Sommario

STORIA DEL GRUPPO

Il Gruppo Maggioli S.p.A. (nel seguito anche "**Maggioli**") è un Gruppo internazionale leader nell'offerta di prodotti e servizi per la Pubblica Amministrazione Locale e Centrale, i Liberi professionisti e le Aziende.

Fondato dalla famiglia Maggioli a Santarcangelo di Romagna (RN) nel 1905 come laboratorio di prodotti per le Scuole Pubbliche, il Gruppo attraverso il suo quartier generale italiano, ha ampliato notevolmente la gamma di prodotti e servizi per i mercati di riferimento. La capacità di fornire risposte anticipate alle esigenze latenti, l'approccio innovativo nel fornire soluzioni tecnologiche e di processo, l'ampia gamma di prodotti e servizi per ogni target, l'impegno continuo sulla qualità e servizio al cliente, ha reso il Gruppo Maggioli con le oltre 40 sedi sul territorio nazionale, con una sede di rappresentanza a Bruxelles e con sedi in Spagna ed in Colombia, un punto di riferimento sia nel settore Editoriale con prodotti e servizi professionali per la Pubblica Amministrazione e liberi professionisti, che nel settore informatico con offerta di software e servizi per il mercato pubblico e privato nonché progetti per la *Digital Transformation* della Pubblica Amministrazione.

Maggioli S.p.A., è una delle poche Società ad aver ottenuto, grazie alla prima suite gestionale completa per gli Enti Locali Sicr@web, la doppia qualifica richiesta da AgID: CSP (Cloud Service Provider) e fornitore di servizi in SaaS (Software as a Service).

Nell'ambito dell'adeguamento delle amministrazioni alle disposizioni del Codice dell'Amministrazione Digitale, il Gruppo Maggioli ha sviluppato diversi servizi rivolti al Responsabile della Transizione Digitale (RTD), figura essenziale per la digitalizzazione coordinata del Paese che a sua volta è presupposto fondamentale per la nascita del mercato unico europeo per il digitale.

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

PREMESSA

Il presente documento ha lo scopo di illustrare le misure tecniche ed organizzative adottate dal Gruppo Maggioli al fine di procedere a riscontrare positivamente le vostre richieste informative e per dimostrare la conformità dei prodotti e servizi offerti al Regolamento UE 2016/679 (nel seguito anche "**GDPR**").

MISURE ORGANIZZATIVE E TECNICHE DEL GRUPPO MAGGIOLI IN RELAZIONE ALL'APPLICAZIONE DEL GDPR

Il GDPR dispone l'adozione di misure tecniche ed organizzative adeguate come previsto dagli artt. 24 e seguenti, ai sensi dei quali le politiche interne e le misure da attuare per soddisfare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default, devono tener conto, in concreto, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà delle persone fisiche.

L'art. 32 del GDPR, disciplinando la sicurezza dei trattamenti, elenca una serie di misure tecniche utili in concreto. Tuttavia tale elenco è preceduto dalla dicitura "se del caso", stando ciò a significare che tali misure di sicurezza rappresentano solo alcune di quelle che possono essere prescelte, ciò che è rilevante è la parametrizzazione interna all'organizzazione, sistema di calcolo del rischio basato su parametri oggettivi al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico; quando si parla di protezione dei dati si intende "la capacità di assicurare su base permanente":

a. la riservatezza;
b. l'integrità;
c. la disponibilità; e
d. la resilienza dei sistemi e dei servizi di trattamento.

Tenuto conto dei fattori di rischio e delle minacce che incombono sui dati personali come evidenziato in figura 1, Maggioli ha adottato le seguenti misure atte a garantire la sicurezza dei dati personali e delle informazioni gestite per conto dei clienti.

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

figura 1

Misure di sicurezza organizzative:

- nomina per iscritto personale;
- nomina ad amministratore di sistema;
- istruzioni per il trattamento;
- accesso controllato;
- procedura modifica credenziali;
- policy aziendali;
- formazione in materia di protezione dei dati personali, di cyber security e security awareness & training.

Misure di sicurezza tecniche:

- protezione delle aree e dei locali;
- sistema di autenticazione;
- autorizzazione;
- firewall;
- antivirus;
- cifratura (ove applicabile);
- business continuity;
- disaster recovery;
- sistema di backup e rispristino dei dati
- intrusion detection;
- vulnerability assessment.

