

IT & GDPR SECURITY MEASURES

Riepilogo delle misure di sicurezza

Release 0.1 del 01/09/2026

AGIC

Via di Castel Giubileo, 62
00138 - Roma

+39 06 888851
info@agic.it

AGIC Technology IT security

Introduzione

AGIC è un provider tecnologico che implementa soluzioni e progetti per organizzazioni basati sulle tecnologie Microsoft. Business Applications (ERP e CRM), Data Analytics, Artificial Intelligence, Cybersecurity, Cloud Platform, IoT, Mobile, Machine Learning, Web, App, Portal & Collaboration sono soltanto alcune delle piattaforme sulle quali basa le sue soluzioni. Professionisti esperti di Governance, Risk e Compliance intervengono a fianco degli specialisti di tecnologie per accompagnare il rilascio delle soluzioni nel rispetto della sicurezza informatica, della normativa sull'Intelligenza Artificiale e del GDPR.

AGIC è attiva in prima linea per tutelare la riservatezza, l'integrità e la disponibilità delle informazioni, dei dati e delle notizie relative ai propri stakeholder, impegnandosi affinché siano salvaguardati da qualsiasi utilizzo illecito.

Per questa ragione, ha ottenuto il riconoscimento delle certificazioni internazionali ISO/IEC 27001:2022 e ISO/IEC 27701:2019.

Politiche per la Sicurezza delle Informazioni

AGIC definisce, approva e comunica all'interno della propria organizzazione procedure, policy e linee guida per la sicurezza informatica e la protezione dei dati personali al fine di regolamentare le attività e fornire un valido supporto metodologico alle risorse impiegate.

Considerati il crescente sviluppo tecnologico e la rapida evoluzione delle minacce, le procedure, le policy e le linee guida sono revisionate e integrate periodicamente al fine di renderle adeguate e al passo con i tempi. Sono altresì modificate ogniqualevolta ciò si renda necessario per l'evoluzione dell'organizzazione o in caso di significativi cambiamenti interni, nel mercato, nelle leggi o nella regolamentazione di settore.

A titolo esemplificativo, sono state adottate apposite procedure atte a regolamentare i processi di back up, di incident management, di gestione delle vulnerabilità e di continuità operativa, nonché di adeguamento dei vari servizi e prodotti offerti alla normativa europea in materia di privacy e protezione dei dati personali.

Organizzazione dell'Information Security System

AGIC definisce ruoli e responsabilità relativi all'assetto dell'Information Security System (IS) e all'organizzazione (es. ICT Manager, etc.), avendo cura di avvalersi di risorse competenti e formate in materia. Si impegna, infatti, affinché il personale mantenga aggiornate le proprie conoscenze attraverso la partecipazione, fra le altre cose, a seminari e workshop.

In aggiunta, nell'ambito dei processi IT più rilevanti, pone particolare attenzione nella separazione dei compiti e delle aree di responsabilità in conflitto tra loro così da ridurre le possibilità di uso improprio, di modifica non autorizzata o non intenzionale degli asset dell'organizzazione.



AGIC regola a fini privacy e data protection i rapporti con il proprio personale dipendente e con soggetti terzi esterni all'organizzazione (es. fornitori, etc.), tramite apposite nomine rilasciate in compliance con la normativa di settore (es. nomina a Responsabile del Trattamento ex art. 28 GDPR).

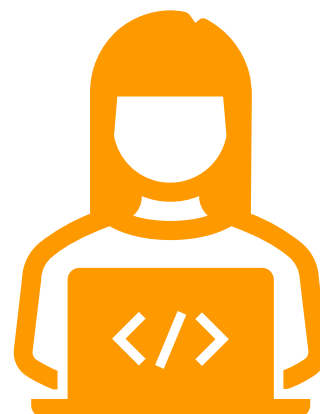
Ha anche adottato presidi organizzativi per la gestione dei progetti interni i quali, preliminarmente al loro kick off, sono oggetto di analisi volta a garantire l'applicazione dei principi "security by design" e "privacy by design".

Sempre per garantire un livello di sicurezza adeguato e un trattamento dei dati compliant con la regolamentazione, ha altresì formalizzato policy ad ampio respiro volte a mitigare i rischi introdotti dall'uso di dispositivi portatili, in particolare in caso di smart working. Esemplificando, il personale dipendente è vincolato all'uso dei soli dispositivi aziendali amministrati centralmente dall'organizzazione.

Risorse Umane

Le risorse umane di AGIC costituiscono un asset aziendale essenziale per la realizzazione e la buona riuscita dei progetti. Pertanto, è fondamentale che l'iter di selezione tenga in considerazione tutte le competenze che un buon professionista deve possedere, fra le quali vi è sicuramente la cyber awareness.

Pertanto, il processo di assunzione viene condotto sulla base di un iter definito che prevede, come primo step, una preliminare verifica di coerenza delle informazioni contenute nei curricula, per poi passare, in secondo luogo, alla valutazione dell'esperienza lavorativa e delle competenze emerse durante il colloquio, nonché, in ultima analisi e una volta formalizzata l'assunzione vera e propria, il coaching e la formazione sulle politiche e procedure interne.



All'esito del percorso di selezione sono formalizzate le responsabilità in materia di sicurezza delle informazioni, tramite apposite clausole contrattuali, il vincolo al rispetto del Codice Etico aziendale (e relative sanzioni disciplinari)

e la formalizzazione delle necessarie nomine (corredate da istruzioni comportamentali customizzate) conferite in considerazione del ruolo e delle mansioni delle varie risorse (es. nomina ex art. 29 GDPR, nomina ad Amministratore di Sistema, etc.). L'architettura documentale di cui sopra obbliga, in via generale, il personale alla riservatezza e alla non divulgazione dei dati e delle informazioni aziendali (anche dopo la cessazione del rapporto di lavoro), nonché al rispetto delle regole e dei codici adottati da AGIC in applicazione delle best practice di settore.

Al fine di mantenere un livello di competenze elevato, AGIC realizza diverse iniziative di formazione e aggiornamento in materia di sicurezza delle informazioni e protezione dei dati personali.

Inoltre, è stato implementato un processo di costante monitoraggio che prevede la partecipazione dei Project Manager nella valutazione delle competenze del personale.

Asset Management

AGIC considera i propri asset fisici tecnologici di estrema importanza per lo svolgimento delle attività aziendali, ragion per cui ha adottato misure organizzative e tecniche a supporto dell'identificazione, della corretta gestione e della sicura restituzione dei beni aziendali impiegati dai dipendenti (es. server, PC, smartphone). L'intero ciclo di vita dell'asset è dunque regolamentato e tracciato.

Esemplificando, i beni sono assegnati a un owner che ne garantisce la custodia e la protezione, impegnandosi ad applicare le misure di sicurezza adottate da AGIC. Inoltre, i beni e gli account possono essere assegnati esclusivamente dopo la presa in carico dell'asset, che avviene tramite sottoscrizione di un'apposita lettera di responsabilità. Infine, gli storage media sono oggetto di particolare attenzione in fase di dismissione, che prevede la cancellazione sicura dei dati ivi contenuti prima della loro riassegnazione.

