POLÍTICA

Grupo doValue
Proteção de dados

ÍNDICE

1 INFORMAÇÕES GERAIS SOBRE O DOCUMENTO

Empresa Emissora	doValue S.p.A.
Empresa(s)-alvo	Todas as empresas do Grupo doValue (empresa-mãe e subsidiárias na Itália e no estrangeiro)
Título	Proteção de dados do grupo doValue
Data de emissão	13/01/2021
Data efetiva	Imediatamente
Código de identificação do documento	PL02-2021-R01
Nível hierárquico do Sistema Regulatório Integrado	Nível Hierárquico III
Tipo de documento	Política
Diretriz reguladora	Sim
Elaborado por (Proprietário):	Conformidade e EPD global
Revisto por:	Conselho Geral
Aprovado por (responsável) em:	Conselho de Administração da doValue em 17/12/2020
Emitido via:	Número da comunicação de serviço PL02-2021-R01
Documentos revogados ou substituídos:	III – Política R & C-11-2018-R02 – Política para assuntos de proteção de dados pessoais
Cronograma de revisões	R01 - Primeira Versão

2 GLOSSÁRIO

Autoridade Supervisora (ou Autoridade)	A Autoridade descrita no art.º 51º do RGPD ("Regulamento Geral de Proteção de Dados"), ou seja, uma ou mais autoridades públicas independentes nomeadas por um Estado-Membro para serem responsáveis pela supervisão da aplicação do Regulamento, a fim de proteger os direitos e liberdades fundamentais de pessoas naturais em relação ao tratamento de dados pessoais.
Subsidiárias	As empresas financeiras e/ou auxiliares integradas no Grupo doValue.
Dados judiciais	Dados pessoais que possam revelar a existência de procedimentos judiciais específicos sujeitos a inclusão num registo criminal (por exemplo, condenações criminais definitivas, libertação condicional, proibição ou obrigação de residência, medidas alternativas não privativas de liberdade) ou estatuto da pessoa acusada ou da pessoa investigada.
Dados pessoais	Qualquer informação relativa a uma pessoa natural identificada ou identificável ('Titular de Dados'); uma pessoa natural identificável é a que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como nome, número de identificação, dados de localização, identificador online ou um ou mais fatores específicos para a identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa natural.
Dados de identificação	Dados de identificação são dados a partir dos quais é possível identificar diretamente o Titular de Dados. Por exemplo, códigos de identificação, incluindo os que fazem parte dos dados pessoais (por exemplo, número de contribuinte) e códigos exclusivos atribuídos a uma pessoa com base em critérios predefinidos (por exemplo, códigos de cliente) são dados de identificação.
Dados sensíveis	Dados pessoais suscetíveis de revelar origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação em sindicatos e tratamento de dados genéticos, dados biométricos com o objetivo de identificar de forma única uma pessoa natural, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de pessoa natural.
Dados bancários	Dados pessoais relativos às relações bancárias ou financeiras do Titular de Dados e instruções relacionadas (por exemplo, instruções de pagamento).

Encarregado da Proteção de Dados (o "EPD")	O "Encarregado da Proteção de Dados" é a pessoa designada pelo Responsável pelo Tratamento de Dados (ou Processador) para cumprir funções de assistência e controlo, consulta, formação e informação em relação à aplicação do RGPD.
Regulamento Geral de Proteção de Dados (ou "RGPD")	O "Regulamento Geral de Proteção de Dados", ou seja, o Regulamento (UE) n.º 679, de 27 de abril de 2016, que estabelece o sistema europeu de regulamentação sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação.
Grupo	O Grupo doValue, incluindo doValue (Empresa-mãe), Italfondiario, doData e subsidiárias estrangeiras para a Região Ibérica e Região Grécia e Chipre.
Titular (de Dados)	Pessoa individual identificada ou identificável, direta ou indiretamente, por um dado pessoal e, em qualquer caso, a quem se referem os dados tratados.
Mandante	O banco, SPV ou outra pessoa coletiva que confira a uma empresa do Grupo doValue um mandato para atividades de recuperação de crédito e/ou serviços relacionados e auxiliares.
Subcontratante (de Dados)	Um terceiro, que não empregado ou representante legal, nomeado Subcontratante para o tratamento de dados pessoais por si realizado em nome do Responsável pelo Tratamento de Dados através de contrato de serviço ou colaboração que especifique o âmbito das responsabilidades delegadas.
Responsável pelo Tratamento de Dados	A pessoa singular ou coletiva, Autoridade Pública, agência ou outro organismo que, isoladamente ou com outros, determine os fins e os meios de tratamento de dados pessoais.
Tratamento	Qualquer operação ou conjunto de operações realizado em dados pessoais ou conjuntos de dados pessoais, seja ou não por meios automatizados, como recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização de outra forma, alinhamento ou combinação, restrição, apagamento ou destruição.
Empresa(s)	Uma ou mais empresas do Grupo doValue

3 INTRODUÇÃO

Num ambiente global interconectado em constante evolução, é fundamental dar a devida atenção à proteção de Dados Pessoais em função das novas vulnerabilidades e ameaças que levam a riscos crescentes em relação ao tratamento de Dados Pessoais e exigem uma gestão cada vez mais cuidadosa de todas as fases do tratamento, da recolha à eliminação dos dados.

O âmbito desta Política é estabelecer:

- A **estratégia de Proteção de Dados do Grupo doValue**, delineando o compromisso do Grupo com a proteção de dados pessoais;
- O **Modelo de Organização para a Proteção de Dados Pessoais (doravante também "OMPDP")**, que descreve as funções, responsabilidades e inter-relações entre as várias figuras identificadas para a governança do sistema de gestão de dados pessoais das empresas do Grupo;
- O **Modelo de Gestão de Dados**, que descreve os principais requisitos do Regulamento Europeu para uma governança adequada do tratamento de Dados Pessoais.

3.1 APLICABILIDADE

Esta política aplica-se a todas as empresas do Grupo doValue, na Itália e no estrangeiro, e é adotada através de resoluções separadas dos Conselhos de Administração da Empresa-mãe e das subsidiárias italianas e não-italianas, que se comprometem, em coordenação com a Empresa-mãe, através do seu órgão dirigente com responsabilidade pela supervisão estratégica, a adotar os seus princípios e diretrizes, tendo em conta as características específicas dos seus negócios e da regulamentação local.
A política destina-se a todo o pessoal interno da doValue e subsidiárias que processem dados pessoais.

3.2 CONTEXTO LEGISLATIVO E REGULATÓRIO

O documento foi elaborado em conformidade com os regulamentos de proteção de dados pessoais, a nível europeu e italiano, indicados abaixo, conforme posteriormente alterados:

- Regulamento Geral de Proteção de Dados (UE) 679/2016 (doravante "RGPD")
- Diretrizes emitidas pelo "Grupo do artigo 29.º para a Proteção de Dados" (doravante, abreviado, "WP29") e/ou o Conselho Europeu de Proteção de Dados (doravante, abreviado, "EDPB")
- Decreto Legislativo n.º 196 de 30 de junho de 2003 "Código de Proteção de Dados Pessoais", conforme alterado e complementado pelo Decreto Legislativo n.º 101/2018 e outros regulamentos locais nacionais aplicáveis às Empresas do Grupo.

3.3 PRINCÍPIOS GERAIS

O RGPD estabelece os princípios relativos ao tratamento de dados pessoais, estabelecendo que os dados pessoais devem ser:

a) Tratados de forma legal, justa e transparente em relação ao Titular de Dados ("**legalidade, justiça e transparência**");
b) recolhidos para finalidades especificadas, explícitas e legítimas e não tratados posteriormente de maneira incompatível com essas finalidades ("**limitação de finalidade**");
c) adequados, relevantes e limitados ao necessário em relação aos fins para os quais são tratados ("**minimização de dados**");
d) Exatos e, se necessário, atualizados; devem ser adotadas todas as medidas razoáveis para garantir que os dados pessoais inexatos, tendo em conta os fins para os quais são tratados, sejam apagados ou retificados sem demora ("**exatidão**");
e) mantidos de forma que permita a identificação dos Titulares de Dados por tempo não superior ao necessário para os fins para os quais os dados pessoais são tratados ("**limitação de armazenamento**");
f) tratados de forma a garantir a segurança adequada dos dados pessoais, incluindo proteção contra tratamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas e organizacionais apropriadas ("**integridade e confidencialidade**").

4 ESTRATÉGIA DE PROTEÇÃO DE DADOS

A atividade principal do Grupo envolve a gestão de empréstimos não produtivos e contas a receber em nome dos Mandantes (por exemplo, Diretores/Bancos/SPV) e todas as outras atividades judiciais e extrajudiciais direta ou indiretamente relacionadas com o negócio principal descrito acima. Neste contexto, as empresas do Grupo doValue devem gerir:

- diferentes tipos de dados pessoais (Identificação, sensíveis, etc.);
- várias categorias de Titulares de Dados em relação às quais as empresas do Grupo podem atuar como Responsável pelo Tratamento de Dados (empregados, clientes, potenciais clientes, terceiros, etc.) e/ou como Subcontratante (ou seja, os dados de partes obrigadas processados sob compromissos de recuperação de crédito em relação aos quais os principais bancos são Responsáveis de pelo Tratamento de Dados).

O Grupo doValue compromete-se a garantir a segurança e proteção dos dados pessoais tratados por todos os seus colaboradores, através de uma abordagem baseada no risco consistente com os requisitos legais e regulamentares aplicáveis e todas as expectativas das partes interessadas (conforme melhor definido abaixo).

O Grupo doValue atenta constantemente os desenvolvimentos legais e regulamentares no campo da proteção de dados pessoais com o objetivo de tomar as medidas adequadas para garantir que o seu sistema de proteção de dados pessoais seja constantemente atualizado e melhorado. Além disso, com base no seu nível de exposição ao risco de perda de confidencialidade, integridade e disponibilidade de dados pessoais, todas as Empresas do Grupo doValue adotam medidas de segurança técnicas e organizacionais adequadas com o objetivo de reforçar a proteção dos dados pessoais processados, respeitando ao mesmo tempo o princípio da responsabilização.

4.1 PARTE INTERESSADA

As Partes Interessadas do sistema de proteção de dados do Grupo doValue são aqueles que beneficiam de configuração adequada do sistema em conformidade com todos os requisitos regulamentares aplicáveis ao contexto específico em matéria de proteção de dados pessoais. Especificamente, incluem:

- **Investidores**, pois qualquer dano à reputação causado pelo tratamento impróprio de dados pessoais pode levar a uma redução no valor das ações e perda de confiança do investidor na organização;
- **Conselho de Administração**, visto que o cumprimento regulatório/legislativo do sistema de PD garante a mitigação do risco de incumprimento que poderá conduzir à imposição de penalizações pela Autoridade Supervisora, com potenciais perdas financeiras e danos de reputação para o Grupo;
- **Titulares de dados**, visto que um fraco sistema de proteção de dados pessoais aumentaria o nível de exposição das empresas do Grupo ao risco de perda de confidencialidade, integridade e disponibilidade dos dados pessoais processados. Portanto, uma ocorrência que afete a confidencialidade, integridade e disponibilidade dos dados pessoais dos Titulares de Dados pode causar danos ao Titular de Dados, possivelmente danos significativos.
- **Mandantes**, porque, em relação aos serviços prestados, as empresas do Grupo doValue podem ser designadas como Subcontratantes que operam por conta de mandantes que atuam como Responsáveis pelo Tratamento de Dados.

Consequentemente, os Mandantes beneficiam da solidez do Sistema de Proteção de Dados das empresas do Grupo doValue e torna-se imprescindível a proteção dos dados pessoais em relação aos quais são Responsáveis pelo Tratamento de Dados.

4.2 PROGRAMAS DE PROTEÇÃO DE DADOS

Um sistema robusto de proteção de dados pessoais é requisito fundamental para as organizações que operam no setor financeiro. A crescente procura de fiabilidade e cumprimento de requisitos específicos conduz, por um lado, a um maior nível de complexidade da gestão do risco cibernético e, por outro, ao aumento da confiança dos clientes nas empresas do Grupo.
Os programas que integram o sistema de Proteção de Dados do Grupo doValue visam garantir o cumprimento da legislação europeia e nacional de proteção de dados, minimizando o risco de perda de confidencialidade, integridade e disponibilidade, protegendo ao mesmo tempo os ativos de informação do negócio, que consistem, em grande parte, em dados pessoais. Portanto, o Grupo doValue compromete-se a:

- Conseguir uma abordagem integrada, consistente e harmoniosa para gestão de dados pessoais, estabelecendo as diretrizes que devem ser seguidas a nível local por todas as subsidiárias, na Itália e no estrangeiro;
- Reduzir o risco de perda de dados através de medidas dirigidas aos empregados e terceiros envolvidos no tratamento de dados pessoais;
- Usar ferramentas de segurança avançadas para detetar ameaças à segurança de dados e tomar medidas eficazes para combater essas ameaças;
- Adotar uma abordagem de segurança por conceção para todas as novas tecnologias adotadas pelas empresas do Grupo.

4.3 RECURSOS ALOCADOS

O Grupo doValue compromete-se a garantir a alocação de recursos adequados em termos operacionais e financeiros com o objetivo de acompanhar a evolução regulamentar no domínio da proteção de dados pessoais e identificar prontamente as ações necessárias para adaptar e atualizar o modelo de gestão e ferramentas de apoio ao tratamento de dados pessoais, também com vista ao reforço das medidas de segurança.

5 O MODELO ORGANIZACIONAL DE PROTEÇÃO DE DADOS

O modelo organizacional de proteção de dados (MOPD) adotado pelo Grupo doValue foi concebido em função das características do negócio das empresas do Grupo e das relações entre essas empresas.
Conforme mostrado no gráfico a seguir (ver Fig.1), o MOPD é organizado em duas áreas:

- **Governança e Supervisão:** cujas funções incluem: (i) determinar a abordagem do sistema de proteção de dados, seus objetivos e métodos relacionados de tratamento de dados pessoais; (ii) garantir que a organização cumpre os requisitos dos regulamentos de proteção de dados; (iii) coordenar as iniciativas aprovadas na área da proteção de dados; (iv) atuar como ponto focal em questões de proteção de

dados, desempenhando um papel consultivo e de contacto em relação à Autoridade Supervisora.

