POLÍTICA DE PROTECÇÃO DE DADOS

1. INTRODUÇÃO

A MSC está comprometida a cumprir a legislação relativa à protecção de dados, no que respeita ao tratamento de Dados Pessoais no âmbito das suas actividades. A MSC cumpre a legislação através das acções dos seus colaboradores, pelo que o cumprimento desta política é da sua responsabilidade.

A presente Política de Protecção de Dados (doravante "Política") estabelece os padrões, bem como os princípios orientadores que devem ser seguidos pela MSC, Agências e Colaboradores no decurso da sua actividade. O incumprimento desta Política pelos colaboradores resultará em medidas disciplinares para os mesmos que podem culminar com a resolução do contrato de trabalho, bem como eventuais responsabilidades civis e criminais daí decorrentes.

A MSC exige que as suas Agências adoptem e implementem princípios e procedimentos adicionais que complementem esta "Política", de forma a cumprir a respectiva legislação nacional de protecção de dados.

O Departamento de Compliance da MSC Genebra (doravante denominado "Departamento de Compliance") delineou esta "Política", pelo que tal reflecte o compromisso da MSC na implementação do programa de protecção de dados. Os colaboradores e Agências devem reportar qualquer problema ao Departamento de Compliance para CH001-data.protection@msc.com.

1.1 ÂMBITO

A Política aplica-se à MSC, às suas Agências e a todos os Colaboradores, conforme definido nos presentes termos.

As Agências e os Colaboradores são responsáveis pelo cumprimento desta Política e devem ser capazes de demonstrar a implementação de medidas legais, organizacionais e técnicas tendo em vista o respectivo cumprimento.

1.2 CONFLITO DE LEIS

À presente "Política" são aplicáveis os princípios internacionais de protecção de dados, mas tal não substitui a legislação nacional que deve ser sempre cumprida pelas respectivas Agências e Colaboradores. Salienta-se que a legislação nacional pode ter requisitos diferentes dos indicados nesta "Política".

Em caso de ausência de legislação nacional, a presente "Política" constituirá o regime jurídico da Protecção de Dados da Agência em questão.

Se uma Agência tiver motivos para acreditar que a respectiva legislação nacional aplicável impedirá a implementação desta Política, ela comunicará imediatamente esse conflito ao Departamento de Compliance. Nesse caso, a MSC fornecerá orientações à Agência, a fim de alcançar uma solução que proteja os interesses da MSC e que esteja em conformidade com a legislação de protecção de dados.

2. DEFINIÇÕES

Os Termos definidos no "Código de Conduta Empresarial" da MSC e da MEDLOG têm os mesmos significados quando usados no âmbito desta Política, a menos que tal seja definido de outra forma.

Para a interpretação desta Política, aplica-se as seguintes definições:

"Agência(s)"- significa (i) as agências mundiais da MSC agindo em nome e por conta da MSC e inclui, quando aplicável, sub-agência(s) agindo em nome e por conta da MSC, (ii) Centros de planeamento da MSC, (iii) Sucursais da MSC, (iv) Filiais da MSC e (v) empresas com as quais a MSC possui acordos de fretagem de navios, incluindo qualquer Filial. A definição de Agência inclui todas as Empresas do Grupo MSC em Portugal:

- Mediterranean Shipping Company (Portugal) – Agente de Navegação, S.A.,
- MSC Terminal do Entroncamento, S.A.,
- MSC Terminal de Aveiro, S.A.,
- Mediterranean Shipping Company Logistics (Portugal) – Operadores Logísticos, S.A.
- MEDWAY – Operador Ferroviário e Logístico de Mercadorias, S.A.
- MEDWAY SGPS, S.A.
- MEDWAY Assets – Gestão de Activos, S.A.
- MSC Competence Center, A.C.E.

"Violação de Dados" - significa uma violação de segurança que leva à destruição acidental ou ilícita, perda, alteração, divulgação não autorizada ou acesso a Dados Pessoais, nomeadamente quando são transferidos para outro país ou por qualquer outro meio ilícito de tratamento.

"Responsável pelo Tratamento" - significa uma empresa ou uma pessoa singular que, isoladamente ou em conjunto com outras pessoas, estabelece as finalidades e os meios do tratamento dos Dados Pessoais.

"Subcontratante" - significa uma empresa ou uma pessoa singular que trata os Dados Pessoais em nome do Responsável pelo Tratamento e em conformidade com suas instruções e acordo escrito.

"Coordenador de Protecção de Dados" - significa a pessoa responsável pelas questões de protecção de dados da Agência e de monitorização e reporte dessas questões ao Departamento de Compliance.

"Titular de Dados" significa qualquer pessoa singular que seja o sujeito dos Dados Pessoais.

"Colaboradores" - significa funcionários, representantes, directores da MSC e das Agências, incluindo os Coordenadores de Protecção de Dados.

“Equipa de segurança cibernética” - significa a equipa de segurança cibernética do departamento de IT da MSC. A equipa de segurança cibernética pode ser contactada através de CH001-itsecurity@msc.com.

