"Privacy e sicurezza dei dati e delle informazioni"

INDICE

1 SEZIONE: "PRIVACY E SICUREZZA DEI DATI E DELLE INFORMAZIONI"

In un contesto globale in continua evoluzione e sempre più interconnesso, le nuove vulnerabilità e minacce incrementano i rischi correlati al trattamento dei Dati Personali e alla sicurezza delle informazioni in tutte le fasi del loro ciclo di vita: dalla raccolta alla dismissione.
In ambito aziendale, tutto il personale facente capo alle società del Gruppo doValue si trova ad acquisire e a trattare una mole significativa di dati personali e di informazioni a carattere confidenziale di clienti, fornitori e altri soggetti portatori di interesse e su cui insistono vari requisiti di natura normativa e di business.
La tutela dei dati e delle informazioni è, pertanto, una priorità del modello di governance e di business di doValue dalla quale dipende la salvaguardia del brand, la riduzione di perdite operative, la qualità dei rapporti con i clienti, il livello di fiducia con tutti i soggetti interessati, il rispetto degli obblighi normativi.
doValue ha pertanto avviato un **programma di tutela dei dati personali e delle informazioni confidenziali** che si concretizza nell'adozione di seguenti Programmi:

- Protezione dei dati personali
- Protezione delle informazioni confidenziali;
- Misure e accorgimenti di natura tecnica (Cyber Security) che insistono sia sui dati personali che sulle informazioni confidenziali

1.1 PROGRAMMA DI PROTEZIONE DEI DATI PERSONALI

Il Regolamento Generale sulla Protezione dei Dati, ufficialmente Regolamento n. 2016/679 e noto con la sigla "GDPR", entrato vigore a maggio 2016 e diventato effettivo a partire dal 25 maggio 2018, ha apportato cambiamenti significativi alla normativa sulla protezione dei dati.
Il Regolamento, che trova applicazione per tutti i trattamenti di dati e la protezione delle informazioni effettuati dagli Stati Membri dell'Unione Europea, garantisce agli individui maggiori diritti di controllo sui propri dati personali e attribuisce alle organizzazioni la responsabilità di adottare adeguate misure di tutela dei dati personali.
Il Gruppo doValue ha provveduto a identificare e adottare adeguate misure tecniche e organizzative volte a rafforzare la protezione dei dati personali trattati, nel rispetto del principio di *accountability* e a garantire la sicurezza e la protezione dei dati personali trattati dal proprio personale attraverso un approccio basato sul rischio, coerente con i requisiti normativi applicabili e con le aspettative dei soggetti interessati.

1.1.1 Le tipologie di dati personali trattati

Il core business del Gruppo è rappresentato dalla gestione di crediti non performing per conto di Terze Parti (es. Mandanti/Banche/SPV) ovvero di tutte le attività ancillari di carattere giudiziale e stragiudiziale direttamente o indirettamente connesse all'attività core sopra descritta.

In questo contesto le Società del Gruppo doValue si trovano a gestire:

- tipologie di Dati Personali diversificate (i.e. Identificativi, Sensibili / Particolari ecc.);

- categorie di interessati diversi nei confronti dei quali agiscono sia come Titolari del Trattamento (dipendenti, clienti, potenziali clienti, terze parti, etc.) sia come Responsabili Esterni del Trattamento (i.e. dati di titolarità delle Banche mandanti riferiti a soggetti obbligati, trattati nell'ambito di mandati per il recupero del credito).

1.1.2 Come il Gruppo doValue dimostra la compliance al GDPR

Un sistema di protezione dei dati personali robusto è un requisito fondamentale nelle organizzazioni che operano nel settore finanziario. La crescente richiesta di affidabilità e conformità a specifici requisiti comporta da un lato l'aumento del livello di complessità per la gestione dei rischi cyber e dall'altro un incremento del livello di fiducia dei clienti verso le società del Gruppo.
Il programma adottato in ambito Data Protection dal Gruppo doValue mira ad assicurare la compliance alla normativa Europea e nazionale applicabile in materia di protezione dei dati personali, a minimizzare il rischio di perdita della riservatezza, integrità e disponibilità e a proteggere il patrimonio informativo aziendale, costituito in gran parte da dati personali.
Il Programma è mantenuto aggiornato sulla base dell'evoluzione normativa, dell'evoluzione del contesto di business, dello scenario dei rischi e delle tecnologie.
Nel contesto di tale programma, sono state definite e implementate specifiche misure tecniche e organizzative atte a gestire i requisiti normativi e i cui risultati sono sintetizzati di seguito:

- **Registro dei trattamenti** – Ciascuna società del Gruppo ha mappato tutti i trattamenti di dati personali svolti, in modo da distribuire correttamente ruoli e responsabilità, analizzare i rischi per i diritti e le libertà fondamentali e garantire l'effettivo esercizio di tali diritti (sul punto *cfr* para. 1.1.4);
- **Modello Organizzativo data protection**- l'effettività delle misure di protezione dipende da un adeguato modello organizzativo dei ruoli preposti al governo delle operazioni svolte sui dati personali, dei ruoli di vigilanza (come il Data Protection Officer), e dei ruoli di garanzia. doValue ha aggiornato il proprio modello organizzativo di riferimento e nominato il Data Protection Officer per tutte le Società del Gruppo (si veda, per approfondimenti, il paragrafo successivo);
- **Informative sulla protezione dei dati** – tutta la documentazione volta a garantire la trasparenza dei trattamenti svolti dal Gruppo è stata aggiornata per rispondere ai nuovi requisiti del GDPR, consentendo ai soggetti interessati di avere piena contezza delle finalità dei trattamenti effettuati, delle altre informazioni obbligatorie, e di come esercitare i loro diritti;
- **Analisi di rischio e valutazione di impatto (DPIA)** – doValue ha sviluppato e adottato una nuova analisi dei rischi e valutazione di impatto da applicare ai trattamenti contenuti nel registro, al fine di indentificare ulteriori misure di tutela sulla base dei potenziali danni materiali e immateriali che i trattamenti di dati possono comportare per i soggetti interessati;
- **Politiche & Procedure** – implementazione di politiche e procedure per rispondere agli obblighi e ai requisiti definiti dal GDPR e da altre leggi in materia, tra cui:
    - Politica Data Protection del Gruppo doValue
    - Procedura per la gestione delle violazioni di sicurezza e relativo registro;
    - Procedura per la gestione dei diritti degli interessati del trattamento;
    - Politica di conservazione e cancellazione dei dati;

- Linee guida per la Privacy by design e by default;
- Data Protection Control Framework del DPO

- **Cyber Security Program** – Sotto il profilo tecnico, il Gruppo doValue ha definito e adottato un pervasivo e robusto programma di Cyber Security che impatta tutte le dimensioni di governo e utilizzo degli strumenti elettronici opportunamente individuati a supporto/protezione dei dati personali che il Gruppo detiene, sia come Responsabile che come Titolare degli stessi.

1.1.3 Data Protection Officer

Il Gruppo doValue, a seguito di valutazioni interne e delle proprie esigenze organizzative, ha individuato e nominato un Global DPO che, a livello Corporate, opera presso la Capogruppo doValue S.p.A.
Nelle società controllate italiane ed estere sono stati individuati dei Local DPO che hanno il medesimo ruolo, e le stesse responsabilità previste dalla normativa applicabile declinate a livello locale.
Nel caso in cui una società del Gruppo doValue non si trovi obbligata a procedere alla nomina di un proprio Local DPO, il presidio per le attività correlate alla tutela dei dati personali è garantito dalla Funzione di Compliance o Legal presente localmente o da altra struttura interna.
Al fine di garantire una maggiore effettività dell'azione di ciascun DPO il Gruppo doValue ha definito un *Data Protection Control Framework* ("DPCF"), che include le attività di controllo su ambiti chiave soggette a periodico monitoraggio. Con cadenza periodica, ciascun DPO valuta l'adeguatezza e l'effettivo funzionamento dei presidi adottati a tutela della protezione dei dati personali e porta all'attenzione degli Organi di controllo e di governo aziendale i risultati al fine di alimentare il piano di miglioramento continuo del sistema di data protection.
Per ogni ulteriore approfondimento sul collocamento gerarchico dei DPO, sui compiti attribuiti e sulle relazioni tra Global, local DPO e Organi di controllo societario, si rimanda alla lettura del documento *Policy Data Protection del Gruppo doValue*

1.1.4 Gestione dei diritti degli interessati

In conformità con quanto previsto dal GDPR, il Gruppo doValue garantisce il riconoscimento dei seguenti diritti agli Interessati (definiti dal GDPR negli artt.15-21):

- ✓ *Diritto di accesso*: l'Interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso;
- ✓ *Diritto di rettifica*: l'Interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano o l'integrazione dei dati personali incompleti tenendo conto delle finalità del trattamento;
- ✓ *Diritto alla cancellazione*: l'Interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano. Si consideri che non possono essere eliminati i dati il cui mantenimento è giustificato o reso necessario ai fini di legge (ad es. nel caso in cui un cliente chiede la cancellazione, ma sia in essere un contenzioso tra questo e la Società, quest'ultima è legittimata a conservare i dati del cliente, nonostante la richiesta);
- ✓ *Diritto di limitazione del trattamento*: l'Interessato ha il diritto di ottenere la limitazione del trattamento, qualora contesti l'esattezza dei dati personali, per il

periodo necessario al Titolare per verificare l'esattezza dei dati personali, o qualora si sia opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'Interessato;

- ✓ *Diritto alla portabilità dei dati*: l'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e ha il diritto di trasmetterli ad un altro Titolare del Trattamento senza impedimenti;
- ✓ *Diritto di opposizione*: l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano per alcune o per tutte le finalità per cui sono stati raccolti. L'Interessato ha, in particolare, il diritto di modificare i consensi e successivamente inibire qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- ✓ *Diritto di non essere sottoposto ad un processo decisionale automatizzato*: l'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Per ognuno dei suddetti diritti, le Società del Gruppo doValue, in qualità di Titolari del trattamento, si sono dotate di opportune procedure interne e strumenti per:

- fornire riscontro all'Interessato senza ingiustificato ritardo in merito alla richiesta ricevuta, giustificando all'Interessato eventuali ritardi o inadempienze nel fornire il riscontro
- gestire le richieste dell'Interessato all'interno del contesto societario eseguendo eventuali attività di estrazione, rettifica, cancellazione dei dati personali;
- Informare eventuali Titolari del trattamento terzi, cui sono stati comunicati i dati, della richiesta dell'Interessato.

Le Società del Gruppo sono tenute a dare riscontro all'esercizio dei diritti da parte di Interessati i cui dati sono trattati in qualità di Titolari del Trattamento o in qualità di responsabili del trattamento qualora sia espressamente richiesto dal Titolare del trattamento all'interno del Data Protection Agreement (DPA).

In conformità con quanto previsto dal GDPR, il LOCAL DPO di ciascuna società del gruppo doValue funge da contatto per gli Interessati per l'esercizio dei loro diritti.

E' fatto in ogni caso salvo il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali.

Per i trattamenti che si fondano sul consenso dell'utente, quest'ultimo potrà revocare il consenso in ogni momento. In ogni caso, la revoca del consenso non pregiudicherà la liceità dei trattamenti effettuati fino a quel momento.

1.2 PROGRAMMA DI CYBER SECURITY

Come evidenziato dal *"The Global Risks Report"* del World Economic Forum[1], il rischio cibernetico costituisce uno dei principali rischi per tutte le organizzazioni internazionali.
Il Gruppo doValue è esposto a tale rischio, in ragione della numerosità degli operatori, dell'utilizzo estensivo di strumenti elettronici per l'erogazione dei servizi, per la natura e i volumi di dati trattati.
Inoltre, la crescente richiesta di affidabilità e conformità a specifici requisiti da parte dei più grandi clienti del Gruppo doValue, i nuovi modelli di business che hanno creato un contesto in cui dati ed informazioni sono largamente condivisi e interconnessi, la sofisticazione, velocità e impatto con cui gli attacchi cyber stanno crescendo comporta l'aumento del livello di complessità di gestione del rischio cibernetico
Il Gruppo doValue, attraverso un vasto Cyber Security Risk Assessment che ha visto interessare tutte le risorse ed i sistemi del Gruppo, secondo gli standard ISO:IEC 27001:2015, ISO:IEC 22301:2019, NIST 800-53 e la Normativa "General Data Protection Regulation" o GDPR, ha definito ed avviato un esteso **Programma di Cyber Security**, che si prefigge di elevare la security posture del Gruppo ai più elevati standard di sicurezza internazionali e di allineare/trasferire le tecnologie di sicurezza scelte a tutte le società dello Stesso, con un approccio sinergico.
La strategia di Cyber Security definita a livello di Gruppo, in particolare, definisce diversi obiettivi finalizzati a minimizzare il rischio cibernetico e a proteggere quindi i clienti, le persone e il brand di doValue a livello internazionale.
Gli obiettivi ed i risultati della Cyber Security Roadmap sono stati raggruppati per funzioni del Framework di Sicurezza Internazionale NIST, tra cui:

- **Obiettivo Interno 1 – Identify**
    a. Governance e risk management, supervisione dei processi critici del Gruppo attraverso un approccio basato sul cyber-security risk;
    b. Gestione del rischio informatico della propria supply chain;
    c. Approccio orientato al continuous improvement delle capabilities delle proprie risorse interne.

Per raggiungere questi risultati, il Gruppo doValue continuerà a sviluppare la propria governance e gestione del rischio attraverso:
• La definizione di un Risk Appetite a supporto del processo decisionale basato sul rischio;
• Il ricorso a strumenti di reporting potenziati per supportare una supervisione efficace del programma;
• La definizione di ruoli e responsabilità chiari;
• La valutazione del rischio relativo alla Supply Chain del Gruppo durante tutto il ciclo di vita di approvvigionamento;
• L'acquisizione di risorse interne ed esterne con competenze verticali di Cyber Security, al fine di soddisfare le necessità presenti e future in termini di sicurezza informatica.

- **Obiettivo Interno 2 – Protect**
    a. Gestire l'accesso alle risorse e ai sistemi in modo efficace e limitato agli utenti autorizzati, secondo i principi chiave del least privilege e need to know;
    b. Identificazione delle vulnerabilità e di mitigazioni appropriate, valutandone rapidamente l'impatto;

1 Si veda: http://reports.weforum.org/global-risks-report-2020/wild-wide-web/

c. Classificazione appropriata dei dati secondo il livello di esposizione al rischio;
d. Innalzamento dei livelli di consapevolezza dei propri dipendenti attraverso corsi puntuali di Sicurezza Informatica.

Per raggiungere questi risultati attesi, il Gruppo doValue:
• Automatizzerà la gestione delle identità e degli accessi, attraverso uno strumento tecnologico che garantirà anche un controllo centralizzato;
• Amplierà il perimetro del programma di security testing volto a misurare in termini di efficacia le difese informatiche e quindi la protezione verso le vulnerabilità intrinseche del software e dei sistemi, le quali vengono riscontrate in accordo con i moderni standard di sicurezza;
• Migliorerà i processi e gli strumenti per la classificazione dei dati sensibili e le misure per prevenire e rilevare la perdita degli stessi;
• Estenderà l'attuale programma di sensibilizzazione alla sicurezza informatica del Gruppo doValue, includendo attività di Phishing Assessment puntuali al fine di innalzare la consapevolezza dei propri dipendenti verso alcune tipologie di attacchi dall'esterno;
• Efficienterà i processi di sicurezza attraverso servizi di nuova generazione, come la gestione centralizzata dei firewall, per migliorare la resilienza e la sicurezza di tutti gli ambienti (BRE - Business Recovery Enhancement).

- **Obiettivo Interno 3 – Detect**
  a. Individuazione e gestione tempestiva degli attacchi cyber;
  b. Monitoraggio continuo delle configurazioni dei sistemi al fine di individuare eventuali misconfiguration;
  c. Adozione di un sistema di Event Management e Threat Intelligence al fine di individuare preventivamente incidenti di Sicurezza che possano compromettere l'integrità, la riservatezza e la disponibilità dei dati, nonché danneggiare la reputazione del Gruppo.

Per raggiungere questi risultati attesi, il Gruppo doValue:
• implementerà strumenti e processi di monitoraggio della sicurezza di nuova generazione, al fine di rilevare *real time* attività dannose e comprendere il potenziale impatto degli eventi;
• condurrà regolarmente test di sicurezza informatica per valutare l'efficacia delle difese informatiche;
• potenzierà i processi e le procedure di rilevamento degli incidenti e di eventuali compromissioni, partendo da un controllo esteso e profondo degli endpoint;
• irrobustirà il processo di hardening dei sistemi monitorando continuamente le modifiche alla configurazione rispetto alle Policy di Sicurezza Informatica del Gruppo;
• attiverà un servizio di threat intelligence ed early warning volto all'individuazione proattiva delle minacce per poterne rilevare attività dannose.

- **Obiettivo Interno 4 – Respond**
  a. Testare regolarmente i piani di difesa e risposta agli Incidenti;
  b. Garantire la risposta agli incidenti con disponibilità 24X7 e automatizzata, laddove possibile;
  c. Svolgimento dell'analisi forense a valle degli incidenti di sicurezza;
  d. Coinvolgere gli stakeholders interni ed esterni nelle attività di Incident Response.

Per raggiungere questi risultati attesi, il Gruppo doValue:

• Aumenterà la frequenza dei test dei piani di risposta per garantire le capacità necessarie e i tempi di risposta stabiliti, tenendo in considerazione anche le terze parti coinvolte;
• Migliorerà gli strumenti e i processi per ridurre gli impatti di un incidente di sicurezza informatica cercando di automatizzare la risposta;
• Implementerà processi e strumenti efficaci che permettano agli esperti tecnici e forensi informatici, di condurre indagini accurate.

- **Obiettivo Interno 5 – Recovery**
    a. Test e miglioramento continuo dei piani di recovery;
    b. Garantire che le procedure di recovery da Incidenti di Sicurezza Informatica vengano eseguite in opportuni frangenti di tempo prestabiliti, rispettando gli obiettivi di continuità operativa (RTO, MTPD, etc) e le comunicazioni verso gli stakeholders interni ed esterni.

Per raggiungere questi risultati attesi il Gruppo doValue:
• Testa regolarmente i piani di Recovery insieme alle Terze Parti coinvolte, al fine di verificarne l'efficacia e migliorarne i piani con un approccio di Continuous Improvement;
• Gestirà i problemi di sicurezza informatica in modo efficiente attraverso il coordinamento e la comunicazione con tutte le parti interessate, utilizzando i processi e gli automatismi messi in campo per verificare l'efficacia dei piani di risposta, principalmente per attacchi di tipo Ransomware e DDoS.

DoValue adotta un approccio proattivo verso la Cyber Security, al fine di riscontrare preventivamente gli agenti di minaccia che potrebbero compromettere in qualsiasi modo la Riservatezza, l'Integrità e la Disponibilità dei dati facenti parte del patrimonio informativo aziendale, permettendo quindi, grazie ad una modalità AGILE di gestire e affrontare tempestivamente tutte le insidie che il cyberspazio nasconde, adattandosi continuamente alle nuove minacce.