Fra gli asset aziendali, inoltre, AGIC include anche la mole di dati e documenti generati durante lo svolgimento delle attività professionali. Trattandosi di un elemento critico per l'organizzazione, AGIC ha deciso di implementare misure di sicurezza adeguate al rischio rilevato.

Access control

La gestione degli accessi è un elemento essenziale per garantire un adeguato livello di sicurezza delle informazioni, oltre che, con riferimento ad alcuni ruoli aziendali di rilievo (es. Amministratore di Sistema), un requisito previsto dalla regolamentazione di settore (Garante per la Protezione dei Dati Personali).

In proposito, AGIC ha adottato delle procedure e delle policy per la gestione dell'intero ciclo di vita degli account e dei relativi accessi ai sistemi informatici, che fanno capo alla Funzione ICT.

I privilegi concessi agli utenti sono commisurati al loro ruolo e definiti nel rispetto del principio “need to know”, così come i diritti di visione dei documenti, in linea con la natura delle attività svolte dalle risorse. Per quanto riguarda i privilegi degli Amministratori di Sistema, invece, questi sono assegnati direttamente dalla Funzione ICT solo dopo la sottoscrizione della lettera di designazione.

Inoltre, AGIC ha adottato un sistema di gestione delle credenziali che prevede un'autenticazione segreta; tuttavia, per i sistemi integrati in Active Directory, a tutti gli utenti viene fornita una coppia di credenziali (ID individuale e password temporanea). In entrambi i casi, sono presenti presidi di Strong Authentication.

Infine, con l'intento di limitare eventuali operazioni non riconducibili all'autore, AGIC utilizza solo ID univoci, fatta eccezione per un numero limitato di account tecnici/di backup generici su sistemi specifici.

Crittografia

La crittografia consente di garantire con un certo grado di sicurezza un requisito di confidenzialità o riservatezza, ragion per cui risulta un elemento imprescindibile per la realizzazione di un adeguato sistema IT. In AGIC, la crittografia viene utilizzata per la protezione di informazioni diversificate fra loro che, all'esito di un processo valutativo, sono risultate particolarmente sensibili e/o meritevoli di extra tutela. Ad esempio, i controlli crittografici sono impiegati a livello di device, tramite l'implementazione di appositi tool informatici, per la protezione dei dati e delle informazioni ivi contenute, oppure per la protezione delle credenziali di autenticazione all'interno delle applicazioni e dei flussi da e per i Clienti.

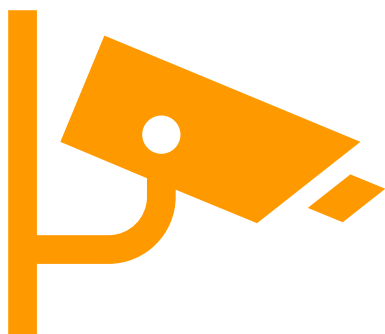
La solidità del controllo crittografico è valutabile, in particolar modo, dalla sicurezza della relativa chiave crittografica, indispensabile per la comprensione delle informazioni cifrate. Per questa ragione, AGIC, anche in questo caso, tutela le chiavi crittografiche in maniera diversificata, ferma

restando la presenza per tutti i certificati di una expiring date rinnovata periodicamente.

Sicurezza fisica e ambientale

I presidi che compongono un valido e sicuro sistema di protezione informatica possono essere classificati in differenti categorie, di cui quella tecnica è solo un esempio. Ciò deriva dal fatto che i rischi e le minacce verso i dati possono avere diversa natura e, pertanto, nascere da altrettante fonti, come l'ambiente circostante (es. luogo di residenza dei server aziendali) o eventi atmosferici dirompenti.

Pertanto, è essenziale implementare adeguati controlli a protezione delle informazioni trattate. In questo senso, AGIC, da un lato, ha organizzato gli uffici in modo da impedire che informazioni, dati personali o attività siano visibili/udibili dall'esterno e, dall'altro, ha adottato misure di sicurezza perimetrali idonee a proteggere le aree critiche per l'azienda e i propri Clienti.



In aggiunta, ha adottato apposite procedure per il controllo degli accessi fisici, tramite le quali i visitatori sono identificati, registrati e accompagnati all'interno dei locali aziendali. Inoltre, l'accesso ai locali sensibili di AGIC è limitato esclusivamente al personale autorizzato.

Fermo restando quanto sopra, è comunque sempre richiesto al personale interno di conformarsi alle politiche e alle procedure per la protezione delle apparecchiature incustodite come, fra le altre cose, le politiche del "clean desktop" e del "clean screen".

Particolare attenzione è stata anche riservata alle infrastrutture di supporto (es. elettricità, telecomunicazioni, aria condizionata, UPS, etc.), essenziali per l'erogazione dell'attività lavorativa, che sono controllate con regolarità (oltre che per necessità), così come tutte le infrastrutture che concorrono alla sicurezza dei locali aziendali.

Un trattamento simile è riservato anche ai canali di trasmissione elettrica (cavi), che sono protetti da intercettazioni, interferenze o danneggiamenti.

Operations Security

In termini di sicurezza delle operazioni, AGIC ha implementato un sistema funzionale all'adeguata gestione della mole di dati e informazioni trattati. Pertanto, in primo luogo, ha definito procedure e linee guida operative per la gestione delle principali attività di processo, costantemente aggiornate e rese disponibili al personale tramite condivisione sulla intranet aziendale.

A tal fine, AGIC monitora i cambiamenti che potrebbero impattare sulla struttura dell'organizzazione, anche dal punto di vista strettamente tecnico-informatico. La gestione dei software è, infatti, centralizzata e controllata dalla Funzione ICT.

Scendendo su di un piano tecnico, AGIC ha implementato presidi idonei a garantire, fra le altre cose, la separazione degli ambienti di sviluppo, test e lavoro, controlli per identificare, prevenire e gestire i malware e procedure di back up.

Esemplificando, nel primo caso, l'assegnazione di privilegi di accesso a sviluppatori e clienti è limitata ad ambienti di produzione e pre-produzione.

Per quanto riguarda il secondo caso, invece, è stato implementato un sistema di monitoring degli update per le nuove vulnerabilità. In proposito, inoltre, un ruolo centrale è anche svolto dai vulnerability assessment i quali, da un lato assicurano la rimozione di eventuali criticità e, dall'altro, consentono la revisione del design della soluzione informatica.

Ed ancora, è stata adottata una procedura di back up che individua i ruoli e le responsabilità, le tempistiche e la destinazione dei salvataggi.

Per garantire la completa tracciabilità delle operazioni compiute e, dunque, una maggiore certezza delle azioni intraprese sui dati trattati, AGIC ha implementato un tool di event logging - adeguatamente protetto - che registra gli accessi, le attività, gli errori e gli eventi di sicurezza verificatisi.



Communications Security

I canali di comunicazione, a qualsiasi livello, all'interno di un'organizzazione sono un elemento essenziale per garantire flussi informativi adeguati e, dunque, una sana circolazione di dati che consentano alla struttura di

funzionare agilmente. All'interno di una realtà come AGIC, la tecnologia viene applicata anche ai presenti canali in maniera massiccia, ragion per cui è necessario garantire, anche in questo caso, sicurezza e affidabilità dei servizi.



