ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI

(ex art. 28 del Regolamento UE 2016/679)

TRA

HDI Assicurazioni S.p.A., con sede legale in Roma, Via Abruzzi, 10, capitale sociale € 96.000.000,00 I.V., Società con unico azionista, C.F. e P. IVA 04349061004, iscritta al numero 7122/92 del Registro delle Imprese di Roma ed al numero 757172 del R.E.A. di Roma, autorizzata all'esercizio dell'attività assicurativa con D.M.I.C.A. n. 19570 dell'8.6.1993 (G.U. 14.06.1993) iscritta alla sezione I dell'Albo delle Imprese Assicurative al n. 1.00022, Capogruppo del Gruppo Assicurativo "HDI Assicurazioni" iscritto all'Albo dei Gruppi Assicurativi al n. 015, in persona del Dr. Tommaso Di Gennaro nella qualità di Vice Direttore Generale della suddetta società, a quanto infra debitamente autorizzato, di seguito denominata "**HDI**"

E

C. & G. Partner di Gudas Anastasio & C. Sas Agente Generale sulla piazza di Firenze (FI) - Cod. 49 - Part. IVA/Cod. Fisc. 4956460481, in persona del legale rappresentante (di seguito il "**Responsabile**"),

(di seguito, congiuntamente, le "**Parti**")

PREMESSO CHE

a) è in vigore tra le Parti un contratto di agenzia (di seguito il "**Contratto**") ;

b) In virtù del Contratto, il Responsabile esegue operazioni di trattamento strettamente necessarie per la prestazione delle attività previste dal Contratto, aventi ad oggetto le seguenti categorie di dati personali (di seguito, "**Dati Personali**") di titolarità di HDI, fermo restando che il Responsabile è autorizzato a trattare soltanto i dati strettamente pertinenti ai singoli prodotti assicurativi di volta in volta intermediati:

   - Dati identificativi, anagrafici, relativi allo stato civile, professionali o relativi all'istruzione, bancari/finanziari o reddituali, dati di contatto dei contraenti, beneficiari, soggetti interessati dai servizi assicurativi del Titolare;
   - Dati relativi allo stato di salute dei contraenti, beneficiari, soggetti interessati dai servizi assicurativi del Titolare;
   - Dati giudiziari dei contraenti, beneficiari, soggetti interessati dai servizi assicurativi del Titolare;
   - Dati relativi alla geolocalizzazione, ove previsto dai prodotti assicurativi intermediati.

c) il Responsabile dichiara e garantisce di possedere competenza e conoscenze tecniche in relazione alle finalità e modalità di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei Dati Personali trattati, alla normativa italiana ed europea in materia di protezione dei dati personali, e di possedere i requisiti di affidabilità idonei a garantire il rispetto delle disposizioni normative in materia;

d) sulla base delle referenze e competenze attestate dal Responsabile in termini di proprietà, risorse umane, attrezzature ed esperienza nella gestione di servizi analoghi a quelli di cui al Contratto nonché degli impegni contrattuali assunti dal Responsabile in tema di rispetto della normativa applicabile in materia di protezione dei dati personali, il Titolare ha condotto una positiva valutazione della idoneità e qualificazione del Responsabile atta a soddisfare, anche sotto il profilo della sicurezza del trattamento, i requisiti di cui alla normativa applicabile (artt. 28 e ss. del Regolamento generale

europeo sulla protezione dei dati n. 679 del 2016, nel seguito "**Regolamento**") e intende designare il Responsabile quale responsabile del trattamento dei dati personali derivante dal Contratto;

e) ai fini del presente Accordo HDI agisce quale Titolare del trattamento, come definito all'art. 4 del Regolamento ("**Titolare**")

f) a far data dalla sottoscrizione del presente accordo (nel seguito "**Accordo**") qualsiasi precedente accordo sul trattamento dei dati personali tra le Parti si intende revocato.