Maggioli impronta il trattamento dei dati personali al pieno rispetto di quanto indicato dal GDPR e in ogni caso provvede ad eseguire le attività secondo quanto prescritto dal titolare nell'atto di nomina ex art. 28; in particolare, tratta -e raccoglie solo se previsto da specifici accordi tra le parti- i dati per conto del Titolare del trattamento per la corretta esecuzione dei servizi offerti e nel pieno rispetto degli obblighi contrattuali.

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

In particolare, per ciascun trattamento di propria competenza, Maggioli S.p.A., tramite i propri incaricati, tratterà i dati secondo i principi di:

- **liceità;**

- **correttezza;**

- **riservatezza.**

In aggiunta a quanto sopra evidenziato, si riportano di seguito le certificazioni di cui la nostra società è in possesso:

- ISO 9001:2015 (Sistema di gestione della qualità dei processi);
- ISO/IEC 27001:2013 con estensioni 27017 e 27018 (Sistema di gestione della sicurezza dei sistemi informativi);
- ISO/IEC 20000-1:2018 (gestione dei servizi IT).

Si evidenzia che Maggioli effettua periodici penetration test e vulnerability assessment, i quali vengono svolti sugli applicativi da due (2) società esterne a ciò appositamente incaricate.

Si precisa che i software di Maggioli, partendo dall'adesione alle prescrizioni della Circolare Agid n. 2/2017 del 18 aprile 2017 - in relazione alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» - garantiscono il pieno rispetto di quanto previsto dal GDPR.

ARCHITETTURA INFORMATICA E SERVER FARM MAGGIOLI S.P.A.

Salvo che si tratti di affidamento on premises, per poter erogare i servizi contrattualizzati Maggioli utilizza infrastrutture IT residenti sul territorio italiano, in particolare presso il datacenter denominato campus Data4, situato in Cornaredo (MI) - struttura deputata ad ospitare servizi di housing ed in possesso della certificazione Tier4- nonché presso un datacenter secondario sito in Mantova. Per tale architettura informatica Maggioli S.p.A. ha ottenuto da AGID la qualificazione di Cloud Service Provider (CSP).

L'infrastruttura tramite la quale Maggioli eroga i propri servizi che non sono installati on premise presso i sistemi del cliente è principalmente il campus Data4 che dispone delle seguenti certificazioni:

❖ ISO 9001 (Gestione della qualità) - ISO 27001 (Gestione Sicurezza dei sistemi informativi)

❖ ISO 14001 (Gestione ambientale)

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

- ISO 45001 (Gestione della salute e della sicurezza sul lavoro)
- ISO 50001 (Gestione dell'energia) - LEED Gold-DC01 (Gestione sostenibilità ambientale)
- ANSI TIA 942 (TIER IV) -DC03 (Fault Tolerant Site Infrastructure)
- Open IX (Punto di interconnessione rete)
- PCI DSS:2020 (Pagamenti elettronici)
- HDS:2018 (Gestione dati sanitari)

Il rapporto intercorrente con il fornitore è di tipologia Housing e non prevede un workflow ed un flusso di dati verso tali fornitori, in quanto il rapporto intercorrente è appunto di locazione fisica di soli locali attrezzati. Tale rapporto si sostanzia nella concessione in locazione di uno spazio fisico, generalmente all'interno di appositi armadi detti rack, dove inserire il server di proprietà Maggioli.

I datacenter in questione sono gestiti quindi come struttura fisica (locali, condizionamento, alimentazione) dagli Internet Service Provider (ISP), che dispongono di tali servizi, mentre tutta l'infrastruttura hardware e software (connettività, apparati di rete, server e storage) è quindi di proprietà di Maggioli e , di conseguenza, l'amministrazione, la gestione della sicurezza cyber e la manutenzione dei server sia sotto il profilo hardware che software è effettuata direttamente dalla stessa.

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

AMMINISTRATORI DI SISTEMA

Gli Amministratori di Sistema sono una categoria di operatori preposti all'esercizio dei sistemi informatici che, in funzione dei compiti ad essi assegnati, occupano i vertici della gerarchia di utenze, in termini di privilegi di accesso alle risorse informatiche e ai dati ivi custoditi.

