SOMMARIO

1. Scopo, ambito e destinatari

Scopo della presente Politica è definire principi e regole che *Advice Group S.p.A.* applica nella gestione delle relazioni con i fornitori di prodotti e servizi IT (di seguito "Fornitori") al fine di assicurare la conformità ai requisiti legali e ai principi legati alla sicurezza delle informazioni, in accordo con le caratteristiche specifiche della fornitura.

Al fine di tutelare gli interessi di *Advice Group S.p.A.* e il suo patrimonio informativo occorre garantire che:

- Siano correttamente individuate le modalità di selezione dei fornitori, sotto il profilo della professionalità, dell'onorabilità e della capacità finanziaria;
- I rapporti intrattenuti con i fornitori siano formalizzati e siano specificati i principi per la tutela della sicurezza delle informazioni;
- Siano illustrate le modalità da adottare per la valutazione del livello delle prestazioni del fornitore anche attraverso la definizione di "SLA" (Service Level Agreement);
- Il rispetto delle regole definite per la sicurezza delle informazioni sia sottoposto ad attento monitoraggio e controllo con previsione di apposita facoltà di uscita.

Questo documento si applica a tutti i fornitori e partner che processano i dati aziendali di *Advice GroupS.p.A.* e che possono influenzare la confidenzialità, integrità e disponibilità delle informazioni sensibili delle due Aziende.
Destinatari di questo documento sono l'Alta Direzione e le persone che hanno la responsabilità di intrattenere rapporti con i fornitori ed i partner all'interno di *Advice Group S.p.A.*

2. Cloud Computing

Altro scopo di questo documento è definire la politica dell'organizzazione nell'area del cloud computing.
Advice S.p.A. fa ampio uso di servizi di cloud computing nella fornitura dei propri sistemi aziendali principali. La natura di questi servizi è tale che i dati vengono archiviati al di fuori della rete interna di *Advice S.p.A.* e sono soggetti all'accesso e alla gestione da parte di terzi. Inoltre, molti servizi cloud sono offerti su base multi-tenant in cui l'infrastruttura è condivisa tra più clienti del Cloud Service Provider (CSP), rendendo la segregazione efficace e sicura un requisito fondamentale.
È quindi essenziale stabilire regole per la selezione e la gestione dei servizi di cloud computing in modo che i dati siano adeguatamente protetti in base al loro valore commerciale e alla loro classificazione.
Il cloud computing è generalmente accettato come composto dai seguenti tipi di servizi:

- Software-as-a-Service (SaaS): la fornitura di un'applicazione ospitata da utilizzare come parte di un processo aziendale. L'hosting di solito include tutti i componenti di supporto per l'applicazione come hardware, software operativo, database ecc.
- Platform-as-a-Service (PaaS): vengono forniti hardware e software di supporto come sistema operativo, database, piattaforma di sviluppo, server Web ecc., ma non applicazioni aziendali
- Infrastructure-as-a-Service (IaaS): vengono forniti solo componenti hardware fisici o virtuali

Questa politica si applica all'uso di tutti i tipi di servizi di cloud computing ed è particolarmente rilevante quando vengono archiviati dati personali.

3. Rapporti con fornitori e partner

3.1 Identificare i rischi

I rischi per la sicurezza legati a fornitori e partner sono identificati durante il processo di valutazione del rischio, come definito nella Metodologia per la Valutazione e il Trattamento del Rischio. Durante la valutazione del rischio, occorre prestare particolare attenzione per identificare i rischi relativi alle tecnologie informatiche e della comunicazione, nonché i rischi connessi alla catena di approvvigionamento dei prodotti/servizi.
Il Settore Sistemi Informativi può autonomamente decidere se è necessario valutare ulteriormente i rischi relativi ai singoli fornitori o partner.

3.2 Criteri di selezione

La selezione dei fornitori viene effettuata attraverso attività di scouting di mercato atte a identificare l'idoneità dell'offerta rispetto alla specifica esigenza. Successivamente i fornitori coinvolti vengono valutati e, nel caso rispondano ai requisiti richiesti, qualificati come idonei a fornire il servizio richiesto.

I beni e i servizi vengono richiesti attraverso ingaggi formali, che possono essere diretti oppure attraverso bandi di gara che prevedono la redazione di documentazione specifica in cui vengono descritte le specificità della richiesta.