- **Áreas Operacionais:** que são responsáveis pelas funções e atividades operacionais relativas ao tratamento de dados pessoais, dependendo da função interna ou externa desempenhada (departamentos comerciais, TIC e terceiros).

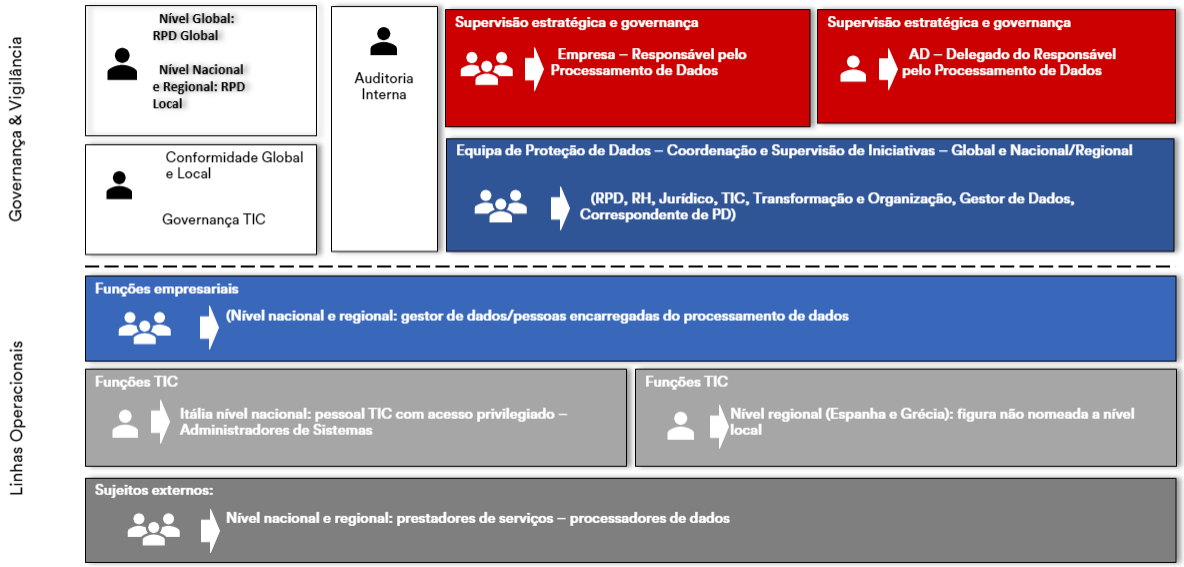


fig. 1 - MOPD do Grupo doValue

As complexidades envolvidas na proteção de dados pessoais fazem com que devam ser designadas uma série de funções, com deveres e responsabilidades específicas em relação à gestão de dados.
Algumas dessas funções são especificamente indicadas pelo RGPD (ou por Ordens da Autoridade Supervisora, quando aplicável), da seguinte forma:

- Responsável pelo Tratamento de Dados (RPD)
- Encarregado da Proteção de Dados (EPD)
- Subcontratante e, quando designado, o –Subcontratante externo
- Administrador de Sistema (quando previsto pelos regulamentos locais).
- Pessoa Encarregada do Tratamento

Outras funções são designadas em resultado de decisões de gestão, tendo em consideração a estrutura organizacional e métodos de tratamento. Ajudam no funcionamento adequado das salvaguardas de gestão de dados pessoais e incluem:

- a Equipa de Proteção de Dados;
- o Gestor de Dados;
- o Representante da Proteção de Dados Pessoais.

5.1 FUNÇÕES DE GOVERNANÇA

A principal tarefa das funções de governança é dirigir as atividades do Grupo, a fim de garantir que os dados pessoais dos Titulares de Dados sejam protegidos e que os seus direitos, nos termos do regulamento, sejam respeitados.

5.1.1 O Responsável pelo Tratamento de Dados e o Delegado

O n.º 7 do artigo 4.º do RGPD define o Responsável pelo Tratamento de Dados como «a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais»
Assim, compete ao Responsável pelo Tratamento de Dados determinar os fins e meios do tratamento efetuado, adotando medidas organizacionais e técnicas capazes de assegurar o cumprimento do regulamento, revendo e atualizando essas medidas sempre que necessário e garantindo aos Titulares de Dados o direito de exercício dos direitos reconhecidos pelo RGPD. Além disso, é dever do Responsável pelo Tratamento de Dados designar o Encarregado da Proteção de Dados (EPD), solicitando-lhe a supervisão do sistema de proteção de dados pessoais.
No Grupo, cada Empresa, representada pelo seu Conselho de Administração, é o Responsável pelo Tratamento de Dados para efeitos do tratamento dos dados por si adquiridos e geridos no âmbito das suas operações.
O Conselho de Administração pode designar o Diretor Executivo como "**Delegado do Responsável pelo Tratamento de Dados**" a fim de cumprir os requisitos de conformidade regulamentar do Responsável pelo Tratamento de Dados em relação à Empresa em questão. Por sua vez, o Delegado do Responsável pelo Tratamento de Dados pode subdelegar o cumprimento de algumas das tarefas do Responsável pelo Tratamento de Dados noutros indivíduos dentro da Empresa, por exemplo, nomeação de Subcontratantes, conforme previsto nas regras internas de subdelegação atualmente em vigor.

5.1.2 Equipa de Proteção de Dados

A Equipa de Proteção de Dados é um grupo de trabalho facultativo, ao qual são atribuídas **funções de coordenação e estratégia** em relação à proteção de dados.
A Equipa de Proteção de Dados é reunida conforme requisitos operacionais específicos para facilitar a colaboração entre os principais participantes que já têm uma função de gestão de dados nas suas atividades normais. Por exemplo, a Equipa de Proteção de Dados pode ser convocada em caso de violação de dados ou em caso de avaliação de novos serviços/tratamento ao abrigo do princípio de Privacidade por conceção e Privacidade por Omissão.
A Equipa de Proteção de Dados é composta pelo EPD, pelo departamento de Compliance e pelos correspondentes de proteção de dados, que podem ser acompanhados por representantes da área de Recursos Humanos, Transformação e Organização, Jurídica, TIC, bem como Gestores de Dados, para questões do seu interesse.
A Equipa de Proteção de Dados cumpre os seguintes requisitos:

- Possibilitar a coordenação e acompanhamento das iniciativas desenvolvidas pelo Responsável pelo Tratamento de Dados com impacto na Proteção de Dados;
- Apoiar o EPD no desempenho das tarefas que requerem visão mais detalhada das estruturas organizacionais do Grupo;
- Apoiar o EPD com atividades de gestão de violação de dados;

- Atuar como ponto de contacto e discussão entre o EPD e os Gestores de Dados.

5.1.3 A Unidade de Conformidade

A unidade de conformidade – onde existe – garante que a organização cumpre os requisitos dos regulamentos de proteção de dados aplicáveis.
A sua principal tarefa consiste em compreender e identificar o âmbito das leis e regulamentos aplicáveis, bem como o seu possível impacto nos processos e procedimentos de negócio. Especificamente, a unidade de conformidade garante o cumprimento constante das normas internas de Proteção de Dados, no que se refere às mudanças organizacionais que possam levar à redefinição das obrigações das pessoas envolvidas.
Caso seja detetado alto risco de não conformidade, a unidade de conformidade identifica procedimentos capazes de prevenir ou, pelo menos, mitigar esse risco. Também pode apoiar a função de RH na identificação do conteúdo de formação de proteção de dados fornecida ao pessoal.
No curso das suas atividades, a unidade de conformidade mantém independência funcional dentro da estrutura empresarial.
Nalgumas das entidades jurídicas do Grupo (por exemplo, Italfondiario, supervisionada pelo Banco da Itália), a função de conformidade pode realizar controlos de segundo nível com base nos regulamentos locais aplicáveis ao contexto da entidade.

5.1.4 Unidade de Governança de TIC

No que diz respeito ao quadro regulamentar de segurança de dados pessoais e cibersegurança, a função de governação de TIC é responsável por todas as atividades relacionadas com a segurança de TI e continuidade de negócios, incluindo a definição de políticas e procedimentos de TI.
Em nível global, o Grupo de TI dentro da função COO garante:

- A definição de estratégias/políticas de TI e Segurança do Grupo, alinhadas com a evolução da estratégia de negócio;
- A conceção, manutenção, supervisão de projetos e otimização da arquitetura de TI;
- A definição e acompanhamento de uma metodologia eficaz de gestão da procura, portfólio e adoção de sistemas informáticos;
- A definição de linhas orientadoras e acompanhamento do planeamento anual do Plano de Continuidade de Negócio e Recuperação de Desastres definido a nível de Grupo;
- A definição e acompanhamento do orçamento de TI do grupo/local, salvaguardando o alinhamento com as decisões estratégicas do Grupo;
- Supervisão da inovação tecnológica do Grupo;
- A gestão de prestadores de serviços terceirizados, vigiando os principais objetivos do nível de serviço de TI local.

A nível local, as funções de TIC, em conformidade com as orientações e coordenação definidas pelo Grupo de TI e os regulamentos locais, garantem a adoção das atividades relacionadas com a segurança de TI e continuidade do negócio, incluindo definição de

políticas e procedimentos de TI locais, também por interface e supervisão de prestadores externos de TI[1], caso existam.

5.2 FUNÇÕES DE SUPERVISÃO

O papel principal das funções de supervisão é supervisionar o cumprimento dos regulamentos de proteção de dados e supervisionar o nível de risco para os direitos e liberdades fundamentais dos Titulares de Dados no que diz respeito ao tratamento de dados pessoais realizado pela empresa.

5.2.1 O Encarregado da Proteção de Dados

O RGPD (Artigos 37-39) introduziu a função de "Encarregado da Proteção de Dados" (em suma, "EPD") e obrigou os Responsáveis pelo Tratamento de Dados e Subcontratantes a fazerem uma nomeação para essa função em certas circunstâncias (a Autoridade também recomenda a designação de um EPD mesmo quando não é obrigatório).
As funções desempenhadas pelo EPD incluem assistência e controlo, consultoria, formação e informações em relação à aplicação do RGPD e das leis e regulamentos nacionais de proteção de dados. Coopera com a Autoridade e representa o ponto de contacto – também para Titulares de Dados – para questões de tratamento de dados pessoais.
O RGPD prevê que os Responsáveis pelo Tratamento de Dados e Subcontratantes sejam obrigados a designar um EPD se as suas atividades de negócios principais envolverem tratamento que exija supervisão regular e sistemática de Titulares de Dados em grande escala ou tratamento em grande escala de tipos específicos de dados pessoais ou dados relacionados com condenações criminais e crimes; a Autoridade de Supervisão esclareceu que tais entidades incluem, por exemplo, bancos, sociedades financeiras, empresas de informação comercial, empresas de recuperação de crédito, etc. O RGPD também prevê que um grupo empresarial possa designar um único EPD, desde que esse EPD possa ser facilmente contactado por cada empresa do Grupo.
Por fim, o regulamento estabelece os requisitos do EPD, estipulando que deve:

- ter conhecimento adequado da legislação e das práticas de proteção de dados, também em termos de medidas técnicas e organizacionais ou destinadas a garantir a segurança dos dados;
- exercer as suas funções com total independência e sem conflito de interesses;
- operar como empregado do Responsável pelo Tratamento de Dados ou do Subcontratante ou sob contrato de serviço (se o EPD designado for externo à Empresa);
- ter autonomia e recursos suficientes para desempenhar as funções com eficácia. Especificamente, o Responsável pelo Tratamento de Dados deve garantir ao EPD:
    - uma estrutura composta por um número adequado de colaboradores que dê assistência às atividades operacionais
    - um orçamento que poderá ser utilizado a critério do EPD para as necessidades operacionais da estrutura, inclusive para adoção de um plano de formação continuado do EPD e seus colaboradores.

[1] Na doValue a nível local italiano, a função de governança TIC é identificada, dentro da Função de Organização Retida, na estrutura de Autoridade de Design/Inovação, Segurança & BCM, na qual está incluída a função do Gestor de Segurança TIC.