Tutto quanto sopra premesso, le Parti convengono quanto segue:

1. OGGETTO

1.1 Con la sottoscrizione del presente Accordo HDI designa il Responsabile quale responsabile del trattamento in relazione alle operazioni di trattamento Dati Personali poste in essere ai soli fini dell'esecuzione del Contratto. Tale nomina non comporta il diritto ad alcuna remunerazione integrativa rispetto al corrispettivo pattuito contrattualmente né ad alcun rimborso spese per l'adempimento di quanto previsto dal presente Accordo.

1.2 I compiti assegnati al Responsabile sono esclusivamente quelli resi necessari dalle attività connesse all'esecuzione del Contratto.

2. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

2.1 Qualora nell'ambito delle operazioni di trattamento dei Dati Personali occorrano istruzioni aggiuntive al fine di adeguarsi alla normativa in materia di protezione dei dati personali, HDI trasmetterà ulteriori istruzioni al Responsabile in merito alle finalità, modalità e procedure per l'utilizzo e il trattamento dei Dati Personali incluse misure tecniche ed organizzative che dovranno essere comunque rispettate dal Responsabile, fermo restando l'obbligo del Responsabile di adottare tutte le ulteriori misure di sicurezza necessarie ai fini del rispetto della normativa applicabile e di informare il titolare in merito a tali ulteriori misure di sicurezza.

3. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

3.1 Ai fini di un corretto trattamento dei Dati Personali, in aggiunta a quanto previsto dalla normativa applicabile e dalle altre previsioni del presente Accordo, il Responsabile si impegna a:

a) svolgere qualsiasi operazione di trattamento di Dati Personali in conformità ai principi e alla regolamentazione previsti dalla normativa vigente in materia di protezione dei Dati Personali, ivi incluso, quanto prescritto dal Regolamento;

b) eseguire fedelmente le istruzioni impartite dal Titolare, evitando attività di trattamento non conformi alle predette istruzioni o volte a perseguire finalità diverse da quelle correlate all'esecuzione del Contratto;

c) non effettuare copie dei Dati Personali diverse da quelle strettamente necessarie alla corretta esecuzione del Contratto;

d) garantire il pieno rispetto degli obblighi di cui il Responsabile, quale responsabile del trattamento, è tenuto in virtù della normativa vigente;

e) in relazione alla raccolta dei Dati Personali degli interessati cui sia tenuto il Responsabile in via diretta ai fini dell'esecuzione del Contratto, il Responsabile vi provvede nel rispetto delle specifiche concordate di volta in volta con HDI al fine di garantire che la raccolta di Dati Personali ed il loro successivo trattamento, siano conformi alla legge (es. rendere l'informativa nel testo fornito dal Titolare e con le forme concordate con esso, raccogliere il consenso al trattamento dei dati, se applicabile);

f) fuori dai casi strettamente necessari per l'esecuzione del Contratto, non divulgare o rendere noti a terzi i Dati Personali e adottare le misure organizzative e tecniche necessarie per assicurare la

massima riservatezza dei Dati Personali acquisiti e utilizzati nello svolgimento delle attività oggetto della presente designazione;

g) garantire che l'accesso ai Dati Personali da parte del personale o collaboratori avvenga solo sulla base del principio di stretta necessità, provvedendo a individuare e istruire, anche ai fini di cui all'art. 32 del Regolamento, le persone fisiche (dipendenti e/o collaboratori) preposti al trattamento dei dati personali per le suddette finalità, impegnando gli stessi con idonei vincoli di riservatezza;

h) formare adeguatamente il personale/collaboratori addetti all'esecuzione del Contratto fornendo loro istruzioni precise e vigilando sulla loro osservanza;

i) collaborare con il Titolare per l'attuazione di qualsiasi misura che si renda necessaria al fine di garantire la conformità del trattamento dei Dati Personali con la normativa in materia di protezione dei dati personali;

j) documentare la propria conformità alla normativa vigente e alle istruzioni ricevute mediante relazioni semestrali a HDI, i cui contenuti minimi sono riportati nell'Allegato 1;