I fornitori interessati rispondono alle richieste, presentando anche la documentazione e le informazioni utili (a titolo esemplificativo bilancio degli ultimi tre anni, visura camerale, proposta tecnico/economica, ecc.) ai fini della valutazione della loro idoneità, sia per quanto attiene agli aspetti societari e finanziari sia con riferimento alla prestazione del servizio specifica.

Advice Group S.p.A. analizza le caratteristiche e la documentazione dei fornitori interessati e provvede alla selezione di quello più idoneo, assicurandosi che il soggetto erogante il servizio sia in possesso dei requisiti di professionalità, onorabilità e solidità finanziaria. In dettaglio:

- Professionalità
  Il requisito di professionalità viene valutato tenendo conto dei seguenti parametri:
  - Comprovata specializzazione nell'attività in oggetto;
  - Certificazioni aziendali possedute (qualità, sicurezza, anticorruzione, ambiente);
  - Evidenza di incidenti o violazioni in cui il Fornitore sia stato coinvolto in passato;
  - Esame delle capacità tecnico/organizzative dei fornitori (es.: il possesso di mezzi, le conoscenze ed esperienze specifiche nel settore di interesse, sensibilità sul rispetto delle normative, ecc.);
  - Acquisizione sul mercato di referenze, in relazione alle attività più significative da essi svolte;

- Dimensioni/fatturato, che devono risultare adeguati all'attività oggetto in fornitura;
- o Consistenza delle strutture e degli organici tecnici di cui dispone il fornitore per la prestazione dei servizi richiesti e per il controllo di qualità.

La maggiore o minore incidenza dei parametri sopra indicati dipenderà dalla tipologia e dall'importanza strategica dell'attività in discorso.

- Onorabilità
  Per la verifica del requisito di onorabilità Advice Group S.p.A. si avvalgono di informazioni esterne che consentono di accertare che il fornitore non abbia subito eventi straordinari quali fallimenti, condanne, ecc.

  Inoltre, Advice Group S.p.A. tengono in considerazione il grado di condivisione, da parte del fornitore, dei valori della Società, quali la trasparenza, la correttezza e la professionalità
- Capacità economica
  La scelta del fornitore deve ricadere su soggetti in grado di dimostrare di possedere risorse finanziarie idonee a garantire gli impegni di spesa connessi al regolare svolgimento dell'attività da esternalizzare.
  Per la verifica del requisito di capacità economica Advice Group S.p.A. si avvalgono di informazioni esterne che consentono di accertare il rating del fornitore e la sua solidità finanziaria e patrimoniale.
- Indipendenza
  La scelta del fornitore deve avvenire in modo tale da garantire l'assoluta indipendenza nei rapporti tra le parti e deve seguire procedure di accesso al mercato tali da evitare equivoci o situazioni di privilegio, così come previsto nel Codice Etico di Advice Group S.p.A.

3.3 Requisiti di sicurezza delle informazioni

L'instaurazione di un rapporto di collaborazione con un fornitore è subordinata alla valutazione dei rischi per la sicurezza delle informazioni connessi con la fornitura di interesse.

Al fine della valutazione dei rischi è necessario ottenere informazioni esaurienti rispetto a diversi aspetti in funzione della tipologia di fornitura.

Una singola fornitura può anche riguardare diverse tipologie di servizi, per ciascuna delle quali vanno acquisite informazioni a vari livelli, secondo lo schema descritto dalle tabelle riportate nel seguito:

Ambito	*Informazioni*
Informazioni generali	Ambiti in cui opera il Fornitore;
	Esecuzione di altri contratti con società di Advice Group S.p.A. ed eventuale esistenza di valutazioni negative o altri motivi di attenzione
	Esistenza di un accordo di non divulgazione (NDA) attivo;
	Sedi (indirizzi fisici) da cui possono essere svolte le attività e sedi interconnesse

