POLICY

Data Protection del Gruppo doValue

INDICE

1 MODALITÀ DI GESTIONE DEL DOCUMENTO

Società Emittente	doValue S.p.A.
Società/e Destinataria/e	Tutte le Società del Gruppo doValue (Capogruppo e Società controllate italiane ed estere)
Titolo	Data Protection del Gruppo doValue
Data emissione	13/01/2021
Data decorrenza	Immediata
Codice identificativo del documento	PL02-2021-R01
Livello gerarchico del Sistema Normativo Integrato	III livello gerarchico
Tipologia del documento	Policy
Direttiva Normativa	Sì
Redatto da (Owner):	Compliance & Global DPO
Verificato da:	General Counsel
Approvato da (Accountable) in data:	Consiglio di Amministrazione di doValue in data 17/12/2020
Emanato con:	Comunicazione di servizio n. PL02-2021-R01
Norme abrogate o sostituite:	III-Policy R&C-11-2018-R02 - Policy in materia di protezione dei dati personali
Cronologia delle revisioni	R01 – Prima Stesura

2 GLOSSARIO

Autorità di Controllo (o Autorità)	L'Autorità di cui all'articolo 51 del GDPR in materia di Protezione dei Dati personali ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali.
Controllate	Le società finanziarie e/o strumentali incluse nel Gruppo doValue.
Dati giudiziari	I Dati personali che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati identificativi	I dati identificativi sono i dati attraverso i quali è possibile ottenere l'identificazione diretta dell'Interessato. A titolo esemplificativo i codici identificativi, sia quelli ricavati da dati anagrafici (e.g. codice fiscale) sia i codici univoci attribuiti a una persona in base a criteri predefiniti (e.g. codici cliente), sono dati identificativi.
Dato sensibile/particolare	I Dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dati bancari	Dati personali che riguardano relativi i rapporti bancari e finanziari dell'Interessato e i relativi ordini (es. ordini di pagamento).

Data Protection Officer ovvero "Responsabile della protezione dei dati" (o "DPO")	Il "Data Protection Officer" è il soggetto designato dal Titolare (o dal Responsabile) del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR.
General Data Protection Regulation (o "GDPR")	Il "General Data Protection Regulation", ossia il Regolamento (UE) n. 679 del 27 aprile 2016, che stabilisce la disciplina europea di regolamentazione in ambito di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.
Gruppo	Il Gruppo doValue, di cui fanno parte doValue (Capogruppo), Italfondiario, doData e le controllate estere per le Region Iberia e Region Greece and Cyprus.
Interessato	La persona fisica identificata o identificabile, direttamente o indirettamente, da un dato personale e comunque cui il dato trattato si riferisce.
Mandante	La banca, SPV o altra persona giuridica che dà mandato ad una Società del Gruppo doValue per le attività di recupero crediti e/o servizi connessi e strumentali.
Responsabile del Trattamento	Il soggetto terzo diverso da un dipendente o da un legale rappresentante cui viene conferita la nomina a Responsabile in relazione ai trattamenti di dati personali da quest'ultimo effettuati per conto del Titolare per effetto di un contratto di servizio o collaborazione che definisce l'ambito di responsabilità delegate.
Titolare del Trattamento	La persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Società	Una o più delle Società del Gruppo doValue.

3 INTRODUZIONE

In un contesto globale, in continua evoluzione ed interconnesso, è fondamentale prestare la necessaria attenzione alla tutela dei dati personali a causa delle nuove vulnerabilità e minacce che conducono all'incremento dei rischi connessi al trattamento dei Dati personali e richiedono una gestione sempre più attenta di tutte le fasi del processo di trattamento che va dalla raccolta alla dismissione dei dati.

Scopo della presente Policy è delineare:

- La **strategia di Data Protection del Gruppo doValue** in cui è declinato l'impegno del Gruppo nella protezione dei dati personali;
- il **Modello Organizzativo per la Protezione dei Dati personali** (di seguito anche "**MOPDP"**), descrivere i ruoli, le responsabilità e le relazioni intercorrenti tra le varie figure individuate per governare il sistema di gestione dei dati personali delle società del Gruppo;
- il **Modello di Gestione dei dati** che delinea i principali adempimenti previsti dal Regolamento Europeo per un corretto governo dei trattamenti dei Dati personali.

3.1 APPLICABILITÀ

La presente policy si applica a tutte le società del Gruppo doValue, italiane ed estere ed è adottata con separati atti di delibera del Consiglio di Amministrazione della Capogruppo e degli organi amministrativi delle società controllate italiane ed estere le quali, coordinandosi con la Capogruppo, si impegnano a recepirne, principi e linee guida, tenendo conto delle proprie peculiarità aziendali e delle normative locali applicabili.
La presente policy è indirizzata a tutto il personale interno di doValue e delle società controllate che trattano dati personali.

3.2 CONTESTO NORMATIVO

Il documento è redatto ai sensi della normativa in materia di trattamento dei dati personali, sia a livello europeo che nazionale, contenuta nelle seguenti disposizioni e successive modifiche:

- Regolamento in Materia di Protezione dei Dati personali n. 679/2016 (General Data Protection Regulation o "GDPR")
- Guidelines emesse a cura dell'*"Article 29 Data Protection Working Party"* (per brevità anche "WP29") e/o dell'European Data Protection Board (per brevità anche "EDPB")
- Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" così come modificato ed integrato dal D.Lgs. n. 101/2018 e altre normative nazionali locali applicabili alle Società del Gruppo.

3.3 PRINCIPI GENERALI

Il GDPR definisce i principi applicabili al trattamento dei dati personali stabilendo che questi siano:

a) trattati in modo lecito, equo e trasparente nei confronti dell'Interessato ("**liceità, equità e trasparenza**");
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità ("**limitazione della finalità**");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("**minimizzazione dei dati**");
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("**esattezza**");
e) conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("**limitazione della conservazione**");
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).

4 STRATEGIA DATA PROTECTION

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 dover gestire:

- tipologie di dati personali diversificate (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. i dati dei soggetti obbligati trattati nell'ambito di mandati per il recupero del credito e pertanto di titolarità delle Banche mandanti).

Il Gruppo doValue si impegna a garantire la sicurezza e la protezione dei dati personali trattati da tutti i propri dipendenti e collaboratori, attraverso un approccio *risk-based*, coerente con i requisiti normativi applicabili e con le aspettative di tutti gli stakeholder, (come meglio definiti di seguito).

Il Gruppo doValue monitora costantemente le evoluzioni normative in materia di protezione dei dati personali con l'obiettivo di porre in essere azioni di adeguamento che portano ad un miglioramento continuo del sistema di protezione dei dati personali. Inoltre, in base al livello di esposizione, della società, ai rischi di perdita di riservatezza, integrità e disponibilità dei dati personali, tutte le Società del Gruppo doValue implementano adeguate misure di sicurezza tecniche ed organizzative volte a rafforzare la protezione dei dati personali trattati nel rispetto del principio di accountability.

4.1 STAKEHOLDER

Gli stakeholder del sistema Data Protection del Gruppo doValue sono i soggetti che beneficiano della corretta impostazione del sistema stesso in coerenza con tutti i requisiti normativi applicabili allo specifico contesto di riferimento in materia di protezione dei dati personali. In particolare:

- **Investitori,** in quanto un eventuale danno reputazione causato da una gestione non corretta dei dati personali potrebbe comportare perdite di valore del titolo e una perdita di fiducia degli investitori verso l'organizzazione;
- **Consiglio di Amministrazione,** in quanto la compliance normativa del sistema DP garantisce una mitigazione del rischio di non conformità che comporterebbe l'applicazione di sanzioni da parte dell'Autorità di controllo con conseguenti perdite finanziarie e danni reputazionali per il Gruppo;
- **Interessati del trattamento,** in quanto un sistema di protezione dei dati personali debole comporterebbe un innalzamento del livello di esposizione della società stessa ai rischi di perdita di riservatezza, integrità e disponibilità dei dati personali trattati. La manifestazione quindi di un evento che inficia la riservatezza, l'integrità e la disponibilità dei dati personali degli Interessati potrebbe causare un danno per il soggetto Interessato, anche di notevole entità.
- **Mandanti,** in quanto, nell'ambito dei servizi resi, le società del Gruppo doValue possono essere nominate Responsabili del trattamento di mandanti che agiscono in qualità di Titolari del trattamento. In quest'ottica le mandanti beneficiano della

robustezza del sistema di Data Protection delle società del Gruppo doValue che diventa basilare per la protezione dei dati personali che ricadono nella loro sfera di titolarità.

4.2 PROGRAMMA DATA PROTECTION

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.
I programmi in essere in ambito Data Protection del Gruppo doValue mirano ad assicurare la compliance alla normativa europea e nazionale 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 Gruppo doValue si impegna quindi a:

- rendere integrato, coerente ed armonico l'approccio alla gestione dei dati personali, attraverso la definizione di linee guida che dovranno essere recepite a livello locale da tutte le società controllate, sia italiane che estere;
- ridurre il rischio di perdita di dati attraverso azioni mirate nei confronti dei dipendenti e delle terze parti coinvolte nei trattamenti di dati personali;
- utilizzare strumenti di sicurezza avanzati per la rilevazione delle minacce che compromettano la sicurezza dei dati e la messa in opera di efficaci azioni di contrasto alle stesse;
- attuare un approccio di security by design per tutte le nuove tecnologie che saranno adottate dalle società del Gruppo.

4.3 RISORSE ALLOCATE

Il gruppo doValue si impegna a garantire l'allocazione di adeguate risorse in termini operativi ed economici con l'obiettivo di monitorare le evoluzioni normative in materia di protezione dei dati personali ed identificare tempestivamente le necessarie azioni di adeguamento al modello di gestione dei dati e agli strumenti di supporto per i trattamenti di dati personali, anche funzionalmente al rafforzamento delle misure di sicurezza.

5 IL MODELLO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI

Il modello organizzativo per la protezione dei dati personali (MOPDP) adottato dal Gruppo doValue è stato definito sulla base delle caratteristiche del business delle Società che ne fanno parte e sulla base dei rapporti fra queste esistenti.
Come indicato nella seguente figura (cfr. fig.1), il MOPDP è articolato in 2 aree:

- **Governo & Sorveglianza:** cui sono demandati i compiti di: (i) determinare l'indirizzo del sistema di Protezione dei dati, le finalità e le relative modalità di trattamento dei dati personali; (ii) assicurare la conformità dell'organizzazione ai

requisiti della normativa privacy; (iii) coordinare le iniziative in ambito protezione dei dati approvate; (iv) fungere da focal point sulle tematiche di Data Protection con funzioni consultive e di contatto con l'Autorità di Controllo.

- **Linee Operative:** cui spettano compiti ed attività di carattere operativo in riferimento al trattamento dei dati personali a seconda del ruolo interno od esterno ricoperto (funzioni di business, ICT e soggetti esterni)

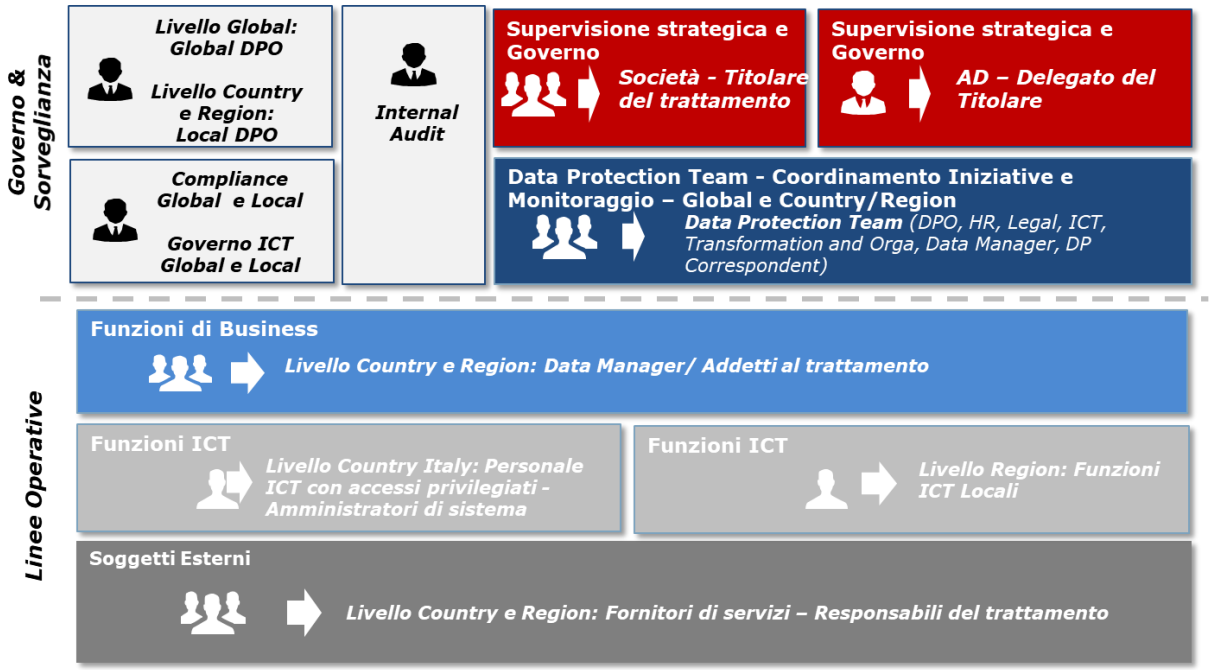


Fig. 1 – MOPDP del Gruppo doValue

La complessità connessa alla protezione dei dati personali richiede l'individuazione di diverse figure, con specifici compiti e responsabilità nell'ambito della gestione dei dati.
Alcune figure sono espressamente previste dal GDPR (o da Provvedimenti dell'Autorità di Controllo ove applicabili) e sono:

- il Titolare del trattamento
- il Data Protection Officer (DPO)
- il Responsabile e, ove eventualmente nominato, il Sub-responsabile del Trattamento
- l'Amministratore di Sistema (ove previsto in base alle normative locali).
- l'Addetto al Trattamento

Altre figure derivano da scelte gestionali, legate alla struttura organizzativa ed alle modalità operative di trattamento e sono funzionali all'effettivo funzionamento dei presidi di gestione dei dati personali, quali:

- il Data Protection team;
- il Data Manager;
- il Corrispondente per la protezione dei dati personali.

5.1 RUOLI DI GOVERNO

I ruoli di governo hanno il compito principale di indirizzare le attività del Gruppo al fine di garantire la protezione dei dati personali degli Interessati e il rispetto dei loro diritti previsti dalla normativa.

5.1.1 Titolare del Trattamento e il Delegato

Il Titolare del trattamento è, ai sensi dell'art. 4 co. 7, GDPR, «*la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*»
Il Titolare è, pertanto, responsabile di definire le finalità e le modalità dei trattamenti effettuati, di adottare le misure organizzative e tecniche adeguate a garantire il rispetto della normativa avendo cura di riesaminare ed aggiornare tali misure quando necessario, e di garantire agli Interessati l'esercizio dei loro diritti riconosciuti dal GDPR. Inoltre, è compito del Titolare del trattamento designare il Data Protection Officer (DPO) demandandogli i compiti di sorveglianza del sistema di protezione dei dati personali.
Nell'ambito del Gruppo, ciascuna Società, rappresentata dal Consiglio di Amministrazione, è Titolare del trattamento per i dati che acquisisce e gestisce in connessione con la propria operatività.
Il Consiglio di Amministrazione può nominare l'Amministratore Delegato quale "**Delegato del Titolare**" per porre in essere gli adempimenti previsti dalla normativa in capo al Titolare nell'ambito della Società di riferimento. A sua volta, il Delegato del Titolare può sub-delegare, ad altre figure interne, l'esercizio di taluni degli adempimenti previsti in capo al Titolare, quale la nomina dei Responsabili del trattamento, come previsto nella normativa interna in materia di sub-deleghe tempo per tempo vigente.

5.1.2 Data Protection Team

Il Data Protection Team è un gruppo di lavoro facoltativo cui sono demandati **compiti di coordinamento e di indirizzo** in materia di protezione dei dati personali.
Il Data Protection Team viene convocato sulla base di specifiche necessità operative per facilitare la collaborazione tra i principali attori che nella loro attività ordinaria hanno già un ruolo nella gestione dei dati. A titolo esemplificativo, il Data Protection Team può essere convocato in caso di gestione dei data breach o in caso di valutazione di nuovi servizi/trattamenti, ovvero nuove progettualità tecnologiche, in accordo con il principio di Privacy by Design e Privacy by Default.
Il Gruppo è composto dal DPO, la funzione Compliance, i Corrispondenti per la protezione dei dati personali, ai quali possono affiancarsi, per tematiche di loro interesse, anche i rappresentanti della funzione Risorse Umane, Transformation e Organizzazione, dell'area legale, del settore ICT, nonché i Data Manager.
Il Data Protection Team risponde alle seguenti esigenze:

- permettere il coordinamento e il monitoraggio delle iniziative promosse dal Titolare del trattamento con impatto in ambito Data Protection;
- supportare il DPO nell'esecuzione di compiti che richiedano una visione di maggior dettaglio degli assetti organizzativi del gruppo;
- supportare il DPO nelle attività connesse alla gestione dei data breach;
- fungere da punto di raccordo e di discussione tra il DPO e i Data Manager.

5.1.3 La funzione compliance

La funzione compliance, ove prevista, assicura la conformità dell'organizzazione ai requisiti della normativa Data Protection applicabile.
Il suo principale compito consiste nella comprensione e nell'identificazione del perimetro delle norme applicabili, così come sul loro possibile impatto su processi e procedure aziendali; in particolare, la funzione compliance garantisce costantemente il rispetto della normativa interna in materia di Data Protection, con riferimento a modifiche organizzative che possano portare ad una ridefinizione degli obblighi dei soggetti coinvolti.
In caso di previsione di un elevato rischio di non conformità, la funzione compliance individua idonee procedure per la prevenzione di tale rischio, o perlomeno, per la sua mitigazione. Inoltre, può supportare la funzione HR nell'individuazione dei contenuti relativi ai corsi di formazione in ambito Data Protection che sono erogati al personale.
Nella sua attività, la funzione compliance mantiene la sua indipendenza funzionale all'interno della compagine societaria.
In alcune legal entity del Gruppo (es: Italfondiario, soggetto vigilato da Banca d'Italia) la funzione compliance può eseguire controlli di secondo livello sulla base delle normative locali applicabili al contesto societario.

5.1.4 Funzione di governo ICT

Con specifico riferimento all'ambito normativo della sicurezza dei dati personali e cybersecurity, la funzione di governo ICT ha in carico tutte le attività connesse alla sicurezza informatica e continuità operativa compresa la definizione di policy e procedure IT.
A livello Global, Group IT, all'interno della funzione del COO, assicura:

- La definizione di strategie/politiche di Gruppo in materia di IT e Sicurezza, allineate all'evoluzione della strategia di business;
- La progettazione, il mantenimento, il monitoraggio dei progetti e l'ottimizzazione dell'architettura IT;
- La definizione e il monitoraggio di una efficace metodologia di gestione della domanda, del portafoglio e dell'implementazione dei sistemi IT;
- La definizione di linee guida ed il monitoraggio della pianificazione annuale del Piano di Business Continuity e Disaster Recovery definito a livello di Gruppo;
- La definizione e il monitoraggio del budget IT di gruppo/locale salvaguardando l'allineamento con le decisioni strategiche del Gruppo;
- La supervisione dell'innovazione tecnologica del Gruppo;
- La gestione di fornitori di servizi di terze parti monitorando gli obiettivi chiave del livello di servizio IT locale.

A livello locale, le Funzioni ICT, nel rispetto delle linee di indirizzo e coordinamento definite da Group IT e delle normative locali, garantiscono l'attuazione delle attività connesse alla

sicurezza informatica e alla continuità operativa, ivi inclusa la definizione di policy e procedure IT locali, anche interfacciandosi e supervisionando gli eventuali outsourcer IT[1].

5.2 RUOLI DI SORVEGLIANZA

I ruoli di sorveglianza svolgono la funzione primaria di monitorare il rispetto della normativa Data Protection e il livello di rischio per i diritti e le libertà fondamentali degli Interessati con riferimento ai trattamenti di dati personali effettuati dalla società.

5.2.1 Il Data Protection Officer

Il GDPR, agli artt. 37-39, ha introdotto la figura del "Data Protection Officer" (per brevità "DPO"), prevedendo in taluni casi l'obbligo per i Titolari e i Responsabili del trattamento di nominare tale figura (laddove non obbligatoria, la nomina del DPO è comunque incoraggiata dalle Autorità).
Il DPO assolve a funzioni di supporto e controllo, consultive, formative ed informative relativamente all'applicazione del GDPR e della normativa nazionale in materia di trattamento dei dati personali, coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli Interessati, per le questioni connesse al trattamento dei dati personali.
Con riferimento ai Titolari e Responsabili del trattamento, il GDPR prevede l'obbligo di designare un DPO per i soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli Interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati. Il Garante Privacy ha chiarito che tra tali soggetti rientrino, a titolo esemplificativo e non esaustivo, istituti di credito, società finanziarie, società di informazioni commerciali, società di recupero crediti. Inoltre, il GDPR prevede che un gruppo imprenditoriale possa designare un unico DPO, purché lo stesso tale sia facilmente raggiungibile da ciascuna società del gruppo.
Infine, la normativa definisce i requisiti propri della figura del DPO, prevedendo che questo:

- possegga un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche ed organizzative o di misure atte a garantire la sicurezza dei dati;
- adempia alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse;
- operi alle dipendenze del Titolare o del Responsabile oppure sulla base di un contratto di servizio (qualora il DPO sia individuato in un soggetto esterno alla società);
- disponga di autonomia e risorse sufficienti per svolgere in modo efficace i propri compiti. In particolare al DPO dovrà essere garantito da parte del Titolare del trattamento:
    - una struttura composta da un numero adeguato di collaboratori che lo supportino nelle attività operative;

[1] In doValue a livello locale italiano, la funzione di governo ICT è identificata, all'interno della Funzione Retained Organization, nella struttura Design Authority/ Innovation, Security & BCM, nella quale è inserito il ruolo dell'ICT Security Manager.

- un budget che potrà essere utilizzato discrezionalmente dal DPO per le necessità operative della propria struttura, ivi compreso per attuare un piano formativo per l'aggiornamento continuo del DPO e dei propri collaboratori.

5.2.1.1 Il Global DPO

Il Gruppo doValue, a seguito dello svolgimento di analisi della normativa e dei documenti di approfondimento emanati a livello europeo e nazionale, ha ritenuto opportuno prevedere la nomina, a livello Corporate, di un Global DPO che opera presso la Capogruppo (doValue S.p.A.).
Come evidenziato nella seguente figura (cfr. fig. 2), sulla base dell'assetto societario ed organizzativo del Gruppo doValue, il Global DPO è collocato all'interno della funzione Compliance & Global DPO e riporta gerarchicamente al General Counsel e funzionalmente al Consiglio di Amministrazione che rappresenta il Titolare dei dati.
Le frecce, di forma e colore diverso, indicano le relazioni intercorrenti i tra le figure presenti nella figura:

- Riporto gerarchico (freccia continua): il Global DPO riporta al General Counsel della Capogruppo;
- Riporto funzionale (freccia blu tratteggiata)**:** il Global DPO si relaziona periodicamente con il CdA di Capogruppo;

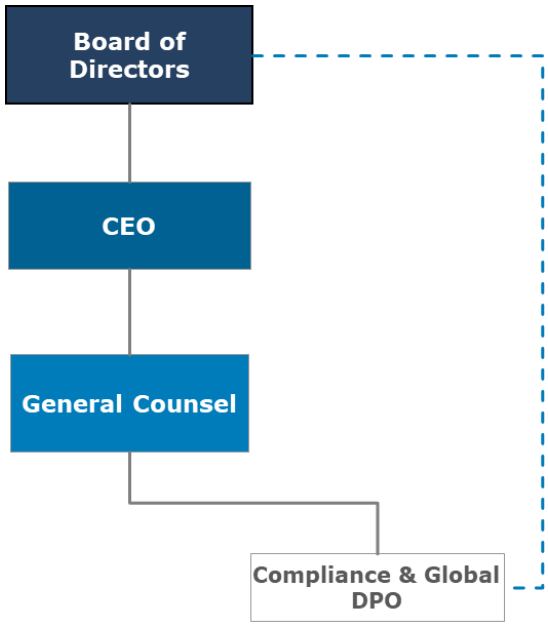


Fig. 2 – Posizionamento del Global DPO nel Gruppo doValue

Con riferimento alle attività di indirizzo e coordinamento, il GLOBAL DPO:

a) definisce il Framework di Controllo del Gruppo in ambito Data Protection ed i relativi strumenti operativi per il monitoraggio della compliance alla normativa Data Protection;

b) riceve da tutti i LOCAL DPO un'informativa in merito alla pianificazione delle attività di monitoraggio che saranno eseguite nell'anno entrante (Piani DPO Local);

c) riceve da tutti i LOCAL DPO un'informativa in merito alle risultanze delle attività di monitoraggio svolte presso le società controllate italiane ed estere, funzionale alla gestione del rischio per i diritti e le libertà degli Interessati, ad eventuali violazioni locali dei dati o reclami degli Interessati che potrebbero avere un impatto rilevante per il Gruppo, ovvero ispezioni delle Autorità locali;

d) consolida le informazioni ricevute e riporta al CDA della Capogruppo una visione consolidata a livello Corporate in merito alle risultanze delle attività di monitoraggio svolte nel Gruppo, funzionale alla gestione del rischio per i diritti e le libertà degli Interessati, nonché ad eventuali violazioni locali dei dati (data breach), reclami e/o istanze privacy che potrebbero avere un impatto rilevante per il Gruppo;

e) coordina le analisi di rischio e le analisi di impatto per i diritti e libertà degli Interessati connesse ad iniziative progettuali trasversali che interessano il Gruppo

f) fornisce pareri su tematiche Data Protection che interessano il Gruppo od interpretazioni di normative in materia di protezione dei dati personali applicabili a tutto il Gruppo;

g) supporta la definizione di piani formativi in materia di protezione dei dati personali destinati a tutto il Gruppo.

con riferimento alle attività di sorveglianza connesse ai trattamenti di dati personali svolti a livello corporate, il GLOBAL DPO:

a) monitora le attività di trattamento dei dati svolte a livello Corporate;
b) informa e fornisce consulenza al Titolare/Data Manager, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi previsti dalla normativa in materia;
c) sorveglia l'osservanza dei requisiti previsti dal Regolamento Europeo e altre normative in materia di protezione dei dati personali, nonché dalla presente Policy e dalla normativa interna in materia di trattamento dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
d) fornisce un parere nell'ambito delle attività di valutazione d'impatto dei trattamenti eseguiti a livello Corporate per i diritti e le libertà degli Interessati e sorveglia lo svolgimento delle eventuali azioni di mitigazione dei rischi proposte;
e) coopera e funge da contatto per l'Autorità di controllo per le questioni connesse al trattamento dei dati personali svolto a livello corporate;

f) funge da contatto per gli Interessati per tutte le questioni relative al trattamento dei loro dati personali eseguiti a livello Corporate e all'esercizio dei loro diritti;
g) predispone la reportistica inerente alle attività di sorveglianza svolte per tutti gli organi di governo e controllo della Capogruppo (CDA, ODV).

5.2.1.2 I Local DPO

I Local DPO sono nominati ed operano nelle Società controllate italiane ed estere ed hanno in carico le seguenti attività:

a) informare e fornire consulenza al Titolare/Data Manager, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi previsti dalla normativa locale in materia di protezione dei dati personali;
b) sorvegliare l'osservanza dei requisiti previsti dal Regolamento Europeo e da altre normative in materia di protezione dei dati personali, nonché dalla presente Policy e dalla normativa interna in materia di trattamento dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. A tal fine, predispone annualmente un piano di attività di controllo che sottopone al CDA della Società, previa condivisione con il Global DPO (il Piano DPO Local);
c) fornire un parere nell'ambito delle attività di valutazione d'impatto dei trattamenti per i diritti e le libertà degli Interessati e sorveglia lo svolgimento delle eventuali azioni di mitigazione dei rischi proposte. Nel caso di trattamenti che, alla luce di una valutazione d'impatto, rivelino rischi specifici in materia di tutela dei dati personali, il LOCAL DPO assiste il Titolare/Responsabile nella consultazione dell'Autorità di controllo, al fine di ottenere da quest'ultimo un parere scritto preliminare in merito alla conformità del trattamento al Regolamento;
d) supportare la funzione HR nella formazione del personale sui temi Data Protection;
e) cooperare e fungere da contatto per l'Autorità di controllo per le questioni connesse al trattamento dei dati personali svolti all'interno della Società controllata;
f) fungere da contatto per gli Interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti;
g) nel caso di episodi di violazione dei dati personali, ai sensi dell'art. 33 GDPR, il LOCAL DPO assistere il Titolare che deve comunicare l'accaduto all'Autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza;
h) predisporre la reportistica inerente alle attività di sorveglianza svolte, funzionali alla gestione del rischio per i diritti e le libertà degli Interessati, per tutti gli organi di governo e controllo societari (CDA, ODV).
i) predisporre un'informativa indirizzata al GLOBAL DPO in merito alle risultanze delle attività di monitoraggio svolte localmente, ad eventuali violazioni locali dei dati o reclami degli Interessati che potrebbero avere un impatto rilevante per il Gruppo o ad eventuali ispezioni dell'Autorità di controllo per la protezione dei dati;
j) Vigilare in merito all'attuazione delle policy e dei regolamenti di Gruppo.

Nel caso in cui una Società del Gruppo doValue non sia obbligata alla nomina del LOCAL DPO (ai sensi dell'art. 37 comma 1) ed è stata esclusa l'adozione di tale ruolo su base volontaria, il presidio dovrà essere garantito dalla Funzione di compliance o Legal locale o da altra

struttura interna, laddove non presenti entrambe le strutture indicate. A tale struttura saranno assegnate le seguenti responsabilità:

- presidiare l'osservanza dei requisiti previsti dal Regolamento Europeo e da altre normative locali in materia di protezione dei dati personali, nonché dalla presente Policy e dalla normativa interna in materia di trattamento dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- supportare il Titolare del trattamento nella gestione delle relazioni con l'Autorità di controllo Locale e/o nella gestione delle richieste di esercizio ricevute dagli Interessati del trattamento;
- predisporre un'informativa indirizzata al Global DPO in merito ad eventuali carenze riscontrate sul sistema Data Protection che potrebbero causare una non conformità del sistema stesso, ad eventuali violazioni locali dei dati o ad eventuali reclami ricevuti dagli Interessati che potrebbero avere un impatto rilevante per il Gruppo o ad eventuali ispezioni dell'Autorità di controllo locale;
- monitorare l'avanzamento delle eventuali attività di adeguamento intraprese per colmare le lacune riscontrate sul sistema di protezione dei dati personali della Società.

Nelle figure che seguono si fornisce una rappresentazione dell'assetto societario e delle relazioni esistenti tra il Global DPO e i Local DPO delle Società controllate. Le frecce, di forma e colore diverso, indicano le relazioni intercorrenti tra le figure presenti nella figura:

- riporto gerarchico (freccia continua): indicano i rapporti gerarchici esistenti negli assetti societari;
- riporto funzionale (freccia blu tratteggiata)**:** i Local DPO si relazionano periodicamente con i rispettivi CdA;
- flusso informativo e reportistica (freccia rossa tratteggiata): i Local DPO si relazionano con il Global DPO su specifiche tematiche DP (i.e. informative in merito ad attività di monitoraggio o alla gestione di specifici eventi, al coordinamento su attività comuni, ad ispezioni dell'Autorità di controllo locale).

Come evidenziato nella seguente figura (cfr. fig. 3), sulla base dell'assetto societario ed organizzativo del Gruppo doValue, il Local DPO di doValue è collocato all'interno della funzione Country Compliance & DPO e riporta gerarchicamente alla funzione Legal e funzionalmente al Consiglio di Amministrazione che rappresenta il Titolare dei dati.

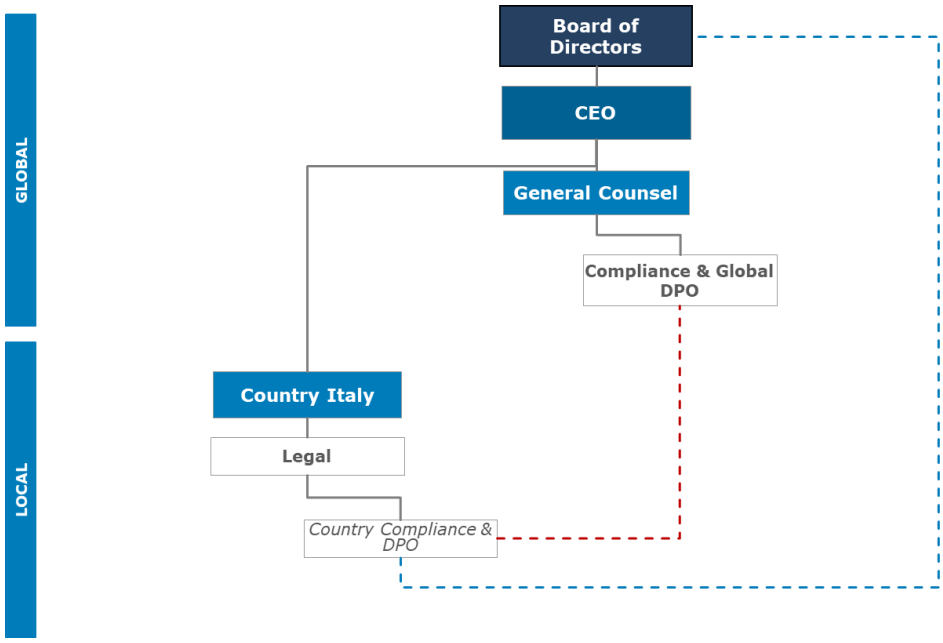


Fig. 3 – Posizionamento del Local DPO in doValue

I Local DPO nelle Società controllate italiane Italfondiario e doData rispondono funzionalmente rispettivamente al Consiglio di Amministrazione e all'Amministratore unico che rappresentano il Titolare dei dati. Inoltre, i Local DPO dovranno informare il Global DPO della Capogruppo in merito ad attività di monitoraggio svolte localmente, violazioni locali dei dati, ispezioni dell'Autorità di controllo o reclami degli Interessati.

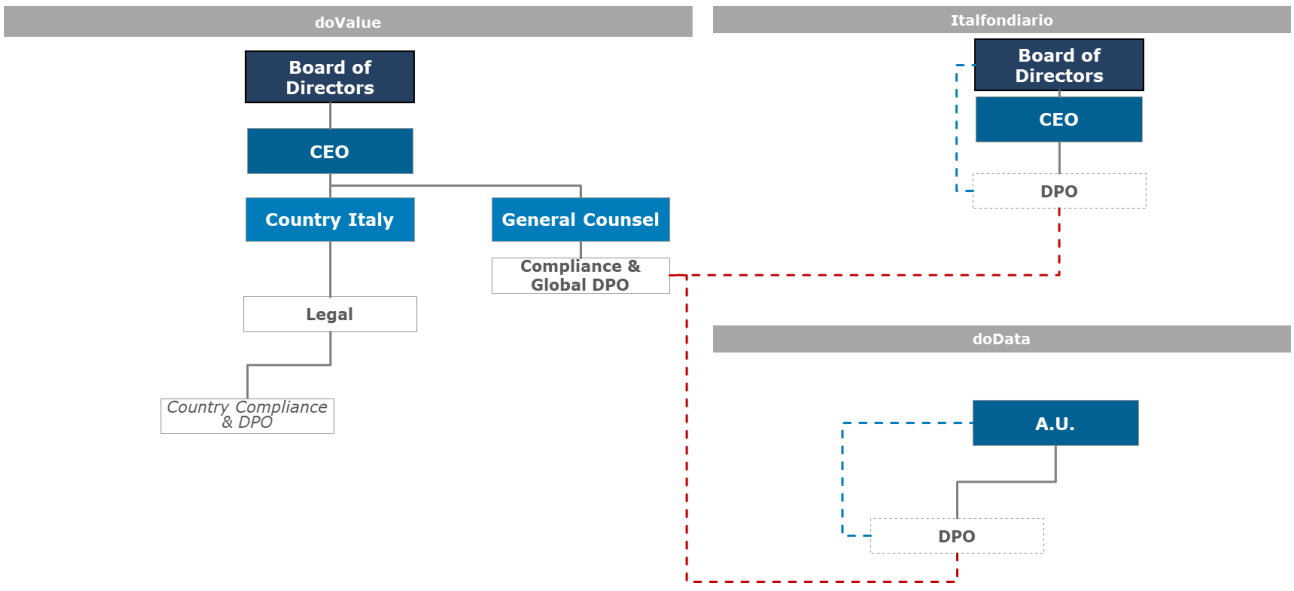


Fig. 4 – Posizionamento del Local DPO nelle Società controllate italiane del Gruppo doValue

Nelle figure seguenti si evidenziano i rapporti tra il Global DPO e i Local DPO delle Società controllate estere.

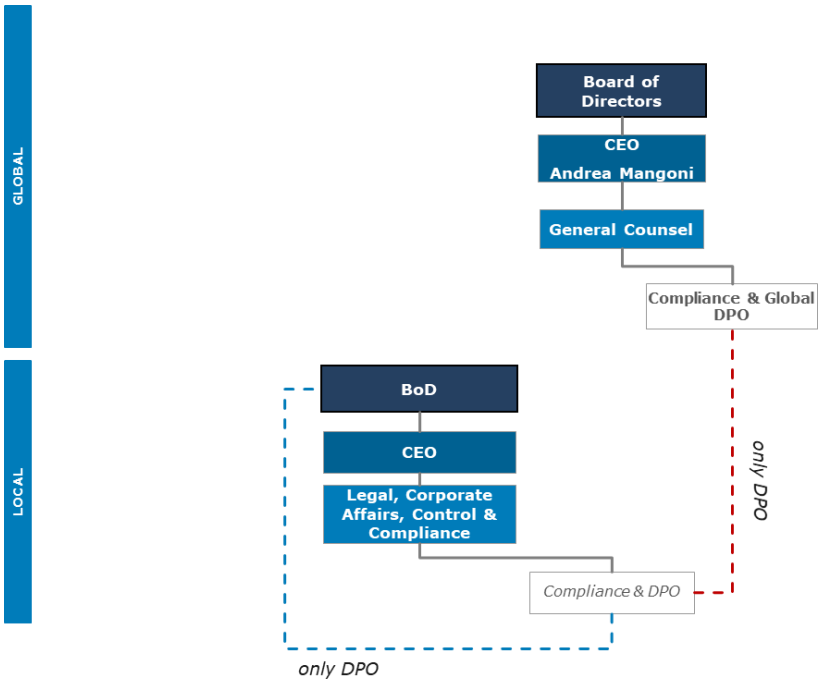


Fig. 5 – Posizionamento del Local DPO nella Società controllata Altamira

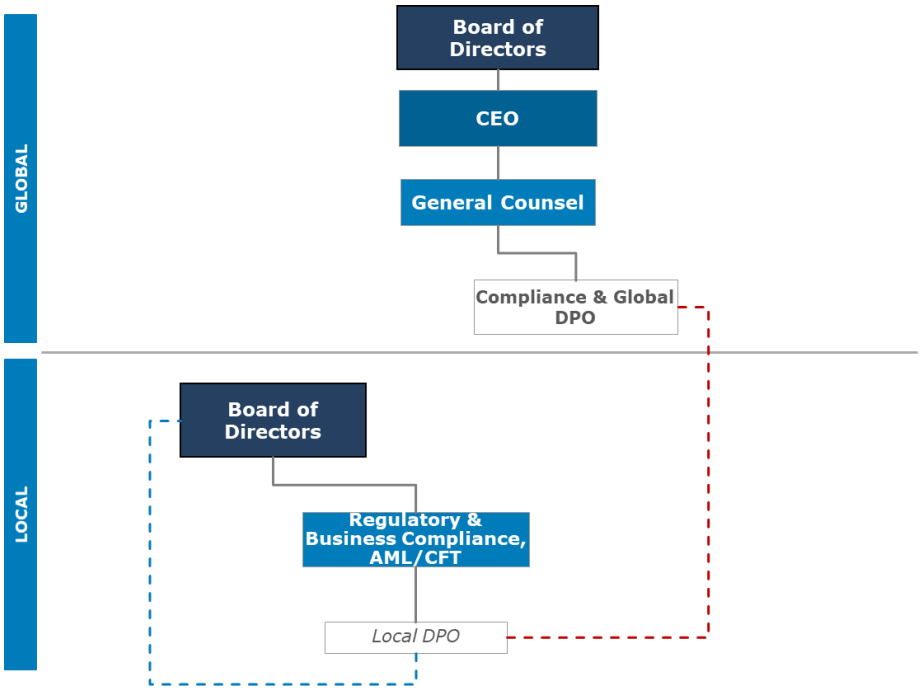


Fig. 6 – Posizionamento del Local DPO nella Società controllata doValue Greece

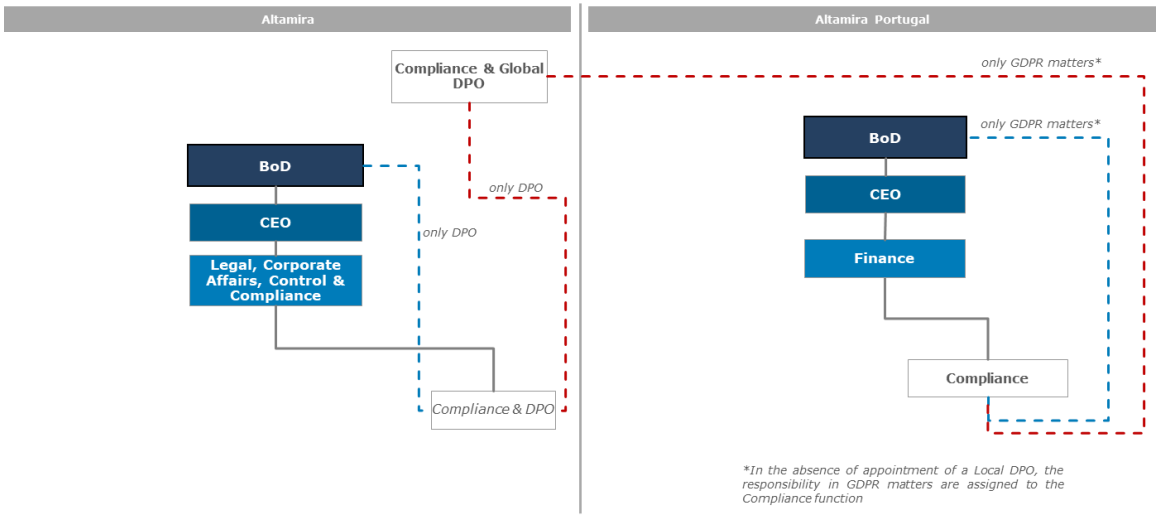


Fig. 7 – Posizionamento del Local DPO nelle Società controllate di Altamira.

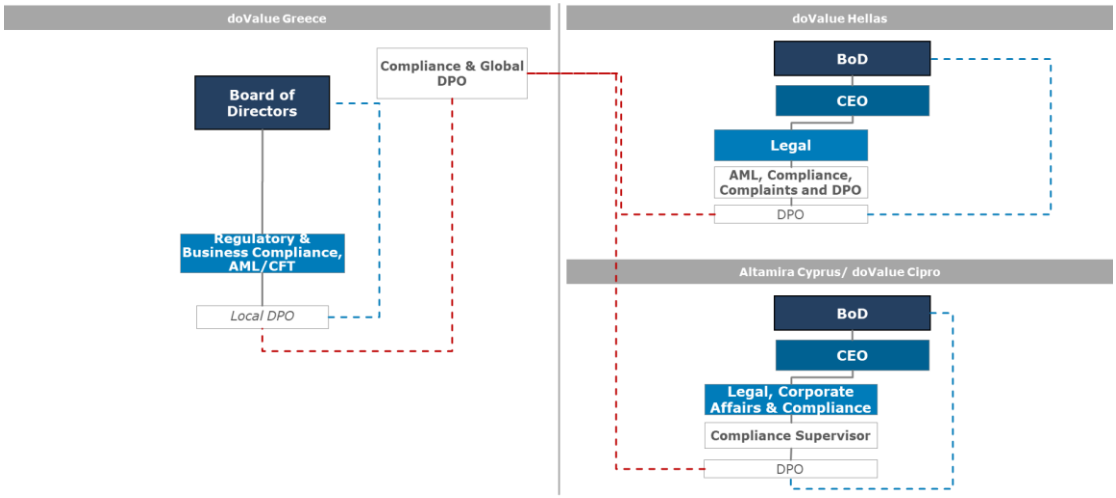


Fig. 8 – Posizionamento del Local DPO nelle Società controllate di doValue Greece.

I dati di contatto dei Local DPO devono essere comunicati all'Autorità di controllo nazionale, resi noti ai dipendenti delle Società tramite apposita comunicazione e comunicati agli Interessati dei trattamenti.

5.2.2 Il Corrispondente per la protezione dei dati personali

Il Corrispondente per la protezione dei dati personali è una figura opzionale, di supporto al Local DPO nella gestione operativa delle tematiche Data Protection, ed agisce, all'interno delle Società, nel caso in cui la figura del LOCAL DPO sia esternalizzata presso un'altra Società del Gruppo o presso un fornitore esterno. Il Corrispondente per la protezione dei dati personali agisce quale punto di contatto con il Local DPO, il Data Protection Team e i Data Manager delle singole funzioni aziendali.
Per le Società controllate, il Corrispondente per la protezione dei dati personali viene nominato dal Delegato del Titolare.

Tra le sue principali attività rientrano:

- allineare periodicamente il Local DPO su tematiche di natura Data Protection in modo da consentire l'intervento tempestivo se necessario;
- supportare il Local DPO nell'esecuzione delle attività a lui affidate (es. monitoraggio circa l'applicazione dei requisiti previsti dal Regolamento, gestione clausole contrattuali, aggiornamento informative ecc.);
- collaborare nell'applicazione del principio di Data Protection by Design e by Default;
- partecipare alle attività di valutazione d'impatto dei trattamenti per i diritti e le libertà degli Interessati
- supportare le attività di definizione e aggiornamento dei registri di Trattamento;
- supportare la gestione del processo di segnalazione dei data breach.

5.2.3 L'Internal Audit

Indipendentemente dalle funzioni di sorveglianza svolte dal DPO, nell'ambito del ciclo di pianificazione triennale definito secondo una logica *risk-based*, la Funzione Internal Audit (sia Locale che di Gruppo), in ottica di controllo di III livello, monitora i rischi cui il Gruppo è esposto nel trattamento dei dati personali dei soggetti Interessati e valuta l'adeguatezza e la conformità con la normativa esterna ed interna di riferimento, tempo per tempo vigente, del sistema dei controlli implementato in materia di privacy.
Inoltre, su richiesta e/o autorizzazione del Consiglio di Amministrazione, la Funzione Internal Audit potrà valutare l'adeguatezza e funzionalità del framework di controllo del DPO riportando tali valutazioni all'interno delle proprie relazione periodiche indirizzate al CdA.

5.3 LINEE OPERATIVE

5.3.1 Data Manager

In considerazione del ruolo di supervisione ed indirizzo delle attività svolte dalle strutture a loro riporto, e avendo essi l'esperienza, capacità ed affidabilità necessaria, i responsabili di Direzione/Funzione a diretto riporto dell'Amministratore Delegato o del Consiglio di Amministrazione delle Società del Gruppo, sono identificati quali Data Manager per le operazioni di trattamento riferite alla propria Direzione /Funzione e coerentemente con quanto riportato nel Registro dei trattamenti della Società di appartenenza.
Il Data Manager, nominato attraverso un apposito atto scritto, ha il compito di verificare che tutti i trattamenti effettuati nelle strutture che ricadono sotto la sua responsabilità siano conformi agli obblighi di legge e alle prescrizioni dell'Autorità di controllo, oltre che alle istruzioni ricevute dal Titolare, e che sia garantita l'attuazione delle misure tecniche ed organizzative individuate a protezione dei dati personali trattati. Il dettaglio sui compiti e le responsabilità loro attribuite sono declinati nelle lettere di nomina a Data Manager, sulla base dei trattamenti effettuati nelle diverse strutture di competenza.

5.3.2 Addetto al trattamento

Gli Addetti al Trattamento sono le persone fisiche che operano sotto l'Autorità diretta di una Società del Gruppo e svolgono specifici compiti e funzioni connessi al Trattamento di dati personali.
Le Società, in qualità di Titolari del Trattamento, designano quali "Addetto al trattamento dei dati personali" ogni lavoratore dipendente (senza distinzione di funzione, inquadramento e/o livello), nonché ogni collaboratore della Società, a prescindere dal rapporto contrattuale (ad esempio, lavoratori somministrati, collaboratori, tirocinanti, consulenti) con la stessa intrattenuto, a cui siano attribuite credenziali di autenticazione per l'accesso alla rete informatica del Gruppo (fatta eccezione per i collaboratori e consulenti operanti per società già nominate Responsabili Esterni del Trattamento e che, a loro volta, dovranno nominare propri addetti del trattamento le persone fisiche che operano sotto la loro Autorità).
Ogni addetto è tenuto ad osservare scrupolosamente le istruzioni e le misure di sicurezza riportate nella lettera di nomina, oltre a quanto previsto dalla presente Policy e dalla normativa interna di dettaglio.
Il contenuto delle istruzioni è dettagliato, per conto del Titolare, dai singoli Data Manager, avuto riguardo agli specifici Trattamenti effettuati nella struttura di competenza e alle relative modalità e finalità degli stessi.

Gli Addetti al Trattamento sono destinatari di interventi formativi finalizzati ad acquisire familiarità con i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, i compiti e le responsabilità che ne derivano e conoscere le misure disponibili per prevenire eventi dannosi.

5.3.3 Funzione ICT – Amministratori di sistema

Per le Società italiane appartenenti al Gruppo doValue, gli Amministratori di sistema devono essere formalmente nominati così come definito all'interno del Provvedimento intitolato *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* (del 27 novembre 2008 e s.m.i.).
Gli Amministratori di Sistema (di seguito anche "AdS") sono i soggetti incaricati della gestione e della manutenzione dei sistemi di elaborazione dei dati e delle informazioni aziendali; con tale termine, si distinguono varie figure quali: gli amministratori di basi di dati, di reti e di apparati di sicurezza e di sistemi software complessi.
Gli AdS, nello svolgimento delle proprie attività tecniche, si trovano nella condizione di svolgere azioni da considerare a tutti gli effetti come trattamenti di dati personali.
Le principali attività degli Amministratori di sistema sono:

- supportare nel quotidiano gli Addetti al Trattamento e i Data Manager per gli aspetti di tipo tecnico informatico inerenti ai sistemi informatici utilizzati per i trattamenti di dati personali;
- riportare ai Data manager eventuali malfunzionamenti dei sistemi informatici;
- supportare i Data manager (e il local DPO) nelle attività di analisi degli eventi che hanno causato una violazione dei dati personali;
- eseguire attività di manutenzione dei sistemi e dei presidi di sicurezza.

Tali attività nelle Società controllate estere, dove non è previsto localmente l'obbligo di nominare gli Amministratori di sistema, sono demandate alla funzione ICT locale.

5.4 SOGGETTI TERZI

A seconda dei casi e della tipologia di trattamento, i soggetti terzi possono assumere un ruolo diverso secondo quanto indicato nei seguenti paragrafi.

5.4.1 Soggetti terzi – Titolare del trattamento

Alcuni soggetti esterni possono ricoprire il ruolo di Titolare autonomo del trattamento in ragione del fatto che procedono con l'erogazione dei propri servizi in forza di codici deontologici di settore e/o mandati di rappresentanza e con l'ausilio della propria organizzazione. Tra coloro che possiedono queste caratteristiche si segnalano: i liberi professionisti (Studi legali, Commercialisti e Notai).

5.4.2 Soggetti terzi – Co-Titolare

Ai sensi dell'art. 26 del GDPR, sono definiti "Co-Titolari" o "Contitolari" del trattamento due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR. Le Società del Gruppo doValue possono assumere il ruolo di co-Titolari su alcuni trattamenti svolti in comune.

5.4.3 Soggetti terzi – Responsabile del trattamento

Il Responsabile del Trattamento è una persona fisica o giuridica, esterna all'organizzazione della Società, che, nell'ambito di rapporti contrattuali con Società del Gruppo, effettui Trattamento di dati personali di cui la medesima Società sia Titolare.
La designazione del Responsabile e i trattamenti da questo effettuato devono essere disciplinati, ai sensi dell'art. 28.3 GDPR in un contratto o altro atto giuridico, che vincoli il Responsabile del Trattamento e disciplini la materia del trattamento, durata, natura e finalità del trattamento, il tipo di dati personali e le categorie di Interessati, gli obblighi e i diritti del Titolare.
In particolare spetterà al Responsabile individuato:

- assicurare la liceità delle operazioni di Trattamento attenendosi alle istruzioni, di volta in volta, fornite dalla Società del Gruppo Titolare del trattamento;
- garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza;
- implementare il processo per rispondere all'Interessato nell'esercizio dei propri diritti, nell'eventualità che il Titolare abbia delegato al Responsabile esterno tale adempimento ovvero che le richieste ricevute siano immediatamente trasferite al Titolare affinché venga predisposto il necessario riscontro nel rispetto dei termini prescritti;
- fornire tutte le informazioni necessarie per dimostrare il rispetto della normativa applicabile e delle istruzioni ricevute fermo restando il diritto per il Titolare di effettuare ispezioni relativamente alla corretta applicazione delle prescrizioni e delle istruzioni fornite;

- cessare immediatamente le operazioni di Trattamento sui dati personali e provvedere alla loro cancellazione o renderli disponibili al Titolare in caso di revoca dell'incarico di Responsabile Esterno del Trattamento o su richiesta del Titolare stesso;
- consentire eventuali audit da parte delle Società del Gruppo e di prestare la più ampia collaborazione nella rilevazione di incidenti di sicurezza che interessino di dati personali (data breach) al fine di dare attuazione alle prescrizioni normative applicabili.

Nell'ambito degli accordi di esternalizzazione delle attività svolte a livello corporate, ciascuna Società fornitrice di servizi infragruppo è nominata Responsabile ovvero Sub-Responsabile (ai sensi del successivo para. 5.4.4) del Trattamento da parte delle altre Società del Gruppo. Inoltre, sono oggetto di nomina i fornitori e le terze parti che trattano dati di titolarità delle Società del Gruppo quali, ad esempio, soggetti coinvolti nell'esecuzione di attività connesse ai prodotti e ai servizi erogati verso gli Interessati.

5.4.4 Soggetti terzi – Sub-responsabile

Previa autorizzazione scritta, generale o specifica, del Titolare, il Responsabile esterno può a sua volta designare un altro Responsabile (cd. Sub-Responsabile del Trattamento), con riferimento a soggetti terzi, persone fisiche o giuridiche, che effettuino Trattamenti di dati personali nell'ambito delle attività per cui questo è nominato Responsabile.
Il rapporto tra Responsabile e sub-Responsabile deve essere regolato, similmente a quello tra Responsabile e Titolare, da un atto contrattuale o altro atto giuridico che specifichi compiti e responsabilità ai sensi dell'art. 28.4 del GDPR. Il Responsabile assume la piena responsabilità nei confronti del Titolare del rispetto degli obblighi da parte del Sub-Responsabile.
Con riferimento ai dati personali dei soggetti obbligati, trattati in connessione alle attività di recupero del credito, come detto, le Società del Gruppo doValue operano in qualità di Responsabili esterni del Trattamento designata dalle Mandanti quali Titolari del Trattamento. Con autorizzazione (generale o specifica) del Titolare, la Società può avvalersi di sub-fornitori e nomina quali sub-Responsabili i fornitori e, in generale, le terze parti che, in virtù di un contratto con le Società, trattino dati personali dei soggetti obbligati, quali i Professionisti Esterni, le società di Recupero Crediti e/o i fornitori di servizi informatici.

5.5 LE RELAZIONI TRA RUOLI DI GOVERNO E SORVEGLIANZA

Nelle tabelle seguenti sono indicate le relazioni tra i diversi ruoli Data Protection identificati dal Gruppo doValue, specificando se la relazione si basa su:

- riporto gerarchico;
- riporto funzionale;
- flusso informativo e coordinamento tra soggetti appartenenti a diverse legal entity del Gruppo;
- flusso informativo interno tra soggetti appartenenti alla stessa legal entity;
- interfaccia con soggetti terzi esterni al Gruppo.

Funzioni coinvolte	Relazione	Descrizione
Titolare – Global/Local DPO	Riporto funzionale	• Il Titolare, coinvolge il GLOBAL DPO o il Local DPO in caso di verifica ispettiva e/o richieste inoltrate da Organi/Autorità di Controllo rispettivamente a livello Corporate e a livello Locale • Il GLOBAL DPO predispone la relazione periodica in merito alle attività di sorveglianza svolta a livello Corporate, presidia le iniziative necessarie per far fronte alle richieste pervenute dall'Autorità di Controllo e riferisce al Titolare sull'andamento delle azioni intraprese a livello Corporate • Il Local DPO predispone la relazione periodica in merito alle attività di sorveglianza svolta a livello locale, presidia le iniziative necessarie per far fronte alle richieste pervenute dall'Autorità di Controllo e riferisce al Titolare sull'andamento delle azioni intraprese a livello locale
GLOBAL DPO – Group IT	Flusso Informativo interno	Il Global DPO e la funzione Group IT si interfacciano per la richiesta di pareri su tematiche Data Protection nell'ambito delle attività di evoluzione e mantenimento del sistema di gestione dei dati personali a livello di Gruppo (ad esempio in caso di progetti IT rilevanti con impatto sulle modalità di gestione e protezione dei dati personali).
Local DPO – Funzione compliance (se esistente) + Governo ICT Local	Flusso Informativo interno	La funzione compliance (se esistente) e la funzione Governo ICT locale si interfacciano con il Local DPO per la richiesta di pareri su tematiche Data Protection nell'ambito delle attività di mantenimento del sistema di gestione dei dati personali.

Funzioni coinvolte	Relazione	Descrizione
Global DPO- Local DPO	Flusso informativo e coordinamento	Nei limiti di cui agli artt. 37-39 GDPR e nel rispetto dell'indipendenza professionale i Local DPO s'interfacciano con il Global DPO per: • Confrontarsi su dubbi interpretativi, sulla normativa Data Protection • Informare su eventi locali dalle quali possano scaturire dei rischi per il sistema di protezione dei dati personali di Gruppo (i.e. data breach, mancata applicazione dei principi sanciti dal GDPR, analisi rischi/valutazioni d'impatto, corretta individuazione delle basi giuridiche per il trattamento) • Informare in merito alle attività di sorveglianza svolte e livello locale e riportate al CdA della Società controllata • Coordinarsi sulle attività di monitoraggio da svolgere localmente • Valutare l'adozione di politiche/procedure/istruzioni operative declinate a livello locale e/o di specifiche sessioni di formazione e sensibilizzazione sui temi della protezione dei dati per le risorse
Local DPO – Corrispondente per la protezione dei dati	Riporto funzionale	Per le Società controllate che esternalizzano la funzione del DPO al Local DPO di Capogruppo o a soggetti esterni al Gruppo: • il Local DPO di capogruppo si interfaccia con il Corrispondente per la protezione dei dati per tutte le questioni riconducibili al trattamento dei dati personali e alle tematiche Data Protection inerenti alla Società controllata • Il Corrispondente per la protezione dei dati cura, sentito il Local DPO, l'emanazione di politiche e linee guida e opera come riferimento per le strategie aziendali e le azioni migliorative che si rendessero necessarie al sistema DP societario • Il Corrispondente per la protezione dei dati interagisce e si relaziona con il Local DPO su specifiche tematiche che richiedono un approfondimento di natura organizzativa e/o normativa; nel caso di anomalie o criticità, le segnala tempestivamente al Local DPO.

Funzioni coinvolte	Relazione	Descrizione
Internal Audit - GLOBAL/LOCAL DPO	Flusso Informativo interno	L'Internal Audit si interfaccia con il Global DPO e con il LOCAL DPO per coordinarsi e ricevere informazioni in merito ad eventi rilevanti es. i data breach. Inoltre, i Global e il Local DPO informano la funzione Internal Audit in relazione ai piani annuali delle attività di sorveglianza e ai risultati emersi dalle attività di monitoraggio svolte.
Funzione Compliance + Governo ICT local – Data Manager	Flusso Informativo interno	La funzione compliance si interfaccia, con i Data Manager per tutte le questioni legate al mantenimento della conformità del sistema Data Protection ai requisiti normativi previsti dalla normativa europea e locale in materia di protezione dei dati personali (i.e. aggiornamento del Registro dei trattamenti, esecuzione della DPIA, definizione di istruzioni operative) La funzione Governo ICT locale si interfaccia con i Data Manager per tutte le questioni legate al mantenimento dei sistemi informatici e delle relative misure di sicurezza tecniche in essere a protezione dei trattamenti di dati personali.
Global/Local DPO – Responsabili esterni	Interfaccia con soggetti terzi	Il GLOBAL DPO e il Local DPO (rispettivamente nell'ambito di trattamenti Corporate e Locali) interagiscono con i soggetti esterni che, ai sensi dell'art.28.3 GDPR, sono stati individuati quali Responsabili del trattamento per tutte le tematiche che, nell'ambito delle attività attribuite contrattualmente, possono comportare una ricaduta di natura organizzativa e/o normativa sul trattamento di dati personali (i.e. comunicazioni di data breach, verifiche ispettive programmate, valutazioni d'impatto, comunicazioni da inoltrare all' Autorità di controllo)
Local DPO – Data Manager	Flusso Informativo interno	Il Data Manager si interfaccia con il Local DPO per richiesta di pareri in ambito Data Protection durante l'esecuzione delle proprie attività che contribuiscono al mantenimento del Sistema di Data Protection aziendale (es: aggiornamento del Registro, esecuzione della DPIA). Il Local DPO si interfaccia con il Data Manager per la richiesta di informazioni relative alle modalità di trattamento, ai dati trattati o a eventuali problematiche riscontrate per il trattamento.

5.6 LE RELAZIONI TRA LE LINEE OPERATIVE

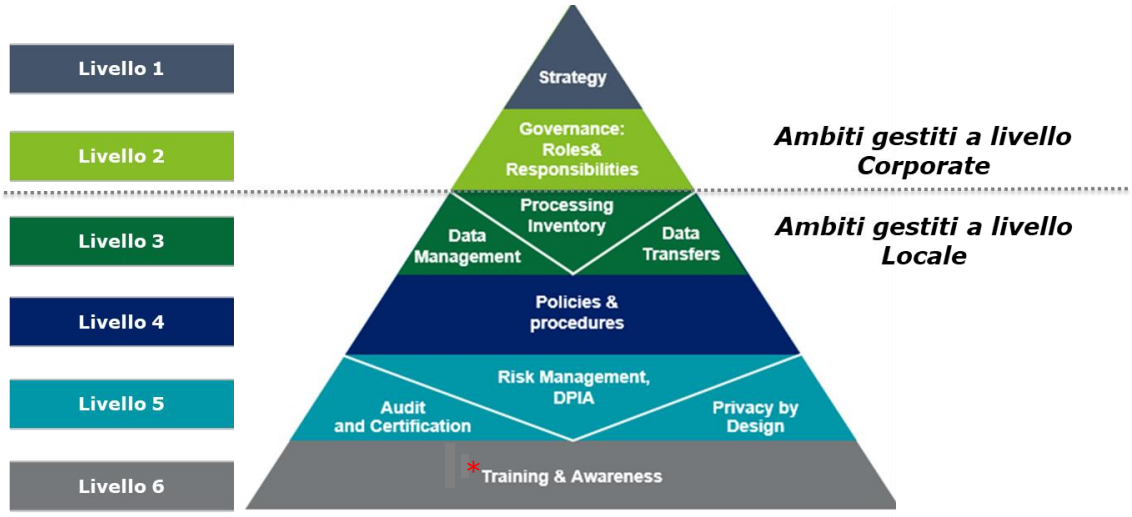
Funzioni coinvolte	Relazione	Descrizione
Data Manager- Addetti trattamento	Riporto gerarchico	A seconda dei casi il Data Manager del trattamento interagisce con gli Addetti al trattamento in caso di: • indicazioni/istruzioni sulle modalità di trattamento, presidio dei dati personali • Aspetti correlati alla corretta applicazione delle misure di sicurezza poste a presidio del trattamento di competenza • revisioni periodiche del censimento dei trattamenti di dati personali • esecuzione delle attività di analisi del rischio e DPIA.
Data Manager - AdS (interni)	Flusso Informativo interno	A seconda dei casi il Data Manager del trattamento interagisce con AdS interni in caso di: • indicazioni/istruzioni sulle modalità di trattamento, presidio dei dati personali • conseguenze derivanti da un malfunzionamento della rete/sistemi IT • Aspetti correlati alla corretta applicazione delle misure di sicurezza poste a presidio del trattamento di competenza • revisioni periodiche del censimento dei trattamenti di dati personali in relazione ai sistemi informatici utilizzati e alle misure di sicurezza poste in essere. • esecuzione delle attività di analisi del rischio e DPIA
Data Manager - **Responsabili esterni**	Interfaccia con soggetti terzi	Il Data Manager, per i trattamenti di sua competenza si interfaccia con i Responsabili del trattamento in caso di: • indicazioni/istruzioni sulle modalità di trattamento, presidio dei dati personali • Richiesta di informazioni specifiche funzionali all'esecuzione della DPIA (i.e. Misure di sicurezza adottate) • ricezione di segnalazioni relative ad eventi di data breach • Gestione degli eventi di data breach (i.e. reperimento di informazioni utili alla notifica della data breach)

6 IL MODELLO DOCUMENTALE DATA PROTECTION

doValue ha definito il proprio **Modello Documentale Data Protection,** applicabile alla **Capogruppo** e a tutte le **Società controllate** del Gruppo (italiane ed estere), costituito da un corpus documentale che comprende:

- a livello **Corporate**:
  - Politica di Gruppo di alto livello che declina la strategia DP del Gruppo, il modello organizzativo DP e gli adempimenti DP generali applicabili a tutte le Società del Gruppo (rappresentata dal presente documento);
  - Framework dei controlli del DPO;
  - Regolamento del DPO.
- a livello **societario**:
  - Procedure/istruzioni operative per la gestione di specifici ambiti come ad esempio la gestione delle data breach, l'aggiornamento del Registro dei trattamenti, la gestione delle richieste degli Interessati ecc.
  - Strumenti/template redatti per adempiere a specifici requisiti normativi come ad esempio i Registri dei trattamenti di dati personali, registri data breach, registri istanze degli Interessati, le nomine DP, le informative privacy, le clausole contrattuali, i DPA ecc.
  - Documenti specifici redatti per dimostrare l'esecuzione di specifiche attività, come ad esempio, le analisi di impatto svolte sui nuovi trattamenti di dati personali (privacy screening e DPIA), l'erogazione si sessioni di formazione in materia di protezione dei dati personali ecc.
  - Framework controlli del DPO specifici per il contesto societario e relativa reportistica.

Il Corpus documentale di Data Protection si compone **6 livelli** ciascuno dei quali è stato sviluppato in coerenza con gli standard internazionali di sicurezza e le best practices in materia di Data Protection, come riportato nella seguente figura. I primi due livelli fanno riferimento a tematiche definite a livello Corporate, mentre i successivi livelli fanno riferimento a tematiche definite a livello locale da tutte le Società del Gruppo.



* I Piani di Training & Awareness vengono stilati anche a livello corporate

Fig. 9 – Sistema documentale DP

Nella tabella seguente, per ciascun livello del Corpus documentale, è riportata la descrizione dei contenuti che devono essere riportati all'interno degli oggetti che compongono il corpus documentale DP.

Livello	Descrizione
Livello 1 Strategy	La Società determina l'indirizzo di alto livello ed il proprio risk appetite, sulla cui base costruisce il proprio sistema di protezione dei dati personali.
Livello 2 Governance, Roles & Responsibilities	La Società persegue gli obiettivi definiti nel livello *Strategy* implementando un modello di governo della protezione dei dati, coerente con il proprio core business ed enfatizzando l'importanza attribuita al concetto di organizzazione della Data Protection ai ruoli e alle responsabilità dei key player in questo settore, come il Data Protection Officer.
Livello 3 Processing inventory, data management & transfers	La Società identifica tutte le attività di trattamento di dati personali condotte al suo interno, nonché i trasferimenti di dati personali tra Società del medesimo Gruppo e terze parti, predisponendo il Registro dei trattamenti dei dati personali. La Società monitora e identifica i mezzi utilizzati per il trattamento e gli eventuali trasferimenti di dati verso paesi extra-UE.
Livello 4 Policies & procedures	La Società assicura la protezione, il controllo e la gestione dei trattamenti dei dati personali tramite l'adozione di un set di Policy e procedure atte a indirizzare il corretto sviluppo di tali processi, in linea con le disposizioni del GDPR (es: Procedura per la gestione dei data breach).
Livello 5 Risk management, DPIA, Privacy By design, Audit & Certifications	La Società applica, in conformità al GDPR, un approccio orientato alla gestione del rischio nella definizione dei propri processi di progettazione e nelle proprie metodologie, attraverso l'analisi del rischio o la conduzione di valutazioni d'impatto (privacy screening e DPIA) nel caso di ideazione di un nuovo prodotto/servizio o modifica di uno esistente. Inoltre, la compliance al GDPR viene garantita da attività di audit periodico del sistema DP e può essere attestata da (eventuali) certificazioni.
Livello 6 Training & Awareness	La Società predispone un piano di formazione sulla tematica Data Protection e crea un alto livello di awareness a livello aziendale che permetta ai propri dipendenti di conoscere e applicare le regole stabilite in materia di protezione dei dati personali. I piani di Training & Awarness vengono definiti anche a livello corporate.

7 IL MODELLO DI GESTIONE DEI DATI PERSONALI

La disciplina della protezione dei dati personali si articola in molteplici piani, quali adempimenti nei confronti degli Interessati (l'informativa, il consenso, la gestione dei diritti), adempimenti organizzativi (la valutazione d'impatto, l'approccio di "privacy by design & by default", il Registro dei trattamenti, le procedure di gestione dei data breach), adempimenti di sicurezza. Inoltre, talune tipologie di trattamenti prevedono specifici adempimenti richiesti dalle Autorità di controllo locali che le Società del Gruppo devono continuamente monitorare per adattare il proprio modello di gestione dei dati personali ai requisiti normativi locali.
In questa sezione sono definite le linee guida per la gestione degli adempimenti previsti dal Regolamento europeo in materia di protezione dei dati personali.

7.1 INFORMATIVA

Al fine di garantire un trattamento dei dati personali corretto e trasparente, il Titolare è tenuto a fornire preliminarmente all'Interessato una serie di informazioni, espressamente citate dalla normativa (ai sensi dell'art. 13 del GDPR):

- l'identità e i dati di contatto del Titolare;
- i dati di contatto del Responsabile della Protezione dei Dati (DPO);
- le finalità del Trattamento;
- la base giuridica sulla quale si basa il trattamento con particolare riferimento all'evenienza dell'utilizzo del "legittimo interesse";
- gli eventuali destinatari o le eventuali categorie dei destinatari dei dati personali (all'interno del Gruppo doValue o terzi);
- se prevista, l'eventuale intenzione del Titolare di trasferire dati personali ad un paese terzo
- il periodo di conservazione dei dati oppure i criteri utilizzati per determinarlo;
- i diritti riconosciuti all'Interessato e le modalità per esercitarli;
- qualora il trattamento si basi sul consenso, il diritto di revocare tale consenso in qualsiasi momento (ferma restano la liceità dei trattamenti basati sul consenso prestato prima della revoca) e le modalità con cui è possibile revocarlo;
- il diritto di proporre reclamo all'Autorità di controllo;
- se la comunicazione dei dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione del contratto e le possibili conseguenze della mancata comunicazione dei dati;
- l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione, le logiche applicate e le conseguenze per l'Interessato.

Qualora i dati non siano raccolti direttamente presso l'Interessato, ai sensi dell'art. 14 del GDPR l'informativa deve esplicitare anche le categorie dei dati personali trattati e la fonte da cui hanno origine i dati.

L'informativa deve essere fornita all'Interessato al momento della raccolta dei dati personali o, al più tardi, entro un mese dall'acquisizione qualora i dati non siano raccolti direttamente presso l'Interessato.

Ciascuna Società del Gruppo doValue deve provvedere alla definizione delle informative da rilasciare agli Interessati, per tutti i trattamenti per cui la Società opera in qualità di Titolare del trattamento, monitorando nel continuo se eventuali modifiche alle modalità di trattamento comportino la necessità di aggiornare l'informativa.

7.2 LICEITÀ DEL TRATTAMENTO E CONSENSO

Ogni trattamento di dati deve trovare fondamento in una idonea base giuridica (cd. liceità del trattamento ai sensi dell'art. 6 del GDPR).

Una condizione di liceità del Trattamento è che questo sia autorizzato dall'Interessato, attraverso la manifestazione del **consenso al trattamento**.

La raccolta del consenso deve avvenire nelle forme e con le modalità previste dal GDPR dovendo rispettare l'esigenza che sia dimostrabile, ossia il Titolare deve poter dimostrare che l'Interessato abbia prestato il consenso.

Il consenso viene ritenuto valido, ai sensi dell'art 7 del GDPR, qualora rispetti i seguenti requisiti:

- Libero: l'Interessato dovrà essere sempre messo in condizione di poter rifiutare di prestare il proprio consenso allo svolgimento di determinate operazioni di Trattamento; in particolare l'esecuzione di un contratto o la prestazione di un servizio non può essere condizionata alla prestazione del consenso al trattamento di Dati non necessari all'esecuzione del contratto stesso;
- Specifico: ciascuna operazione di Trattamento che, in mancanza di un diverso presupposto di legittimità del Trattamento, necessiti del consenso degli Interessati deve essere oggetto di uno specifico consenso;
- Informato: il consenso deve essere preceduto dalla consegna o, in ogni caso, dalla presa visione da parte dell'Interessato dell'informativa sul trattamento dei Dati e la finalità del consenso prestato; la richiesta di consenso deve essere presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile e con un linguaggio semplice e chiaro;
- Inequivocabile: l'intenzione dell'Interessato di prestare il proprio consenso alle operazioni di Trattamento che lo riguarderanno deve essere espressa tramite una dichiarazione o un'azione positiva;
- Esplicito: per il trattamento di dati sensibili particolari, il consenso deve essere prestato in modo esplicito.

L'Interessato ha sempre la facoltà di revocare il consenso prestato, ferma restando la liceità dei trattamenti effettuati fino a quel momento; la revoca deve poter essere effettuata con modalità facili e tempestive.

Tra i Trattamenti che richiedono il consenso vi sono, a titolo esemplificativo, l'utilizzo dei dati per finalità commerciali o di marketing di prodotti e servizi propri o di terze parti, richiesti tramite la compilazione di form sui siti web delle Società o tramite modulistica cartacea, la trasmissione di dati personali a Società del Gruppo doValue nel caso di trattamenti che non hanno finalità amministrativo contabili (come definiti all'interno del considerando 48 del GDPR), la trasmissione a sistemi di informazione creditizia di dati positivi relativamente alla regolarità dei pagamenti dei clienti con rapporti di finanziamento.

Vi sono poi altre fattispecie di liceità del Trattamento, per cui i dati personali possono essere trattati anche **in assenza del consenso**, quali ad esempio quando il trattamento:

- è necessario per l'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- è necessario per adempiere ad un obbligo legale al quale il soggetto al quale è soggetto il titolare del trattamento
- è necessario per il perseguimento del legittimo interesse del Titolare de trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali.

In tutti i casi in cui i dati sono trattati per riscontrare una richiesta dell'Interessato stesso, quali la richiesta di contatto o informazioni, la prestazione di un servizio o l'esecuzione degli obblighi previsti da un contratto, il riscontro ad un reclamo, o laddove i dati sono trattati per adempiere ad altre normative applicabili al contesto societario (es: l'adeguata verifica a fini antiriciclaggio, la registrazione negli elenchi previsti dalla normativa in materia di market abuse, l'adempimento degli accertamenti e delle comunicazioni societarie per i membri degli Organi societari e le verifiche richieste dalla normativa in materia di soggetti collegati) non è necessario richiedere ed ottenere il consenso dell'Interessato.

Qualora i dati personali siano trattati da una Società del Gruppo in qualità di Titolare del trattamento è consentito il trasferimento dei dati ad altra Società del Gruppo che opera in qualità di Responsabile del trattamento sulla base di un accordo di servizi intercompany senza richiedere il consenso agli Interessati.

Infine, in tutti i casi in cui i dati sono trattati dalle Società del Gruppo in qualità di Responsabili (esterni) del trattamento, quali le attività di gestione e recupero dei crediti per conto delle Mandanti o di servicer per SPV, non è necessario richiedere il consenso all'Interessato per il trattamento dei dati effettuato in qualità di Responsabili, nel presupposto che, laddove necessario, il consenso sia stato già richiesto e validamente ottenuto dal Titolare.

7.3 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, devono dotarsi 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).

Resta inteso che le richieste di esercizio dei diritti presentate dagli Interessati non potranno riguardare dati personali riferiti a terzi, salvo casi particolari (ad esempio per il tramite di procuratore o avvocato).

In conformità con quanto previsto dal GDPR, il LOCAL DPO funge da contatto per gli Interessati per l'esercizio dei loro diritti e il riscontro da fornire agli Interessati deve essere preventivamente concordato con il LOCAL DPO.

Nei casi in cui le Società del Gruppo doValue operano quali Responsabili esterni del trattamento (ad esempio nell'ambito delle attività di recupero credito), dovranno poter supportare il Titolare nella gestione delle richieste degli Interessati sulla base dei compiti definiti nell'ambito dei relativi contratti di servizio e eventuali istruzioni operative associate. Le modalità di gestione delle richieste degli Interessati sono definite a livello locale all'interno di specifiche normative interne.

7.4 GESTIONE DELLA DATA RETENTION

In coerenza con il citato principio di limitazione del trattamento i dati devono essere conservati per un periodo utile per le finalità del loro trattamento, limitato al minimo necessario (cd. Data Retention). Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il Titolare del trattamento deve stabilire un termine per la cancellazione, anche differenziato a seconda della tipologia di dato e della finalità del trattamento, e mettere in atto misure tecniche e organizzative adeguate per garantire il rispetto del periodo massimo di conservazione stabilito.

Nella definizione del termine di conservazione occorre pertanto tenere conto di:

- requisiti di conservazione previsti dalla normativa (es. privacy, obblighi di conservazione fiscali, termini di conservazione delle scritture contabili, corrispondenza, contrattualistica);
- finalità della raccolta e del trattamento in relazione alle esigenze di business e operative;
- istruzioni fornite dal Titolare del Trattamento (ad es. Mandanti/SPV) per i Dati trattati in qualità di Responsabili del Trattamento (i.e. dati dei debitori).

Nel caso in cui una Società del Gruppo intenda cessare lo svolgimento di una o più operazioni di trattamento effettuato in qualità di Titolare autonomo, i dati personali precedentemente utilizzati nel contesto di tali operazioni dovranno essere distrutti o anonimizzati (ove applicabile), fatti salvi gli adempimenti legati ad obblighi di legge o a finalità difensive.

Nel caso in cui le Società del Gruppo doValue operino in qualità di Responsabili del trattamento vengono rispettai i requisiti per la cancellazione dei dati forniti dal Titolare dal trattamento all'interno del Data Processing Agreement (DPA).

I requisiti di Data Retention, con riferimento alle diverse tipologie di dati / trattamenti, sono declinati nella normativa interna specifica.

7.5 DATA PROTECTION BY DESIGN E BY DEFAULT - DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Al fine di garantire la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei loro dati personali, Il GDPR richiede che il titolare del trattamento adotti politiche interne e attui misure che soddisfino i principi della protezione dei dati fin dalla progettazione (c.d. "Data Protection by design") e della protezione dei dati di default (c.d. "Data Protection by default").

In particolare, il principio di "**Data Protection by design**" prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il Titolare del trattamento metta in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli Interessati.

Il principio di "**Data Protection by default**" consiste nel mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, con riferimento alla

quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità.

I principi di Data Protection by Design e by Default devono essere integrati nell'intera organizzazione del Gruppo, pertanto, tutte le Società dovranno prestare attenzione a che lo sviluppo di nuovi prodotti, servizi, l'utilizzo di strumenti di supporto venga sottoposta ad una preventiva verifica al fine di valutare se l'eventuale trattamento dei dati previsto avvenga nel rispetto delle previsioni normative generali e locali: ciò richiede che vi sia una estrema consapevolezza che ciascuna struttura societaria dovrà fornire il proprio contributo alla corretta e tempestiva applicazione dei principi richiamati.

In particolare, fin dalla fase di progettazione di un nuovo prodotto/servizio, di implementazione di nuovi strumenti, di variazioni significative alle modalità di Trattamento dei dati, occorre, per quanto possibile tenendo conto dello stato dell'arte e dei costi di attuazione nonché dei rischi connessi allo specifico trattamento:

- prevedere per impostazione predefinita dei processi/sistemi che vengano trattati solo i Dati personali necessari per ogni specifica finalità del trattamento;
- prevedere, per impostazione predefinita dei processi/sistemi, che i Dati personali trattati non siano resi accessibili solo ai soggetti che hanno necessità di trattarli in relazione alla finalità per cui sono raccolti;
- considerare l'intero ciclo di vita dei Dati personali nei quali vengono trattati Dati personali dalla raccolta alla cancellazione tenendo in debita considerazione anche il trasferimento, la conservazione, l'elaborazione, la consultazione e la comunicazione.

Per garantire i principi di Privacy by design e Privacy by default all'interno di ciascuna società del Gruppo è necessario che queste si dotino di una propria metodologia per determinare quali trattamenti risultano ad elevato rischio per gli Interessati e per valutare gli eventuali impatti su di esso (Data Protection Impact Assessment). In funzione delle risultanze dell'analisi ciascuna società deve identificare adeguate misure di sicurezza tecniche ed organizzative che una volta applicate mitigano gli eventuali impatti per l'Interessato causati da perdita di confidenzialità, integrità e disponibilità dei dati personali.
Qualora la società operi in qualità di Responsabile del trattamento deve contribuire a mettere a disposizione del titolare del trattamento tutte le informazioni di interesse per permettere al titolare di eseguire la valutazione di impatto.

7.6 REGISTRO DEI TRATTAMENTI

L'elenco completo delle attività di trattamento di dati personali e delle relative finalità effettuate dalle Società del Gruppo sia in qualità di Titolari che di Responsabili esterni del Trattamento, è contenuto all'interno del c.d. Registro dei trattamenti dei dati personali.

Nel Registro sono riportate quantomeno le seguenti informazioni:

con riferimento ai Trattamenti effettuati in qualità di Titolare

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del Responsabile della protezione dei dati;
- le finalità del trattamento;
- la descrizione delle categorie di Interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

con riferimento ai Trattamenti effettuati in qualità di Responsabile

- il nome e dati di contatto del Responsabile o dei Responsabili del Trattamento, di ogni titolare del trattamento per conto del quale agisce il Responsabile del Trattamento, del rappresentante del titolare del trattamento o del Responsabile del Trattamento e, ove applicabile, del Responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il LOCAL DPO ha la responsabilità dell'aggiornamento e conserva in formato elettronico la versione ufficiale del Registro dei trattamenti, anche al fine di renderla disponibile all'Autorità di controllo in caso di ispezione.

7.7 GESTIONE DATA BREACH

Una violazione dei dati personali (c.d. "data breach") può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, ai sensi dell'articolo 33 del GDPR, il Titolare del trattamento deve notificare la violazione dei dati personali al Garante Privacy, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (a meno che il Titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche). Oltre il termine di 72 ore, tale notifica deve essere corredata delle ragioni del ritardo. La notifica deve almeno contenere:

- La descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- La comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati (Local DPO) o di altro punto di contatto presso cui ottenere più informazioni;
- La descrizione delle probabili conseguenze della violazione dei dati personali;
- La descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui le società del Gruppo doValue operino in qualità di Responsabili del trattamento vengono rispettati i requisiti le Società del Gruppo dovranno informare tempestivamente il Titolare del trattamento di eventuali data breach entro i termini previsti dal Data Protection Agreement (DPA). Inoltre dovranno fornire al Titolare tutte le indicazioni relativamente all'evento occorso necessarie a notificare l'evento all'Autorità di controllo.

A titolo esemplificativo e non esaustivo, gli eventi di possibile violazione dei Dati personali possono essere costituiti da:

- distruzione di dati informatici o documenti cartacei (intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi), conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato) o fisica (es. rottura di dispositivi di memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti);
- perdita di dati, conseguente a smarrimento/furto di supporti informatici (es. laptop, HD, memory card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- accesso non autorizzato o intrusione a sistemi informatici (es. sistemi di contact management gestiti dai call center), tramite lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. userid e password) per l'accesso ai sistemi;
- modifica non autorizzata di dati, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o intervento umano;
- rivelazione di dati e documenti a soggetti terzi non legittimati, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale o esecutivo a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici.

Se nell'ambito della valutazione interna si rileva anche un rischio elevato per i diritti e le libertà dell'Interessato esponendo questo a particolari rischi in considerazione dei dati oggetto di data breach, è necessario dare diretta comunicazione anche all'Interessato senza ingiustificato ritardo. La comunicazione all'Interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno il nome e i dati di contatto del DPO, le probabili conseguenze della violazione e le misure adottate o che si intendono adottare per porvi rimedio.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

Il Garante Privacy può comunque richiedere che venga effettuata la comunicazione agli Interessati.

Ciascuna società del Gruppo doValue deve dotarsi di procedure interne e strumenti per rilevare, contrastare e gestire eventuali incidenti di sicurezza che comportano una data breach. Inoltre all'interno delle procedure interne devono essere esplicitate la metodologia per la valutazione del data breach, le modalità di escalation verso gli organi di governo aziendale e le modalità di notifica dell'evento all'Autorità di controllo locale ed eventualmente agli Interessati del trattamento, nonché, per il caso in cui la società opera come responsabile anche le modalità di notifica al Titolare.

7.8 MISURE DI SICUREZZA

Nell'ambito delle operazioni di trattamento svolte, il Titolare e il Responsabile Esterno del Trattamento devono porre in essere, ai sensi dell'art. 32 del GDPR, tutte le misure necessarie per tutelare i dati personali, dovendo garantire:

- l'implementazione di misure di protezione delle reti, dei sistemi e dei software con i quali vengono trattati i dati personali, quali ad esempio:
    - soluzioni di profilatura e segregazione delle utenze e di protezione degli accessi, tali da garantire l'accesso e il Trattamento di Dati personali ai soli soggetti che hanno necessità di trattarli
    - la pseudonimizzazione, l'offuscamento e la cifratura dei Dati personali;
    - soluzioni di continuità di servizio in grado di garantire la disponibilità e l'integrità dei dati (backup, Disaster Recovery, ecc.);
- Il test e la valutazione periodica di efficacia delle procedure e delle misure implementate;
- L'implementazione di soluzioni in grado di rilevare tentativi non leciti di accesso ai dati personali in grado di garantire il rispetto delle prescrizioni del GDPR in merito alle violazioni (data breach);
- L'adozione di soluzioni per il tracciamento delle attività effettuate sui dati personali che siano compatibili con i requisiti imposti dalle Leggi Applicabili.

7.9 TRASFERIMENTI DI DATI EXTRA-UE

L'entrata in vigore del GDPR ha introdotto un livello di protezione dei dati personali uniforme all'interno dell'Unione Europea, permettendo perciò la libera circolazione dei dati all'intero dei Paesi UE.

Il Regolatore richiede invece che, quando i dati personali sono trasferiti dall'Unione a Titolari del trattamento e Responsabili del trattamento o altri destinatari in Paesi al di fuori dell'Unione europea, sia garantito il medesimo il livello di tutela delle persone fisiche assicurato nell'Unione.

Pertanto, il trasferimento dei dati personali dell'Interessato in Paesi extra UE può avvenire, ad esempio, nei seguenti casi:

- trasferimento verso Paesi che secondo la Commissione Europea garantiscono un adeguato livello di tutela dei Dati personali;

- trasferimento tra società facenti parte dello stesso gruppo d'impresa in presenza di accordi di *Binding Corporate Rules (BCR)*, laddove applicabili, o tra società che abbiano sottoscritto le "clausole tipo" per la protezione dei dati personali approvate dalla Commissione;
- trasferimento necessario all'esecuzione di un contratto concluso tra l'Interessato e il Titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'Interessato;
- trasferimento necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del trattamento e un'altra persona fisica o giuridica a favore dell'Interessato;
- trasferimento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

Qualora non ricorra uno dei casi sopra espressi, il trasferimento dei dati deve essere espressamente approvato dall'Interessato.

È pertanto particolarmente importante che le Società del Gruppo verifichino, in fase di avvio di un Trattamento o nel corso dello stesso, il luogo in cui avviene il trattamento dei dati, in particolare laddove siano coinvolte terze parti che dovranno comunicare in quale Paese effettuano i Trattamenti.

7.10 TRATTAMENTI SPECIFICI

Ciascuna Società del Gruppo deve monitorare nel continuo se le Autorità di controllo locali per la protezione dei dati personali emettono provvedimenti in materia di protezione dei dati personali più restrittivi rispetto al Regolamento europeo. In tal caso, il Titolare del trattamento, supportato dal LOCAL DPO, dovrà valutare se le modalità di trattamento dei dati personali adottate risultino conformi alle nuove disposizioni locali e, in caso contrario, adottare le necessarie azioni di adeguamento.

8 FRAMEWORK DI CONTROLLO

Per garantire che le organizzazioni abbiano una struttura chiara che separi le funzioni che definiscono le linee guida da quelle responsabili della loro esecuzione, i regolatori chiedono sempre più spesso un modello di governance "a tre linee di difesa" che garantisce un controllo interno forte ed efficace e per garantire molteplici livelli di protezione.

La figura che segue rappresenta il sistema dei controlli data protection di Gruppo:

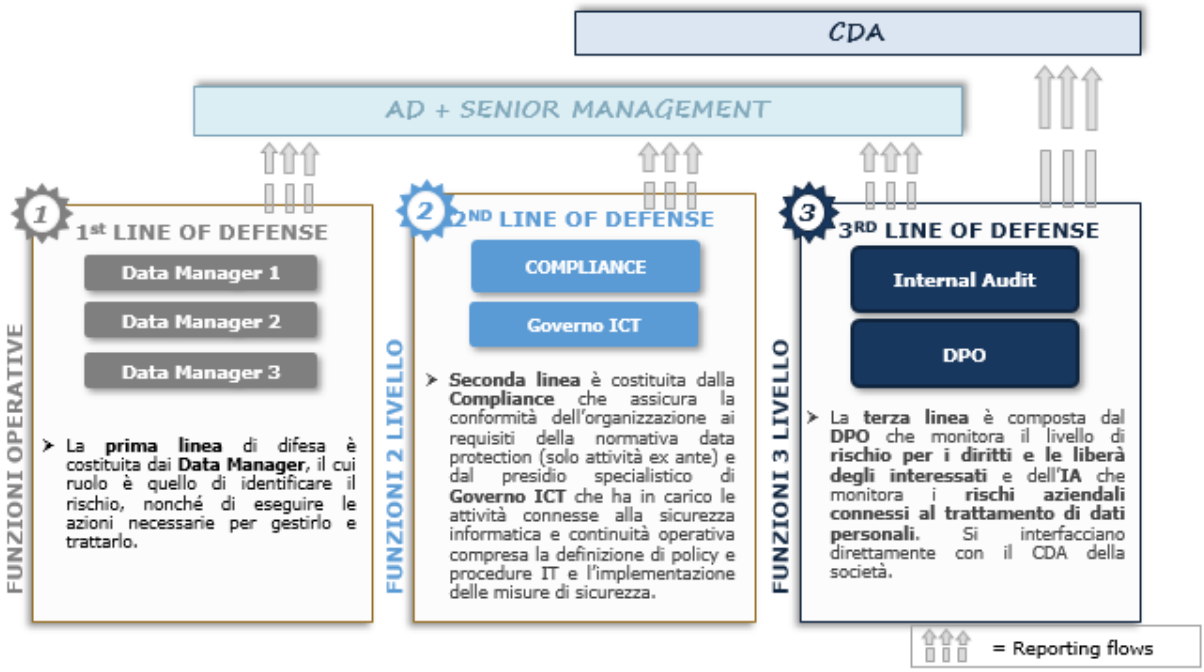


Fig. 10 – Sistema controlli interni DP

Il Global DPO definisce e manutiene il framework di controllo, di 3° livello, comune per tutte le Società del Gruppo a servizio del Global DPO e del Local DPO nell'ambito delle attività di sorveglianza e finalizzato alla determinazione del livello di rischio per i diritti e le libertà degli Interessati.
All'interno del framework di controllo sono riportate le attività di controllo specifiche che devono essere testate dal Local DPO.
Le attività di controllo definite nel framework sono suddivise tra i seguenti principali domini:

1. GDPR Strategia e Responsabilità;
2. Registro delle attività di trattamento;
3. Definizione delle basi legali per il trattamento;
4. Consenso, correttezza e trasparenza;
5. Diritti degli Interessati;
6. Delimitazione della conservazione;
7. Formazione e consapevolezza;
8. Data breach e gestione degli incidenti;
9. Privacy by Design & Privacy by Default;
10. Data Protection Impact Assessment (DPIA);
11. Gestione delle terze parti;
12. Misure di sicurezza;
13. Trasferimento dei dati personali.

Il Local DPO deve declinare i controlli del Framework a livello locale sulla base delle specifiche caratteristiche dell'organizzazione aggiungendo, eventualmente, attività di controllo specifiche al fine di valutare la conformità del sistema di Data Protection societario anche con eventuali provvedimenti applicabili, emanati dall'Autorità Locale.

Le verifiche possono essere pianificate su tutti i trattamenti di dati personali svolti dalla società nell'arco temporale di più anni, assicurando però che ogni anno all'interno del perimetro delle verifiche siano inseriti:

- i trattamenti che presentano un rischio (inerente) per i diritti e le libertà degli Interessati elevato.
- un subset di trattamenti che presentano un rischio (inerente) per i diritti e le libertà degli Interessati Non elevato.

Il Local DPO al termine delle attività di verifica produce la reportistica indirizzata al Consiglio di Amministrazione locale e informa il Global DPO in riferimento ai risultati emersi dall'attività di monitoraggio ed a specifici eventi rilevanti occorsi durante il periodo di riferimento.

9 SANZIONI

La violazione della normativa in materia di protezione dei dati personali può esporre il Titolare e/o il Responsabile a diverse tipologie di responsabilità e conseguenti sanzioni (di carattere amministrativo e/o penale), in base alle norme concretamente violate. Occasionalmente può essere richiesto dai soggetti Interessati un risarcimento danni, nel caso in cui essi abbiano subito danni materiali o immateriali causati da una violazione della normativa e/o rischino di subire un danno alla reputazione.
Il GDPR ha innalzato significativamente l'importo delle sanzioni amministrative, portandole fino ad un massimo di Euro 20 milioni o al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore. Nei singoli casi, l'Autorità di controllo può decidere se applicare le sanzioni amministrative pecuniarie in aggiunta alle misure di carattere prescrittivo o interdittivo, o al posto di tali misure.
In ogni caso, ai sensi dell'art. 83 del GDPR, le sanzioni amministrative pecuniarie devono essere in concreto effettive, proporzionate e dissuasive e pertanto, nella determinazione dell'ammontare della sanzione, il Garante tiene conto di una serie di fattori, tra i quali la natura, la gravita e la durata della violazione, il carattere doloso o colposo della violazione, eventuali precedenti violazioni pertinenti, le misure adottate dal Titolare o dal Responsabile per attenuare il danno subito dagli Interessati, il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, le categorie di dati personali interessate dalla violazione; la maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.