Aziendalmente in Maggioli, in considerazione del nutrito numero di soluzioni software distribuite, di servizi erogati ed in considerazione dell'altrettanto importante numero di clienti, è stata stabilita una metodologia di informativa verso i clienti relativamente agli amministratori di Sistema che differisce rispetto alla condivisione di un elenco di AdS *tout court*.

In particolare, la nostra società tiene un elenco di AdS suddiviso per ciascuna delle linee di prodotti software, ciò in abbinamento alla profondità dei privilegi di volta in volta riconosciuti all'incaricato a ciò debitamente nominato.

In ogni caso, il Titolare del trattamento, così come previsto dal provvedimento del Garante Privacy, può richiedere un elenco di AdS, che avremo cura di condividere. Maggioli adotta sistemi idonei per garantire la registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema; le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Maggioli ha delineato le procedure di nomina e di attribuzione delle funzioni degli amministratori di sistema, attuando gli adempimenti in materia di protezione dei dati personali e, in particolare, l'adozione di specifiche misure e cautele in riferimento alle mansioni svolte dagli amministratori di sistema e dai soggetti (di profilo anche non strettamente tecnico-informatico) ad essi assimilabili, previsti dalla normativa vigente (Reg. UE 2016/679 e D. Lgs. n. 196/2003) e dai provvedimenti dell'Autorità Garante per la protezione dei dati personali (in particolar modo il Provvedimento del Garante Privacy del 27 novembre 2008).

PRINCIPI DEL GDPR APPLICATI AL TRATTAMENTO DEI DATI PERSONALI

Maggioli S.p.A., in qualità di Responsabile del trattamento dei dati personali, si impegna al pieno rispetto della normativa sulla protezione dei dati personali sancita dal GDPR - Regolamento Ue 2016/679.

Le attività effettuate da Maggioli S.p.A. relativamente al trattamento dei dati personali sono specificatamente indicate e descritte nel presente documento in seguito al conferimento di incarico "Responsabile del trattamento" ai sensi dell'art. 4 e dell'art. 28 del suddetto GDPR.

Il Titolare del trattamento dei dati è il cliente e resta tale anche dopo la nomina suddetta.

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

Ogni trattamento dei dati personali avviene nel rispetto di quanto previsto dal GDPR e dei principi di ordine generale. Maggioli raccoglie e tratta i dati per conto del Titolare al trattamento secondo quanto previsto dall'art. 28 del GDPR e solo per la corretta esecuzione dei servizi offerti ed al rispetto degli obblighi contrattuali. Nello specifico, i dati vengono trattati sia con l'ausilio di strumenti informatici messi a disposizione del Cliente che collegandosi, laddove previsto dagli accordi contrattuali, in remoto.

I dati vengono trattati in osservanza di quanto previsto dal GDPR in termini di misure idonee e adeguate, attenendosi comunque alle disposizioni del titolare al trattamento in tema di sicurezza.

Maggioli dispone e mantiene aggiornato un proprio sistema di sicurezza informatico applicativo idoneo a rispettare le prescrizioni del GDPR sia in termini di misure minime che idonee.

Maggioli S.p.A. non è responsabile in nessuna forma di eventuali carenze o inadempienze nel sistema di sicurezza previsto dal Titolare del trattamento dei dati.

Maggioli S.p.A. individua i soggetti preposti al trattamento che operano sotto la propria responsabilità; oltre a ciò, forma e mantiene aggiornati i soggetti preposti al trattamento, in materia di privacy e sicurezza. In particolare, chi è preposto al trattamento dovrà effettuare il trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal titolare e/o dal responsabile in applicazione dei dettami del GDPR, oltre a quelle che successivamente verranno indicate in aggiornamento a quelle ivi previste. Dovrà inoltre rispettare le istruzioni impartite dal titolare attraverso l'atto di nomina a responsabile del trattamento ex art. 28 del GPDR, adottando le misure di sicurezza dallo stesso suggerite ed in particolare a conformarsi a quanto di seguito precisato:

- per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale mantenendolo riservato, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
- conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate, o procedere alla distruzione dei documenti in copia come da accordi contrattuali;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro dal titolare, e comunque in modo lecito e secondo correttezza;
- fornire al titolare o alle persone dallo stesso designate, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Maggioli S.p.A., nel rispetto dell'art. 33 del Regolamento, si è dotata di una propria procedura di gestione degli eventi di sicurezza e un relativo response plan, applicabile sia nel caso in cui quest'ultima agisca come responsabile del trattamento, sia in qualità di titolare del trattamento. Ciò permette di gestire e affrontare l'incidente, e effettuarne le dovute comunicazioni in tempo utile al titolare del trattamento, in modo che se l'incidente ha prodotto perdita, furto o danni ai dati personali trattati, possano esser fatte entro i tempi di legge le opportune comunicazioni all'Autorità Garante e ai soggetti interessati se ritenuto necessario.

Maggioli S.p.A., come previsto dall'art. 37 del GDPR, ha provveduto a nominare il Responsabile della protezione dei dati (DPO) che potrà essere contattato ai seguenti indirizzi:
e-mail dpo.privacy@maggioli.it
pec dpo.privacy@maggioli.legalmail.it

Il Titolare del trattamento, come previsto dalla vigente normativa, sarà chiamata ad esercitare vigilanza e controllo sull'osservanza delle istruzioni impartite al responsabile e delle vigenti disposizioni in materia di trattamento dei dati personali. L'attività di verifica potrà concretizzarsi attraverso la richiesta al Responsabile di compiere attività di autovalutazione rispetto alle misure di sicurezza adottate, all'osservanza delle misure impartite, fornendone, a richiesta, documentazione scritta. Il Titolare ha il diritto di esercitare controlli o attività di audit relative all'oggetto del contratto stipulato tra le parti, presso le sedi del Responsabile o da remoto, finalizzati ad una verifica della puntuale applicazione delle istruzioni impartite, nonché della conformità alla legge delle operazioni di trattamento. Tali controlli dovranno essere effettuati mediante comunicazione preventiva a Maggioli, da comunicarsi con congruo anticipo (almeno con quattordici giorni di anticipo), con richiesta di convocazione di un meeting pre-audit tra le parti volto a concertare gli step da seguire.

In fine, all'atto della cessazione, per qualsiasi causa, delle operazioni di trattamento da parte di Maggioli, quest'ultima, trascorsi dodici (12) mesi, provvede alla integrale distruzione dei dati, salvo diverso accordo tra le parti, fatta eccezione per la documentazione amministrativa la cui tenuta è gestita in ottemperanza agli obblighi di conservazione stabiliti per legge.

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato

CONCLUSIONI

Le presenti linee guida vengono fornite in allegato al conferimento dell'incarico a Maggioli S.p.A. quale Responsabile del trattamento ex art. 28 del GDPR.

Maggioli in ottemperanza a quanto previsto dal considerando 76 del GDPR, si è dotata di un sistema di calcolo del rischio basato su parametri oggettivi, al fine di stabilire se esiste un rischio e se tale rischio è elevato per il trattamento specifico.

L'oggettivazione del rischio, pertanto, passa attraverso un modello di correlazione della probabilità e della gravità, diversificata per fonte di rischio, in grado di rispecchiare il contesto in cui l'organizzazione opera considerando opportune griglie per il calcolo delle probabilità e gravità con riguardo all'impatto per i diritti e libertà dell'interessato.

Le misure di sicurezza tecniche, organizzative ed infrastrutturali applicate hanno l'obiettivo di mitigare l'effetto dei rischi e delle minacce sui dati oggetto di trattamento.

Maggioli tramite le soprariportate misure tecniche, organizzative ed infrastrutturali, conferma la volontà di garantire ed assicurare un livello di sicurezza adeguato e in linea con quanto previsto dalla normativa vigente, nello specifico il GDPR, ma non solo, con la finalità di supportare professionisti, aziende e Pubbliche Amministrazioni nel raggiungimento dei propri obbiettivi.

Maggioli S.p.A.

Il Procuratore Speciale

Maggioli S.P.A.
via del Carpino, 8
47822 Santarcangelo di Romagna (RN)

Tel. 0541 628111
Fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro Imprese c/o la CCIAA della Romagna Forlì-Cesena e Rimini
R.E.A. RN-219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200,00
interamente versato