	Rapporti di audit o altre ispezioni svolte in passato presso il Fornitore;
	Incidenti di sicurezza notificati all'Autorità negli ultimi due anni;
	Certificazioni aziendali possedute (qualità, sicurezza, anticorruzione, ambiente)
	Certificazioni e/o competenze del personale;
	Livello di personalizzazione del servizio offerto (se il servizio offerto è già stato o meno realizzato per altri clienti);
	Dati trattati nell'esecuzione della fornitura;
	Modalità di accesso alle infrastrutture e/o ai dati previste (accesso e trasporto sia logico che fisico);
	Modalità e luoghi di conservazione ed elaborazione dei dati trattati.
Subfornitori	Elenco dei subfornitori e delle attività assegnate.
Sistema di Gestione della sicurezza delle informazioni	Disponibilità di policy per la Sicurezza delle Informazioni aggiornata (controllo accessi, utenti privilegiati, password policy, classificazione informazioni, gestione asset, dispositivi mobili, ecc.);
	Disponibilità di ruoli e responsabilità assegnati in ambito Sicurezza delle Informazioni
	Evidenza di processi di: o verifica periodica attuazione ed efficacia delle misure di sicurezza adottate e della conformità alle normative applicabili (disponibilità di report recenti) o analisi dei Rischi per la sicurezza delle informazioni (disponibilità report recenti – redatti non oltre 12 mesi prima) o verifica dell'affidabilità del personale; o formazione e sensibilizzazione del personale sui temi di sicurezza delle informazioni
	Esistenza di procedure per la gestione degli incidenti di sicurezza delle informazioni e di notifica verso Titolari e Autorità (disponibilità di classificazione incidenti, moduli di notifica).
	Misure di controllo perimetrale attuate (FW, AV, WAF, IDS/IPS, NAC, DLP, ANTI-DDOS, ecc.).
	Misure di isolamento/separazione dei dati critici di Advice Group S.p.A.
	Misure di sicurezza fisica: o Gestione ingresso visitatori; o Sicurezza fisica perimetrale (sistemi antintrusione, badge, videosorveglianza, ecc.); o Sicurezza ambientale sale dati (antincendio, anti allagamento, condizionamento, continuità alimentazione).
Sviluppo Sicuro	In caso di sviluppo software, evidenza di processi di: o Change Management; o Test; o Sviluppo sicuro (procedure impiegate, competenze del personale);

	o Vulnerability/penetration test su infrastrutture e applicazioni.
Continuità Operativa	Esistenza di un piano di Business Continuity / Disaster Recovery: o Scenari di interruzione previsti; o Criteri di attivazione e notifiche previste; o Contatti per la gestione dell'emergenza; o RTO, RPO. Modalità ed evidenze di attività di test (report recenti, avanzamento piani di miglioramento).

Nei casi in cui i servizi prevedano il trattamento di dati personali:

Misure protezione dati personali	o Presenza di un DPO; o Personale incaricato (interno ed esterno); o Misure di crittografia, pseudonimizzazione, anonimizzazione adottate; o Politiche di back-up e retention; o Misure per la cancellazione dei dati; o Modalità di notifica in caso di incidenti o Stato (UE/EXTRA UE) dove vengono trattati e conservati i dati

4.1. Contratti

Il Settore Sistemi Informativi è responsabile di decidere quali clausole della sicurezza saranno incluse nel contratto con il fornitore o il partner. Tale decisione deve essere basata sui risultati della valutazione e del trattamento del rischio; tuttavia, le clausole che stabiliscono la riservatezza e la restituzione dei beni dopo la risoluzione del contratto sono obbligatorie. Inoltre, i contratti devono garantire la fornitura affidabile dei prodotti e dei servizi, che risultano particolarmente importanti per i fornitori di servizi di cloud.

Il Settore Sistemi Informativi verificherà se i singoli dipendenti del fornitore / partner hanno firmato le Dichiarazioni di Riservatezza quando lavorano per *Advice Group S.p.A.*

Il Settore Sistemi Informativi verificherà che sia stato identificato il responsabile di ciascun contratto, ovvero chi sarà responsabile per un particolare fornitore o partner.