Per questa ragione, AGIC affida alla Funzione ICT la gestione di tutte le reti di comunicazione, che sono peraltro adeguatamente protette da accessi illeciti o attacchi esterni tramite procedure di accesso, specifici software e soluzioni ingegneristiche (es. le reti sono segregate in più domini tramite VLAN separate in modo tale da avere una rete interna e un'altra per gli ospiti). Inoltre, considerato che i servizi forniti da terzi (es. internet) svolgono un ruolo

nevralgico per il funzionamento dei canali informativi, SLA e requisiti di sicurezza sono formalmente concordati negli accordi con i fornitori.

Dal punto di vista organizzativo, infine, AGIC stabilisce regole e procedure per garantire uno scambio sicuro delle informazioni, sia al proprio interno sia all'esterno, mettendo a disposizione piattaforme di condivisione controllate (es. SharePoint, VPN, Office 365).

System Acquisition, Sviluppo e Manutenzione

AGIC applica metodologie sicure per lo sviluppo di soluzioni informatiche. Infatti, identifica i requisiti per la sicurezza delle informazioni e la protezione dei dati personali in fase di progettazione o revisione dei prodotti, in applicazione dei principi di “privacy by design” e “security by design”.

In aggiunta, da un punto di vista tecnico, AGIC provvede a proteggere i servizi applicativi tramite protocolli sicuri “at rest” e meccanismi di crittografia e autenticazione dei dati in transito, unitamente a sistemi di user-id e MFA personali. Inoltre, la Virtual Private Network è utilizzata per la connessione remota ad ambienti di sviluppo e repository software.

In aggiunta, per meglio garantire la sicurezza degli ambienti informatici, la modifica dei software è limitata alle integrazioni necessarie (es. evoluzioni normative, correzione di bug, sviluppo di nuove funzionalità richieste dalle aziende clienti) e viene verificata tramite attività di test. In ogni caso, l'accesso agli ambienti di sviluppo avviene tramite Remote Desktop Protocol ed è limitato agli indirizzi di rete delle sedi AGIC.

Come anticipato, le attività di modifica sono oggetto di appositi test volti a verificare la funzionalità dei sistemi di sicurezza implementati durante lo sviluppo, il cui esito positivo risulta essenziale per il go-live del prodotto.

Inoltre, per l'esecuzione dei test sulla sicurezza vengono messe a disposizione del cliente librerie con dati non reali e/o repliche degli ambienti di produzione.

Gestione dei fornitori

AGIC si relaziona con fornitori accuratamente individuati secondo un processo di selezione che comprende, fra gli altri, controlli volti alla verifica di adeguati presidi in ambito IT e data protection attraverso il ricorso a checklist improntate alle best practice di settore. Ne consegue che i contratti sono integrati con specifiche clausole funzionali a garantire la sicurezza delle informazioni e, non meno importante, la protezione dei dati personali (es. NDA, nomina a Responsabile del Trattamento ai sensi dell'art. 28 GDPR).

Inoltre, al fine di verificare che gli accordi siano effettivamente rispettati, AGIC ha sviluppato procedure per monitorare i servizi erogati dai fornitori critici, essenziali per lo svolgimento dell'attività aziendale. Pertanto, all'interno dei contratti di fornitura, è espressamente prevista a beneficio di AGIC la possibilità di svolgere audit e controlli sull'operato, lato IT e privacy, del fornitore stesso.

Rimanendo in tema di controllo del fornitore terzo, eventuali cambiamenti alle condizioni di erogazione del servizio da parte del fornitore sono costantemente monitorati dall'organizzazione la quale, a seconda dei casi, può prevedere una propria specifica approvazione o, in alternativa, una preventiva valutazione dei rischi a carico del terzo.

Gestione degli incidenti

L'attuale panorama informatico globale presenta gravi rischi e criticità - basti pensare a virus e malware - che possono seriamente compromettere la stabilità di una struttura informatica e la produttività di un'organizzazione se non previamente valutati o in assenza di adeguate contromisure preventive.

Per questa ragione, AGIC ha stabilito un set di responsabilità e adottato apposite procedure per garantire una risposta rapida, efficace e ordinata agli incidenti relativi alla sicurezza delle informazioni in ambienti Customer e Corporate. Infatti, eventuali incidenti o presunte minacce sono gestiti secondo un processo strutturato in fasi, a partire dalla segnalazione fino alla chiusura

dell'evento. Inoltre, nel caso in cui l'evento colpisca informazioni e dati personali del Cliente, troverà applicazione l'apposita procedura per la gestione dei Data Breach.

Diversi sono i canali tramite i quali è possibile segnalare gli episodi (es. help desk, e-mail): il personale esperto è, in primo luogo, chiamato a valutarli ed eventualmente a classificarli come critici e, in secondo luogo, tenuto a registrarli tramite appositi tool di supporto.

Le informazioni così raccolte e strutturate saranno acquisite dall'organizzazione e verranno impiegate dalla Funzione ICT per ridurre la probabilità o l'impatto di incidenti futuri.

Business Continuity Management

Rimanendo in tema di rischi che possono compromettere la stabilità di una struttura informatica, è possibile che un episodio di minaccia possa compromettere la corretta erogazione dei servizi, con un conseguente considerevole impatto sul business societario.

Per questa ragione, AGIC ha condotto una Business Impact Analysis e, successivamente, ha formalizzato un Business Continuity Plan che contempla diversi scenari di minaccia in grado di incidere sulla disponibilità dei più importanti servizi al Cliente.

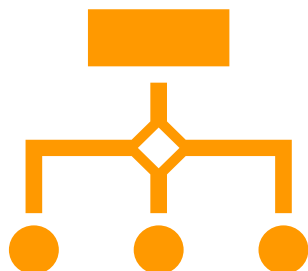
In particolare, il Business Continuity Plan comprende strategie e soluzioni per garantire la continuità dei processi di business ed è funzionale a garantire la sicurezza delle informazioni e la protezione dei dati personali in condizioni avverse, anche attraverso una politica di ridondanza delle strutture per l'elaborazione delle informazioni.

Privacy by design & Privacy by default

AGIC, in conformità a quanto previsto dal GDPR, ha formalizzato un'apposita policy funzionale a recepire internamente i principi di "privacy by design" e "privacy by default".

Il documento ha lo scopo di garantire che ogni progetto, fin dalla sua fase iniziale, sia strutturato in modo da proteggere i dati personali e rispettare i diritti degli interessati, e prevede una chiara distinzione tra gli adempimenti in capo ad AGIC quale Titolare del trattamento (es. rilascio dell'informativa sul trattamento dei dati personali, acquisizione di eventuali consensi, etc.) e quelli

invece posti in essere nel ruolo di Responsabile del trattamento (es. compilazione, per la parte di propria competenza, della nomina, verifica delle istruzioni ricevute dal Titolare del trattamento, nomina del personale con mansioni da Amministratore di Sistema, verifica di eventuali trasferimenti extra UE, etc.).