k) informare immediatamente il Titolare qualora, a suo parere, un'istruzione fornita dal Titolare violi il Regolamento o altra normativa applicabile in materia di protezione dei dati personali;

l) informare il Titolare e il suo Data Protection Officer (all'indirizzo e-mail privacy@hdia.it) entro 24 ore dal momento in cui ne è venuto a conoscenza, di qualsiasi violazione o rischio di violazione concernente i Dati Personali di cui il Responsabile è venuto a conoscenza nell'esecuzione del Contratto;

m) adottare le misure di sicurezza previste dall'articolo 6 del presente Accordo;

n) informare senza indugio HDI e il suo Data Protection Officer (all'indirizzo e-mail privacy@hdia.it) in caso di qualsiasi richiesta di informazione, attività ispettiva o provvedimento delle autorità in relazione ai Dati Personali e collaborare con HDI al fine di dare riscontro all'Autorità

o) in caso di presentazione di una richiesta di accesso o di esercizio dei diritti da parte degli interessati, inoltrare senza indugio la richiesta e la relativa documentazione ad HDI ed al suo Data Protection Officer (all'indirizzo e-mail privacy@hdia.it) e collaborare con quest'ultima al fine di soddisfare la richiesta dell'interessato fornendo le necessarie informazioni.

3.2 Quanto sopra si applica salvo il caso in cui il Responsabile, per adempiere ad eventuali obblighi imposti al Responsabile dalla normativa vigente o da un organo di vigilanza o controllo competente, sia tenuto a effettuare trattamenti in modalità difforme rispetto a quanto sopra previsto, incluse eventuali comunicazioni di dati personali a terzi. In tale ultimo caso il Responsabile ne darà comunicazione scritta ad HDI, salvo il caso in cui ciò sia vietato dalla legge.

3.3 In caso di esercizio del diritto di opposizione da parte di un interessato, il Responsabile dovrà astenersi dal porre in essere qualsiasi ulteriore attività di trattamento dei dati, salvo quelle strettamente necessarie ad informare il Titolare del trattamento e il Suo Data Protection Officer (all'indirizzo e-mail privacy@hdia.it) dell'esercizio di tale diritto, e si atterrà alle istruzioni impartite dal Titolare in relazione alla registrazione del diritto di opposizione direttamente sui sistemi resi disponibili al Responsabile ai fini dell'esecuzione del Contratto; il Titolare del trattamento provvederà di volta in volta ad impartire eventuali successive istruzioni se necessario.

3.4 Il Responsabile fornirà assistenza al Titolare nell'individuazione e raccolta delle informazioni necessarie per garantire al Titolare il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento.

3.5 Qualora la Commissione Europea stabilisca, o un'autorità di vigilanza adotti, clausole contrattuali tipo per le materie di cui all'Articolo 28(3) e all'Articolo 28(4) del Regolamento ai sensi dell'Articolo 28(7) o dell'Articolo 28(8) del Regolamento (se del caso), e il Titolare informi il Responsabile della propria intenzione di includere qualunque elemento di tali clausole contrattuali tipo nel presente Accordo, il Responsabile accetterà le modifiche richieste dal Titolare al fine di includere tali elementi per iscritto.

4. AFFIDAMENTO A TERZI E LIMITAZIONI AL TRASFERIMENTO DEI DATI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

4.1 Qualora il Responsabile del trattamento dei Dati Personali intenda avvalersi di un soggetto terzo che lo assista nell'esecuzione del Contratto ("**Responsabile Ulteriore**") e tale assistenza preveda il trattamento dei Dati Personali il Responsabile dovrà:

a) ottenere il previo consenso scritto di HDI;
b) assicurarsi che il Responsabile Ulteriore, prima di iniziare il trattamento dei Dati Personali, sottoscriva un contratto con il Responsabile in cui si assume obblighi in materia di protezione che non siano meno tutelanti di quelli contenuti nel presente Accordo e prescritti dalla normativa vigente;
c) agire con la dovuta diligenza e monitorare il rispetto delle obbligazioni da parte del Responsabile Ulteriore.