Inoltre, sarà necessario prevedere che, i contratti debbano contenere specifiche clausole su:

- Responsabilità nell'esecuzione del servizio, garanzie e recesso senza che vi sia la presenza di oneri eccessivi;
- Notifica eventi: obbligo di comunicazione degli eventi di sicurezza e collaborazione nelle fasi di risoluzione e investigazione;
- Responsabili trattamento: clausola o specifico contratto per nomina a responsabile, corretta gestione delle credenziali di accesso, identificazione e comunicazione degli Amministratori di Sistema;

- Riservatezza: obbligo di riservatezza per tutte le informazioni (non solo dati personali) di proprietà di *Advice Group S.p.A.* di cui verrà a conoscenza il fornitore durante il rapporto;
- Subfornitori: uso di subfornitori solo su autorizzazione da parte di Advice Group S.p.A. e obbligo di propagazione e controllo di tutti i requisiti di sicurezza delle informazioni ai subfornitori;

Inoltre, per i contratti che prevedono la gestione dei dati, personali e non, presso i sistemi del fornitore (outsourcing), sono altresì presenti le seguenti clausole:

- Ubicazione dati: obbligo di informazione preventiva sull'ubicazione di eventuali dati di proprietà di *Advice Group S.p.A.* archiviati presso le infrastrutture del fornitore;
- Diritto di audit: autorizzazione ad interventi di verifica presso le sedi di erogazione del servizio, obbligo di trasparenza e comunicazione rispetto alle misure di sicurezza applicate ai dati di proprietà/pertinenza di *Advice Group S.p.A.*(misure che potranno essere oggetto di audit);
- Fine rapporto: definizione modalità di restituzione dati, cancellazione sicura dati, supporto migrazione verso altri servizi/fornitori;
- Presenza di piani di gestione di eventi straordinari quali interruzione di servizio, blocco della disponibilità dei dati, se necessario in funzione del tipo di servizio offerto.

In funzione delle attività specifiche che il fornitore si trova a svolgere, tra le clausole contrattuali debbono essere presenti riferimenti quali:

- Rispetto dell'accesso alle informazioni secondo le politiche di *Advice Group S.p.A.* e secondo la criticità dei dati trattati;
- Rispetto di requisiti di sviluppo sicuro, se necessario in funzione del tipo di servizio;
- Definizione della titolarità delle licenze, se nell'oggetto del servizio;
- Obbligo del rispetto dei diritti di proprietà intellettuale (uso software licenziato);
- Assicurazione del mantenimento dei requisiti di sicurezza e assunzione di responsabilità in caso di violazione.

4.2. Formazione e sensibilità

Il responsabile del contratto verificherà che gli impiegati dei fornitori e dei partner siano stati sensibilizzati e formati sui temi della sicurezza.

4.3. Monitoraggio e riesame

Il responsabile del contratto (congiuntamente con il Settore Sistemi Informativi deve controllare e monitorare regolarmente il livello del servizio e l'adempimento delle clausole di sicurezza da parte di fornitori o partner, i rapporti e le registrazioni create dal fornitore / partner, nonché effettuare verifiche presso il fornitore o il partner periodicamente perlomeno una volta all'anno.

Tutti gli incidenti della sicurezza relativi alle attività del partner / fornitore devono essere comunicati immediatamente al Settore Sistemi Informativi.

Per ogni contratto di fornitura *Advice Group S.p.A*. presidia attraverso la funzione che ha richiesto il servizio, le prestazioni del fornitore e il rispetto delle condizioni indicate nel contratto.

La valutazione delle prestazioni, se possibile, avviene attraverso modalità formalizzate attraverso opportune modalità di controllo sui livelli di servizio attesi, anche attraverso "SLA" Service Level Agreement che prevedano la misurabilità dei livelli di servizio, tramite specifici parametri oggettivi (es.: puntualità, correttezza, affidabilità, ecc.) individuati con riferimento agli standard di mercato.

La valutazione della prestazione deve tenere conto di:

- Qualità del servizio offerto;
- Tempi di esecuzione;
- Assistenza tecnica;
- Garanzia di aggiornamento tecnologico;
- Gestione delle criticità in termini di intervento e tempi di risoluzione;
- Il rispetto delle misure di sicurezza stabilite da Advice Group S.p.A.;
- Il rispetto della normativa applicabile e delle norme contrattuali;
- I livelli di performance del servizio ed il rispetto degli SLA se concordati;
- L'acquisizione di informazioni su eventuali incidenti di sicurezza;
- L'analisi e la gestione di ogni eventuale problema identificato.

Tali indicazioni devono essere riportate, per quanto possibile negli accordi contrattuali ed è competenza della funzione che ha richiesto il servizio segnalare eventuali malfunzionamenti o criticità.