“MSC” - significa a MSC Mediterranean Shipping Company SA, com sede em 12-14 Chemin Rieu, 1208 Genebra, Suíça.

“Dados Pessoais” - significa qualquer informação ou dados relacionados com uma pessoa singular identificada ou identificável. Os Dados Pessoais englobam toda a informação relacionada com essa pessoa, independentemente da forma como a mesma é expressa e do formato da informação (arquivos, papel, gravação, filme, suporte electrónico, etc.). Para os fins desta “Política”, as pessoas colectivas devem ser excluídas do seu âmbito, salvo disposição em contrário da legislação nacional sobre a protecção de dados.

Os Dados Pessoais englobam qualquer informação relacionada a uma pessoa identificável. Existem diversas situações pelas quais uma pessoa pode ser considerada "identificável". O nome completo de uma pessoa é um identificador directo. Outras informações combinadas podem também ser suficientes para identificar uma pessoa.

A título meramente exemplificativo, os dados pessoais podem incluir informação relacionada com:

- nome, data de nascimento, endereço;
- endereço de e-mail pessoal e profissional e número de telefone, independentemente de ser usado para fins pessoais ou profissionais;
- descrição do cargo associado ao nome ou dados de contacto das partes do contrato de transporte;
- geolocalização dos contentores dos clientes;
- detalhes profissionais dos funcionários, categoria profissional, número de empregado;
- detalhes de contacto dos clientes ou detalhes financeiros dos clientes ou qualquer outra informação necessária para a verificação de créditos;
- Endereço IP ou um número de série do dispositivo.

Os "Dados Pessoais Sensíveis" incluem Dados Pessoais relacionados com:

- origem racial ou étnica;
- crenças religiosas ou filosóficas;
- opiniões ou actividades políticas;
- filiação sindical;
- saúde física ou mental;
- dados genéticos ou biométricos;
- procedimentos administrativos e criminais, e respectivas sanções; ou
- criação ou uso de um perfil que permita avaliar as características essenciais da personalidade de um sujeito de Dados.

“Processo” ou “Processamento” ou “Processado” ou “Tratamento” - significa qualquer operação ou conjunto de operações que são realizadas em Dados Pessoais ou em 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, alinhamento ou combinação, restrição, apagamento ou destruição.

"Subprocessamento" - significa o tratamento de dados realizado por qualquer Subcontratante.

"Subprocessador" - significa qualquer empresa ou pessoa singular contratada por um Subcontratante, ou por qualquer outro Subprocessador, que concorde em receber do Responsável pelo Tratamento ou de outro Subcontratante, os Dados Pessoais destinados exclusivamente ao seu tratamento por conta do Responsável pelo Tratamento de acordo com suas instruções e documentos escritos.

3. PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

A MSC está, em todas as fases de tratamento, empenhada em tratar os Dados Pessoais, que estão na sua posse, em conformidade com a legislação vigente e com os princípios fundamentais (doravante "Princípios").

Para tal, cada Colaborador deve: (i) estar ciente das suas responsabilidades e obrigações no que respeita aos Dados Pessoais e respectiva confidencialidade, e (ii) seguir as instruções do Departamento de Compliance e dos Coordenadores de Protecção de Dados das respectivas Agências.

Os Princípios abrangem, por um lado, a recolha e a utilização dos Dados Pessoais e, por outro lado, o tratamento dos mesmos.

3.1 PRINCÍPIOS PARA A RECOLHA E UTILIZAÇÃO DE DADOS PESSOAIS

A recolha ou utilização de dados pessoais deve ser efectuada:

- de forma lícita, em conformidade com a lei e por motivos legítimos;
- de forma transparente no que diz respeito às obrigações de informação;
- para fins específicos, explícitos e legítimos e nunca tratados de maneira incompatível com essas finalidades;
- por um período de tempo adequado, relevante, limitado e necessário em relação às finalidades;
- de forma que garanta a segurança apropriada dos Dados Pessoais, incluindo protecção contra o tratamento não autorizado ou ilegal, contra a perda, a destruição ou o dano acidental, usando sempre medidas técnicas ou organizacionais apropriadas; e
- de modo a que os titulares de dados não sofram qualquer efeito adverso, a menos que tal utilização seja autorizada pela legislação aplicável à protecção de dados.

3.2 PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

Os dados pessoais devem ser:

- mantidos exactos, completos e, sempre que necessário, actualizados;
- mantidos apenas pelo tempo necessário para cumprir a(s) finalidades(s) para a(s) qual(is) foram recolhidos, salvo disposição em contrário da legislação aplicável à protecção de dados, e sempre mantidos de acordo com a declaração de protecção de dados ou o formulário de consentimento entregue ao titular dos Dados;

- monitorizados em todas as fases, assegurando, quando necessário, que as diversas acções de tratamento são adequadamente documentadas;
- divulgados ou compartilhados com terceiros apenas naquilo que seja estritamente necessário e de acordo com a(s) finalidade(s) para a(s) qual(is) os dados foram recolhidos, salvo disposição em contrário da legislação aplicável à protecção de dados; e
- transferidos internacionalmente apenas com base numa justificação legítima, cumprindo todos os requisitos legais aplicáveis e depois de ser consultado o Coordenador da Protecção de Dados para que seja garantido que tais transferências sejam documentadas, legítimas e lícitas.