4.2 Qualora il Responsabile Ulteriore non adempia ai propri obblighi in materia di protezione dei dati i Responsabile risponderà per l'intero nei confronti di HDI.

4.3 Il Responsabile non trasferirà i Dati Personali al di fuori del SEE senza il previo consenso scritto esplicito del Titolare. Al riguardo il Responsabile dichiara che le infrastrutture/i software di cui si avvale fanno capo a data center situati in Italia.

4.4 Qualora il Titolare acconsenta al trasferimento al di fuori del SEE, tale consenso sarà subordinato al fatto che il Responsabile adotti e continui ad adottare costantemente le misure che potranno essere ragionevolmente richieste dal Titolare per garantire la protezione adeguata di tali Dati Personali in conformità alla normativa in materia di protezione dei Dati Personali, che potranno includere la sottoscrizione delle clausole contrattuali tipo previste nella Decisione della Commissione europea 2010/87/UE, del 5 febbraio 2010, per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi (le "**Clausole Contrattuali Tipo**") o altra base giuridica valida al momento del trasferimento dei Dati Personali.

5. DURATA - CESSAZIONE

5.1 L'efficacia del presente Accordo decorre dalla data di sottoscrizione dello stesso ad opera di entrambe le Parti sino alla cessazione, per qualsiasi causa intervenuta, del Contratto, ovvero alla revoca del presente Accordo, che comporterebbe la necessaria risoluzione del Contratto.

5.2 All'atto della cessazione del presente Accordo il Responsabile dovrà cessare qualsiasi operazione di trattamento dei Dati Personali e restituire ad HDI tutti gli eventuali Dati Personali trattati ai fini dell'esecuzione del Contratto di cui il Responsabile dovesse disporre o, su richiesta del Titolare, provvedere alla loro distruzione, fornendone apposita attestazione, eccettuate eventuali esigenze di loro conservazione in adempimento di obblighi normativi di cui andrà data contestuale attestazione ad HDI.

6. MISURE DI SICUREZZA

6.1 Con riferimento alle operazioni di trattamento dei Dati Personali necessarie ai fini della esecuzione del Contratto, il Responsabile si obbliga a (i) mantenere quantomeno le misure di sicurezza di cui all'Allegato 2 al presente Accordo ed ogni e qualsiasi ulteriore misura di sicurezza idonea a prevenire i rischi di distruzione, perdita, anche accidentale, dei Dati Personali nonché di accesso non autorizzato o trattamento illecito dei medesimi come previsto nel Contratto (ii) far sì che tali misure siano conformi ai principi di cui all'art. 32 del Regolamento, nonché ogni altra misura obbligatoria di legge e della normativa in materia di protezione dei dati personali, e alle *best practice* di settore iii) ad adottare misure di sicurezza e usare un livello di diligenza, rispetto ai Dati Personali, non inferiori a quelli che il Responsabile applica ai Dati Personali di sua titolarità, iv) verificare regolarmente l'idoneità delle misure adottate.

6.2 Il Responsabile, non appena ragionevolmente possibile e non oltre 5 giorni lavorativi dalla richiesta del Titolare, fornirà a quest'ultimo una descrizione scritta dettagliata delle misure tecnico-organizzative che ha adottato o che sono state adottate per suo conto, al fine di dimostrare e garantire il rispetto del presente articolo 6.

6.3 Il Responsabile eseguirà regolarmente, ma in qualunque caso, ogni 24 ore, un back-up dei Dati Personali in conformità alle proprie procedure di back-up.

6.4 Il Responsabile dovrà inoltre attenersi alle ulteriori istruzioni integrative impartite, caso per caso, dal Titolare del trattamento oltreché alla normativa in materia tempo per tempo vigente.