A ciò si accompagnano puntuali indicazioni operative per ciascuna figura coinvolta nel processo sopra descritto. In ogni caso, per ogni dubbio o necessità di supporto, le figure aziendali possono rivolgersi al team dedicato competente in

materia.

Così facendo, AGIC intende non solo garantire la conformità normativa, ma promuovere una cultura aziendale orientata alla responsabilità, alla trasparenza e alla protezione dei dati personali, rafforzando la fiducia dei clienti e degli stakeholder nei confronti di AGIC.

Principali adempimenti GDPR

AGIC ha formalizzato una procedura dedicata alla gestione dei principali adempimenti in ambito privacy e data protection. Al suo interno, infatti, sono individuati ruoli, responsabilità e step procedurali funzionali a rispondere agli obblighi normativi in capo alla stessa in applicazione della normativa di settore.

Esemplificando, è affrontato il tema delle informative privacy di modo che ogni trattamento di dati personali sia preceduto dalla comunicazione trasparente delle finalità e delle modalità del trattamento agli interessati. Qualora AGIC intenda trattare i dati per finalità ulteriori rispetto a quelle originarie, provvederà altresì a fornire preventivamente agli interessati tutte le informazioni necessarie relative alla nuova finalità.

Ed ancora, AGIC assicura che ogni attività di trattamento venga svolta in maniera conforme alla disciplina di settore mediante atti di nomina diversificati a seconda del destinatario (es. autorizzazioni al trattamento ex art. 29 GDPR, nomina a responsabile del trattamento, ex art. 28 GDPR). Visto il proprio core business, inoltre, ha formalizzato una solida procedura anche per la nomina e la gestione degli Amministratori di Sistema (interni ed esterni rispetto all'organizzazione) che si fonda su di una matrice di responsabilità coerente con i principi della segregation of duties e del least privilege.

Registro dei Trattamenti

AGIC ha definito una procedura dedicata alla predisposizione, all'aggiornamento e alla gestione del Registro dei Trattamenti, finalizzata a censire in modo sistematico tutte le attività di trattamento svolte dall'organizzazione.

Il Registro include i trattamenti effettuati in qualità di Titolare del trattamento e di Responsabile del trattamento nell'ambito dei servizi erogati ai Clienti.

La procedura individua un supporto specialistico interno incaricato della gestione operativa del Registro, definendo le informazioni essenziali da documentare in conformità alle disposizioni normative e alle best practice di settore.

Il Registro consente di avere una visione chiara e strutturata dei dati personali trattati, delle finalità, delle categorie di interessati e destinatari, nonché delle misure di sicurezza adottate. Pertanto, una procedura formalizzata per il suo aggiornamento assicura che le informazioni siano sempre corrette e complete, soprattutto in contesti dinamici in cui i trattamenti possono variare nel tempo, facilitando l'intervento tempestivo in caso di ispezioni da parte delle autorità di controllo o di richieste da parte degli interessati e rafforzando la trasparenza e la governance aziendale in materia di privacy.

Trasferimento dei dati extra UE

In aggiunta a quanto sopra, qualora si renda necessario il trasferimento di dati personali verso Paesi terzi, AGIC ha formalizzato un processo coerente con la normativa di settore e le best practice applicabili.

In primo luogo, infatti, è individuato uno degli strumenti applicabili ai sensi dell'art. 46 GDPR, al quale segue una valutazione d'impatto specifica (Transfer Impact Assessment - TIA) secondo template sviluppati internamente.

Tale valutazione è finalizzata a garantire che il trasferimento non comprometta le garanzie fondamentali, i diritti degli interessati e la protezione dei dati, assicurando la piena conformità alle normative europee e internazionali.

Data Retention

AGIC, in conformità alle normative europee e internazionali in materia di sicurezza delle informazioni e protezione dei dati personali, ha adottato una

policy specifica di Data Retention quale espressione concreta del proprio impegno verso la tutela dei dati personali, delle informazioni aziendali e dei dati dei clienti.

La policy stabilisce che ogni dato raccolto venga gestito con la massima attenzione, conservato esclusivamente per il tempo strettamente necessario e trattato secondo criteri di sicurezza, trasparenza e integrità. Inoltre, prevede che i dati siano archiviati in ambienti sicuri - fisici o digitali - e che, una volta cessata la finalità del trattamento, vengano cancellati o anonimizzati, anche su richiesta dell'interessato.

Considerati i potenziali coinvolgimenti di terze parti nel perseguimento delle finalità di trattamento, AGIC garantisce altresì che tutti i soggetti coinvolti nel trattamento dei dati, inclusi eventuali fornitori esterni, siano vincolati da istruzioni operative dettagliate in merito ai tempi e alle modalità di conservazione.

Questo approccio non solo assicura il rispetto dei diritti degli interessati, ma promuove la trasparenza e la responsabilità come valori distintivi dell'organizzazione, rafforzando la fiducia dei clienti e dimostrando l'attenzione costante di AGIC alla compliance normativa e alla gestione etica delle informazioni.



Diritti degli interessati

AGIC ha formalizzato una procedura dedicata alla gestione delle richieste degli interessati relative all'accesso, alla modifica, alla revoca o all'opposizione al trattamento dei dati personali. Tali richieste possono essere inoltrate attraverso i canali ufficiali predisposti dall'organizzazione, che garantiscono tracciabilità, sicurezza e tempestività nella gestione, e prevedono - ove agisca quale Responsabile del trattamento - un preventivo coinvolgimento del Titolare, come da nomina ricevuta.



Per assicurare un trattamento conforme e trasparente, AGIC ha individuato un team interno di esperti incaricato di valutare la legittimità delle richieste ricevute. Qualora necessario, il team procede con le opportune comunicazioni e azioni operative, coinvolgendo le funzioni aziendali competenti, previa verifica dell'identità del richiedente.

In sintesi, attraverso un processo strutturato e controllato, AGIC garantisce la corretta gestione delle richieste degli interessati, il coinvolgimento delle parti eventualmente interessate - inclusi eventuali sub-responsabili del trattamento - e la verifica dell'effettiva evasione delle istanze ricevute. Questo approccio consente di offrire ai clienti e agli stakeholder la massima garanzia di rispetto dei diritti privacy, assicurando al contempo una piena collaborazione con le autorità competenti.

Nomina di un Data Protection Officer (DPO)

AGIC ha designato un Data Protection Officer (DPO) quale referente principale dell'organizzazione in merito alle tematiche privacy e data protection.

Il DPO, supportato da un team dedicato, gestisce le interazioni con le autorità competenti, inclusi il Garante per la Protezione dei Dati Personali, l'Agenzia per la Cybersicurezza Nazionale, la Guardia di Finanza, la Polizia di Stato e altre autorità giudiziarie o amministrative, anche in occasione di ispezioni o richieste formali.

In aggiunta, si fa garante delle responsabilità attribuite dal GDPR, in linea con le mansioni e i compiti attribuiti dalla normativa di settore.

Risk assessment e valutazione di impatto

AGIC, al fine di garantire la massima protezione dei dati personali trattati e in conformità alle normative vigenti in materia di privacy e data protection, ha definito e implementato una procedura strutturata per l'analisi e la valutazione dei rischi privacy e data protection.

