POLÍTICA DE PROTEÇÃO DE DADOS

Políticas de Conformidade - Política 7.4 - Proteção de Dados

Aprovado por	Conselho de Administração
Data de criação:	24 de agosto de 2014
Data da última atualização:	02 de junho de 2018
Proprietário da Política:	Responsável do Grupo pela Proteção de Dados
Contato(s):	Responsável do Serviço Internacional de Proteção de Dados

1. Objetivo

1.1 Cada Empresa do Grupo, ao exercer sua atividade comercial, coleta, armazena e trata as informações relativas às pessoas físicas. Estas podem incluir colaboradores, contratados, fornecedores, clientes, vogais do Conselho de Administração, diretores, acionistas e convidados. As Empresas do Grupo respeitam a confidencialidade dos referidos titulares de dados pessoais e seu direito de saber como as Empresas do Grupo tratam suas informações. As empresas do Grupo tratam com tolerância zero o incumprimento da legislação respetiva, incluindo, mas não se limitando, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados" (Regulamento Geral sobre a Proteção de Dados).

1.2 Esta Política tem por objetivos de:

1.2.1 garantir que cada Empresa do Grupo exerce sua atividade comercial no respeito de todas as leis aplicáveis e requisitos normativos referentes à coleta, armazenagem, tratamento e transmissão de dados pessoais e, bem assim, que os dados pessoais são protegidos e tratados em conformidade com as normas da legislação aplicável[1];

1.2.2 definir os tipos de Dados Pessoais que as Empresas do Grupo coletam e os objetivos desta coleta;

1.2.3 expor as funções de cada colaborador relativas à coleta e tratamento de dados nos termos da legislação aplicável em matéria de proteção de dados; assim como

---

[1] *Na **União Europeia**, por exemplo, o tratamento de dados pessoais é regulado pelo Regulamento Geral sobre a Proteção de Dados, Regulamento (UE) 2016/679) e outros diplomas normativos. No **Reino Unido**, é, em primeiro lugar, o Regulamento Geral sobre a Proteção de Dados e a "Lei de Proteção de Dados" de 2018 ("Lei"), além de outros;*

*Na **Suíça**, é a Lei Federal de 19 de junho de 1992 "Sobre a Proteção de Dados Pessoais";*
*No **Cazaquistão**, é a Lei de 21 de maio de 2013 nº 94-V "Sobre os Dados Pessoais e sua Proteção";*
*Na **Rússia**, a Lei Federal "Dos Dados Pessoais" de 27 de julho de 2006 nº 152-FZ e outros diplomas normativos (por exemplo, o Código das Infrações Administrativas);*
*Na **África do Sul**, a Lei nº 4 de 2013 relativa à Proteção das Informações Pessoais;*
*No **Brasil**, não existe lei específica em matéria de proteção de dados. Não obstante, há vários diplomas, como o Marco Civil da Internet e o Código de Defesa do Consumidor que regulam os vários aspetos da confidencialidade e da proteção de dados. Está em debate no Congresso brasileiro um projeto de lei sobre a proteção de dados.*
*Na **China**, a Decisão destinada a reforçar a proteção das informações de rede de 28 de dezembro de 2012; o Regulamento do Serviço de Emprego e dos Serviços de Recursos Humanos; Medidas de Punição da Violação dos Direitos e Interesses dos Consumidores;*
*Nos **Emirados Árabes Unidos** não existe legislação geral sobre a proteção de dados pessoais equiparável às leis em vigor na Europa, embora as entidades pertencentes ao Centro Financeiro Internacional de Dubai (DIFC) sejam reguladas pelas leis gerais sobre a proteção de dados.*

1.2.4 garantir que cada Empresa do Grupo utiliza um ambiente normal de proteção de dados pessoais para assegurar a possibilidade de transmissão de dados pessoais entre Empresas do Grupo e garantir a proteção necessária dos dados pessoais em conformidade com a legislação aplicável relativa à transmissão internacional de dados nos casos de sua transferência transfronteiras.

2. Âmbito

2.1 Esta política é aplicável:

2.1.1 a todas as Empresas do Grupo, conforme definido adiante, e a seus agentes;

2.1.2 a todos os Colaboradores; e

2.1.3 a todos os Dados Pessoais coletados, armazenados e tratados pelas Empresas do Grupo no âmbito de sua atividade comercial qualquer que seja o suporte em que estão registrados.

3. Definições

As definições abaixo são de uso interno que, mantendo o significado previsto pela legislação aplicável, podem ter uma outra designação na legislação local. Ao elaborarem os procedimentos locais, as Regiões devem seguir os termos e os conceitos jurídicos utilizados na legislação correspondente de seus países, em conformidade com os princípios da presente Política.

3.1 **Conselho** – o Conselho de Administração do *Eurasian Resources Group S.A.R.L*..

3.2 **Dados Pessoais dos Clientes** – dados pessoais coletados no processo regular de gerenciamento de relações com os clientes, tais como informações de contato dos mesmos, seus nomes e endereços profissionais.

3.3 **Controlador de Dados Pessoais** – pessoa física ou jurídica, autoridade pública, agência ou qualquer outro organismo que individual ou conjuntamente com outros determina os objetivos e métodos de processamento de Dados Pessoais.

3.4 **Responsável pela proteção de dados** – pessoa física encarregada de prestar consultas e fiscalizar o cumprimento pelo Grupo da legislação local relativa à proteção de dados, assim como exercer as funções de pessoa de contato para solicitações internas e externas dos Titulares de dados relativamente à coleta e tratamento de seus Dados Pessoais.

3.5 **Processador de Dados** – pessoa física ou jurídica (incluindo a Empresa do Grupo), autoridade pública, agência ou qualquer outro organismo processando Dados Pessoais em nome de uma Empresa do Grupo.

3.6 **Titular de Dados** – qualquer pessoa física identifiicada ou identificável a que dizem respeito os Dados Pessoais.

3.7 **Colaboradores** – pessoal de qualquer Empresa do Grupo, trabalhando em tempo integral ou parcial ou a título temporário, estagiários e contratados trabalhando em uma das instalações do Grupo ou acessando os sistemas de TI de uma Empresa do Grupo.

