle relative procedure. L'accesso alla rete e le connessioni prevedono delle limitazioni.

Gestione dell'accesso degli utenti

L'allocazione dei diritti d'accesso da parte degli utenti è controllata dalla registrazione iniziale dell'utente fino alla rimozione del profilo quando esso non sia più necessario, incluse speciali restrizioni per i diritti di accesso privilegiato e la gestione delle password (definita come "informazione di autenticazione segreta"); peraltro, si procede regolarmente alla revisione e all'aggiornamento dei diritti di accesso.

Responsabilità degli utenti

Gli utenti sono res consapevoli delle loro responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad es. scegliendo password complesse e mantenendole riservate.

Sistemi e applicazioni per il controllo degli accessi

L'accesso alle informazioni è limitato coerentemente a quanto previsto dalla Policy sul controllo degli accessi, ad es. attraverso autenticazioni sicure, gestione delle password, controllo delle utilità privilegiate e limitazioni all'accesso ai codici sorgente dei programmi.

Crittografia

Controllo crittografico

È prevista una Policy sull'uso della cifratura dei dati, oltre ad autenticazioni criptate e controlli di integrità, come firme digitali e messaggi con codici di autenticazione, nonché una gestione delle chiavi di cifratura.

Sicurezza fisica e ambientale

Aree sicure

La definizione di un perimetro fisico e di una recinzione, con controllo fisico degli accessi e procedure operative, sarebbe in grado di proteggere i locali, gli uffici, le stanze, le aree di carico/scarico da accessi non autorizzati. Inoltre, si prevede la consulenza di uno specialista per quanto riguarda le misure di protezione contro incendi, allagamenti, terremoti, esplosioni, ecc.

Apparecchiatura

L'apparecchiatura (intesa perlopiù come apparecchiatura in ambito ICT), i servizi di supporto e il cablaggio sono resi sicuri e

manutenuti. L'apparecchiatura e le informazioni non escono dal loro luogo di riferimento se non previa autorizzazione, e in ogni caso sono adeguatamente protette sia all'interno che all'esterno del loro luogo di riferimento. Le informazioni sono distrutte prima di procedere allo smaltimento o al riciclo dei dispositivi sui cui erano conservate. Le apparecchiature non protette sono rese sicure ed è previsto un apposito spazio ed una chiara Policy di verifica.

Sicurezza delle operazioni

Procedure e responsabilità operative

Le procedure e le responsabilità operanti per l'area IT sono documentate. I cambiamenti alle infrastrutture ed ai sistemi IT controllati. Sono gestiti i singoli poteri e le relative prestazioni. I sistemi di sviluppo, quelli di verifica e quelli operativi sono separati.

Protezione da malware

È richiesto il controllo dei malware, comprensivo di un'idonea consapevolezza sul punto da parte degli utenti.

Backup

Idonei backup sono eseguiti e custoditi coerentemente ad una Policy per i backup.

Autenticazione e monitoraggio

Le attività, le eccezioni, gli errori e gli eventi relativi alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avvengono previo inserimento delle credenziali di autenticazione e adeguatamente protette. Gli orologi sono sincronizzati.

Controllo di software operativi

L'installazione di software sui sistemi operativi è controllata.

Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche sono corrette con idonee patch, e sono previste regole per l'installazione dei software da parte degli utenti.

Considerazioni sull'audit per le informazioni di sistema

L'audit per l'area IT è programmato e controllato per minimizzare l'effetto avverso sui sistemi di produzione o l'accesso abusivo ai dati.

Sicurezza delle comunicazioni

Gestione della sicurezza della rete

Le reti e i servizi in rete sono resi sicuri, ad esempio attraverso la loro separazione.

Trasferimento delle informazioni

Sono previste policy, procedure ed accordi (ad es. accordi di riservatezza) relativi al trasferimento delle informazioni verso/da terze parti, compresi i messaggi elettronici.

Acquisizione, sviluppo e manutenzione del sistema

Requisiti di sicurezza dei sistemi di informazione

I requisiti per il controllo di sicurezza sono analizzati e specificati, comprese le applicazioni web e le transazioni.

Sicurezza nello sviluppo e processi di supporto

Le regole che governano la sicurezza dello sviluppo dei software/sistemi sono definite in una Policy. Le modifiche al sistema (sia per le applicazioni che per i sistemi operativi) sono controllate. I pacchetti software teoricamente non sono modificati, e sono osservati i principi di sicurezza ingegneristica. È necessario rendere sicuro l'ambiente di sviluppo e controllare lo sviluppo esternalizzato. La sicurezza del sistema è testata e sono definiti criteri di ammissibilità che includano gli aspetti di sicurezza.

Test di verifica dei dati

I test di verifica dei dati sono accuratamente selezionati/generati e controllati.

Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori

Sono previste policy, procedure, sistemi di consapevolezza volti a proteggere le informazioni dell'organizzazione che siano accessibili ai soggetti esterni operanti nell'area IT e ad altri fornitori esterni per l'intera catena di fornitura, concordata nei contratti o negli accordi.

Gestione dei servizi resi dal fornitore

L'erogazione dei servizi resi dal fornitore è monitorata e rivista/verificata in relazione al contratto/accordo. Le modifiche al servizio sono controllate.

Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti alla sicurezza delle informazioni e miglioramenti

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

Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Continuità della sicurezza delle informazioni

La continuità della sicurezza delle informazioni è pianificata, implementata e revisionata come parte integrante del sistema organizzativo di continuità aziendale.

Ridondanze

Le strutture IT sono sufficientemente ridondanti per soddisfare i requisiti di disponibilità.

Conformità

Conformità ai requisiti legali e contrattuali

L'organizzazione identifica e documenta i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.

Revisione della sicurezza delle informazioni

I progetti dell'organizzazione relativamente alla sicurezza delle informazioni sono revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. I manager inoltre revisionano periodicamente la conformità dei dipendenti e dei sistemi alle policy di sicurezza, alle procedure, ecc., e promuovono azioni correttive ove necessario.

Ultimo aggiornamento: 13 gennaio 2023