Tale procedura prevede il coinvolgimento di un team multidisciplinare di esperti e l'adozione di una metodologia dedicata (integrata in quella a fini IT), volta a garantire un approccio sistematico e rigoroso.

In linea generale, AGIC procede in primo luogo alla determinazione del rischio inerente (in termini di probabilità per impatto), per tale intendendosi il livello di esposizione al rischio in assenza di eventuali presidi di sicurezza; in un secondo momento viene eseguita una valutazione dei presidi e dei controlli in essere implementati dall'organizzazione - funzionale a valutarne l'efficacia e l'adequatezza - che, da ultimo, porta alla determinazione di un valore aggregato di esposizione al rischio noto come rischio residuo.

Fatto ciò, i risultati dell'assessment sono confrontati con il risk appetite definito internamente e, ove necessario, si procede con l'implementazione di misure di mitigazione customizzate sulla natura del rischio (azioni correttive o preventive), rafforzando la governance aziendale, migliorando la resilienza operativa e tutelando in modo proattivo la reputazione dell'organizzazione.

In aggiunta a quanto sopra, sono portate avanti anche ulteriori analisi (note come "valutazioni di impatto") finalizzate a verificare l'impatto che un determinato trattamento può avere sui diritti e sulle libertà delle persone fisiche.

Il processo si articola in più fasi e contempla, in prima istanza, un'analisi preliminare dell'attività di trattamento, funzionale a verificare l'effettiva presenza di informazioni riconducibili a persone fisiche individuate e/o individuabili (c.d. PIA). Solo in un secondo momento, in caso di esito positivo, si procede con un'analisi più approfondita che si sofferma, fra le altre cose, sul contesto normativo di riferimento, sui presupposti di liceità, sulle modalità di



esercizio dei diritti da parte degli interessati nel contesto in esame e, più in generale, su ogni aspetto che concorre alla definizione dell'esposizione al rischio (c.d. DPIA).

In aggiunta, AGIC si è dotata di strumenti funzionali a supportarla in caso di trattamenti basati su propri interessi legittimi (c.d. LIA) o di trasferimenti extra UE (c.d. TIA).

Attraverso questa procedura, AGIC assicura che ogni trattamento di dati personali sia sottoposto a un processo di valutazione e gestione del rischio conforme alle best practice internazionali e alla normativa europea, rafforzando la fiducia degli stakeholder e promuovendo una cultura aziendale orientata alla responsabilità e alla protezione dei dati.

Gestione dei data breach

AGIC ha definito un'apposita procedura di gestione dei data breach che prevede la compartecipazione di diverse competenze interne.

Pertanto, una volta ricevuta (o rilevata) una potenziale segnalazione relativa a una violazione dei dati personali, si procede con la classificazione dell'evento secondo la metodologia interna, per poi procedere - in un secondo momento - all'attivazione di step procedurali predefiniti attribuiti ad altrettante figure

chiave, responsabili dell'intervento e del rispetto delle tempistiche per la notifica alle autorità competenti (ove necessaria).

Ogni fase del processo deve essere formalmente documentata, con particolare attenzione alle azioni correttive e alle misure di ripristino.

Al termine del processo è verificata l'efficacia delle soluzioni adottate e, se necessario, sono implementate ulteriori misure preventive per ridurre la probabilità di ricorrenza.

Presidi organizzativi

In applicazione di quanto sopra, AGIC ha formalizzato e implementato presidi organizzativi (es. procedure operative, policy, linee guida, etc.) attinenti ai seguenti ambiti:

- Cyber threat intelligence
- Utilizzo delle risorse informatiche da parte del personale (anche in caso di smart working)
- Classificazione delle informazioni
- Crittografia e gestione delle chiavi e dei controlli
- Gestione delle password
- Gestione degli asset informatici
- Access Rights Management
- Incident Management
- Back up e restore dei dati aziendali
- Gestione delle vulnerabilità
- Log Management
- Continuità operativa
- Controllo degli accessi alle sedi aziendali e sicurezza fisica
- Data retention
- Gestione della privacy e del trattamento dei dati personali (e relativo framework documentale)
- Sviluppo sicuro del software e AMS
- Privacy by design & privacy by default
- Gestione dei metadati di posta elettronica
- Gestione dei data breach

IT & GDPR SECURITY MEASURES

Summary of security measures

Release 0.1 del 01/09/2026

AGIC

Via di Castel Giubileo, 62
00138 - Rome

+39 06 888851
info@agic.it

AGIC Technology IT security

Introduction

AGIC is a technology provider that implements solutions and projects for organizations based on Microsoft technologies. Business Applications (ERP and CRM), Data Analytics, Artificial Intelligence, Cybersecurity, Cloud Platform, IoT, Mobile, Machine Learning, Web, App, Portal & Collaboration are just some of the platforms on which it bases its solutions. Experienced Governance, Risk and Compliance professionals work alongside technology specialists to accompany the release of solutions in compliance with IT security, Artificial Intelligence legislation and GDPR.

AGIC is active in the front line to protect the confidentiality, integrity and availability of information, data and news relating to its stakeholders, committing itself to ensuring that they are safeguarded from any unlawful use.

For this reason, it has obtained the recognition of the international certifications ISO/IEC 27001:2022 and ISO/IEC 27701:2019.

Information Security Policies

AGIC defines, approves and communicates procedures, policies and guidelines for IT security and personal data protection within its organization in order to regulate activities and provide valid methodological support to the resources employed.

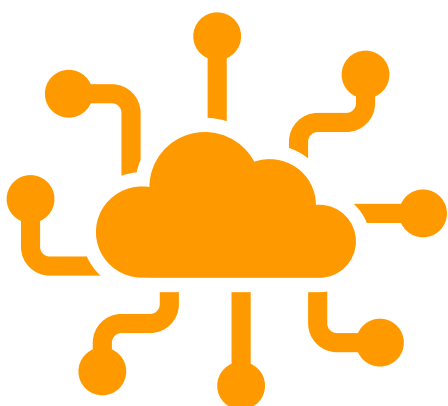
Considering the growing technological development and the rapid evolution of threats, procedures, policies and guidelines are periodically reviewed and supplemented in order to make them adequate and in step with the times. They are also modified whenever it is necessary to change the organization or in the event of significant changes in the market, laws or sector regulations.

By way of example, specific procedures have been adopted to regulate the process of: back-up, incident management, vulnerability management and business continuity, as well as the adaptation of the various services and products offered to European legislation on privacy and personal data protection.

Organization of the Information Security System

AGIC defines roles and responsibilities relating to the structure of the Information Security System and the organization (e.g. ICT Manager, etc.), taking care to make use of competent and trained resources on the subject. In fact, it is committed to ensuring that staff keep their knowledge up to date by participating in seminars and workshops, among other things.

In addition, in the context of the most relevant IT processes, it pays particular attention to the separation of conflicting tasks and areas of responsibility so as to reduce the possibility of misuse, unauthorized or unintentional modification of the organization's assets.



For privacy and data protection purposes, AGIC regulates relations with its employees and with third parties outside the organization (e.g. suppliers, etc.), through specific appointments issued in compliance with sector regulations (e.g. appointment as Data Processor pursuant to Article 28 of the GDPR).