7. CONTROLLI

7.1 Il Responsabile riconosce e accetta che il Titolare, nell'ambito dei poteri e obblighi ad esso spettanti in quanto Titolare del trattamento, possa controllare le operazioni di trattamento di Dati Personali svolte dal Responsabile, come anche le misure di sicurezza attuate da quest'ultimo per le finalità di cui al presente Accordo, attraverso richieste di informazioni/documenti, che dovranno essere tempestivamente forniti dal Responsabile ovvero mediante apposite ispezioni presso i locali e sistemi del Responsabile.

8. RESPONSABILITA'

8.1 Il Responsabile si impegna a tenere integralmente indenne, manlevare e a risarcire HDI per ogni danno dallo stesso subito in conseguenza di un inadempimento imputabile al Responsabile (e/o a suoi dipendenti, collaboratori, rappresentanti, subappaltatori) agli obblighi su di esso gravanti ai sensi del presente Accordo e della normativa in materia di protezione dei dati personali, siano essi derivanti da perdite, danni, costi, pretese, sanzioni amministrative, spese e/o richieste, subiti o sostenuti dal Titolare, azioni o pretese di terzi.

8.2 Il Responsabile riconosce e accetta che nei casi in cui sia riconosciuta la corresponsabilità del Titolare con il Responsabile in relazione a violazioni di Dati Personali occorse in relazione ai trattamenti di Dati Personali di cui al presente Accordo, e il Titolare sia destinatario di provvedimenti risarcitori e/o sanzionatori da parte delle autorità competenti, il Titolare potrà rivalersi pro quota sul Responsabile ai sensi dell'art. 82, comma 5, del Regolamento.

8.3 Il Titolare avrà diritto di risolvere il Contratto ai sensi e per gli effetti dell'art. 1456 del codice civile mediante invio di una comunicazione scritta al Responsabile a mezzo raccomandata a.r., o mezzo equipollente, in caso di violazione delle misure di sicurezza, e in caso di violazione degli obblighi derivanti dalla normativa in materia di protezione dei Dati Personali come previsti nel presente Accordo. È fatto salvo in ogni caso il risarcimento dei danni subiti.

Le premesse costituiscono parte integrante ed essenziale del presente Accordo. Qualora vi sia incongruenza tra i termini dell'Accordo e una qualsiasi delle previsioni contrattuali di cui al Contratto, prevarrà quanto indicato nel presente Accordo.

HDI Assicurazioni SpA
Vice Direzione Generale
Commerciale
Il Vice Direttore Generale
Dott. Tommaso Di Gennaro

L'Agente
Nome e Cognome: ANASTASIO GUDAS
Titolo: AGENTE
Firma:
Luogo e data: FIRENZE 09/05/2019

Allegato 1

Contenuti minimi report semestrali

Di seguito si riportano le informazioni minime di dettaglio che devono essere contenute all'interno dei report semestrali forniti dal Responsabile:

1- Riferimenti al contratto di agenzia e all'accordo per il trattamento dei dati (oggetto e data)
2- Compiti e responsabilità. In particolare specificare se:
    a. sono state rilasciate le informative agli interessati e raccolti i relativi consensi nelle forme previste dal contratto
    b. sono stati definiti i profili di accesso ai dati personali secondo necessità
    c. il personale/collaboratori hanno ricevuto istruzioni dettagliate e come
    d. sono stati erogati corsi di formazione privacy a tutto il personale/collaboratori coinvolti nel trattamento dei dati
    e. sono state condotte verifiche sull'operato del personale/collaboratori (quante, su quale perimetro e con che esito, quali azioni di rimedio sono state individuate)
    f. sono state ricevute richieste di esercizio dei diritti da parte degli interessati (se sì, quante, e come gestite)
    g. sono state ricevute ispezioni o richieste di informazioni dalle Autorità (se si, quante, quali e che esito hanno dato)
    h. si sono verificate violazioni di dati personali (quante, quali, che rimedi sono stati adottati)
    i. è stato nominato un DPO (se no, per quale ragione)
3- Misure di sicurezza inerenti i trattamenti effettuati con l'ausilio di strumenti elettronici
    a. Informazioni sul rilascio di credenziali, e sulle procedure di gestione, e di controllo
    b. Informazioni su test di vulnerabilità condotti (se sì, come e con quale frequenza ed esito) antivirus, antiphishing, antispamming, aggiornamento del pattern ecc.
    c. Informazioni sui back up eseguiti (ogni 24 ore), verifiche, e tempi di conservazione
    d. Informazioni su cancellazione dati nel periodo intercorso
    e. Variazioni intervenute sui sistemi d protezione dei dati e su misure specifiche per dati particolari (sensibili) e giudiziari
4- Misure di sicurezza inerenti i trattamenti effettuati senza l'utilizzo di strumenti elettronici
    a. Informazioni su sistemi antiintrusione e antincendio ed eventuali incidenti
    b. Informazioni su modalità di archiviazione dei documenti cartacei e accesso alle aree di conservazione dei dati
    c. Variazioni intervenute sui sistemi di protezione dei dati e su misure specifiche per dati particolari (sensibili) e giudiziari
5- Modifiche organizzative e tecniche programmate e stima tempi di realizzazione