3.8 **União Europeia** – 28 países membros que compõem a União Europeia e a que se aplica a legislação europeia.

3.9 **Zona Econômica Europeia (ZEE)** – os países europeus que transferiram para suas legislações nacionais vários diplomas normativos da União Europeia e aceitaram observar integralmente a legislação europeia relativa à proteção de dados pessoais.

3.10 **Dados Pessoais dos Colaboradores** – Dados Pessoais coletados no processo regular de administração de recursos humanos, tais como nome, endereço, nacionalidade, sexo, estado civil, número de Previdência Social e dados bancários.

3.11 **Regulamento Geral sobre a Proteção de Dados** - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados", assim como o Regulamento 679/2018 que é um diploma normativo da UE em matéria de confidencialidade e proteção de dados pessoais destinado a harmonizar as regras neste domínio. Este regulamento se aplica a todos os países da União Europeia e à ZEE e regula a transmissão e o tratamento de dados pessoais dos titulares dos mesmos na UE e na ZEE independentemente de serem estas ações executadas dentro ou fora da União Europeia e da ZEE.

3.12 **Empresas do Grupo** – o *Eurasian Resources Group SARL* e qualquer outra empresa em que aquela detenha, direta ou indiretamente, mais de cinquenta por cento (50%) dos direitos de voto, ou na qual os poderes de controle da empresa pertençam ao *Eurasian Resources Group SARL* ou a uma pessoa agindo em seu nome.

3.13 **Acionistas das Empresas do Grupo** – pessos físicas e/ou empresas públicas ou privadas detentoras de ações das Empresas do Grupo que lhes conferem direitos de voto.

3.14 **Representante exterior** – pessoa exterior à Empresa do Grupo, nomeada pelo Departamento de Conformidade para representar os interesses dos escritórios da Empresa do Grupo na ausência do Responsável pela Proteção de Dados. O representante exterior intervém na qualidade de pessoa de contato para questões relativas aos Dados Pessoais emanando de cidadãos e residentes habituais da UE e ZEE que se encontrem permanente ou temporariamente fora dos países da UE ou da ZEE.

3.15 **Dados Pessoais** – quaisquer informações, seja qual for o suporte utilizado, incluindo gravações sonoras e imagens, relativas a uma pessoa física identificada ou identificável. Uma pessoa física é considerada identificável quando pode ser identificada direta ou indiretamente, em particular por referência aos dados de identificação tais como nome, número de identificação, dados de localização geográfica, nome de usuário na Internet ou com base em suas caraterísticas físicas, fisiológicas, genêticas, intelectuais, culturais, sociais ou econômicas. Mesmo quando à partida não seja óbvia a possibilidade de identificar uma pessoa, esta é identificável caso as Empresas do Grupo disponham ou possam dispor de meios lícitos que permitam a identificar.

3.16 **Violação da segurança de Dados Pessoais** – violação da segurança que tenha levado a uma destruição acidental ou ilícita, perda, alteração, divulgação não autorizada de Dados Pessoais transmitidos, armazenados ou tratados por outros processos ou à obtenção de acesso não autorizado a tais dados.

3.17 **Processamento** – qualquer operação ou conjunto de operações executada sobre Dados Pessoais, mesmo com recurso a processos automáticos ou eletrônicos ou não, tais como coleta, gravação, organização, armazenamento, adaptação ou alteração, extração, consulta, uso, divulgação por transmissão, disseminação ou disponibilização por qualquer outro recurso, agregação ou combinação, bloqueio, apagamento ou destruição.

3.18 **Regiões** – grupo de uma ou mais Empresas do Grupo situadas na mesma área geográfica. As regiões do grupo são o Cazaquistão, África, Brasil e Europa.

3.19 **Dados Pessoais de Categoria Específica** – Dados Pessoais (conforme definido no Regulamento Geral da Comissão Europeia sobre a Proteção de Dados e na legislação local dos países que não integram a UE) que revelem informações relativas à saúde física ou mental do Titular dos Dados, a sua crenças religiosas ou similares, opiniões políticas, origem racial ou étnica, filiação sindical, infrações penais, orientação e vida sexuais, assim como informações de natureza genêtica.

3.20 **Dados Pessoais dos Fornecedores** – Dados Pessoais coletados no processo regular de gerenciamento de relações com os fornecedores, tais como dados de contato do fornecedor, seu nome e endereço profissional.

4. Disposições de Política

4.1 Cada Empresa do Grupo processa Dados Pessoais em conformidade com as leis e diplomas normativos aplicáveis sobre a proteção de dados.

4.2 Cada Empresa do Grupo e as estruturas que a integram, independentemente de sua jurisdição, devem seguir as seguintes normas mínimas:

4.2.1 Tratamento idôneo e lícito de Dados Pessoais: as Empresas do Grupo tratam os Dados Pessoais de maneira honesta e legal, o que requer, entre outros, o seguinte:

(a) Utilização legal: os Dados Pessoais não podem ser utilizados de forma ilegal e/ou suscetível de ter um impacte negativo injustificado ou não proporcional sobre o Titular dos Dados;

(b) Transparência: as Empresas do Grupo devem assegurar transparência no processo de tratamento de dados para o Titular dos mesmos (em particular, relativamente à efetividade de tal processo e a suas condições);

(c) Limitação do objetivo: os Dados Pessoais devem ser coletados unicamente para fins determinados e legais e utilizados unicamente da forma que o Titular de dados razoavelmente pode esperar; o modo de tratamento dos dados também deve ser compatível com os fins de sua coleta;

(d) Proporcionalidade/ minimização do volume de dados: os Dados Pessoais devem ser proporcionais e limitados ao volume necessário para os fins de seu processamento;

(e) Exatidão: os Dados Pessoais devem ser exatos e atualizados em tempo hábil;

(f) Armazenagem: os Dados pessoais devem ser armazenados em conformidade com o requerido pelas respetivas políticas do Grupo e pela legislação aplicável, mas não devem ser conservados, na forma permitindo identificar o Titular dos Dados, mais tempo do que é necessário para as finalidades de seu processamento. De um modo geral, os Dados Pessoais devem ser destruídos ou despersonalizados após a finalidade de seu tratamento deixar de existir;

(g) Respeito dos direitos dos Titulares de Dados: cada Empresa do Grupo deve observar e respeitar os direitos legais dos Titulares de Dados no processo de tratamento de seus Dados Pessoais.