It has also adopted organizational safeguards for the management of internal projects which, prior

to their kick-off, are the subject of analysis aimed at ensuring the application of the principles of "security by design" and "privacy by design".

Again to ensure an adequate level of security and data processing compliant with regulations, it has also formalized wide-ranging policies aimed at mitigating the risks introduced by the use of portable devices, particularly in the case of smart working. By way of example, employees are bound to use only the company devices centrally administered by the organization.

Human resources

AGIC's human resources are an essential corporate asset for the implementation and success of projects. Therefore, it is essential that the selection process takes into account all the skills that a good professional must possess, among which there is certainly cyber awareness.

Therefore, the recruitment process is conducted on the basis of a defined process that includes, as a first step, a preliminary verification of the consistency of the information contained in the CVs, and then moves on, secondly, to the evaluation of the work experience and skills that emerged during the interview, as well as, in the final analysis and once the actual recruitment has been formalized, coaching and training on internal policies and procedures.

At the end of the selection process, the responsibilities in the field of information security are formalized, through specific contractual clauses, the obligation to comply with the company Code of Ethics (and related disciplinary sanctions) and the formalization of the necessary appointments (accompanied by customized behavioral instructions) conferred in consideration of the role and duties of the various resources (e.g. appointment pursuant to Article 29 of the GDPR, appointment as System Administrator, etc.). The above document architecture generally obliges personnel to confidentiality and non-disclosure of company data and information (even after the termination of the employment relationship) as well as to comply with the rules and codes adopted by AGIC in application of the best practices in the sector.

In order to maintain a high level of skills, AGIC carries out various training and refresher courses on information security and personal data protection.

In addition, a constant monitoring process has been implemented that sees the participation of Project Managers in the assessment of staff skills.

Asset Management

AGIC considers its physical technological assets to be of extreme importance for the performance of business activities, which is why it has adopted organizational and technical measures to support the identification, correct management and safe return of company assets used by employees (e.g. servers, PCs, smartphones). The entire life cycle of the asset is therefore regulated and tracked.



By way of example, the assets are assigned to an owner who guarantees their custody and protection by committing to apply the security measures adopted by AGIC. In addition, assets and accounts can only be assigned after the asset has been taken over, which takes place by signing a special letter of responsibility. Finally, storage media are the subject of attention during the decommissioning phase, which involves a general deletion of the data contained therein in

security before their reassignment.

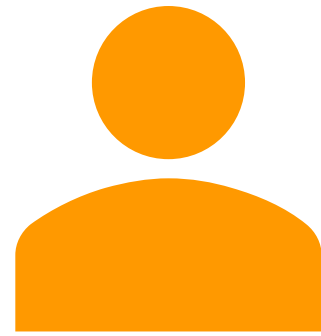
Furthermore, AGIC also considers among its assets the data and documents generated during the performance of professional activities. As a critical element of the organization, it has decided to implement security measures appropriate to the risk detected.

Access control

Access management is an essential element to ensure an adequate level of information security, as well as, with reference to some important company roles (e.g. System Administrator), a requirement provided for by sector regulations (Italian Data Protection Authority).

In this regard, AGIC has adopted procedures and policies for the management of the entire life cycle of accounts and related access to IT systems, which are part of the ICT Function.

The privileges granted to users are commensurate with their role and defined in accordance with the "need to know" principle, as are the rights to view documents, in line with the nature of the activities carried out by the resources. As for the privileges of the System Administrators, however, these are assigned directly by the ICT Function only after signing the designation letter.



In addition, AGIC has adopted a credential management system that provides for secret authentication; however, for Active Directory-integrated systems, all users are provided with a credential pair (individual ID and temporary password). In both cases, there are Strong Authentication safeguards.

Finally, with the intent of limiting any operations that cannot be attributed to a specific author, AGIC uses only unique IDs, excluding a limited number of generic technical/backup accounts on specific systems.

Cryptography

Cryptography makes it possible to guarantee a requirement of confidentiality or secrecy with a certain degree of security, which is why it is an essential element for the creation of an adequate IT system. At AGIC, cryptography is used to protect diversified information which, at the end of an evaluation process, is found to be particularly sensitive and/or deserving of extra protection. For example, cryptographic controls are used at the device level, through the implementation of special IT tools, for the protection of data and information contained therein, or for the protection of authentication credentials within applications and flows to and from customers.

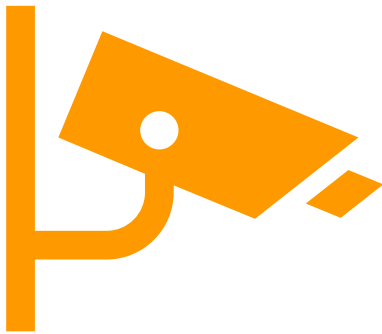
The solidity of the cryptographic control can be assessed, in particular, by the security of the relative cryptographic key, which is essential for understanding the encrypted information. For this reason, AGIC, also in this case, protects cryptographic software in a diversified way, without prejudice to the presence of an expiry date periodically renewed for all certificates.

Physical and environmental security

The safeguards that make up a valid and secure IT protection system can be classified into different categories, of which the technical one is just one

example. This derives from the fact that risks and threats to data can be of different nature, and therefore arise from as many sources, such as the surrounding environment (e.g. place of residence of company servers) or disruptive weather events.

Therefore, it is essential to implement appropriate controls to protect the information processed. In this sense, AGIC, on the one hand, has organized the offices in such a way as to prevent information, personal data or activities from being visible/audible from the outside and, on the other hand, has adopted perimeter security measures suitable for protecting critical areas for the company and its customers.



In addition, it has adopted special procedures for the control of physical access, through which visitors are identified, registered and accompanied within the company premises. In addition, access to AGIC's sensitive premises is restricted to authorized personnel only.

Notwithstanding the above, internal staff are always required to comply with policies and procedures for the protection of unattended equipment such as, among other things, the "clean desktop" and "clean screen" policies.

Particular attention has also been paid to support infrastructures (e.g. electricity, telecommunications, air conditioning, UPS, etc.), essential for the provision of work activities, which are checked regularly (as well as out of necessity), as well as all the infrastructures that contribute to the security of company premises.

A similar treatment is also reserved for electrical transmission channels (cables) that are protected against eavesdropping, interference or damage.

Operations Security

In terms of operations security, AGIC has implemented an operations security system functional to the adequate management of the amount of data and information processed. Therefore, first of all, it has defined procedures and operational guidelines for the management of the main process activities, constantly updated and made available to personnel through sharing on the company intranet.

To this end, AGIC monitors changes that could impact the structure of the organization, also from a strictly technical-IT point of view. In fact, software management is centrally managed and controlled by the ICT Function.

Going down to a technical level, AGIC has implemented suitable safeguards to ensure, among other things, the separation of development, test and work environments, controls to identify, prevent and manage malware and backup procedures.

To exemplify, in the first case, the assignment of access privileges to developers and customers is limited to production and pre-production environments.

As for the second case, however, an update monitoring system for new vulnerabilities has been implemented. In this regard, moreover, a central role is also played by vulnerability assessments which, on the one hand, ensure the removal of any critical issues and, on the other, allow the revision of the design of the IT solution.