Controllo di accesso fisico agli uffici e al Sistema di elaborazione dei dati	**Implementazione**	
Obiettivo: Nessun accesso fisico non autorizzato ai sistemi di elaborazione dati.	Perimetro di sicurezza	Sono definiti perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.
	Controlli di accesso fisico	Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato avvia il permesso di accedervi.
	Rendere sicuri uffici, locali e strutture	Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti.
	Protezione contro le minacce esterne ed ambientali	Deve essere progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli e accidentali.
	Aree di carico e scarico	I punti di accesso, come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, devono essere controllati e, se possibile, Isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati.

Controllo di accesso logico al sistema di elaborazione dei dati	**Implementazione**	
Obiettivo: Nessun accesso non autorizzato ai sistemi di informazione.	Apparecchiature incustodite degli utenti	Gli utenti devono assicurare che i device/sistemi, se incustoditi, siano appropriatamente protetti.
	Politica schermo e scrivania puliti	Adozione di una politica di CLEAR DESK POLICY e CLEAR SCREEN POLICY.
	Politica controllo degli accessi logici	Adozione di una politica di controllo degli accessi logici aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni

Controllo di accesso logico al sistema di elaborazione dei dati	Implementazione	
	Accesso alle reti e ai servizi di rete	Agli utenti devono essere forniti solo gli accessi alle reti ed ai servizi di rete per il cui uso sono stati specificamente autorizzati.
	Provisioning degli accessi utenti	Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi.
	Gestione dei diritti di accesso privilegiato	L'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati.
	Gestione delle informazioni segrete di autenticazione degli utenti	L'assegnazione delle informazioni segrete di autenticazione deve essere controllata attraverso un processo di gestione formale e gli utenti devono essere tenuti a seguire la prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione.
	Riesame dei diritti di accesso degli utenti	I responsabili degli asset devono riesaminare ad intervalli regolari i diritti di accesso degli utenti.
	Rimozione o adattamento dei diritti di accesso	I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate a ogni variazione.
	Limitazione dell'accesso alle informazioni	L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato.
	Procedure di log-on sicure	Quando richieste dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni deve essere controllato da procedure di log-on sicure (Strong Authentication).
	Sistema di gestione delle password	I sistemi di gestione delle password devono essere interattivi e devono assicurare password di con criteri di complessità definiti dall'organizzazione.

Controllo di accesso logico al sistema di elaborazione dei dati	Implementazione	
	Uso di programmi di utilità privilegiali	L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema deve essere limitato e strettamente controllato.
	Controllo degli accessi al codice sorgente dei programmi	Gli accessi al codice sorgente dei programmi devono essere limitati al solo personale autorizzato.
	Controlli di rete	Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
	Sicurezza dei servizi di rete	I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o dall'esterno.
	Segregazione delle reti	Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi sulla base del loro livello di criticità per permettere l'adozione di misure di sicurezza proporzionate al rischio.