4.2.2 Informação e/ou consentimento prévio: sempre que tal seja exigido por lei local, as Empresas do Grupo devem prestar aos Titulares de Dados informações básicas necessárias sobre os Dados Pessoais que coletam e a forma como os mesmos são processados[2] e, sempre que exigido pela legislação local, obter um consentimento explícito do Titular dos Dados para isso. O Titular dos Dados não pode expressar seu consentimento sob forma de omissão ou de utilização de uma casa de um documento contendo qualquer nota. Os avisos de confidencialidade devem ser acessíveis aos Titulares dos Dados (por exemplo, devem ser publicados nas páginas web de todas as Empresas do Grupou ou através de outros meios de comunicação).

---

[2] Por exemplo, conforme as regras locais aplicáveis sobre a proteção de dados, cada Empresa do Grupo pode ter a obrigação de comunicar aos Titulares de Dados: (i) seus dados de identificação ou sua designação jurídica; (ii) (em certos casos) que dados são coletados ou processados; (iii) quais os fins da coleta de dados; (iv) se esses dados serão transmitidos a mais alguém; assim como (v) seus direitos legais e o modo de exercê-los.

4.2.3 Segurança de Dados: Cada Empresa do Grupo deve tomar as devidas medidas técnicas, físicas e organizacionais, nomeadamente as medidas de proteção contra o Tratamento Não Autorizado ou Ilícito de Dados Pessoais, assim como contra sua perda, destruição ou danificação acidentais.

(a) A segurança da informação é regulada pelas politicas e procedimentos de Segurança da Informação;
(b) As Empresas do Grupo são igualmente responsáveis por todas as ações de Tratamento executadas pelos Processadores de Dados em nome daquelas. As Empresas realizam essa responsabilidade através de uma escrupulosa verificação integrada dos potenciais Processadores de Dados e da inclusão de termos e disposições especiais sobre a proteção de dados nos contratos celebrados com aqueles, de acordo com a legislação em vigor em matéria de proteção de dados, especialmente, nos termos do artigo 28 do Regulamento Geral sobre a Proteção de Dados.
(c) Os colaboradores que queiram encarregar um Processador de Dados de processar dados em nome de uma Empresa do Grupo, devem proceder a uma escrupulosa verificação integrada dos padrões de tratamento de dados do Processador de Dados e contatar o principal consultor jurídico local e o Contact-Center para a proteção de dados da região para se certificar da conveniência das condições contratuais aplicados relativamente à proteção de dados e garantir que cada Processador de Dados cumpre com os requsitos legais relativos à proteção de dados através de uma análise de riscos, auditorias e inspeções.

4.3 Cada Região deve designar de entre seus dirigentes uma Pessoa de Contato responsável pela proteção de dados, que:

4.3.1 será responsável pela implementação local e aplicação desta política e das leis e diplomas normativos de proteção de dados aplicáveis;

4.3.2 será responsável pela implementação de procedimentos destinados a assegurar a observância desta política e das leis e diplomas normativos de proteção de dados aplicáveis;

4.3.3 será responsável pela interação com as autoridades públicas em matéria de proteção de dados pessoais;

4.3.4 definir, juntamente com os responsáveis das estruturas envolvidas no Processamento de Dados, os objetivos e os métodos de processamento de Dados Pessoais por cada Empresa do Grupo, assim como averiguar se os mesmos objetivos e métodos estão de harmonia com a legislação local;

4.3.5 organizar a apreciação das questões e dificuldades dos Colaboradores e Empresas do Grupo relacionadas com a implementação e o cumprimento da presente Política e das leis e diplomas normativos de proteção de dados aplicáveis;

4.3.6 receber pedidos ou queixas dos Titulares de Dados relativos à proteção e segurança de dados, assim como intervir como primeira pessoa de contato sempre que os Titulares de Dados levantem questões referentes ao exercício de seus direitos legais;

4.4 Caso não esteja prevista qualquer forma de delegação a nível regional, por Pessoa de Contato em matéria de proteção de dados será tido, exercendo as respetivas funções, o Responsável Regional Sênior pela Proteção de Dados ou outra pessoa por ele designada.

4.5 Os responsáveis das estruturas orgânicas, com o apoio das Pessoas de Contato para a Proteção de Dados, devem implementar as devidas medidas de proteção de dados que sejam mais ou, pelo menos, tão rigorosas como as definidas na presente Política, e que garantam a observância pelos Colaboradores da presente Política e legislação aplicável relativa à proteção de dados.

4.6 Os Colaboradores devem comunicar imediatamente quaisquer fatos de fuga de dados, confirmados ou presumíveis, ao Responsável pela proteção de dados. Caso contrário, serão tomadas medidas disciplinares até o despedimento ou a cessação das relações contratuais.

4.7 O responsável pela proteção de dados deve imediatamente informar o consultor jurídico sênior ou o diretor-geral para os assuntos jurídicos do Grupo, o Diretor de Conformidade do Grupo, o diretor do

Departamento de Riscos do Grupo e o diretor do Departamento de Segurança da Informação do Grupo sobre quaisquer riscos à proteção de dados, problemas potenciais de conformidade e violações da segurança de dados pessoais.

4.8 De acordo com as regras da política, ao responsável pela proteção de dados, independentemente do parecer do consultor jurídico sênior local ou do diretor-geral para os assuntos jurídicos do Grupo, do Diretor de Conformidade do Grupo, do diretor do Departamento dos Riscos do Grupo e do diretor do Departamento de Segurança da Informação do Grupo e, bem assim, dos vogais do Conselho ou outros colaboradores da Empresa do Grupo, compete tomar uma decisão definitiva no sentido de comunicar à autoridade local de proteção de dados a Violação da segurança de dados pessoais no prazo de 72 horas após a deteção dessa irregularidade.

4.9 È obrigação do responsável pela proteção de dados registrar todos os casos de Violação da segurança de Dados Pessoais, incluindo as ações empreendidas para limitar os riscos que as empresas do Grupo correm, os contatos com as autoridades estatais locais em matéria de proteção de dados pessoais, assim como a razão por que a Violação da segurança de Dados Pessoais não foi comunicada às autoridades estatais nacionais responsáveis pela proteção de dados pessoais.