And again, a back-up procedure has been adopted that identifies the roles and responsibilities, the timing and the destination of the backups.

To ensure complete traceability of the operations carried out, and therefore greater certainty of the actions taken on the data processed, AGIC has implemented an event logging tool - adequately protected - that records accesses, activities, errors and security events that have occurred.



Communications Security

Communication channels, at any level, within an organization are an essential element to ensure adequate information flows and, therefore, a healthy circulation of data that allows the structure to function agilely. Within an organization such as AGIC, technology is also applied to these channels in a massive way, which is why it is necessary to guarantee, also in this case, the security and reliability of the services.



For this reason, AGIC entrusts the ICT Function with the management of all communication networks, which are also adequately protected from illicit access or external attacks through access procedures, specific software and engineering solutions (e.g. the networks are segregated into several domains through separate VLANs so as to have an internal network and another for guests). Furthermore, considering that services provided by third parties (e.g. internet) play a crucial role for the functioning of information channels, SLAs and security requirements are formally agreed in the agreements with the suppliers.

Finally, from an organizational point of view, AGIC establishes rules and procedures to ensure a secure exchange of information, both inside and outside it, by providing controlled sharing platforms (e.g. SharePoint, VPN, Office 365).

System Acquisition, Development and Maintenance

AGIC applies secure methodologies for the development of IT solutions. In fact, it identifies the requirements for information security and the protection of personal data during the design or review of products, in application of the principles of "privacy by design" and "security by design".

In addition, from a technical point of view, AGIC provides protection of application services through secure "at-rest" protocols and encryption and authentication mechanisms for data in transit, together with personal user-id and MFA systems. In addition, the Virtual Private Network is used for remote connection to development environments and software repositories.

In addition, to better guarantee the security of IT environments, software modification is limited to the necessary integrations (e.g. regulatory developments, bug fixes, development of new features requested by client companies) and is verified through testing activities. In any case, access to development environments takes place via Remote Desktop Protocol, and is limited to the network addresses of AGIC offices.

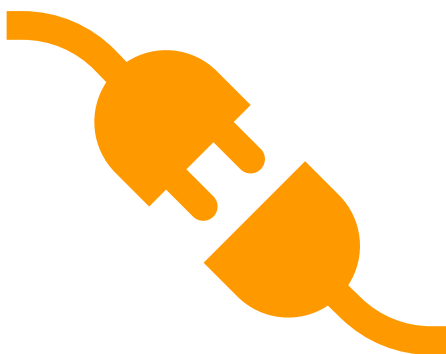
As anticipated, the modification activities are subject to special tests aimed at verifying the functionality of the security systems implemented during

development, the positive outcome of which is essential for the go-live of the product.

In addition, libraries with non-real data and/or replicas of production environments are made available to the customer for the execution of security tests.

Supplier management

AGIC deals with suppliers carefully identified according to a selection process that includes, among others, controls aimed at verifying adequate IT and data protection safeguards through the use of checklists based on the best practices in the sector. As a result, the contracts are integrated with specific clauses functional to ensure the security of information and, last but not least, the protection of personal data (e.g. NDA, appointment as Data Processor pursuant to Article 28 of the GDPR).



In addition, in order to verify that the agreements are actually respected, AGIC has developed procedures to monitor the services provided by critical suppliers essential for the performance of the company's business. Therefore, within the supply contracts, the possibility of carrying out audits and controls on the work, on the IT and privacy side, of the supplier itself is expressly provided for the benefit of AGIC.

Remaining on the subject of the control of the third-party supplier, any changes to the conditions of service provision by the supplier are constantly monitored by the organization which, depending on the case, may provide for its own specific approval or, alternatively, a prior assessment of the risks borne by the third party.

Incident Management

The current global IT landscape presents serious risks and critical issues - just think of viruses and malware - which can seriously compromise the stability of an IT structure and the productivity of an organization if not previously evaluated or in the absence of adequate preventive countermeasures.

For this reason, AGIC has established a set of responsibilities and adopted appropriate procedures to ensure a rapid, effective and orderly response to incidents related to information security in Customer and Corporate environments. In fact, any incidents or alleged threats are managed according to a process structured in phases, starting from the report to the closure of the event. In addition, in the event that the event affects the Customer's personal information and data, the appropriate procedure for the management of Data Breaches will apply.



There are several channels through which it is possible to report episodes (e.g. help desk, e-mail) that expert personnel are, firstly, called upon to evaluate and possibly classify as critical and, secondly, required to record through special support tools.

The information collected and structured in this way will be acquired by the organization and will be used by the ICT Function to reduce the probability or impact of future incidents.

Business Continuity Management

Remaining on the subject of risks that can compromise the stability of an IT structure, it is possible that a threat episode can compromise the correct provision of services, with a consequent considerable impact on the company's business.

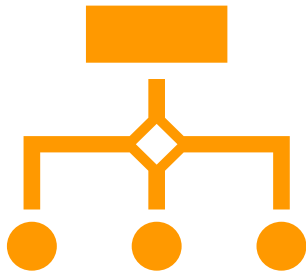
For this reason, AGIC has conducted a Business Impact Analysis and, subsequently, drawn up a Business Continuity Plan that contemplates different threat scenarios capable of affecting the availability of the most important services to the Customer.

In particular, the Business Continuity Plan includes strategies and solutions to ensure the continuity of business processes and is functional to ensure the security of information and the protection of personal data in adverse conditions, also through a policy of redundancy of information processing structures.

Privacy by design & Privacy by default

AGIC, in compliance with the provisions of the GDPR, has formalized a specific policy functional to internally implement the principles of "privacy by design" and "privacy by default".

The document aims to ensure that each project, from its initial phase, is structured in such a way as to protect personal data and respect the rights of data subjects, and provides for a clear distinction between the obligations of



AGIC as Data Controller (e.g. release of information on the processing of personal data, acquisition of any consents, etc.) and those instead put in place in the role of Data Processor (e.g. compilation, for the part of their competence, of the appointment, verification of the instructions received from the Data Controller, appointment of personnel with System Administrator duties, verification of any extra-EU transfers, etc.).

This is accompanied by precise operational indications for each figure involved in the process described above. In any case, for any doubts or support needs, company figures can contact the dedicated team competent in the matter.

In doing so, AGIC intends not only to ensure regulatory compliance, but to promote a corporate culture oriented towards accountability, transparency and the protection of personal data, strengthening the trust of customers and stakeholders in AGIC.



Main GDPR obligations

AGIC has formalized a procedure dedicated to the management of the main obligations in the field of privacy and data protection. In fact, it identifies roles, responsibilities and procedural steps functional to meeting its regulatory obligations in application of the sector regulations.

By way of example, the issue of privacy policies is addressed so that any processing of personal data is preceded by transparent communication of the purposes and methods of processing to the data subjects. If AGIC intends to process the data for purposes other than the original ones, it will also provide the data subjects with all the necessary information relating to the new purpose in advance.