4.4. Cambiamenti o risoluzione del contratto di servizi del fornitore

Il responsabile del contratto può proporre delle modifiche o l'eventuale risoluzione del contratto, coinvolgendo il Settore Sistemi Informativi per la gestione dell'evento.

4.5. Rimozione dei diritti di accesso / restituzione delle risorse

Quando il contratto viene modificato o risolto, i diritti di accesso per i dipendenti dei partner / fornitori devono essere rimossi in accordo alla Policy per il Controllo degli Accessi.
Inoltre, quando il contratto viene modificato o risolto, il responsabile del contratto (congiuntamente con il Settore Sistemi Informativi) deve assicurarsi che tutte le attrezzature, il software o le informazioni in formato elettronico o cartaceo vengano restituiti.

4. Cloud Computing

È politica di *Advice S.p.A.* nell'area del cloud computing che:

I dati appartenenti a *Advice S.p.A.* verranno archiviati all'interno dei servizi cloud solo previa autorizzazione del Chief Technological Officer .
Deve essere effettuata un'adeguata valutazione del rischio per quanto riguarda l'uso proposto o continuato dei servizi cloud, compresa una piena comprensione dei controlli di sicurezza delle informazioni implementati dal CSP.
La due diligence deve essere condotta prima dell'iscrizione a un provider di servizi cloud per garantire che siano in atto controlli appropriati per proteggere i dati. Verrà data preferenza ai fornitori che sono certificati secondo lo standard internazionale ISO/IEC 27001:2022 e che rispettano i principi dei codici di condotta ISO/IEC 27017 e ISO/IEC 27018 per i servizi cloud .
Gli accordi sul livello di servizio e i contratti con i fornitori di servizi cloud devono essere esaminati, compresi e accettati prima dell'iscrizione al servizio.
I contratti che riguardano dati personali devono essere controllati per garantire che siano conformi alla legislazione applicabile sulla protezione dei dati. In caso contrario, potrebbe essere richiesto un accordo separato sul trattamento dei dati.
I ruoli e le responsabilità per attività quali backup, patch, gestione dei registri, protezione da malware e gestione degli incidenti devono essere concordati e documentati prima dell'inizio del servizio cloud.
Devono essere stabilite procedure per garantire che le attività irreversibili in ambiente cloud (es. cancellazione di server virtuali, cessazione di un servizio cloud o ripristino da backup) siano sottoposte ad opportuni controlli per evitare errori. La supervisione di una seconda persona adeguatamente qualificata deve essere una parte dichiarata di tali procedure.
L'ubicazione dei dati archiviati con il CSP deve essere intesa, ad esempio Regno Unito, UE, USA e la base giuridica applicabile stabilita, come il paese la cui legge si applica al contratto.
Se disponibile, l'autenticazione a più fattori deve essere utilizzata per accedere a tutti i servizi cloud.
Deve essere disponibile una registrazione di controllo sufficiente per consentire a *Advice S.p.A.*di comprendere le modalità di accesso ai propri dati e di identificare se si è verificato un accesso non autorizzato.
I dati riservati archiviati nei servizi cloud devono essere crittografati a riposo e in transito utilizzando tecnologie e tecniche accettabili. Ove possibile, le chiavi di crittografia saranno detenute da *Advice S.p.A.* piuttosto che dal fornitore.
Advice S.p.A per la creazione e la gestione degli account utente si applicheranno ai servizi cloud.
Devono essere eseguiti backup di tutti i dati archiviati nel cloud. Ciò può essere eseguito direttamente da *Advice S.p.A.* o su contratto dal fornitore di servizi cloud.
Tutti i dati di *Advice S.p.A.* devono essere rimossi dai servizi cloud in caso di scadenza di un contratto per qualsiasi motivo. I dati non devono essere archiviati nel cloud più a lungo del necessario per fornire i processi aziendali.

5. Validità e gestione del documento

Il responsabile per questo documento è il Settore Sistemi Informativi, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.
Durante la valutazione dell'efficacia e adeguatezza di questo documento, devono essere tenuti in considerazione i seguenti criteri:

- numero e significatività degli incidenti causati dalle attività dei fornitori e dei partner
- numero di contratti per i quali non è stato definito il responsabile del contratto