4.10 Cada Empresa do Grupo atuando como Controlador de Dados Pessoais ou Processadora de Dados deve avisar o Responsável pela Proteção de Dados sobre todas as operações de Processamento de Dados Pessoais, conforme a legislação em vigor. O Responsável pela Proteção de Dados pode eventualmente encarregar os colaboradores de proceder à avaliação do impacte sobre a proteção de dados, caso estabeleçam que uma operação de Processamento, dados a natureza, a extensão, o contexto e os objetivos do processamento, irá com toda a probabilidade expor a um alto risco os direitos e as liberdades dos Titulares de Dados.

5. Regras

Objetivos do Processamento de Dados Pessoais:

5.1 As Empresas do Grupo podem processar Dados Pessoais unicamente para os seguintes fins:

Dados Pessoais dos Colaboradores

5.1.1 O pessoal de Recursos Humanos pode processar Dados Pessoais dos colaboradores para cumprimento das cláusulas dos contratos de trabalho e tomada das medidas necessárias antes da celebração de contratos, com vista ao cumprimento dos compromissos jurídicos ou à salvaguarda dos interesses legítimos dos Empresas do Grupo (nos casos permitidos pela legislação laboral local) relativamente:

(a) à gestão de pessoal e equipes (local e internacional) em diferentes jurisdições; à rotatividade de pessoal no interior do Grupo;
(b) à administração dos Colaboradores, inclusive para cumprimento das cláusulas do contrato de trabalho e à observância das normas das legislações social, fiscal e laboral; bem como
(c) à gestão geral de pessoal, inclusive seleção, contratação, remuneração do trabalho, concessão de férias, formação, avaliação, análise de efetivos, planejamento de carreira e sucessão de equipe dirigente;
(d) às informações de identificação, incluindo nome, endereço residencial, data de nascimento, sexo, fotografias associadas ao trabalho e número de telefone residencial;
(e) aos números de identificação atribuídos pelo Estado, incluindo o número de identificação pessoal, para efeitos de remuneração do trabalho e gestão do acesso aos sistemas de informação;
(f) ao status imigratório, direitos trabalhistas, status residencial;
(g) às informações de contato para emergências e às informações relativas aos familiares (volume restrito);
(h) às informações profissionais, incluindo antiguidade, entidade empregadora, identificador de função, carteira de trabalho, férias e dados relativos ao contrato;
(i) às informações relativas à formação acadêmica e formação profissional, à contratação e à eficiência de trabalho, incluindo os objetivos, avaliações, comentários, feedbacks recebidos,

experiência profissional, equipamento de trabalho, planejamento de carreira e continuidade, conhecimentos, competências e outras qualificações de trabalho;

(j) às informações relativas à utilização de ativos de TI do ERG;

(k) às informações necessárias ao gerenciamento de conformidade e de riscos, incluindo as relativas às sanções, aos resultados da verificação da biografia e à segurança, assim como

(l) às informações referentes à remuneração do trabalho, benefícios ou incentivos, incluindo as relativas aos salários e seguros, informações fiscais, dados bancários, suplementos remuneratórios e benefícios laborais.

5.1.2 O superior imediato e o empregador de um Colaborador igualmente podem, quando necessário, processar seus Dados Pessoais para cumprimento dos compromissos previstos nos contratos de trabalho, dos compromissos jurídicos e proteção dos interesses legítimos da empresa relativamente à gestão de pessoal e equipes (local e internacional) em diferentes jurisdições; assim como à administração, seleção, contratação e avaliação de desempenho de pessoal e planejamento da sucessão de pessoal dirigente.

5.1.3 O pessoal de contabilidade pode processar Dados Pessoais dos Colaboradores para cumprimento dos compromissos jurídicos das Empresas do Grupo relativos à gestão de contas, liquidação dos salários, prêmios, impostos e outras deduções, contribuições e benefícios.

5.1.4 O Comitê de Remunerações pode processar Dados Pessoais dos Colaboradores para cumprimento dos compromissos estipulados nos contratos de trabalho ou compromissos jurídicos das Empresas do Grupo com vista à determinação do montante da remuneração do colaborador.

Dados Pessoais de Clientes

5.1.5 Os Colaboradores podem processar Dados Pessoais de Clientes unicamente no apoio à gestão de relacionamento com os clientes para cumprimento dos compromissos contratuais das empresas do Grupo, para assegurar a igualdade de tratamento de clientes e para gestão dos contratos das Empresas do Grupo e gestão dos contratos com clientes (sistemas de gestão das informações sobre clientes, CRM), para cumprimento dos compromissos jurídicos ou prossecução dos interesses legítimos das Empresas do Grupo.

Dados Pessoais dos Fornecedores

5.1.6 Os Colaboradores podem processar Dados Pessoais dos Fornecedores unicamente no apoio à gestão de relacionamento com os fornecedores para cumprimento dos compromissos contratuais das empresas do Grupo, para cumprimento dos compromissos jurídicos ou prossecução dos interesses legítimos das Empresas do Grupo no respeitante à satisfação de suas necessidades em recursos, assegurar igualdade de tratamento dos fornecedores e para gestão dos contratos das Empresas do Grupo com fornecedores.

Dados Pessoais dos Acionistas

5.1.7 Os Secretários Corporativos de cada uma das empresas do Grupo e os funcionários designados do Serviço Jurídico (escolhidos pelo Diretor-Geral para as Questões Jurídicas do Grupo) podem processar, armazenar e utilizar Dados Pessoais dos Acionistas, seus diretores, vogais do Conselho de Administração, beneficiários do Grupo, funcionários executivos e dirigentes da Empresas do Grupo unicamene quando a respetiva Empresa do Grupo o necessite para cumprimento da legislação em vigor e prossecução dos interesses do Grupo, assim como por outras razões empresariais legítimas.