Furthermore, AGIC ensures that each processing activity is carried out in accordance with the sector regulations through diversified acts of appointment depending on the recipient (e.g. authorizations for processing pursuant to Article 29 of the GDPR, appointment as Data Processor pursuant to Article 28 of the GDPR). Furthermore, given its core business, it has formalized a solid procedure also for the appointment and management of System Administrators (internal and external to the organization), which is based on a matrix of responsibilities consistent with the principles of segregation of duties and least privilege.

Register of Processing and Data Transfer

AGIC has defined a procedure dedicated to the preparation, updating and management of the Register of Processing, aimed at systematically surveying all the processing activities carried out by the organization.

The Register includes the processing carried out in its capacity as Data Controller and Data Processor in the context of the services provided to Customers.

The procedure identifies an internal specialist support in charge of the operational management of the Register, defining the essential information to be documented in accordance with regulatory provisions and industry best practices.

The register allows for a clear and structured view of the personal data processed, the purposes, the categories of data subjects and recipients, as well as the security measures adopted. Therefore, a formalized procedure for its updating ensures that the information is always correct and complete, especially in dynamic contexts where processing may vary over time, facilitating timely intervention in the event of inspections by supervisory authorities or requests from data subjects and strengthening transparency and corporate governance in the field of privacy.

Transfer of data outside the EU

In addition to the above, if it is necessary to transfer personal data to third countries, AGIC has formalized a process consistent with the sector regulations and applicable best practices.

Firstly, one of the instruments applicable pursuant to Article 46 of the GDPR is adopted, which is followed by a specific impact assessment (Transfer Impact Assessment - TIA) carried out according to internally developed templates.

This assessment is aimed at ensuring that the transfer does not compromise fundamental safeguards, data subject rights and data protection, ensuring full compliance with European and international regulations.

Data Retention

AGIC, in compliance with European and international regulations on information security and personal data protection, has adopted a specific Data Retention policy as a concrete expression of its commitment to the protection of personal data, corporate information and customer data.

The policy establishes that any data collected is handled with the utmost care, kept only for the time strictly necessary and treated according to criteria of security, transparency and integrity. In addition, it provides that the data are stored in secure environments - physical or digital - and that, once the purpose of the processing has ceased, they are deleted or anonymized, also at the request of the data subject.



Considering the potential involvement of third parties in the pursuit of the processing purposes, AGIC also ensures that all parties involved in the processing of data, including any external suppliers, are bound by detailed operating instructions regarding the times and methods of storage.

This approach not only ensures respect for the rights of data subjects, but promotes transparency and accountability as distinctive values of the organization, strengthening customer trust and demonstrating AGIC's constant attention to regulatory compliance and ethical information management.

Rights of the data subjects

AGIC has formalized a procedure dedicated to the management of requests from data subjects relating to access, modification, revocation or opposition to the processing of personal data. These requests can be forwarded through the official channels set up by the organization, which guarantee traceability, security and timeliness in management, and provide - where it acts as Data

Processor - a prior involvement of the Data Controller, as per the appointment received.

To ensure compliant and transparent processing, AGIC has identified an internal team of experts in charge of assessing the legitimacy of the requests received. If necessary, the team proceeds with the appropriate communications and operational actions, involving the relevant company functions, after verifying the identity of the applicant.

In summary, through a structured and controlled process, AGIC guarantees the correct management of requests from data subjects, the involvement of any interested parties - including any sub-processors - and the verification of the effective processing of the requests received. This approach allows AGIC to offer customers and stakeholders the maximum guarantee of respect for privacy rights, while ensuring full cooperation with the competent authorities.

Appointment of a Data Protection Officer (DPO)

AGIC has appointed a Data Protection Officer (DPO) as the organization's main contact person on privacy and data protection issues.

The DPO, supported by a dedicated team, manages interactions with the competent authorities, including the Italian Data Protection Authority, the National Cybersecurity Agency, the Guardia di Finanza, the State Police and other judicial or administrative authorities, including during inspections or formal requests.

In addition, it guarantees the responsibilities attributed by the GDPR, in line with the tasks and duties assigned by the sector regulations.

Risk assessment and impact assessment

AGIC, in order to ensure maximum protection of the personal data processed and in compliance with current regulations on privacy and data protection, has defined and implemented a structured procedure for the analysis and assessment of privacy and data protection risks.

This procedure entails the involvement of a multidisciplinary team of experts and the adoption of a dedicated methodology (integrated into the IT methodology), aimed at ensuring a systematic and rigorous approach.

In general, AGIC first proceeds to determine the inherent risk (in terms of probability by impact), where this means the level of risk in the absence of any security measures; subsequently, an assessment of the controls and safeguards in place implemented by the organization is carried out - functional to assessing their effectiveness and adequacy - which, ultimately, leads to the determination of an aggregate risk value known as residual risk.

Once this is done, the results of the assessment are compared with the risk appetite defined internally and, where necessary, AGIC proceeds with the implementation of mitigation measures tailored to the nature of the risk (corrective or preventive actions), strengthening corporate governance, improving operational resilience and proactively protecting the reputation of the organization.

In addition to the above, further analyses (known as "impact assessments") are also carried out to assess the impact that a given processing may have on the rights and freedoms of individuals.

The process is divided into several phases and contemplates, in the first instance, a preliminary analysis of the processing activity, functional to verify the actual presence of information attributable to identified and/or identifiable natural persons (so-called PIA). Only later, in the event of a positive outcome, does it proceed with a more in-depth analysis that focuses, among other things, on the regulatory context of reference, on the conditions of lawfulness, on the methods of exercising rights by the data subjects in the context under consideration and, more generally, on any aspect that contributes to the definition of exposure to risk (so-called DPIA).

In addition, it has also equipped itself with functional tools to support it in the event of processing based on its legitimate interests (so-called LIA) or extra-EU transfers (so-called TIA).

Through this procedure, AGIC ensures that any processing of personal data is subjected to a risk assessment and management process in accordance with international best practices and European legislation, strengthening stakeholder trust and promoting a corporate culture oriented towards responsibility and data protection.

Data breach management

AGIC has defined a specific data breach procedure that provides for the co-participation of various internal skills.

Therefore, once a potential report relating to a personal data breach has been received (or detected), the event is classified according to the internal methodology and, at a later stage, the predefined procedural steps are activated, attributed to as many key figures, responsible for the intervention and for compliance with the timing for notification to the competent authorities (where necessary).

Each step of the process must be formally documented, with a focus on corrective actions and restoration measures.

At the end of the process, the effectiveness of the solutions adopted is verified and, if necessary, additional preventive measures are implemented to reduce the likelihood of recurrence.

Process and procedures

In application of the above, AGIC has formalized and implemented organizational safeguards (e.g. operating procedures, policies, guidelines, etc.) relating to the following areas:

- Cyber threat intelligence
- Use of IT resources by staff (even in the case of smart working)
- Classification of information
- Encryption and key and control management
- Password management
- IT asset management
- Access rights management
- Incident management
- Back-up and restore of company data
- Vulnerability management
- Log management
- Business continuity
- Access control to company premises and physical security
- Data retention
- Management of privacy and processing of personal data (and related document framework)
- Secure software development and AMS
- Privacy by design & privacy by default
- Management of e-mail metadata
- Management of data breaches