4. FUNÇÕES E RESPONSABILIDADES DO COORDENADOR DE PROTECÇÃO DE DADOS

Cada Agência designará um Coordenador de Protecção de Dados. Este último deve: (1) reportar ao Encarregado de Protecção de Dados ou à(s) pessoa(s) por eles designada(s), (2) ser o ponto de contacto do Departamento de Compliance e (3) implementar quaisquer instruções, bem como todas as outras políticas protecções de dados da MSC.

Conforme as situações, o Departamento de Compliance pode aprovar a nomeação de um Coordenador de Protecção de Dados responsável por várias Agências.

O Coordenador de Protecção de Dados está incumbido de implementar os “Princípios” na sua Agência, colocando tais princípios na prática do dia-a-dia e tomando todas as medidas necessárias para garantir a conformidade com esta Política e com a legislação aplicável à protecção de dados.

Por conseguinte, o Coordenador de Protecção de Dados deve, nomeadamente:

- manter um registo que enumere o processamento de dados realizado nas suas Agências;
- fomentar a consciencialização da protecção de dados de acordo com as instruções do Departamento de Compliance;
- ser o ponto de contacto directo para os Colaboradores e para os Titulares dos Dados, no que respeita ao cumprimento da presente Política;
- informar, receber instruções e fornecer todo o suporte necessário do Departamento de Compliance para tratar das solicitações dos sujeitos dos Dados em relação aos seus direitos de protecção dos dados; e
- informar, receber instruções e fornecer todo o apoio necessário ao Departamento de Compliance para atender aos pedidos das autoridades de supervisão da protecção de dados.

5. TRATAMENTO DE DADOS E SUBCONTRATAÇÃO

Quando, no âmbito das suas actividades, a MSC ou uma Agência utilizar um Subcontratante ou permitir um Subprocessador de Dados Pessoais, deverá:

- escolher um Subcontratante ou Subprocessador confiável que ofereça garantias suficientes para implementar medidas técnicas e organizacionais apropriadas de maneira que tal tratamento cumpra os requisitos desta Política e da legislação aplicável à protecção de dados;
- antes de qualquer tratamento ser realizado, deve: (1) celebrar um contrato escrito que regule o tratamento de Dados Pessoais realizado pelo Subcontratante ou pelo Subprocessador, que deve ser consistente com os Princípios, legislação aplicável à protecção de dados e instruções do Departamento de Compliance e (2) ser submetido o assunto ao Departamento de Compliance ou ao Coordenador de Protecção de Dados para que seja emitido parecer; e
- tomar todas as medidas necessárias para assegurar que as transferências de dados internacionais cumprem os Princípios e a legislação aplicável à protecção de dados dos países onde os Dados Pessoais são transferidos e recebidos.

6. VIOLAÇÃO DE PROTECÇÃO DE DADOS

6.1 COMUNICAÇÃO DE INCUMPRIMENTO DA POLÍTICA

Qualquer Colaborador da Agência que tomar conhecimento da violação desta Política deverá comunicá-lo imediatamente ao Coordenador de Protecção de Dados. Caso a violação reportada origine conflito de interesses para o Coordenador de Protecção de Dados, o assunto deverá ser encaminhado para o Departamento de Compliance.

O Coordenador de Protecção de Dados deve informar imediatamente o Departamento de Compliance da violação em causa.

Para os colaboradores que trabalham em Genebra, na Suíça, a comunicação de qualquer violação deverá ser imediatamente comunicada ao Departamento de Compliance.

6.2 COMUNICAÇÃO DE VIOLAÇÃO DE DADOS

As Agências têm a responsabilidade de implementar um processo efectivo de comunicação para garantir que cada violação de dados seja tratada apropriadamente assim que tal ocorrer. As agências devem seguir estritamente as políticas, os procedimentos e as instruções emitidas pelo Departamento de Compliance no que diz respeito ao tratamento de tal violação.

As agências podem ser obrigadas pela legislação nacional a notificar imediatamente os titulares dos Dados afectados e/ou qualquer autoridade supervisora relevante ou terceiros. Qualquer comunicado emitido aos meios de comunicação, ou qualquer notificação à autoridade supervisora, ao titular dos Dados ou a qualquer outro terceiro, deve ser aprovada, em primeiro lugar, pelo Departamento de Compliance.

De acordo com a presente Política, qualquer Colaborador da Agência deve informar imediatamente cada violação de dados:

- aos Gestores de IT locais, quando aplicável; e

- ao Coordenador de Protecção de Dados.

É obrigatório que as pessoas acima mencionadas reportem, imediatamente, ao Departamento de Compliance e à Equipa de Segurança Cibernética qualquer violação de Dados, o mais rapidamente possível e, em qualquer outro caso, no prazo máximo 24 horas após a descoberta da referida violação.

Os colaboradores que trabalham em Genebra, Suíça, devem reportar a violação de dados pessoais imediatamente para o Departamento de Compliance e equipa de segurança cibernética.