5.1.8 Os Dados Pessoais dos Acionistas das Empresas do Grupo, do Conselho de Administração e dos dirigentes máximos são conservados pelo Secretário Corporativo do Grupo em um lugar seguro acessível unicamente ao Secretariado Corporativo do Grupo e ao representante jurídico nomeado pelo Diretor-Geral para as Questões Jurídicas, com o apoio necessário do Serviço de TI. O Secretário Corporativo confirma aos colaboradores dos serviços jurídicos (nomeados pelo Diretor-Geral para as Questões Jurídicas) quaisquer alterações ocorridas nestes dados pessoais semestralmente e com mais frequência, caso do Secretário Corporativo tome conhecimento de tais alterações.

5.1.9 Os Dados Pessoais dos Acionistas ou do Conselho de Administração de cada uma das empresas do Grupo no interior das regiões devem ser conservados pelo respetivo Secretário Corporativo ou pelo consultor jurídico principal local (ou por colaboradores por ele mandatado), caso não tenha havido designação de Secretário Corporativo. Estes dados devem ser guardados em um lugar seguro acessível unicamente ao Secretariado corporativo ou ao Serviço Jurídico (conforme as circunstâncias) com o apoio necessário do Serviço de TI. O Secretário Corporativo regional ou o consultor jurídico principal local confirmam quaisquer alterações ocorridas nestes dados pessoais semestralmente ou com mais frequência, caso o Secretário Corporativo tome conhecimento de tais alterações. Estas informações devem ser facultadas ao Secretário Corporativo do Grupo semestralmente após confirmação das alterações ocorridas nos Dados Pessoais.

5.1.10 Quaisquer pedidos de informações relativos aos Proprietários Beneficiários Finais (Ultimate Beneficial Owners – UBO) ou outros feitos no âmbito dos procedimentos "Conheça seu Cliente" (Know your Customer" – KYS) com respeito aos Acionistas das Empresas e ao Conselho de Administração de cada uma das empresas do Grupo, aos beneficiários do Grupo e diretores, aos funcionários executivos e dirigentes máximos das empresas do Grupo, que dão entrada no Grupo, devem ser encaminhados ao Secretário Corporativo do Grupo.

5.1.11 Sempre que o entenda no interesse do Grupo, o Secretário Corporativo atenderá oportunamente os pedidos, utilizando as informações guardadas nos termos do nr. 5.1.6., facultadas semestralmente ou com mais frequência, se tiver conhecimento de quaisquer alterações ou se se dirigir aos respetivos Titulares de Dados.

5.1.12 O Secretário Corporativo deve informar semestralmente os acionistas e o Conselho de Administração da utilização desses dados.

5.1.13 Quaisquer colaboradores do Grupo que o Secretário Corporativo entenda útil apoiar no processamento, armazenagem e gestão de Dados Pessoais dos acionistas e membros do conselho de administração de cada uma das empresas do Grupo, beneficiários do Grupo e diretores, executivos e dirigentes máximos das empresas do Grupo, devem confirmar que têm conhecimento da atual Política e irão a cumprir.As listas de pessoas autorizadas a tratar esses Dados Pessoais, são guardadas pelo Secretário Corporativo. As listas de pessoas elaboradas pelos Secretários Corporativos regionais ou pelos consultores jurídicos principais locais (conforme as circunstâncias) para efeitos de processamento, armazenagem e gestão de Dados Pessoais relacionados com as empresas do Grupo administradas pelas Regiões, são geridas pelos secretários corporativos regionais ou pelos consultores jurídicos principais locais (conforme as circunstâncias). Os colaboradores que trabalham ou necessitam trabalhar esses Dados Pessoais, devem ser autorizadas para o efeito por seu responsável imediato e informar o Secretário Corporativo do Grupo ou o Diretor-Geral para as Questões Jurídicas, assim como o Diretor de Empresa ou de Região (conforme as circunstâncias). Cópias dessas listas devem ser disponibilizadas semestralmente ao Secretário Corporativo do Grupo.

5.1.14 Ao diretor-geral executivo e ao diretor-geral financeiro do Grupo compete conjuntamente elaborar e aprovar quaisquer novos procedimentos internos, indicações, a atribuição de poderes e padrões necessários para garantir o cumprimento dos nrs. 5.1.6-5.1.13 inclusive.

Categoria Específica de Dados Pessoais

O pessoal de Recursos Humanos e o pessoal médico contratado pela Empresa (quando aplicável) são os únicos autorizados a tratar a Categoria Específica de Dados Pessoais para cumprimento das obrigações jurídicas da Empresa do Grupo relativas à preparação das respostas aos pedidos das autoridades estatais e à proteção do trabalho dos colaboradores da Empresa. Antes do tratamento da Categoria Específica de Dados Pessoais, o Responsável Regional pela Proteção de Dados deve proceder a uma verificação destinada a avaliar o eventual impacte do tratamento de tais dados sobre os direitos e as liberdades do Titular de Dados Pessoais.

5.1.15 As seguintes Categorias Específicas de Dados Pessoais são as únicas que podem ser tratadas pelas Empresas do Grupo:

a) filiação religiosa para efeitos de tributação por retenção na fonte[3];
b) documentação médica[4].

5.1.16 O pessoal de Recursos Humanos deve proceder a tal tratamento nos termos dos diplomas normativos aplicáveis.

5.1.17 A documentação médica pode ser tratada unicamente por especialistas médicos registrados nos termos legais.

5.1.18 Dados Pessoais confidenciais são disponibilizados a Colaboradores desde que tal seja autorizado pela legislação trabalhista local e legislação em matéria de proteção de dados pessoais e ocorra em estrita conformidade com o princípio de necessidade de serviço. O acesso à Categoria Específica de Dados Pessoais pode ser facultado unicamente às Empresas do Grupo que têm a obrigação de tratar tais dados em conformidade com a legislação local aplicável.

Dados Pessoais de TI

5.1.19 Qualquer Empresa do Grupo pode tratar Dados Pessoais relacionados com o uso do sistema de IT normalizado que permite aos colaboradores e terceiros, entre outras coisas, trocar mensagens eletrônicas, visitar websites na internet, salvar arquivos e dados, utilizar aplicações, assim como criar, utilizar e guardar mensagens de diagnóstico e arquivos de log, quando tal seja requerido ou permitido pela legislação em vigor.

5.1.20 Caso a legislação e as normais locais requeiram a obtenção de autorização (por exempo, da autoridade reguladora da proteção de dados e de outra autoridade local) para tratamento dos Dados Pessoais referidos no nr. 5.1.19 (por exemplo, para IT-monitoramento de Colaboradores), a Empresa interessada do Grupo deve obter tal autorização em tempo hábil.

5.1.21 Ao tratarem Dados Pessoais de TI, as Empresas do Grupo devem respeitar as normas aplicáveis de privacidade, tais como o sigilo de correspondência ou de correspondência eletrônica privada.

Outros Dados Pessoais

5.1.22 Os Colaboradores podem igualmente tratar Dados Pessoais em conformidade com as políticas e os procedimentos de segurança de informação e a Política de Uso Lícito. O objetivo de tal tratamento e o volume de dados tratados estão descritos em detalhe nas referidas políticas.

Transparência, informação e direitos dos Titulares de Dados Pessoais

5.2 A maior parte dos Dados Pessoais recebidos pelas Empresas do Grupo é disponibilizada diretamente pelo Titular dos Dados. Aquando da coleta de Dados Pessoais, ao Titular dos mesmos, sempre que o requeira a legislação local, devem ser facultadas as seguintes informações[5]:

5.2.1 Firma da Empresa do Grupo (ou Empresas do Grupo) que coleta(m) informações como Controladora de Dados Pessoais;

5.2.2 Nomes e dados de contato das Pessoas de Contato Regionais para a Proteção de Dados ou do Representante Externo que o Titular dos Dados pode consultar sobre questões relativas a seus Dados Pessoais;

5.2.3 Objetivo(s) de tal Tratamento e sua justificação jurídica;

5.2.4 Interesses legítimos prosseguidos (quando aplicável);

5.2.5 Grupo ou destinatários de entre terceiros (referidos separadamente ou conjuntamente com uso de gêneros, por exemplo, “Empresas do Grupo” ou “autoridades locais”) que receberão Dados Pessoais para os tratar com seus objetivos independentes (para se evitarem incertezas, convém explicar que não é obrigatório divulgar as informações sobre os Processadores de Dados junto dos Titulares de Dados Pessoais);

---

[3] *Por exemplo, no caso da Suíça.*

[4] *Aplica-se às estruturas empresariais que prestam serviços dos próprios especialistas médicos ou que executam análises médicas ou coletam seus resultados (por exemplo, testes de alcooolemia ou drogas, etc.).*

[5] *Tais informações podem fazer parte do contrato, modelo de requerimento de contratação, etc..*

5.2.6 Se o Controlador de Dados Pessoais é um nacional da UE ou da Suíça e, quando aplicável, se o Controlador pretende transmitir os Dados Pessoais a um destinatário localizado fora da União Europeia/ EEE, e ainda:
- se esse país terceiro assegurará um nível suficiente de proteção de Dados Pessoais conforme os padrões da UE (ou seja, se existe uma decisão da Comissão Europeia relativa à proteção suficiente) e (em caso de resposta negativa),
- referência a medidas de proteção, adequadas ou pertinentes, tomadas pelo Controlador de Dados Pessoais para garantir a segurança da transmissão, o modo de obtenção de sua cópia ou local de sua disponibilização; assim como
- nomes e dados de contato do Responsável regional pela proteção de dados ou Representante Externo que o Titular dos Dados pode consultar sobre questões relacionadas com seus Dados Pessoais;

5.2.7 Prazo de conservação de Dados Pessoais ou, caso tal seja impossível, critérios utilizados para determinar a duração desse prazo;

5.2.8 Caso o Controlador de Dados Pessoais seja um nacional da UE ou da Suíça, assistem ao Titular dos Dados, por exemplo, na União Europeia, os seguintes direitos legítimos:
- solicitar o acesso aos Dados Pessoais, de precisá-los ou apagá-los;
- requerer uma limitação do Tratamento com respeito ao Títular de Dados (desde que observadas determinadas condições);
- objetar contra o Tratamento (desde que observadas determinadas condições). Os Titulares de Dados Pessoais podem, a qualquer momento, formular uma objeção contra o tratamento de seus Dados Pessoais por motivos legítimos convincentes relacionados com sua situação, salvo casos em que tal tratamento seja requerida pelas normais legais. Eles podem apresentar, a título gratuito, uma objeção contra o tratamento de Dados Pessoais para fins de marketing direto;
- transferir Dados Pessoais para outras plataformas, assim como
- apresentar uma queixa junto das autoridades competentes em matéria de proteção de dados.

5.2.9 Caso os Dados Pessoais tenham sido recebidos de terceiros, as Empresas do Grupo devem, dentro de um prazo razoável, mas não superior a um mês, após a receção dos Dados Pessoais, atendendo às circunstâncias concretas do tratamento dos Dados Pessoais, informar o Titular dos mesmos sobre as categorias respetivas de Dados Pessoais, a fonte de que foram recebidos, e, em casos aplicáveis, o fato de terem sido recebidos de fontes públicas.

Porém, a obrigação de informar o Titular de Dados nesse caso pode não ser aplcável se o Titular de Dados já estiver em poder da respetiva informação.

5.2.10 Solicitações dos Titulares de Dados relativas a seus direitos devem ser encaminhadas ao Responsável Regional pela Proteção de Dados. A resposta deve ser enviada ao Titular de Dados dentro de um mês. No entanto, se a solicitação for complexa ou se as Empresas do Grupo receberem um grande número de solicitações, esse prazo poderá ser dilatado por mais dois meses.

Soluções automatizadas[6]

5.3 A avaliação do Titular de Dados ou as decisões referentes a ele que tenham um forte impacte sobre ele, não podem se basear unicamente no tratamento automatizado/ eletrônico de Dados Pessoais, exceto quando tal decisão:

5.3.1 seja tomada no âmbito da celebração ou execução de um contrato, desde que a solicitação apresentada pelo Titular dos Dados esteja satisfeita ou tenham sido tomadas medidas correspondenes com vista à proteção dos interesses legítimos do Titular dos Dados, tais como acordos que permitam ao Titular dos Dados exprimir sua opinião; ou

5.3.2 seja autorizada por lei, a qual prevê igualmente medidas protegendo os interesses legítimos do Titular dos Dados

Os titulares de dados têm o direito de requerer a participação humana em qualquer tratamento automatizado de dados.

---

[6] *Como exemplos de soluções automatizadas podem ser referidas a análise automatizada de pedidos de inscrição em concurso ou análise automatizada de questionários de candidato a emprego.*

Armazenamento de dados

5.4 Os colaboradores devem armazenar Dados Pessoais tanto em suporte digital, como em suporte papel, de acordo com as políticas respetivas da Empresa do Grupo, e em casos determinados, conforme o calendário de armazenamento aprovado pelo Diretor-Geral Executivo do Grupo e referido no Anexo A. O Diretor-Geral Executivo é autorizado pelo Conselho a adotar e a introduzir alterações no calendário de armazenamento sob proposta do consultor jurídico principal, mas por acordo com o Responsável pela Proteção de Dados.

Segurança e confidencialidade

5.5 Em conformidade com as Políticas e os procedimentos de segurança de informação, todas as Empresas do Grupo devem implementar e aplicar as medidas técnicas e organizacionais apropriadas para a proteção de Dados Pessoais contra uma destruição acidental ou ilegal, perda acidental ou divulgação ou acesso não autorizados.

5.6 Em caso de destruição acidental ou ilegal ou perda acidental, alteração ou divulgação não autorizada de Dados Pessoais, as Empresas do Grupo devem seguir os procedimentos previstos pela legislação aplicável sobre a proteção de dados, as políticas e os procedimentos da Empresa do Grupo, assim como as instruções das autoridades competentes em matéria de proteção de dados. Caso como Processador de Dados intervenha uma Empresa do Grupo na UE:
- a mesma deve notificar ao Controlador de Dados Pessoais a fuga de Dados Pessoais imediatamente após a deteção desta violação, assim como
- caso o entenda útil, o Responsável pela Proteção de Dados deve notificar a fuga de Dados Pessoais à autoridade competente local em matéria de proteção de dados sem demoras injustificadas e, na medida do possível, dentro de 72 horas após a deteção dessa violação. Tal notificação deve incluir todas as informações requeridas pela legislação em vigor sobre a proteção de dados. Além disso, se a fuga de Dados Pessoais expuser, com alta probabilidade, os direitos e as liberdades do Titular de Dados a um elevado risco, o Controlador de Dados Pessoais deve notificar a fuga de Dados Pessoais aos respetivos Titulares de Dados sem demoras injustificadas, exceto os casos em que possa ser documentalmente provado que se aplica uma isenção prevista por lei.

Transmissão de Dados Pessoais no interior do Grupo de Empresas

5.7 O ERG é uma empresa internacional que periodicamente necessita transmitir Dados Pessoais entre suas empresas subsidiárias e filiais.

5.8 Os Dados Pessoais podem ser disponibilizados a outras Empresas do Grupo unicamente em conformidade com a presente Política. Os Dados Pessoais são protegidos, quando tratados por qualquer Empresa do Grupo, pela observância das rigorosas medidas de segurança organizacionais e técnicas gerais previstas pelas políticas e procedimentos de segurança de informação e pela presente Política.

5.9 Para garantir uma eventual transmissão de dados pessoais entre as Empresas do Grupo, convém utilizar as cláusulas padrão dos contratos.

Transmissão de Dados Pessoais a Processadores de Dados

Transmissão de Dados Pessoais por Empresas do Grupo localizadas na UE a Processadores de Dados localizados na UE ou em países associados

5.10 Se uma Empresa do Grupo localizada na UE pretender trasmitir Dados Pessoais a um Processador de Dados localizado na UE, CEE ou num país reconhecido pela Comissão Europeia como garantindo um nível de proteção adequado[7], antes da transmissão de dados convém executar o seguinte:

5.10.1 celebrar um contrato por escrito entre a Empresa do Grupo e o Processador de Dados; e

5.10.2 este contrato deve se basear no modelo de Acordo sobre o Tratamento de Dados Pessoais (ou conter cláusulas equivalentes) aprovado pelo Grupo e que encontra-se em poder do Responsável pela Proteção de Dados na Europa.

Transmissão de Dados Pessoais por Empresas do Grupo situadas na UE a Processadores de Dados situados fora da UE ou dos países associados

5.11 Se uma Empresa do Grupo situada na UE pretender transmitir Dados Pessoais a um Processador de Dados situado fora da UE, da CEE ou num país não reconhecido pela Comissão Europeia como garantindo um nível adequado de proteção, o Colaborador responsável deve se certificar do seguinte:

5.11.1 que tal transmissão se processa nos termos do Acordo Intragrupo obrigatório;

5.11.2 na ausência de tal Acordo Intragrupo, as Empresas do Grupo devem celebrar um contrato por escrito que baseia-se no modelo de Acordo sobre o Tratamento de Dados Pessoais (ou contem cláusulas equivalentes) aprovado pelo Grupo e encontrando-se em poder do Departamento Jurídico do Grupo;

5.11.3 Qualquer transmissão de dados deve ser protegida e executada em conformidade com a legislação aplicável em matéria de transmissão internacional de dados;

5.11.4 A respetiva Empresa do Grupo que transmite Dados Pessoais devia, antes da transmissão de Dados Pessoais, ter (i) celebrado com o Processador de dados um contrato incluindo uma série de cláusulas padrão na forma aprovada pela Comissão Europeia; e (ii) cumprido as formalidades e apresentar os documentos necessários em conformidade com a legislação local.

Transmissão de Dados Pessoais por Empresas do Grupo situadas fora da UE

5.12 Se uma Empresa do Grupo situada fora da UE pretender transmitir Dados Pessoais a um Processador de Dados localizado fora do seu país de registro, o consultor jurídico principal local deve se certificar que a transmissão se processa em plena conformidade com as leis locais e os diplomas normativos reguladores da proteção de dados e da transmissão internacional de dados pessoais.

5.13 Em caso de demissão/ despedimento de um colaborador de uma Empresa do Grupo, a mesma deve:

5.13.1. facultar ao colaborador em demissão/ despedimento a possiibilidade de fazer cópia de seus Dados Pessoais guardados nas caixas de entrada de seu correio eletrônico, assim como nos computadores corporativos e dispositivos móveis.

5.13.2. desativar, tão depressa quanto possível após a demissão/ despedimento, seu endereço corporativo de correio eletrônico.

Programa de formação

5.14 Todos os colaboradores que possuem um acesso permanente e/ou regular aos Dados Pessoais, devem periodicamente receber formação em coleta e processamento de Dados Pessoais ou em desenvolvimento de ferramentas utilizadas no tratamento de Dados Pessoais.

5.15 Todos os outros colaboradores devem receber formação nesta Política após serem admitidos à Empresa e, na medida da necessidade, ulteriormente.

6. Gestão de questões, preocupações e dúvidas

6.1 Sempre que tenha dúvidas ou dificuldades relacionadas com a proteção de dados, o Colaborador deve contatar o Responsável pela Proteção de Dados.

6.2 Entendendo um Titular de Dados que há violação desta Política no tratamento de seus dados, o mesmo deve notificar sua preocupação ao respetivo Responsável pela Proteção de Dados.

6.3 Se um Colaborador receber uma queixa de um Titular de Dados de fora do Grupo, a mesma deve imediatamente ser encaminhada ao respetivo Responsável pela Proteção de Dados.

[7] *A Comissão Europeia reconheceu como países que asseguram uma proteção adequada Andorra, Argentina, Austrália, Canadá (entidades comerciais), Suíça, Ilhas Faroé, Guernsey, Israel, Ilha de Man, Nova Zelândia e Uruguai (Veja: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, para informações atualizadas).*

6.4 O Responsável pela Proteção de Dados deve apreciar a queixa em uma base confidencial. Caso o Responsável pela Proteção de Dados seja inacessível, a queixa será apreciada pelo consultor jurídico principal local, o qual a encaminhará ao Responsável pela Proteção de Dados assim que este seja acessível.

6.5 As Empresas do Grupo, tendo informado o Responsável Regional pela Proteção de Dados, devem abrir imediatamente uma investigação a respeito de qualquer queixa relativa a uma violação da presente Política.

6.6 Os Colaboradores têm a obrigação de prestar apoio na realização de investigações internas relativas a eventuais violações da Política.

6.7 Para o Grupo poder efetuar apropriadamente uma investigação, a queixa relativa ao incumprimento ou violação da Política deve conter informações suficientes sobre o incidente ou violação.

6.8 O Grupo garante a confidencialidade do autor da queixa. Em determinadas circunstâncias, porém, a lei pode obrigar o Grupo a comunicar informações sobre a pessoa que apresentou a queixa ou denúncia.

6.9 O respetivo Responsável pela Proteção de Dados deve guardar qualquer queixa e quaisquer informações a ela relativas, em forma escrita ou digital, antes da conclusão da apreciação da queixa ou de um outro momento previsto por lei e pelas políticas da Empresa do Grupo.

7. Responsabilidade

7.1 O Conselho é responsável pela adoção desta política.

7.2 O Serviço de Conformidade na respetiva Região é responsável:

7.2.1. pela prestação de recomendações e aconselhamento à Administração Regional em matéria de implementação desta Política e supervisão da implementação desta política.

7.2.2. pelo monitoramento do cumprimento desta Política.

7.2.3. pela prestação de relatórios periódicos sobre o andamento da implementação e observância desta Política.

7.3 A Administração Regional é responsável por uma implementação eficaz desta Política em suas respetivas áreas de responsabilidade e implementação dos apropriados mecanismos de controle para garantir sua observância permanente.

7.4 A Administração Regional tem a obrigação de nomear uma Pessoa de Contato para a proteção de dados, assim como aprovar e assegurar a execução em sua Região das políticas e procedimentos elaborados pelo Responsável pela Proteção de Dados.

7.5 As pessoas de contato para a proteção de dados devem implementar os respetivos procedimentos, a distribuição de funções, a formação e os mecanismos internos de controle em suas Regiões para garantir uma implementação consequente da presente Política e a observância de suas metas.

7.6 A Administração Regional deve garantir que os respetivos Colaboradores e os Processadores de dados envolvidos estão informados desta Política e que os colaboradores que tratam Dados Pessoais ou têm acesso aos mesmos, recebem treinamentos periódicos sobre requisitos aplicados à proteção de dados.

8. Monitoramento

8.1 O Diretor-Geral para as Relações Jurídicas e o Responsável pela Proteção de Dados devem apresentar anualmente no Comitê de Conformidade junto do Conselho relatórios sobre a observância

desta Política. Os Serviços Regionais de Conformidade devem anualmente apresentar relatórios sobre a observância da presente Política ao Diretor-Geral para as Relações Jurídicas.

8.2 O Departamento de Auditoria Interna deve proceder periodicamente à fiscalização do cumprimento desta Política, denunciar deficiências e aprestar as respectivas recomendações à Administração do Grupo e ao Comitê de Conformidade do Conselho.

9. Incumprimento da Política

9.1 Quaisquer casos de incumprimento da Política devem ser devidamente registrados e comunicados ao Responsável pela Proteção de Dados, ao Departamento de Conformidade ou através da Linha Direta do ERG.

9.2 É obrigação de cada colaborador da empresa observar as disposições desta Política. Aos colaboradores que violem a presente Política podem ser aplicadas as medidas disciplinareses previstas pela legislação local até o despedimento.

10. Processo de Revisão

10.1 Esta Política do ERG será atualizada periodicamente (mas com uma frequência não inferior à bianual) com vista a refletir quaisquer alterações do ambiente jurídico e tecnológico, assim como as as necessidades da comunidade empresarial.

10.2 Quaisquer solicitações de alteração devem ser encaminhadas a um dos proprietários da Política ou às Pessoas de Contato.

10.3 As alterações substanciais introduzidas nesta Política do ERG devem ser aprovadas pelo Conselho ou (em caso do Anexo A) pelo Diretor-Geral Executivo.

10.4 A versão 4.0 desta Política do ERG entra em vigor aos 25 de maio de 2018.

Versão	Data da última alteração	Aprovado pelo	Data de aprovação	Comentários
1.0	24.08. 2014	Conselho	24.08.2014	
1.0	05.05.2015	Departamento de Conformidade	05.05.2015	
2.0	04.03.2016	Conselho	13.03.2016	
3.0	20.08.2017	Conselho	27.08.2017	
4.0	02.06.2018	Conselho	02.06.2018	