Controllo del trasferimento	Implementazione	
Obiettivo: Nessuna operazione di lettura, copia, modifica o cancellazione non autorizzata durante la trasmissione o il trasporto elettronico.	Politiche e procedure per il trasferimento delle informazioni	Devono esistere politiche, procedure e controlli a protezione del trasferimento delle informazioni.
	Accordi di trasferimento delle informazioni	I trasferimenti sicuri di informazioni di business tra l'organizzazione e le parti esterne devono essere indirizzati in appositi accordi.
	Messaggistica elettronica	Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato.
	Accordi di riservatezza o di non divulgazione	I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni devono essere identificati, riesaminati periodicamente e documentati.

Controllo del trasferimento	Implementazione	
	Utilizzo di controlli crittografici	Devono essere utilizzati controlli crittografici per la protezione delle informazioni critiche. Le chiavi crittografiche sono protette per il loro intero ciclo di vita.

Controllo modifiche ai dati	Implementazione	
Obiettivo: Tracciatura di inserimenti, modifiche o cancellazione di dati dai sistemi informativi.	Raccolta di log degli eventi	La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente.
	Protezione delle informazioni di log	Le strutture per la raccolta del log e le informazioni di log devono essere protette da manomissioni e accessi non autorizzati.
	Log di amministratori e operatori	Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente.
	Sincronizzazione degli orologi	Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento.

Controllo della disponibilità dei dati	Implementazione	
Obiettivo: Protezione contro perdite o distruzioni accidentali o intenzionali	Disposizione delle apparecchiature e loro protezione	Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato.
	Infrastruttura di supporto	Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causali da malfunzionamenti dei servizi ausiliari.

Controllo della disponibilità dei dati	Implementazione	
	Sicurezza dei cablaggi	I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informatici devono essere protetti da intercettazioni, interferenze o danneggiamenti.
	Manutenzione delle apparecchiature	Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità.
	Procedure operative	Devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano.
	Gestione dei cambiamenti	I cambiamenti all'organizzazione, ai processi di business, alle infrastrutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni devono essere controllati.
	Controlli contro malware	Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti.
	Installazione del software sui sistemi di produzione	Devono essere attuate procedure per controllare l'installazione del software sui sistemi di produzione.
	Gestione delle vulnerabilità tecniche	Le informazioni sulla vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi.
	Limitazioni all'installazione del software	Devono essere stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti.
	Controlli per l'audit sui sistemi informativi	I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione devono essere attentamente pianificati e concordati per minimizzare le interferenze con i processi di business

Capacità di recupero (Art. 32 Sezione 1 lit. c GDPR)	**Implementazione**	
Obiettivo: Capacità di recupero entro un periodo di tempo appropriato dopo un evento di disturbo.	Backup delle informazioni	Devono essere effettuate copie di backup delle informazioni, dei software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.
	Pianificazione della continuità della sicurezza delle informazioni	L'organizzazione deve determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri.
	Attuazione della continuità della sicurezza delle informazioni	L'organizzazione deve stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.
	Verifica, riesame e valutazione della continuità della sicurezza delle informazioni	L'organizzazione deve verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse.
	Disponibilità delle strutture per l'elaborazione delle informazioni	Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.

Gestione della protezione dei dati	**Implementazione**
Approccio sistematico alla gestione della protezione dei dati.	Funzionamento di un sistema di gestione della sicurezza delle informazioni e della protezione dei dati secondo ISO 27001, ISO 27002, e ISO 27018.

Gestione della risposta agli incidenti	**Implementazione**	
Obiettivo: Capacità di gestire gli incidenti efficacemente ed efficientemente.	Responsabilità e procedure	Devono essere stabilite le responsabilità e le procedure di gestione degli incidenti per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni.

Gestione della risposta agli incidenti	**Implementazione**	
	Segnalazione degli eventi relativi alla sicurezza delle informazioni	Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali.
	Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni.
	Risposta agli incidenti relativi alla sicurezza delle informazioni	Si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate.
	Raccolta evidenze	L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze