

# Política de Proteção de Dados

## Grupo ISS



# DECLARAÇÃO DE POLÍTICA

A ISS é um dos maiores empregadores do mundo que presta serviços a milhares de clientes a nível global, tratando Dados Pessoais diariamente. Enquanto prestador de serviços e empregador responsável, a ISS assume com rigor a obrigação de tratar os Dados Pessoais de uma forma ordenada e segura. A proteção da integridade dos Dados Pessoais dos nossos funcionários, clientes e utilizadores revestem-se de extrema importância para a ISS.

Esta Política define a forma como a ISS trata os Dados Pessoais, bem como quais as medidas que devem ser cumpridas e implementadas para assegurar que os Dados Pessoais dos nossos clientes são tratados de uma forma ordenada e segura.

O objetivo da Política é alinhar os requisitos mínimos obrigatórios em todo o Grupo ISS no que diz respeito a processos e procedimentos a serem aplicados à recolha e tratamento de Dados Pessoais. A Política também define determinados procedimentos que permitem à ISS cumprir as obrigações normativas relevantes.

O cumprimento desta Política é obrigatório.

O presente documento não pretende, nem pode responder a todas as questões que poderão surgir, por isso contate a sua Área Legal local da ISS ([dataprotectioniberia@es.issworld.com](mailto:dataprotectioniberia@es.issworld.com)) ou o Departamento Legal do Grupo (telefone: +45 38 17 00 00 ou e-mail: [dpo@group.issworld.com](mailto:dpo@group.issworld.com)) com as suas questões ou sugestões para melhorar a aplicação da Política.

Atentamente,

Bjørn Raasteen  
Diretor Legal Corporativo do Grupo

Morten Lindegaard  
Encarregado da Proteção de Dados do Grupo  
(DPO)

# ÍNDICE

|          |   |            |
|----------|---|------------|
| <b>1</b> | <b>INTRODUÇÃO.....</b>  | <b>3</b>   |
| 1.1      | Regras fundamentais.....  | 3          |
| 1.2      | Controlo e governança .....   | 4          |
| 1.3      | Como ler e usar a presente Política e as ferramentas fornecidas .....     | 4          |
| 1.4      | Definições aplicadas nesta Política.....                                  | 4          |
| 1.5      | Questões – Revisão da Política .....                                      | 6          |
| <br>     |   |            |
| <b>2</b> | <b>PRINCÍPIOS EM MATÉRIA DE PROTEÇÃO DE DADOS .....</b>                   | <b>7</b>   |
| 2.1      | Cumprimento da legislação aplicável em matéria de proteção de dados ..... | 7          |
| 2.1.1    | Legitimidade do tratamento de dados .....                                 | 7          |
| 2.1.2    | Finalidade do tratamento de dados .....                                   | 7          |
| 2.1.3    | Transparência no tratamento de dados.....                                 | 7          |
| 2.1.4    | Qualidade e proporcionalidade dos dados .....                             | 8          |
| 2.1.5    | Transferência dos Dados Pessoais e utilização de Subcontratados.....      | 8          |
| 2.1.6    | Categorias Especiais de Dados Pessoais .....                              | 10         |
| <br>     |   |            |
| <b>3</b> | <b>SEGURANÇA DOS DADOS .....</b>  | <b>111</b> |
| 3.1      | Política da ISS .....   | 111        |
| 3.2      | Como procedemos .....   | 111        |
| <br>     |   |            |
| <b>4</b> | <b>VIOLAÇÃO DA PROTEÇÃO DE DADOS .....</b>                                | <b>122</b> |
| 4.1      | Política da ISS .....   | 122        |
| 4.2      | Como procedemos .....   | 122        |
| <br>     |   |            |
| <b>5</b> | <b>FORMAÇÃO &amp; SENSIBILIZAÇÃO .....</b>                                | <b>144</b> |
| 5.1      | Política da ISS .....   | 144        |
| 5.2      | Como procedemos .....   | 144        |
| <br>     |   |            |
| <b>6</b> | <b>CONTROLO E AUDITORIA .....</b>   | <b>155</b> |
| 6.1      | Política da ISS .....   | 155        |
| 6.2      | Como procedemos .....   | 155        |
| 6.2.1    | Auditoria interna.....  | 155        |
| 6.2.2    | Auditoria solicitada pelo cliente da ISS.....                             | 155        |
| 6.2.3    | Auditoria aos fornecedores da ISS.....                                    | 16         |