5.2.1.1 O EPD Global

Na sequência da análise do regulamento e dos respetivos documentos emitidos a nível europeu e italiano, o Grupo doValue decidiu designar um EPD Global, a nível empresarial, que opera fora da empresa-mãe (doValue S.p.A.).
Conforme mostrado no gráfico a seguir (Fig. 2), na estrutura empresarial e organizacional do Grupo doValue, o EPD Global faz parte da Divisão de Conformidade e EPD Global e reporta hierarquicamente ao Conselho Geral e funcionalmente ao Conselho de Administração, que representa o Responsável pelo Tratamento de Dados.
As linhas – diferentes em forma e cor – indicam as inter-relações entre as pessoas/organismos indicados no gráfico:

- Relação hierárquica (linha a cheio): o EPD Global reporta ao Conselho Geral da Empresa-mãe;
- Relação funcional (linha azul quebrada)**:** o EPD Global reporta periodicamente ao CA da Empresa-mãe;

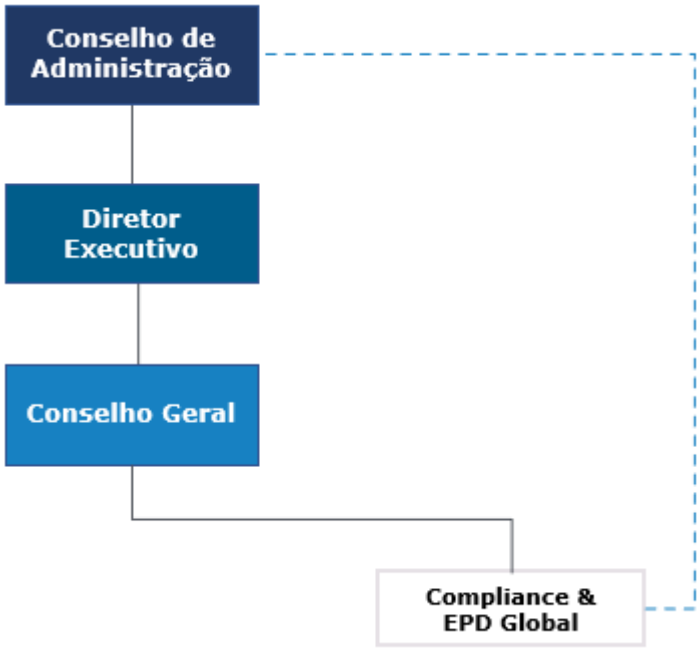


Fig. 2 - Posicionamento do EPD Global no Grupo doValue

Relativamente às atividades de orientação e coordenação, o EPD Global:

a) define a Estrutura de Controlo do Grupo no campo da Proteção de Dados e as ferramentas operacionais relacionadas para vigiar a conformidade com os regulamentos de Proteção de Dados;
b) recebe de todos os EPD locais um relatório sobre o planeamento das atividades de supervisão a realizar no ano seguinte (Planos de EPD locais);

c) recebe de todos os EPD locais um relatório sobre os resultados das atividades de supervisão realizadas em subsidiárias italianas e estrangeiras com o objetivo de gerir riscos para os direitos e liberdades dos Titulares de Dados, possíveis violações de

dados locais ou reclamações dos Titulares de Dados que possam ter impacto significativo no Grupo, ou fiscalizações pelas autoridades locais;

d) consolida a informação recebida e reporta ao Conselho de Administração da Empresa-mãe uma visão consolidada a nível Empresarial dos resultados das atividades de acompanhamento desenvolvidas no Grupo, funcionais para gestão do risco para os direitos e liberdades dos Titulares de Dados, bem como quaisquer violações de dados locais, reclamações e/ou pedidos de privacidade que possam ter impacto relevante no Grupo;

e) coordena análises de risco e análises de impacto para os direitos e liberdades dos Titulares de Dados ligados a iniciativas de projetos transversais que afetem o Grupo

f) dá opiniões sobre questões de proteção de dados que afetem o Grupo ou interpretações dos regulamentos de proteção de dados aplicáveis a todo o Grupo

g) apoia a definição de planos de formação em proteção de dados pessoais para todo o Grupo.

no que diz respeito às atividades de vigilância relacionadas com o tratamento de dados pessoais realizado a nível empresarial, o EPD Global:

a) Vigia as atividades de tratamento de dados realizadas a nível Empresarial;
b) Informa e assessora o Responsável pelo Tratamento de Dados/Gestor de Dados e os colaboradores que realizam o tratamento sobre as suas obrigações ao abrigo do regulamento;
c) Supervisiona o cumprimento dos requisitos do Regulamento Europeu e outras leis/regulamentos sobre proteção de dados pessoais, bem como o cumprimento desta Política e dos regulamentos internos sobre proteção de dados pessoais; isso inclui atribuição de responsabilidades, sensibilização e formação do pessoal envolvido no tratamento e nas atividades de controlo relacionadas;
d) Emite uma opinião em relação às avaliações de impacto do tratamento de dados realizadas a níveis empresariais em relação aos direitos e liberdades dos Titulares de Dados e supervisiona o desempenho de qualquer ação de redução de risco proposta;
e) Coopera e serve de contacto da Autoridade de Supervisão para as questões relativas ao tratamento de dados pessoais efetuado a nível empresarial;
f) Age como contacto dos Titulares de Dados para todos os assuntos relativos ao tratamento dos seus dados pessoais efetuados a nível Empresarial e ao exercício dos seus direitos;
g) Elabora relatórios internos para os órgãos de governo e controlo da Empresa-mãe (CA, CRC, Conselho Fiscal) sobre a atividade de fiscalização desenvolvida.

5.2.1.2 EPD locais

Os EPD locais são nomeados e operam em subsidiárias italianas e não-italianas e têm as seguintes responsabilidades:

a) Informar e aconselhar o Responsável pelo Tratamento de Dados/Gestor de Dados e os colaboradores que realizam o tratamento sobre as suas obrigações ao abrigo do regulamento de proteção de dados a nível local;
b) Supervisionar o cumprimento dos requisitos do Regulamento Europeu e outras leis/regulamentos de proteção de dados pessoais, bem como o cumprimento desta Política e dos regulamentos internos sobre proteção de dados pessoais; isso inclui atribuição de responsabilidades, sensibilização e formação do pessoal envolvido no tratamento e nas atividades de controlo relacionadas. Para tanto, elabora um plano anual de atividades de controlo, que submete ao Conselho de Administração da Empresa, após partilhá-lo com o EPD Global (Plano Local EPD);
c) Dar opinião em relação às avaliações de impacto do tratamento de dados realizadas em níveis empresariais relativas a direitos e liberdades dos Titulares de Dados e supervisionar o desempenho de qualquer ação de redução de risco proposta. No caso de operações de tratamento que, à luz de uma avaliação de impacto, revelem riscos específicos no que diz respeito à proteção de dados pessoais, o EPD Local deve auxiliar o Responsável pelo Tratamento de Dados/Processador na consulta à Autoridade Supervisora com vista à obtenção de parecer prévio por escrito desta última sobre a conformidade da operação de tratamento com o regulamento;
d) Prestar assistência à Unidade de RH para formação de pessoal em questões de Proteção de Dados;
e) Cooperar e agir como contacto da autoridade supervisora para questões relativas ao tratamento de dados pessoais efetuado na subsidiária;
f) Atuar como contacto dos Titulares de Dados para todas as questões relativas ao tratamento dos seus dados pessoais e ao exercício dos seus direitos;
g) Em caso de incidentes de violação de dados pessoais, nos termos do artigo 33º do RGPD, o EPD Local auxiliará o Responsável pelo Tratamento de Dados, que deverá notificar a Autoridade Supervisora do incidente no prazo de 72 horas após tomar conhecimento do mesmo;
h) Elaborar relatórios internos para órgãos de direção e controlo (CA, CRC, Conselho de Supervisão) sobre as atividades de supervisão realizadas com o objetivo de gerir os riscos de proteção de dados para os direitos e liberdades dos Titulares de Dados.
i) Elaborar um relatório de informação para o EPD Global com os resultados das atividades de supervisão realizadas localmente, detalhes ou quaisquer violações de dados locais ou reclamações de titulares de dados que possam ter impacto significativo no Grupo e detalhes de quaisquer inspeções realizadas pela Autoridade;
j) Supervisionar a adoção das políticas e regras do Grupo.

Quando uma Empresa do Grupo doValue não for obrigada a designar EPD Local (nos termos do artº 37º (1)) e a designação voluntária for excluída, a função em causa deve ser garantida pela Unidade de Compliance ou Legal local ou por outra estrutura interna, se nenhuma das unidades mencionadas existir. As seguintes responsabilidades devem ser atribuídas à estrutura em questão:

- supervisionar a conformidade com os requisitos do Regulamento Europeu e outras leis/regulamentos sobre proteção de dados pessoais, bem como o cumprimento desta Política e regulamentos internos sobre proteção de dados pessoais; isso inclui atribuição de responsabilidades, sensibilização e formação do pessoal envolvido no tratamento e nas atividades de controlo relacionadas;

- fornecer apoio ao Responsável pelo Tratamento de Dados na gestão das relações com a Autoridade Local e/ou no tratamento das solicitações de exercício dos direitos recebidos dos Titulares de Dados;
- elaborar um relatório de informações para o EPD Global sobre quaisquer deficiências identificadas no sistema de proteção de dados que possam tornar o sistema não conforme, sobre quaisquer violações de dados locais ou quaisquer reclamações recebidas de titulares de dados que possam ter impacto significativo no Grupo e em quaisquer inspeções pela Autoridade local;
- vigiar o progresso de quaisquer atividades realizadas para corrigir quaisquer deficiências identificadas no sistema de proteção de dados pessoais da empresa.

Os gráficos abaixo mostram a estrutura empresarial e as relações entre o EPD Global e os EPD locais das subsidiárias. As linhas – diferentes em forma e cor – mostram as inter-relações entre as pessoas/corpos mostrados no gráfico:

- relação hierárquica (linha a cheio): mostra as relações hierárquicas dentro das estruturas empresariais
- relação funcional (linha tracejada azul)**:** os EPD locais reportam periodicamente aos seus respetivos CA
- fluxo de informações e relatórios (linha tracejada vermelha): Relatório do EPD Local ao EPD Global sobre questões específicas de PD (ou seja, relatórios de informações sobre atividades de supervisão e gestão de acontecimentos específicos, coordenação de atividades partilhadas, inspeções pela autoridade local).

Conforme mostra o gráfico a seguir (Fig. 3), com base na estrutura empresarial e organizacional do Grupo doValue, o EPD Local doValue está situado na Divisão Nacional de Conformidade e EPD. Reporta hierarquicamente à Unidade Jurídica e funcionalmente ao Conselho de Administração, que representa o Responsável pelo Tratamento de Dados.

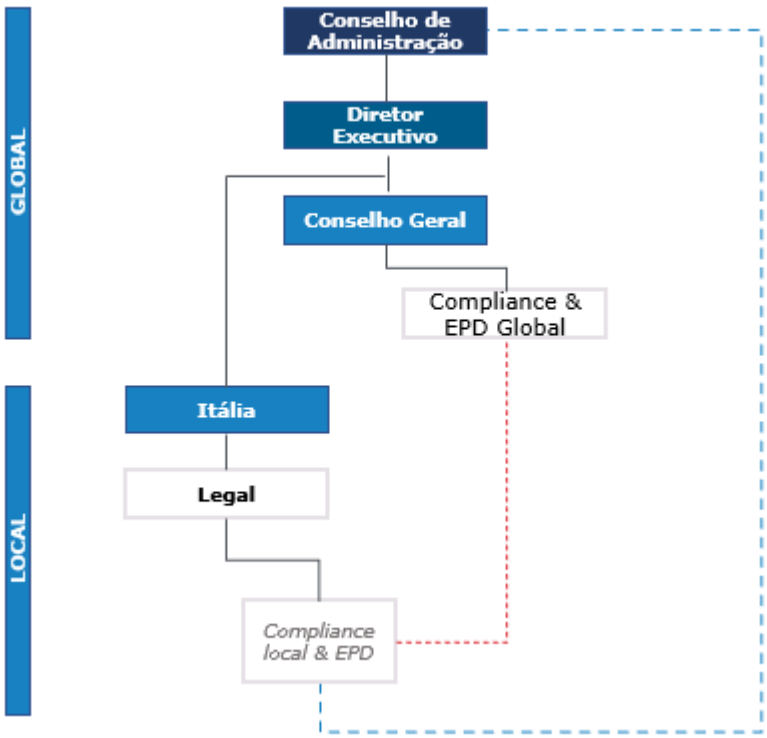


Fig. 3 - Posicionamento do EPD Local no Grupo doValue

Os EPD locais das subsidiárias italianas Italfondiario e doData reportam funcionalmente, respetivamente, ao Conselho de Administração e ao Administrador Único, que representam o Responsável pelo Tratamento de Dados. Além disso, os EPD locais devem informar o EPD Global da Empresa-mãe das atividades de supervisão realizadas localmente, violações de dados locais e inspeções pela Autoridade ou reclamações dos Titulares de Dados.

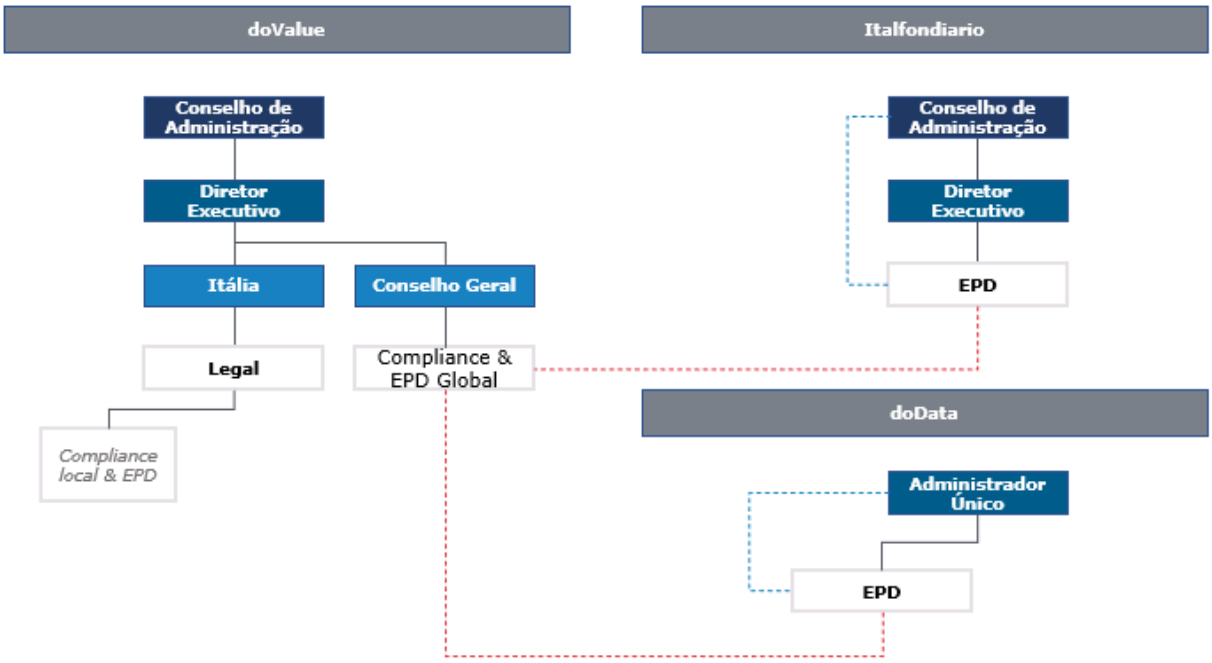


Fig. 4 - Posicionamento do EPD Local nas subsidiárias italianas do Grupo doValue

As figuras abaixo mostram a relação entre o EPD Global e os EPD locais das subsidiárias estrangeiras.

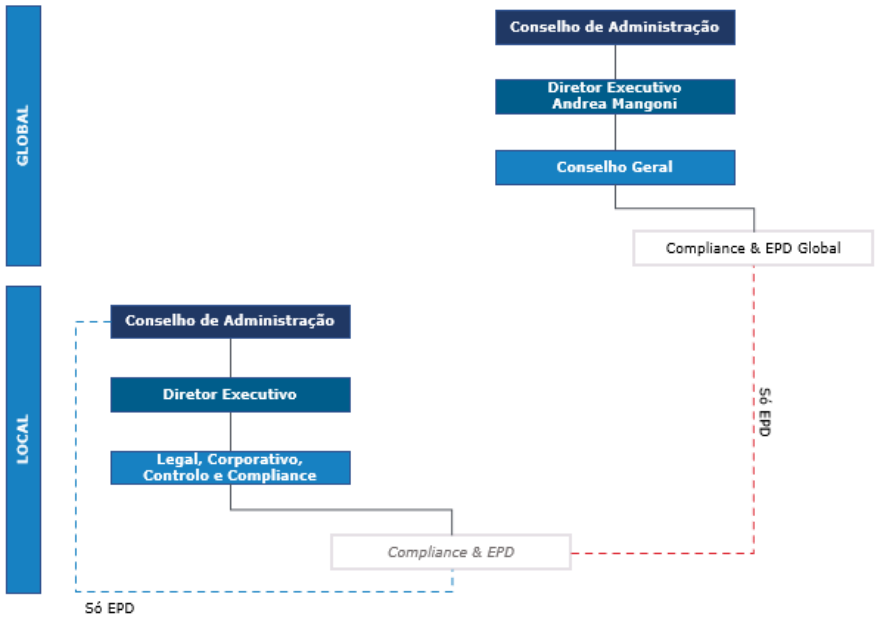


fig. 5 - Posicionamento do EPD Local na subsidiária Altamira

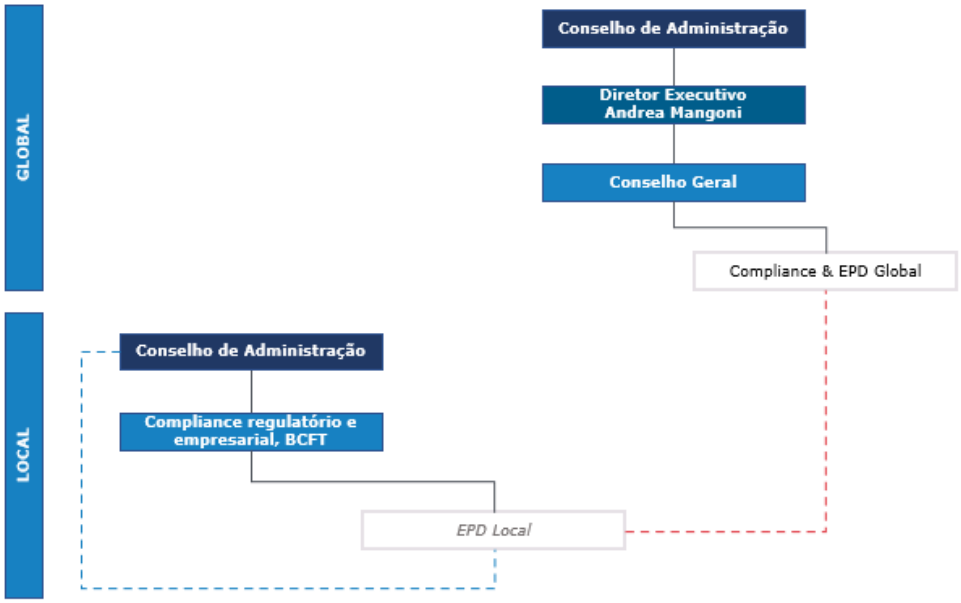


Fig. 6 - Posicionamento do EPD Local na subsidiária doValue Grécia

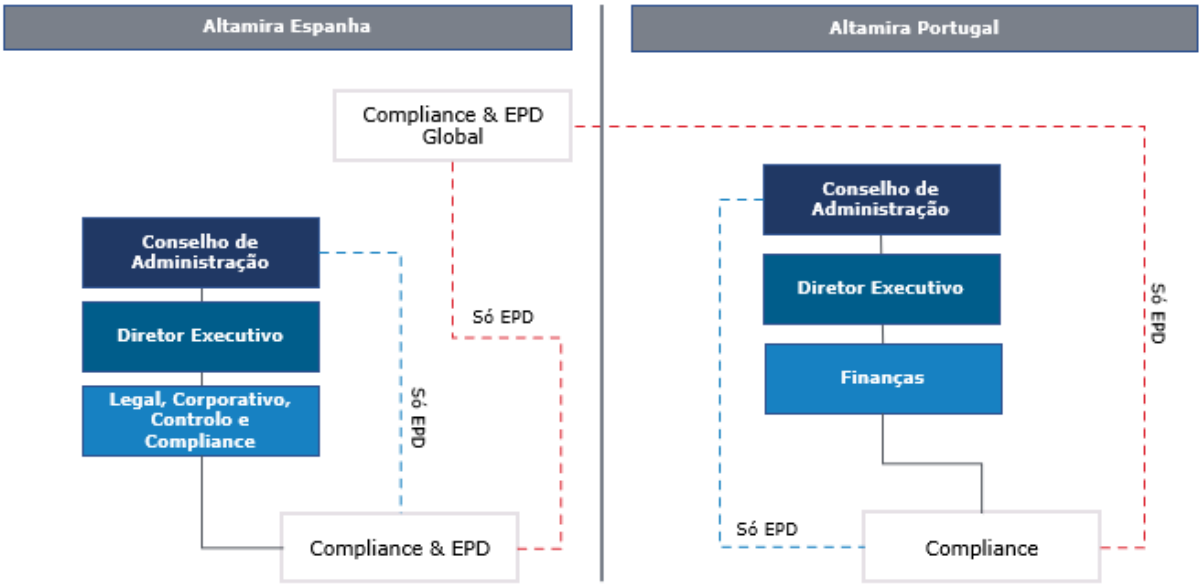


Fig. 7 - Posicionamento do EPD Local nas subsidiárias de Altamira.

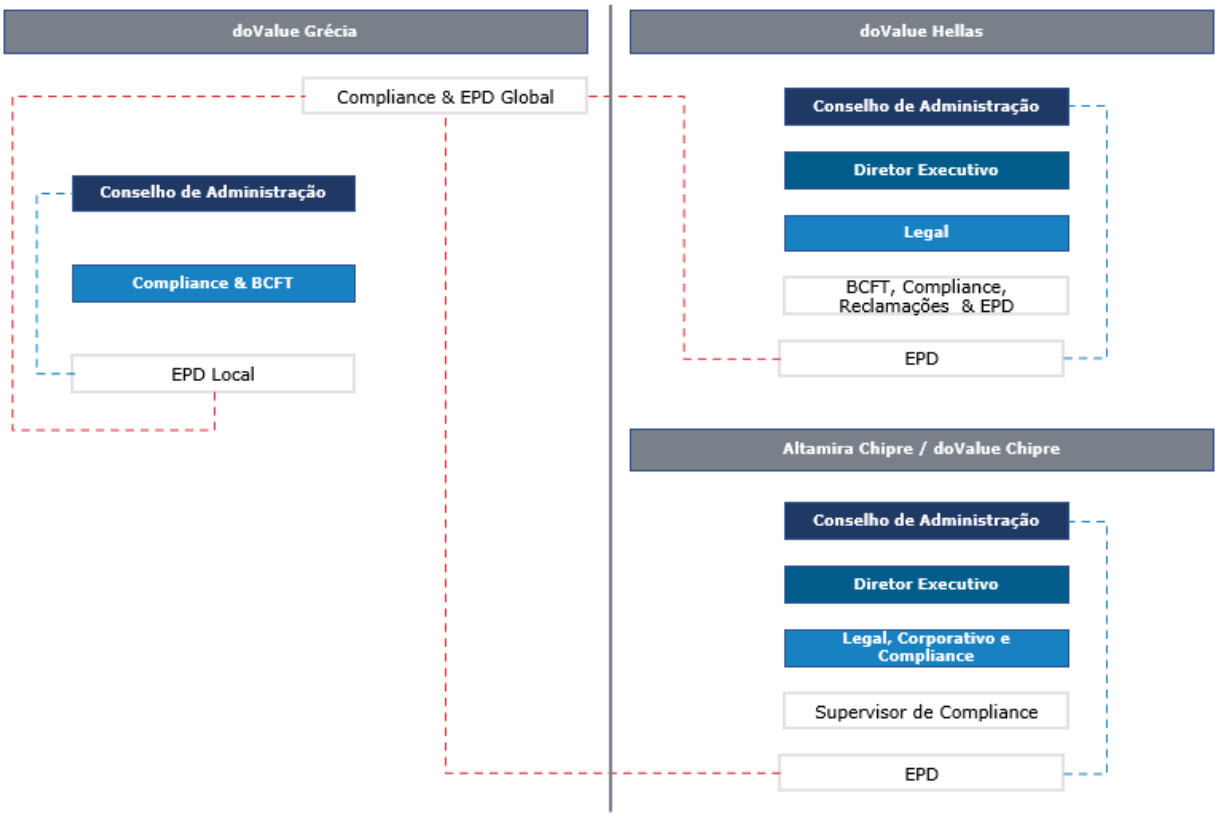


Fig. 8 - Posicionamento do EPD Local nas subsidiárias da doValue Grécia.

Os contactos dos EPD locais devem ser comunicados à Autoridade Supervisora nacional, dados a conhecer aos colaboradores da Sociedade através de correspondência específica e comunicados aos Titulares de Dados.

5.2.2 O representante de proteção de dados pessoais

O representante da proteção de dados pessoais é uma figura opcional que auxilia o EPD Local na gestão operacional de questões de proteção de dados. Opera dentro da empresa onde a função de EPD local é terceirizada para outra empresa do Grupo ou para um prestador externo. O representante da proteção de dados pessoais atua como ponto de contacto com o EPD Local, a Equipa de Proteção de Dados e os gestores de Dados de departamentos de negócios individuais.
Para as subsidiárias, o representante da proteção de dados pessoais é nomeado pelo Delegado do Responsável pelo Tratamento de Dados.
As suas principais atividades incluem:

- atualizar periodicamente o EPD Local em relação às questões de proteção de dados para que possa ser tomada ação imediata, se necessário;
- apoiar o EPD Local no desempenho das atividades que lhe são confiadas (por exemplo, supervisão da aplicação dos requisitos do regulamento, gestão dos termos do contrato, atualização de avisos de informação, etc.);
- colaborar na aplicação do princípio de Proteção de Dados por conceção e por defeito;
- participar na avaliação do impacto do tratamento de dados em relação aos direitos e liberdades dos Titulares de Dados
- apoiar a criação e atualização de registos de Tratamento;

- apoiar a gestão do processo de relato de violação de dados.

5.2.3 A Unidade de Auditoria Interna

Independentemente das funções de supervisão desempenhadas pelo EPD, no quadro do ciclo de planeamento trienal definido ao abrigo de uma lógica baseada no risco, a Função de Auditoria Interna (tanto Local como de Grupo), com vista ao controlo de nível III, supervisiona os riscos a que o Grupo está exposto no tratamento de dados pessoais dos Titulares de Dados e avalia a adequação e o cumprimento da legislação de referência externa e interna em vigor, do sistema de controlo adotado no domínio da proteção de dados pessoais.
Além disso, mediante solicitação e/ou autorização do Conselho de Administração, a Unidade de Auditoria Interna pode avaliar a adequação e funcionalidade da estrutura de controlo do EPD, relatando essas avaliações em seus relatórios periódicos ao Conselho de Administração.

5.3 FUNÇÕES OPERACIONAIS

5.3.1 Gestor de dados

Atendendo ao seu papel de fiscalização e gestão das atividades desenvolvidas pelas unidades por si dirigidas e por possuírem a necessária experiência, capacidade e fiabilidade, são designados Gestores Departamentais, que reportam diretamente ao Diretor Executivo ou ao Conselho de Administração das empresas do Grupo, como Gestores de Dados para as atividades de tratamento relativas ao seu próprio Departamento, conforme documentado no Registo de Atividades de Tratamento da Empresa a que pertencem.
O Gestor de Dados – nomeado através de documento escrito específico – deve verificar e garantir que todos os tratamentos efetuados pelas unidades à sua responsabilidade estejam em conformidade com as obrigações legais e requisitos da Autoridade, e com as instruções recebidas do Responsável pelo Tratamento de Dados. Devem também assegurar a adoção das medidas técnicas e organizacionais necessárias para proteger os dados pessoais processados; as funções e responsabilidades que lhes são confiadas são descritas em pormenor na carta de nomeação do Gestor de Dados, com base no tratamento efetuado nas várias unidades pelas quais são responsáveis.

5.3.2 Pessoas responsáveis pelo tratamento

Os responsáveis pelo tratamento são pessoas singulares que operam sob a autoridade direta de uma empresa do Grupo e desempenham tarefas e funções específicas relacionadas com o tratamento de dados pessoais.
Como Responsáveis pelo Tratamento de Dados, as Empresas designam como "Pessoas responsáveis pelo tratamento de dados pessoais" todos os empregados (independentemente da função, grau e/ou nível) e todos os colaboradores da Empresa – independentemente da relação contratual (por exemplo, trabalhadores temporários, colaboradores, estagiários, consultores) com a Empresa – a quem sejam emitidas credenciais de autenticação para acesso à rede de TI do Grupo (exceto colaboradores e consultores que trabalhem para empresas já designados como Subcontratantes terceiros, que, por sua vez, devem designar

as pessoas singulares que operam sob a sua autoridade como responsáveis pelo tratamento).
Cada pessoa encarregada do tratamento deve cumprir escrupulosamente as instruções e medidas de segurança estabelecidas na sua carta de nomeação, bem como esta Política e regulamentos internos detalhados.
O conteúdo das instruções é detalhado, em nome do Responsável pelo Tratamento de Dados, por cada Gestor de Dados, tendo em conta as atividades específicas de Tratamento – e os respetivos meios e objetivos – realizados na unidade/departamento em causa e os respetivos métodos e objetivos.

Os responsáveis pelo tratamento recebem formação destinada a aumentar a sua familiaridade com os aspetos das normas de proteção de dados pessoais mais relevantes para a sua atividade, os deveres e responsabilidades decorrentes e as medidas disponíveis para prevenir acontecimentos prejudiciais.

5.3.3 Unidade TIC – Administradores de Sistema (designado apenas para empresas italianas)

Para as empresas italianas pertencentes ao Grupo doValue, os Administradores de Sistema devem ser formalmente nomeados conforme previsto na Ordem intitulada Medidas exigidas de Responsáveis pelo Tratamento de Dados que realizam tratamento usando dispositivos eletrónicos em relação à designação de Administradores de Sistema (27 de novembro de 2008, conforme posteriormente alterado e suplementado).
Os Administradores de Sistema (doravante também "AS") são pessoas encarregadas da gestão e manutenção dos sistemas de informação e tratamento de dados da empresa; o termo abrange várias funções, como: administradores de base de dados, administradores de rede e equipamentos de segurança e Administradores de Sistema de software.
No desempenho das suas atividades especializadas, os Administradores de Sistema podem realizar atividades que podem ser consideradas tratamento de dados pessoais.
As principais atividades dos Administradores de Sistema são:

- fornecer aos Responsáveis pelo tratamento e Gestores de Dados assistência e assistência no dia-a-dia em questões técnicas relativas aos sistemas de informação utilizados no tratamento de dados pessoais;
- relatar qualquer falha do sistema de informação aos gestores de Dados;
- apoiar os gestores de Dados (e EPD locais) com análise de acontecimentos que tenham causado violações de dados;
- realizar manutenção de sistemas e protocolos de segurança.

Essas atividades em subsidiárias estrangeiras, onde não há exigência local de nomear Administradores de Sistema, são delegadas na função de TIC local.

5.4 TERCEIROS

Dependendo das circunstâncias e do tipo de tratamento, terceiros podem assumir várias funções, conforme descrito nos parágrafos abaixo.

5.4.1 Terceiros – Responsável pelo Tratamento de Dados

Alguns terceiros podem assumir o papel de Responsável pelo Tratamento de Dados autónomo pelo facto de prestarem serviços ao abrigo de códigos profissionais do sector e/ou

mandatos de agência e com apoio da sua própria organização. Os terceiros com as características acima mencionadas podem incluir: assessores profissionais (escritórios de advocacia, escritórios de contabilidade e notários).

5.4.2 Terceiros – Corresponsável pelo Tratamento de Dados

De acordo com o artº 26º do RGPD, se dois ou mais Responsáveis pelo Tratamento de Dados determinam em conjunto as finalidades e meios de tratamento, serão "Corresponsáveis pelo Tratamento de Dados". Devem determinar de forma transparente, com base em acordo interno, as respetivas responsabilidades pelo cumprimento das obrigações decorrentes do RGPD. As Empresas do Grupo doValue podem assumir o papel de Corresponsáveis pelo Tratamento de Dados em relação a determinados tratamentos de dados realizados em conjunto.

5.4.3 Terceiros - Subcontratante

O Subcontratante é uma pessoa individual ou coletiva, externa à organização da Sociedade, que, no âmbito das relações contratuais com as empresas do Grupo, trata os Dados Pessoais dos quais a Sociedade é Responsável.
Ao abrigo do artº28º nº 3do RGPD, a designação do Subcontratante e o tratamento realizado por ele serão regidos por contrato ou outro ato jurídico vinculativo para o Subcontratante e que estabeleça o objeto e duração do tratamento, natureza e finalidade do tratamento, o tipo de dados pessoais e categorias de titulares de dados e obrigações e direitos do Responsável pelo Tratamento de Dados.
Em particular, o Subcontratante deve:

- garantir que as atividades de tratamento sejam legítimas, seguindo as instruções fornecidas, em cada ocasião, pela Empresa do Grupo que é Responsável pelo Tratamento de Dados;
- garantir que as pessoas autorizadas a processar dados pessoais se comprometam com a confidencialidade;
- adotar um processo de resposta a um Titular de Dados que queira exercer os seus direitos, se o Responsável pelo Tratamento de Dados tiver delegado esta função num Subcontratante ou se as solicitações recebidas forem imediatamente transferidas para o Responsável pelo Tratamento de Dados para que a resposta necessária possa ser dada em conformidade com o prazo aplicável;
- fornecer todas as informações necessárias para demonstrar a conformidade com o regulamento aplicável e as instruções recebidas, sem afetar o direito do Responsável pelo Tratamento de Dados de verificar a aplicação adequada do regulamento e o cumprimento das instruções fornecidas;
- interromper imediatamente as atividades de tratamento de dados pessoais e eliminá-los ou disponibilizá-los ao Responsável pelo Tratamento de Dados se o subcontratante for destituído dessa função ou a pedido do Responsável pelo Tratamento de Dados;
- permitir quaisquer Auditorias pelas Empresas do Grupo e dar colaboração total na deteção de quaisquer Violações de Dados, a fim de adotar os requisitos regulamentares aplicáveis.

No quadro dos contratos externalizados das atividades desenvolvidas a nível empresarial, cada Empresa que preste serviços dentro do grupo é nomeada Gestora ou Subgestora (nos termos do parágrafo 5.4.4 abaixo) do Tratamento pelas restantes empresas do Grupo. Além disso, fornecedores e terceiros que tratem dados em relação de que as empresas do grupo

sejam Responsáveis pelo Tratamento de Dados também são designados como subcontratantes, por exemplo, partes envolvidas na execução de atividades relacionadas com produtos e serviços oferecidos e atividades de marketing para titulares de dados.

5.4.4 Terceiros – Subcontratante

Com a autorização geral ou específica por escrito do Responsável pelo Tratamento de Dados, o Subcontratante pode, por sua vez, designar outro Subcontratante relativamente a terceiros – pessoas individuais ou coletivas – que processem dados pessoais no decorrer das atividades para as quais é designado como Subcontratante.
A relação entre o Subcontratante e o Subcontratante contratado deve, como a relação entre o Processador e o Responsável pelo Tratamento de Dados, ser regida por um contrato ou outro ato legal que especifique deveres e responsabilidades nos termos do art.º 28º nº 4 do RGPD. O Subcontratante assume total responsabilidade perante o Responsável pelo Tratamento de Dados pelo cumprimento do Subcontratante das respetivas obrigações.
Conforme indicado acima, em relação a Dados Pessoais de entidades obrigadas, conforme processados no âmbito de atividades de recuperação de crédito, as Empresas do Grupo doValue operam como Subcontratantes designados pelos Mandantes na qualidade de Processadores. Com autorização do Responsável pelo Tratamento de Dados (geral ou específico), a Empresa pode usar subcontratados e designar como subcontratantes os fornecedores e, em geral, os terceiros que, ao abrigo de um contrato com as empresas, processem Dados Pessoais de entidades obrigadas, por exemplo, consultores profissionais terceirizados, empresas de recuperação de crédito e/ou prestadores de serviços de TI.

5.5 RELAÇÕES ENTRE FUNÇÕES DE GOVERNANÇA E DE SUPERVISÃO

As tabelas abaixo mostram as relações entre as várias funções de proteção de dados identificadas pelo Grupo doValue. Especificam se os relacionamentos são baseados em:

- reporte hierárquico;
- reporte funcional;
- fluxo de informação e coordenação entre partes pertencentes a várias entidades jurídicas do Grupo
- fluxo interno de informações entre partes pertencentes a uma mesma pessoa coletiva;
- Interação com terceiros não pertencentes ao Grupo.

Funções envolvidas	Relação	Descrição
Responsável pelo Tratamento de Dados - EPD Global/Local	Reporte funcional	• O Responsável pelo Tratamento de Dados recorre ao EPD Global ou o EPD Local em caso de inspeção e/ou solicitações dos Órgãos/Autoridade de Supervisão a nível Empresarial ou Local, respetivamente. • O EPD Global elabora um relatório regular sobre as atividades de supervisão desempenhadas a nível corporativo, supervisiona as ações necessárias para satisfazer pedidos recebidos da Autoridade Supervisora e reporta ao Responsável pelo Tratamento de Dados sobre a situação das ações tomadas a nível corporativo. • O EPD Local elabora um relatório regular sobre as atividades de supervisão realizadas a nível local, supervisiona as ações necessárias para satisfazer pedidos recebidos da Autoridade de Supervisão e reporta ao Responsável pelo Tratamento de Dados sobre o estado da ação tomada a nível local.
EPD Global – Grupo de TI	Fluxo de Informação Interno	O EPD Global e a função de TI do Grupo interagem para solicitar opiniões sobre questões de Proteção de Dados no contexto da evolução e manutenção do sistema de gestão de dados pessoais ao nível do Grupo (por exemplo, no caso de grandes projetos de TI com impacto na forma como os dados pessoais são geridos e protegidos).
EPD Local - Unidade de Conformidade (a havê-la) + Governança de TIC local	Fluxo de Informação Interno	A função de conformidade (a havê-la) e a função de governança de TIC interagem com o EPD Local para solicitar feedback sobre questões de proteção de dados no âmbito das atividades de manutenção do sistema de gestão de dados pessoais

Funções envolvidas	Relação	Descrição
PD Global - EPD Local	Fluxo de informação e coordenação	Sujeito aos limites estabelecidos nos artigos 37º ao 39º do RGPD e, embora respeitando os requisitos de independência profissional, os EPD locais interagem com o EPD Global para: • Discutir dúvidas sobre interpretação do Regulamento Geral de Proteção de Dados • Informar sobre acontecimentos locais que possam desencadear riscos para o sistema de proteção de dados pessoais do Grupo (por exemplo, violações de dados, não aplicação dos princípios estabelecidos pelo RGPD, análise de risco/avaliação de impacto, identificação adequada da base legal para tratamento) • Informar sobre atividades de supervisão realizadas a nível local e reportadas ao CA da Subsidiária • Coordenar atividades de supervisão a serem realizadas localmente • Avaliar a adoção de políticas/procedimentos/instruções operacionais concebidos a nível local e/ou formação específica de pessoal e sessões de sensibilização sobre questões de proteção de dados.
EPD local – Correspondente de proteção de dados	Reporte funcional	Para as subsidiárias que externalizam a função de EPD para o EPD Local do Responsável pelo Tratamento de Dados ou para terceiros não pertencentes ao Grupo: • O EPD Local da empresa-mãe interage com o representante de proteção de dados pessoais em todas as questões relacionadas com o tratamento de dados pessoais e em questões de proteção de dados relacionadas à subsidiária • Após consulta ao EPD Local, o representante da proteção de dados pessoais emite políticas e diretrizes e atua como referência para a estratégia de negócios e melhorias que se mostrem necessárias ao sistema de PD da empresa. • O representante da proteção de dados pessoais interage e trata com o EPD Local de questões específicas relativas à análise organizacional e/ou regulatória; caso sejam identificadas anomalias ou problemas, são devidamente comunicados ao EPD Local.

Funções envolvidas	Relação	Descrição
Auditoria Interna - EPD Global/Local	Fluxo de Informação Interno	A Auditoria Interna interage com o EPD Global e o EPD Local para coordenar e receber informações sobre acontecimentos relevantes, por exemplo, violações de dados. Além disso, os EPD Global e Local informam a função de Auditoria Interna dos planos anuais para as atividades de supervisão e resultados das atividades de supervisão realizadas.
Unidade de Conformidade + Governança de TIC local – Gestores de Dados	Fluxo de informação interno	A Unidade de Conformidade interage com os Gestores de Dados para todas as questões envolvidas para garantir que o sistema de proteção de dados permaneça em conformidade com os requisitos dos regulamentos de proteção de dados europeus e locais (por exemplo, atualização do registo de atividades de tratamento, desempenho de AIPD – avaliação de impacto sobre a proteção de dados - elaboração de instruções operacionais) A função de Governança de TIC local interage com os Gestores de Dados para todas as questões relativas à manutenção de sistemas de informação e medidas técnicas de segurança relacionadas em vigor para proteger o tratamento de dados pessoais.
EPD Globais/Locais – subcontratantes	Interação com terceiros	O EPD Global e o EPD Local (nos ambientes de tratamento corporativo e Local, respetivamente) interagem com terceiros que, nos termos do artigo 28º nº 3 do RGPD, foram designados Subcontratantes externos para todos os assuntos que, no âmbito das atividades atribuídas por contrato, possam ter efeito organizacional e/ou regulamentar sobre o tratamento de dados pessoais (por exemplo, comunicação de violações de dados, inspeções/auditorias programadas, avaliações de impacto, comunicações a serem enviadas à Autoridade Supervisora)
EPD local – gestores de Dados	Fluxo de informação interno	O Gestor de Dados interage com o EPD Local para pedidos de pareceres na área da Proteção de Dados no exercício das suas atividades que contribuam para a manutenção do sistema de proteção de dados da empresa (ex: atualização do registo das atividades de tratamento, atuação do DPIA). O EPD Local interage com o Gestor de Dados para solicitações de informações sobre os meios de tratamento, os dados processados e quaisquer problemas de tratamento identificados.

5.6 RELAÇÕES ENTRE FUNÇÕES OPERACIONAIS

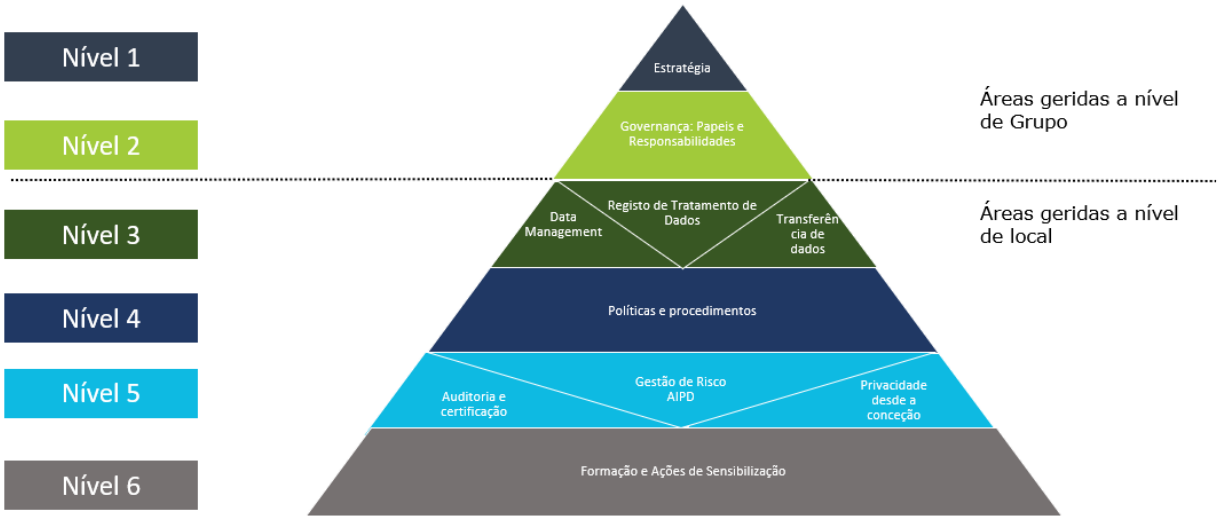
Funções envolvidas	Relação	Descrição
Gestores de dados – responsáveis pelo tratamento	Reporte hierárquico	Dependendo das circunstâncias, o gestor de dados interage com as pessoas responsáveis pelo tratamento em caso de: • instruções/orientações sobre meios de tratamento, proteção de dados pessoais • questões relativas à aplicação adequada das medidas de segurança introduzidas para proteger o tratamento em causa • revisões periódicas do registo das atividades de tratamento de dados • realização de análise de risco e atividades AIPD
Gestores de dados – Administradores de Sistema (interno)	Fluxo de informação interno	Dependendo das circunstâncias, o Gestor de Dados interage com os administradores do sistema em caso de: • instruções/orientações sobre meios de tratamento, proteção de dados pessoais • consequências resultantes do mau funcionamento da rede/sistemas de TI • questões relativas à aplicação adequada das medidas de segurança introduzidas para proteger o tratamento em causa • revisões periódicas do registo das atividades de tratamento de dados em relação aos sistemas de informação utilizados e às medidas de segurança adotadas. • Realização de análise de risco e atividades de AIPD
Gestores de Dados – Processadores de terceiros	Interação com terceiros	Para o tratamento por que é responsável, o Gestor de Dados interage com os Processadores em caso de: • instruções/orientações sobre meios de tratamento, proteção de dados pessoais • Pedidos de informações específicas necessárias para o desempenho do AIPD (por exemplo, medidas de segurança adotadas) • Aceitação de relatórios de violação de dados • Gestão de violações de dados (ou seja, recolha de informações úteis para fins de notificação de violação de dados)

6 O MODELO DE DOCUMENTO DE PROTEÇÃO DE DADOS

A **doValue** criou o seu próprio **Modelo de Documento de Proteção de Dados**, aplicável à **Empresa-mãe** e a todas as **subsidiárias** do Grupo (na Itália e no estrangeiro). Consiste num corpo de documentos, incluindo:

- a nível **Corporativo**:
  - Política de Grupo de alto nível que descreve a estratégia de PD do Grupo, o modelo organizacional de PD e os requisitos gerais de PD aplicáveis a todas as empresas do Grupo (conforme representado neste documento);
  - Estrutura de controlo EPD;
  - Regulamento EPD.
- a nível de **empresa**:
  - Procedimentos/instruções operacionais para gestão de assuntos específicos, por exemplo, gestão de violação de dados pessoais, atualização do Registo de Atividades de Tratamento, exercício de direitos por parte dos titulares de dados, etc.
  - Ferramentas/modelos preparados para cumprir requisitos regulamentares específicos, por exemplo, registos de tratamento de dados pessoais, registos de violações de dados pessoais, registos de reclamações por titulares de dados, designações de DP, avisos de informações de privacidade, cláusulas contratuais, AIPD, etc.
  - Documentos específicos elaborados para demonstrar o desempenho de atividades específicas, por exemplo, análises de impacto realizadas em novas atividades de tratamento de dados (triagem de privacidade e AIPD), organização de sessões de formação sobre questões de proteção de dados pessoais, etc.
  - Estrutura de controlo EPD específicas para contexto empresarial e relatórios relacionados.

A documentação de Proteção de Dados consiste em **6 níveis**, cada um dos quais foi desenvolvido em conformidade com padrões internacionais de segurança e melhores práticas de Proteção de Dados, conforme indicado no diagrama a seguir. Os dois primeiros níveis referem-se a questões tratadas a nível de Grupo, enquanto os níveis subsequentes referem-se a questões tratadas a nível local por todas as Empresas do Grupo.



* Os planos de formação e sensibilização também são definidos a nível de grupo.

Fig.9 - Modelo de Documento DP

A tabela a seguir contém, para cada nível de documentação, uma descrição do conteúdo que deve ser incluído em cada elemento de componente da documentação de DP.

Nível	Descrição
Nível 1 Estratégia	A Empresa determina a abordagem de alto nível e o seu apetite ao risco, sobre o qual desenvolverá o seu sistema de proteção de dados
Nível 2 Funções e responsabilidades de Governança	A Empresa prossegue os objetivos definidos ao nível da Estratégia, adotando um modelo de governança de proteção de dados consistente com o seu negócio central e enfatizando a importância atribuída dentro da organização de proteção de dados às funções e responsabilidades de intervenientes chave, como o Encarregado da Proteção de Dados.
Nível 3 de Inventário de tratamento, gestão de dados e transferências	A Empresa identifica todas as atividades de tratamento de dados realizadas internamente, bem como as transferências de dados entre empresas do Grupo e terceiros, e elabora o Registo de Tratamento de Dados. A Empresa vigia e identifica os meios usados para tratamento e quaisquer transferências de dados para países fora da UE.
Nível 4 Políticas e procedimentos	A Empresa garante a proteção, controlo e gestão do tratamento de dados pessoais através da adoção de um conjunto de políticas e procedimentos que visam o bom desenvolvimento destes processos, em conformidade com os requisitos do RGPD (ex.: Procedimento de gestão de violação de dados).
Nível 5 Gestão de risco, AIPD, privacidade por conceção, auditoria e certificações	Em conformidade com o RGPD, a Empresa aplica uma abordagem orientada para o risco ao determinar os seus processos de planeamento e metodologias. Isso envolve análise de risco ou avaliações de impacto (triagem de privacidade e AIPD) ao conceber um novo produto/serviço ou alterar um existente. Além disso, a conformidade com o RGPD é garantida por auditorias regulares do sistema de PD e pode ser confirmada por relatórios/certificações de auditoria.
Nível 6 Formação e Sensibilização	A Empresa elabora um plano de formação em proteção de dados e cria um elevado nível de sensibilização em toda a empresa permitindo aos seus colaboradores compreender e aplicar as regras estabelecidas em matéria de proteção de dados. Os planos de formação e sensibilização também são definidos a nível de Grupo.

7 O MODELO DE GESTÃO DE DADOS

Os regulamentos de proteção de dados pessoais envolvem muitos requisitos diferentes. Tal inclui medidas para proteger os Titulares de Dados (aviso de informação, consentimento,

gestão de direitos), requisitos organizacionais (avaliação de impacto, abordagem "privacidade por conceção e defeito", registo de atividades de tratamento, procedimentos de gestão de violação de dados) e requisitos de segurança. Além disso, certos tipos de tratamento estão sujeitos ao cumprimento de requisitos específicos das Autoridades de Supervisão locais, que as empresas do Grupo devem vigiar constantemente, a fim de adaptar o seu modelo de gestão de dados para cumprir os requisitos regulamentares locais. Esta secção define as diretrizes para conformidade com os requisitos do Regulamento Geral de Proteção de Dados.

7.1 REQUISITOS DE INFORMAÇÃO

Para garantir o tratamento correto e transparente dos dados pessoais, o Responsável pelo Tratamento de Dados é obrigado a fornecer antecipadamente ao Titular de Dados uma série de informações, especificamente mencionadas no Regulamento (nos termos do art.º 13º do RGPD):

- a identidade e os dados de contacto do Responsável pelo Tratamento de Dados;
- os dados de contacto do Encarregado da Proteção de Dados (EPD);
- as finalidades do tratamento;
- a base jurídica para tratamento com referência específica, se aplicável, a quaisquer "interesses legítimos" prosseguidos;
- os destinatários e categorias de destinatários dos Dados Pessoais (dentro do Grupo doValue ou terceiros);
- se aplicável, o facto de o Responsável pelo Tratamento de Dados pretender transferir dados pessoais para um país terceiro;
- o período durante o qual os dados pessoais serão retidos ou os critérios usados para determinar esse período;
- os direitos concedidos ao Titular de Dados e como exercê-los;
- quando o tratamento é baseado no consentimento, a existência do direito de retirar o consentimento a qualquer momento (sem afetar a legalidade do tratamento com base no consentimento antes de sua retirada) e como é possível retirar o consentimento;
- o direito de apresentar queixa à Autoridade de Supervisão;
- se o fornecimento de dados pessoais é requisito legal ou contratual, ou requisito necessário para celebrar um contrato, e as possíveis consequências do não fornecimento de tais dados;
- a existência de tomadas de decisão automatizadas, incluindo elaboração de perfis, a lógica envolvida e as consequências para o Titular de Dados.

Nos termos do artigo 14.º do RGPD, caso os dados não tenham sido obtidos diretamente do Titular de Dados, as informações devem também especificar as categorias de dados pessoais processados e a origem dos dados.

As informações devem ser fornecidas ao Titular de Dados no momento da recolha dos dados pessoais ou, o mais tardar, no prazo de um mês após a obtenção dos dados, caso não tenham sido obtidos diretamente do Titular de Dados.

Cada Empresa do Grupo determinará a informação a ser prestada aos Titulares de Dados, para todos os tratamentos sobre os quais essa empresa atue como Responsável pelo

Tratamento de Dados, supervisionando continuamente se as alterações nos meios de tratamento resultam na necessidade de atualização da informação.

7.2 LICITUDE DO TRATAMENTO E CONSENTIMENTO

Qualquer tratamento de dados deve ter base legal adequada (licitude do tratamento nos termos do art.º 6º do RGPD).

Uma condição para a licitude do tratamento é que tenha sido autorizado pelo Titular de Dados, dando **consentimento ao tratamento**.

O consentimento deve ser obtido no formulário e usando os métodos fornecidos pelo RGPD deve ser demonstrável, ou seja, o Responsável pelo Tratamento de Dados deve ser capaz de demonstrar que o Titular de Dados deu seu consentimento.

Ao abrigo do artigo 7.º do RGPD, o consentimento é considerado válido quando os seguintes requisitos são cumpridos:

- Livre: o Titular de Dados estará sempre em posição de recusar-se a dar consentimento para a execução de certas atividades de tratamento; em particular, a execução de um contrato ou execução de um serviço não pode estar subordinada à concessão de consentimento para tratamento de dados desnecessários à execução do contrato;
- Específico: cada operação de tratamento que, à falta de outro fundamento para a licitude do tratamento, exija consentimento dos Titulares de Dados, está sujeita a consentimento específico;
- Informado: o consentimento deve ser antecedido da prestação de informações sobre o tratamento dos dados e os objetivos do consentimento dado e, em qualquer caso, da respetiva revisão pelo Titular de Dados; o pedido de consentimento deve ser apresentado de forma claramente distinta das demais, de forma inteligível e facilmente acessível, em linguagem clara e simples;
- Claro: a intenção do Titular de Dados de consentir com o tratamento dos dados pessoais que lhe digam respeito deve ser expressa através de declaração ou ato afirmativo;
- Explícito: o consentimento para o tratamento de determinados dados sensíveis deve ser dado de forma explícita.

O Titular de Dados terá o direito de retirar o consentimento a qualquer momento. A retirada do consentimento não afetará a legalidade do tratamento realizado até àquele momento; deve ser possível retirar o consentimento fácil e prontamente.

Os tipos de tratamento que exigem consentimento incluem, por exemplo, uso de dados para fins comerciais ou comercialização de produtos e serviços da empresa ou de terceiros, conforme solicitado através do preenchimento de formulários nos sites da empresa ou através de formulários impressos, a transmissão de dados pessoais às empresas do Grupo doValue em caso de tratamento não efetuado para efeitos contabilísticos e administrativos (conforme definido no considerando 48 do RGPD), a transmissão aos sistemas de informação de crédito de dados positivos sobre a regularidade de pagamentos de clientes com relações de financiamento.

Existem outras situações de tratamento legal em que os dados pessoais podem ser processados mesmo **sem consentimento**. Incluem, por exemplo, casos em que o Tratamento:

- é necessário para execução de um contrato de que o Titular de Dados é parte ou para tomar medidas a pedido do Titular de Dados antes de celebrar um contrato;

- é necessário para cumprimento de uma obrigação legal a que o Responsável pelo Tratamento de Dados esteja sujeito;
- é necessário para efeitos dos interesses legítimos prosseguidos pelo Responsável pelo Tratamento de Dados ou por um terceiro, exceto quando tais interesses sejam anulados pelos interesses ou direitos e liberdades fundamentais do Titular de Dados que requeiram proteção de dados pessoais.

Em todos os casos em que os dados sejam processados para atender a um pedido do Titular de Dados, por exemplo, solicitação de contacto ou informações, prestação de serviço ou cumprimento de obrigações contratuais, a resposta a uma reclamação ou quando os dados são processados para cumprir outras leis ou regulamentos aplicáveis à empresa (por exemplo: diligência do cliente para fins de combate ao branqueamento de capitais, registo em listas exigidas pelos regulamentos sobre abuso de mercado, conformidade com verificações e comunicações empresariais para membros de órgãos de direção e verificações exigidas por lei em relação a partes relacionadas), não é necessário solicitar e obter o consentimento do Titular de Dados.

Se os dados pessoais forem processados por uma empresa do Grupo na qualidade de Responsável pelo Tratamento de Dados, a transferência dos dados para outra empresa do Grupo atuando como Subcontratante com base em contrato de serviço entre empresas é permitida sem solicitar consentimento aos Titulares de Dados.

Por fim, em todos os casos em que os dados são processados pelas empresas do Grupo na qualidade de Subcontratantes (Terceiros), por exemplo, gestão de crédito e recuperação em nome de Mandantes ou *servicers* de SPV, não é necessário solicitar consentimento ao Titular de Dados para o tratamento de dados realizado na qualidade de Subcontratante

no pressuposto de que, quando necessário, o consentimento já tenha sido solicitado e validamente obtido pelo Responsável pelo Tratamento de Dados.

7.3 GESTÃO DE DIREITOS DOS TITULARES DE DADOS

Em conformidade com o RGPD, o Grupo doValue garante o reconhecimento dos seguintes direitos dos Titulares de Dados (conforme definido pelos artigos 15º ao 21º do RGPD):

- ✓ *Direito de acesso*: o Titular de Dados tem o direito de obter a confirmação do tratamento ou não dos dados pessoais que lhe dizem respeito e, se for o caso, de aceder aos dados pessoais;
- ✓ *Direito à retificação*: o Titular de Dados tem o direito de obter a retificação dos dados pessoais inexatos que lhe digam respeito ou de que os dados pessoais incompletos sejam completados, tendo em conta as finalidades do tratamento;
- ✓ *Direito ao apagamento dos dados*: o Titular de Dados tem o direito de obter a eliminação dos dados pessoais que lhe digam respeito. Note-se que os dados cuja retenção seja justificada ou necessária para fins legais não podem ser eliminados (por exemplo, quando um cliente solicita a eliminação, mas há disputa jurídica entre ele e a Empresa, a Empresa pode reter legitimamente os dados do cliente, independentemente da solicitação);
- ✓ *Direito à limitação do tratamento*: o Titular de Dados tem o direito de obter limitação ao tratamento, caso a exatidão dos dados pessoais seja contestada pelo Titular de Dados, por um prazo que permita ao responsável pelo tratamento verificar a exatidão dos dados pessoais; ou quando o Titular de Dados se tenha oposto ao tratamento, enquanto se verifica se os fundamentos legítimos do Responsável pelo Tratamento de Dados prevalecem sobre os do Titular de Dados;
- ✓ *Direito à portabilidade de dados*: o Titular de Dados tem o direito de receber os dados pessoais relativos a si em formato estruturado, comummente usado e legível por

máquina e o direito de transmitir esses dados a outro responsável pelo tratamento sem impedimentos;

- ✓ *Direito à oposição*: o Titular de Dados tem o direito de se opor a qualquer momento ao tratamento de dados pessoais relativos a si para qualquer ou todos os fins para os quais tenham sido recolhidos. Em particular, o Titular de Dados tem o direito de alterar o seu consentimento e, posteriormente, interromper qualquer operação ou conjunto de operações realizado, seja ou não por meios automatizados, como recolha, registo, organização, armazenamento, consulta, adaptação ou alteração, seleção, recuperação, comparação, uso, restrição, comunicação, disseminação, eliminação ou destruição, mesmo que não registado em base de dados;
- ✓ *Direito de não sujeição a processo automatizado de tomada de decisão*: o Titular de Dados tem o direito de não ser sujeito a uma decisão baseada exclusivamente no tratamento automatizado, incluindo criação de perfis, que produza efeitos jurídicos a seu respeito ou que o afete de forma significativa.

Para cada um dos direitos acima, as empresas do Grupo doValue, na qualidade de Responsáveis pelo Tratamento de Dados, devem adotar procedimentos e ferramentas internas adequadas para:

- Dar resposta ao Titular de Dados sem atrasos indevidos em relação aos pedidos recebidos, ao mesmo tempo que justifica ao Titular de Dados quaisquer atrasos ou falhas no fornecimento de resposta
- gerir solicitações de titulares de dados dentro da empresa enquanto realiza a recuperação, alteração ou eliminação apropriada dos dados pessoais;
- informar quaisquer Responsáveis pelo Tratamento de Dados terceirizados aos quais os dados tenham sido comunicados dos pedidos do Titular de Dados.

As empresas do Grupo são obrigadas a dar resposta ao exercício de direitos por titulares de dados cujos dados são tratados por si enquanto Responsáveis pelo Tratamento de Dados ou como Subcontratantes, quando for especificamente solicitado pelo Responsável pelo Tratamento de Dados no Acordo de Proteção de Dados (DPA).

Entende-se que os pedidos de exercício de direitos por parte dos Titulares de Dados não podem dizer respeito a dados pessoais referentes a terceiros, exceto em circunstâncias particulares (por exemplo, através de representante legal ou advogado).

Em conformidade com o RGPD, o EPD Local atua como contacto para os Titulares de Dados que exercem direitos e a resposta a ser fornecida aos Titulares de Dados deve ser acordada previamente com o EPD Local.

Nos casos em que as empresas do Grupo doValue operam como Subcontratantes externalizados (por exemplo, em relação a atividades de recuperação de crédito), devem ser capazes de dar assistência ao Responsável pelo Tratamento de Dados na gestão de pedidos de titulares de dados com base nas obrigações estabelecidas nos contratos de serviço relevantes e em quaisquer instruções de operação associadas. Os métodos a serem usados para lidar com as solicitações dos Titulares de Dados são determinados a nível local em regras e regulamentos internos específicos.

7.4 GESTÃO DE RETENÇÃO DE DADOS

Ao abrigo do referido princípio de restrição de tratamento, os dados devem ser conservados pelo período mínimo necessário para efeitos do seu tratamento (Retenção de Dados). A fim de garantir que os dados pessoais não sejam armazenados por mais tempo do que o necessário, o Responsável pelo Tratamento de Dados deve estabelecer um prazo para a sua eliminação – o qual pode variar dependendo do tipo de dados e da finalidade do tratamento

– e adotar as medidas técnicas e organizacionais adequadas garantir o cumprimento do prazo máximo de retenção estabelecido.

O seguinte deve ser levado em consideração ao determinar o período de retenção:

- requisitos de retenção estabelecidos por lei (por exemplo, privacidade, obrigação de reter registos fiscais, período de retenção de registos contabilísticos, correspondência, contratos);
- fins de recolha e tratamento em relação a requisitos comerciais e operacionais;
- instruções fornecidas pelo Responsável pelo Tratamento de Dados (por exemplo, Diretores/SPV) para dados processados na capacidade de Subcontratantes (por exemplo, dados de devedores).

Quando uma empresa do Grupo pretende interromper a realização de uma ou mais atividades de tratamento realizadas como Responsável pelo Tratamento de Dados autónomo, os Dados Pessoais anteriormente utilizados no contexto de tais operações devem ser destruídos ou tornados anónimos (quando aplicável), exceto para fins de cumprimento de obrigações legais ou de defesa.

Nos casos em que as empresas do Grupo doValue atuem como Subcontratantes, são respeitados os requisitos contidos no Contrato de Tratamento de Dados (DPA) para eliminação dos dados fornecidos pelo Responsável pelo Tratamento de Dados.

Os regulamentos internos específicos estabelecem os requisitos de retenção de dados para os vários tipos de dados/tratamento.

7.5 PROTEÇÃO DE DADOS POR CONCEÇÃO E DEFEITO – AVALIAÇÃO DE IMPACTO DA PROTEÇÃO DE DADOS (DPIA)

Para salvaguardar os direitos e liberdades das pessoas singulares em relação ao tratamento dos seus dados pessoais, o RGPD exige que o responsável pelo tratamento adote políticas internas e aplique medidas que satisfaçam os princípios da proteção de dados por conceção e da proteção de dados por defeito.

Em particular, o princípio de "**Proteção de Dados por conceção**" prevê que, tendo em consideração o estado de arte, o custo de implementação, e a natureza, âmbito, contexto e finalidades de tratamento, bem como riscos de probabilidade variável e, tanto no momento da determinação dos meios de tratamento como no momento do próprio tratamento, o Responsável pelo Tratamento de Dados adote medidas técnicas e organizacionais adequadas, como pseudonimização, concebidas para adotar princípios de proteção de dados, como a minimização de dados, de maneira eficaz e para integrar as salvaguardas necessárias ao tratamento, a fim de cumprir os requisitos do RGPD e proteger os direitos dos Titulares de Dados.

O princípio de "**Proteção de Dados por defeito**" envolve a adoção de medidas técnicas e organizacionais adequadas para garantir que, por defeito, apenas os dados pessoais necessários para cada finalidade específica do tratamento sejam processados. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao período de armazenamento e à acessibilidade.

Os princípios de proteção de dados por Conceção e por Defeito devem ser integrados em toda a organização do Grupo. Portanto, todas as empresas devem estar atentas para que o desenvolvimento de novos produtos e serviços e a utilização de ferramentas de assistência passem por uma verificação preliminar para avaliar se o tratamento de dados planeado ocorre em conformidade com os requisitos regulatórios gerais e locais: isso requer grande sensibilização para o dever de cada estrutura empresarial de dar o seu contributo para a correta e atempada aplicação dos princípios acima descritos.

Mais detalhadamente, desde a fase de planeamento de um novo produto/serviço, da adoção de novas ferramentas ou de alterações significativas nos meios de Tratamento de Dados, na medida do possível, tendo em conta o estado da técnica, custos de adoção e riscos relacionados com o tratamento específico, é necessário:

- garantir que, de acordo com a configuração padrão de processos/sistemas, apenas os Dados Pessoais necessários para cada finalidade específica de tratamento sejam processados;
- garantir que, de acordo com a configuração padrão de processos/sistemas, os Dados Pessoais tratados sejam disponibilizados apenas às partes que devam tratá-los em relação aos fins para os quais foram recolhidos;
- considerar todo o ciclo de vida dos Dados Pessoais durante o qual são processados, desde a recolha até à eliminação, tendo também em devida conta a sua transferência, armazenamento, adaptação ou alteração, consulta e comunicação.

Para garantir a aplicação dos princípios de Privacidade por conceção e de Privacidade por defeito dentro de cada empresa do Grupo, é necessário que cada empresa adote a sua própria metodologia para determinar que atividades de tratamento envolvem alto risco para os Titulares de Dados e avaliar o impacto nas mesmas. (Avaliação do impacto da proteção de dados). Com base nos resultados desta análise, cada empresa deve identificar as medidas técnicas e organizacionais de segurança adequadas que, uma vez aplicadas, devem mitigar os possíveis impactos sobre o Titular de Dados causados pela perda de confidencialidade, integridade e disponibilidade dos dados pessoais.
Se a empresa atuar como Subcontratante, deve ajudar a disponibilizar todos os dados de interesse para o Responsável pelo Tratamento de Dados para que este possa realizar a avaliação de impacto.

7.6 REGISTO DE ATIVIDADES DE TRATAMENTO

Uma lista completa das atividades de Tratamento de Dados realizadas pelas Empresas do Grupo, seja como Responsáveis pelo Tratamento de Dados ou Subcontratantes, e os fins relacionados, está contida no Registo de Atividades de Tratamento.

O Registo contém pelo menos as seguintes informações:

no que diz respeito ao Tratamento realizado como Responsável pelo Tratamento de Dados

- o nome e os dados de contacto do Responsável pelo tratamento e, se aplicável, do Corresponsável pelo Tratamento de Dados, do representante do responsável pelo tratamento e do responsável pela proteção de dados;
- as finalidades do tratamento;
- uma descrição das categorias de titulares de dados e das categorias de dados pessoais;
- as categorias de destinatários aos quais os dados pessoais foram ou serão divulgados, incluindo destinatários em países terceiros ou organizações internacionais;
- quando aplicável, transferências de dados pessoais para um país terceiro ou organização internacional, incluindo a identificação desse país terceiro ou organização internacional e a documentação das salvaguardas adequadas;
- sempre que possível, os prazos previstos para a eliminação das diferentes categorias de dados;
- sempre que possível, uma descrição geral das medidas de segurança técnicas e organizacionais.

Em relação ao Tratamento realizado como Subcontratante

- o nome e dados de contacto do subcontratante ou subcontratantes e de cada Responsável pelo Tratamento de Dados em nome do qual o subcontratante atue e, se aplicável, do Responsável pelo Tratamento de Dados ou do representante do subcontratante e do Responsável pela Proteção de Dados;
- as categorias de tratamento efetuado por conta de cada responsável pelo tratamento;
- quando aplicável, transferências de dados pessoais para um país terceiro ou organização internacional, incluindo a identificação desse país terceiro ou organização internacional e documentação das salvaguardas adequadas;
- sempre que possível, uma descrição geral das medidas de segurança técnicas e organizacionais.

O EPD Local é responsável pela atualização e armazenamento em formato eletrónico da versão oficial do Registo de Atividades de Tratamento, também para que possa ser disponibilizado à Autoridade em caso de fiscalização.

7.7 GESTÃO DE VIOLAÇÃO DE DADOS

Uma violação de dados pessoais pode, se não tratada de forma adequada e oportuna, resultar em danos físicos, materiais ou não materiais a pessoas singulares, como perda de controlo sobre os seus dados pessoais ou limitação dos seus direitos, discriminação, roubo de identidade ou fraude, perda financeira, reversão não autorizada de pseudonimização, danos à reputação, perda da confidencialidade de dados pessoais protegidos pelo sigilo profissional ou qualquer outra desvantagem económica ou social significativa para a pessoa em causa. Portanto, assim que o responsável pelo tratamento tomar conhecimento de uma violação de dados pessoais, o Responsável pelo Tratamento de Dados deve comunicar a violação de dados pessoais à autoridade supervisora sem atrasos indevidos e, se possível, o mais tardar 72 horas após ter tomado conhecimento (a menos que o Responsável pelo Tratamento de Dados seja capaz de demonstrar, ao abrigo do princípio da responsabilidade, que é improvável que a violação de dados pessoais resulte em risco para os direitos e liberdades dos titulares dos dados). Se a notificação não puder ser realizada no prazo de 72 horas, os motivos do atraso devem ser indicados na notificação. A notificação deve conter pelo menos:

- uma descrição da natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e número aproximado de titulares de dados em causa e as categorias e o número aproximado de registos de dados pessoais em causa;
- comunicação do nome e dados de contacto do EPD Local ou outro ponto de contacto onde possam ser obtidas mais informações;
- uma descrição das prováveis consequências da violação de dados pessoais;
- uma descrição das medidas tomadas ou propostas pelo responsável pelo tratamento para resolver a violação de dados pessoais, incluindo, se apropriado, medidas para mitigar os seus possíveis efeitos adversos.

Quando as empresas do Grupo doValue atuam como Subcontratantes, devem informar imediatamente o Responsável pelo Tratamento de Dados de quaisquer violações de dados dentro do prazo previsto no Acordo de Proteção de Dados (DPA). Devem também fornecer ao Responsável pelo Tratamento de Dados todas as informações necessárias para comunicar o acontecimento à Autoridade Supervisora.

Por exemplo, possíveis violações de dados pessoais podem envolver:

- destruição de dados eletrónicos ou documentos impressos (na aceção de perda irreversível de dados com sua restauração confirmada como impossível), resultante de apagamento lógico (por exemplo, eliminação indevida de dados durante uma intervenção manual ou automatizada) ou danos físicos (por exemplo, avaria de

dispositivos de memória eletrónicos, incêndio/inundação nas instalações onde os contratos e outros documentos do cliente são armazenados);

- perda de dados como resultado de perda/roubo de dispositivos de assistência de TI (por exemplo, laptop, HD, cartão de memória) ou de documentação contratual ou outros documentos impressos (originais ou cópias);
- acesso não autorizado ou intrusão em sistemas de informação (por exemplo, sistemas de gestão de contacto geridos por centrais de atendimento), explorando vulnerabilidades em sistemas internos e redes de comunicação ou comprometendo ou obtendo indevidamente credenciais de autenticação (por exemplo, ID de utilizador e senha) para ter acesso aos sistemas;
- alteração não autorizada de dados, resultante, por exemplo, de intervenções indevidas em sistemas de informação ou intervenção humana;
- divulgação de dados e documentos a terceiros não autorizados, possivelmente não identificados. Isso pode resultar, por exemplo, do fornecimento de informações – possivelmente informações orais – a pessoas que não sejam parte legítima (sem autorização por escrito dessa parte), do envio de faturas ou outros documentos contratuais ou executivos a terceiros que não o destinatário pretendido, ou de gestão imprópria de dispositivos de assistência de TI.

Se a avaliação ou auditoria interna identificar risco elevado para os direitos e liberdades do Titular de Dados, expondo-o a riscos específicos à luz dos dados envolvidos na violação de dados, o Titular de Dados deve ser informado diretamente, sem atrasos indevidos. A comunicação ao Titular de Dados deve descrever em linguagem clara e simples a natureza da violação de dados pessoais e conter pelo menos o nome e os dados de contacto do EPD, as prováveis consequências da violação e as medidas tomadas ou propostas para resolver a violação de dados pessoais.

A comunicação com o Titular de Dados não é necessária se qualquer das seguintes condições for cumprida:

- o responsável pelo tratamento adotou medidas de proteção técnica e organizacional adequadas e essas medidas foram aplicadas aos dados pessoais afetados pela violação de dados pessoais, em particular as que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a consultá-los, como encriptação
- o responsável pelo tratamento tomou medidas subsequentes que garantem que o alto risco para os direitos e liberdades dos Titulares de Dados deixa de ser provável;
- envolveria esforço desproporcional. Nesse caso, deve haver comunicação pública ou medida semelhante em que as pessoas em causa sejam informadas de forma igualmente eficaz.

A Autoridade Supervisora pode ainda solicitar comunicação aos Titulares de Dados.

Cada empresa do Grupo doValue deve adotar procedimentos e ferramentas internas para detetar, combater e gerir quaisquer incidentes de segurança que envolvam violação de dados. Além disso, tais procedimentos internos devem especificar a metodologia a seguir na avaliação da violação de dados, os meios de escalonamento aos órgãos de direção empresarial e os meios de notificação do acontecimento à autoridade supervisora local e, possivelmente, aos Titulares de Dados, também como meio de notificação ao Responsável pelo Tratamento de Dados se a empresa atuar como subcontratante.

7.8 MEDIDAS DE SEGURANÇA

No decurso das atividades de Tratamento realizadas, o Responsável pelo Tratamento de Dados e o Subcontratante deverão, nos termos do artigo 32.º do RGPD, adotar todas as medidas necessárias para proteger os Dados Pessoais. Devem garantir:

- a adoção de medidas para proteger as redes, sistemas e software com que os Dados Pessoais são processados. Por exemplo:
    - perfis de utilizador e soluções de segregação e proteção de acesso, de modo a garantir que os dados pessoais possam ser consultados e processados apenas por partes que precisem de processá-los
    - pseudonimização, ofuscação e encriptação de dados;
    - soluções de continuidade de serviço capazes de garantir a disponibilidade e integridade dos dados (cópia de segurança, recuperação de desastre, etc.);
- Ensaios e avaliação periódica da eficácia dos procedimentos e medidas adotados;
- Adoção de soluções capazes de detetar tentativas não autorizadas de acesso a Dados Pessoais para garantir o cumprimento dos requisitos do RGPD sobre Violações de Dados;
- Adoção de soluções de rastreamento de atividades de Dados Pessoais consistentes com os requisitos legais aplicáveis.

7.9 TRANSFERÊNCIAS DE DADOS PARA FORA DA UE

Quando o RGPD entrou em vigor, introduziu um nível uniforme de proteção de dados pessoais em toda a União Europeia e permitiu a livre circulação de dados nos países da UE.

No entanto, quando os Dados Pessoais são transferidos da União Europeia para Responsáveis pelo Tratamento de Dados e Subcontratantes ou para outros destinatários em países fora da União Europeia, o Regulador exige o mesmo nível de proteção que aquele garantido na União Europeia.

Portanto, os Dados Pessoais do Titular de Dados podem ser transferidos para países fora da UE nas seguintes circunstâncias, por exemplo:

- transferências para países que, segundo a Comissão Europeia, garantam um nível adequado de proteção de Dados Pessoais;
- transferências entre empresas pertencentes ao mesmo grupo empresarial na presença de Regras Empresariais Vinculativas (BCR), quando aplicável, ou entre empresas que tenham subscrito as "cláusulas padrão" de proteção de Dados Pessoais aprovadas pela Comissão;
- transferências necessárias à execução de contrato celebrado entre o Titular de Dados e o responsável pelo tratamento ou à execução de medidas pré-contratuais adotadas a pedido do Titular de Dados;
- transferências necessárias à celebração ou execução de contrato assinado entre o responsável pelo tratamento e outra pessoa singular ou coletiva a favor do Titular de Dados;
- transferências necessárias para fazer valer, exercer ou defender um direito em processo judicial.

Se nenhum dos casos específicos acima se aplicar, a transferência de dados deve ser explicitamente aprovada pelo Titular de Dados.

Portanto, durante a fase inicial de uma atividade de Tratamento ou durante a referida atividade, é particularmente importante que as empresas do Grupo verifiquem onde ocorre

o Tratamento de Dados, especialmente quando envolve terceiros, que deverão comunicar em que país estão a realizar o tratamento.

7.10 TRATAMENTO ESPECÍFICO

Cada Empresa do Grupo deve vigiar continuamente se as Autoridades locais de proteção de dados emitem leis e regulamentos de proteção de dados mais restritivos do que o Regulamento Europeu. Nesses casos, o Responsável pelo Tratamento de Dados, com o apoio do EPD Local, deve avaliar se os métodos de tratamento de dados adotados estão em conformidade com os novos regulamentos locais e, se não estiverem, deve tomar as medidas adequadas para atingir a conformidade.

8 QUADRO DE CONTROLO

Para garantir que as organizações tenham uma estrutura clara que separe as funções que definem as diretrizes dos responsáveis pela sua execução, os reguladores exigem cada vez mais um modelo de governança de 'três linhas de defesa' que garanta controlo interno forte e eficaz e assegure vários níveis de proteção.

A figura abaixo representa a estrutura de controlo de proteção de dados do Grupo:

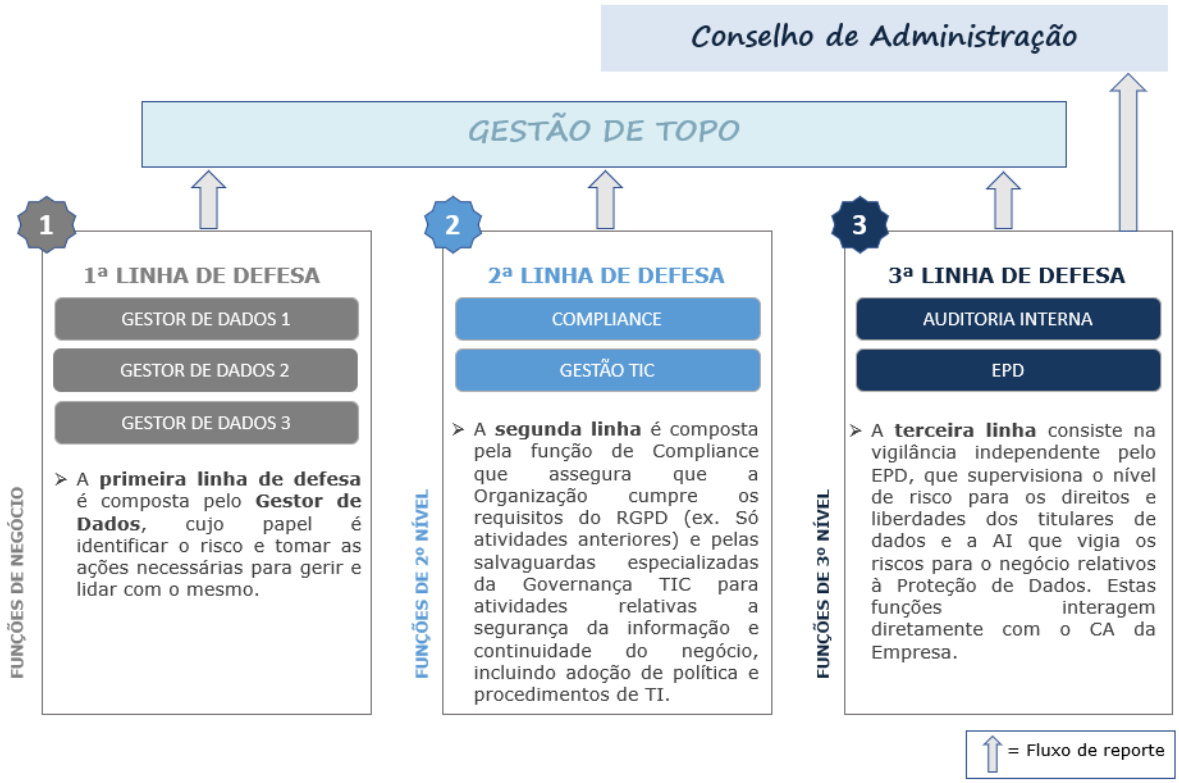


Figura 10: Estrutura de controlo de proteção de dados

O EPD Global estabelece e mantém uma estrutura de controlo comum de terceiro nível para todas as Empresas do Grupo, ao serviço do EPD Global e do EPD Local, que a usam no âmbito das suas atividades de supervisão. As atividades de supervisão realizadas pelo EPD Global e pelos EPD locais visam determinar o nível de risco relativo aos direitos e liberdades dos Titulares de Dados.
A estrutura de controlo inclui atividades de controlo específicas que devem ser testadas pelo EPD Local.
As atividades de controlo definidas na estrutura são divididas nas seguintes categorias:

1. Estratégia e responsabilidade por RGPD;
2. Registo das atividades de tratamento;
3. Determinação da base jurídica para o tratamento;
4. Consentimento, propriedade e transparência;
5. Direitos dos Titulares de Dados;
6. Delimitação de retenção de dados;
7. Formação e sensibilização;
8. Violações de dados e gestão de incidentes;
9. Privacidade por Conceção e Defeito;
10. Avaliação de impacto de proteção de dados (AIPD);
11. Gestão de terceiros;
12. Medidas de segurança;
13. Transferência de dados pessoais.

O EPD Local deve adaptar os controlos da estrutura a nível local, com base nas características específicas da organização. Devem ser adicionadas atividades de controlo específicas, conforme necessário, a fim de testar a conformidade do sistema de Proteção de Dados da empresa com os regulamentos aplicáveis emitidos pela Autoridade Local.
As verificações podem ser planeadas em todo o tratamento de dados pessoais realizado pela empresa ao longo de vários anos, garantindo, no entanto, que a cada ano os seguintes sejam incluídos no âmbito da auditoria:

- operações de tratamento que apresentem alto risco (inerente) para os direitos e liberdades dos Titulares de Dados.
- um subconjunto de operações de tratamento que apresente risco não alto (inerente) para os direitos e liberdades dos Titulares de Dados.

Após a conclusão dessas atividades, o EPD Local deve produzir um relatório dirigido ao Conselho de Administração local e informar o EPD Global dos resultados das atividades de supervisão e de quaisquer acontecimentos específicos e significativos que tenham ocorrido durante o período em questão.

9 PENALIDADES

A violação do Regulamento Geral de Proteção de Dados sujeita o Responsável pelo Tratamento de Dados e/ou o Subcontratante a vários tipos de responsabilidades e penalidades decorrentes (administrativas e/ou penais), dependendo das regras que tenham sido violadas. Ocasionalmente, poderá ser necessário indemnizar os Titulares de Dados,

caso tenham sofrido danos materiais ou imateriais causados por violação do regulamento e corram o risco de sofrer danos à reputação.
O RGPD aumentou significativamente o montante das sanções administrativas, elevando-as a um máximo de 20 milhões de euros ou 4% da receita total mundial no ano anterior. Em cada caso, a Autoridade Supervisora pode decidir a aplicação de multas administrativas, além de outras sanções não financeiras, ou sua substituição.
Em qualquer caso, nos termos do art. 83.º do RGPD, as multas administrativas devem ser efetivas, proporcionais e dissuasivas. Portanto, ao determinar o montante da multa, o Órgão de Fiscalização leva em conta uma série de fatores, incluindo a natureza, gravidade e duração da infração, o caráter intencional ou negligente da infração, quaisquer infrações anteriores relevantes, qualquer ação tomada pelo responsável pelo tratamento ou processador, para mitigar os danos sofridos pelos Titulares de Dados, o grau de cooperação com a autoridade de supervisão para sanar a infração e mitigar os seus possíveis efeitos adversos, as categorias de dados pessoais afetados pela infração; a maneira pela qual a infração se tornou conhecida pela autoridade supervisora, qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, por exemplo, benefícios financeiros obtidos ou perdas evitadas, diretamente ou indiretamente, pela infração.