## Versão do documento

Versão do documento: Versão 2

## Localização do documento:

<https://dataprotection.grupo.issworld.com>

Última atualização: Abril de 2019

Aprovado pela: EGM

Responsável pela manutenção: Departamento Legal do Grupo

Próxima revisão/ atualização: Abril de 2020

## 1.1 Regras fundamentais

A ISS presta serviços aos seus clientes em muitos locais do mundo. É importante para a ISS que os Dados Pessoais sejam tratados de acordo com padrões muito rigorosos. Por este motivo, dentro do Grupo de empresas ISS, a ISS optou por aderir, em todo o mundo, aos princípios do Regulamento de Proteção de Dados da UE, salvo se forem exigidos, pela legislação local, requisitos mais exigentes.

Para assegurar um nível consistentemente rigoroso para o tratamento de Dados Pessoais, a ISS adere aos seguintes princípios básicos:

- (a) **Equidade e boas práticas no tratamento de Dados Pessoais**  
A ISS garante que os Dados Pessoais são tratados de uma forma segura e ordenada de acordo com as boas práticas para o tratamento de Dados Pessoais. Em relação ao princípio geral de equidade, a ISS apenas tratará Dados Pessoais na medida necessária para completar a finalidade do tratamento.
- (b) **Apenas tratará Dados Pessoais para um fim específico**  
A ISS apenas procederá ao tratamento dos Dados Pessoais para o(s) efeito(s) para o(s) qual(is) os dados foram recolhidos originalmente.
- (c) **Transparência**  
A ISS garante que ao recolher dados dos titulares (Titulares dos Dados), estes serão informados conforme exigido pela lei. Além disso, os titulares dos dados e os clientes da ISS têm sempre direito a solicitar informações sobre quais os Dados Pessoais que a ISS recolheu e de que forma tais dados vão ser tratados.
- (d) **Confidencialidade**  
Quaisquer Dados Pessoais que a ISS tratar serão considerados informação confidencial. Para assegurar a confidencialidade dos Dados Pessoais, a ISS instruirá os seus funcionários sobre como os Dados Pessoais deverão ser tratados e sensibilizá-los-á para a natureza confidencial dos Dados Pessoais.
- (e) **Transferência de dados para outros países**  
A ISS apenas transferirá Dados Pessoais do país do qual são originários de acordo com a legislação local e outras regulamentações como as regras de proteção de dados da UE/EEE. A ISS assegurará que todos os acordos de transferência necessários estão em vigor com os subcontratados do tratamento de tais Dados Pessoais.
- (f) **Conservação e eliminação de Dados Pessoais**  
A ISS apenas armazenará e utilizará os Dados Pessoais enquanto for necessário para os efeitos para os quais foram recolhidos. A ISS estabeleceu procedimentos de

conservação e eliminação para assegurar que os Dados Pessoais são eliminados de forma adequada e em tempo.

## 1.2 Controle e governança

Para assegurar o cumprimento das regras de proteção dos dados mundialmente, a ISS nomeou um Encarregado pela proteção de dados do Grupo (Data protection officer - DPO do Grupo) e na maioria dos países designou um gestor local da proteção de dados (Data Protection Manager - DPM) ou um responsável local pelo cumprimento.

O DPO do Grupo controla o cumprimento global das regras de proteção de dados a nível mundial, realiza a formação dos Gestores Locais de Proteção de Dados locais (DPM) e lida com todas as questões respeitantes a esta Política e à sua implementação.

Os dados de contato do DPO do Grupo são: [dpo@group.issworld.com](mailto:dpo@group.issworld.com)

## 1.3 Como ler e usar a presente Política e as ferramentas fornecidas

Cada parte da Política é estruturada da seguinte forma:

- **Política da ISS:** Uma breve descrição e enquadramento da parte relevante da presente Política.
- **Como procedemos:** Uma descrição dos requisitos gerais e diretrizes e a forma como a presente Política é aplicada.
- **Requisitos mínimos de cumprimento:** Os requisitos mínimos em cada parte da Política que deverão ser implementados e cumpridos continuamente.
- **Ferramentas disponíveis:** Uma descrição das ferramentas e modelos disponíveis para implementar os requisitos da presente política. Todas as ferramentas e modelos estão disponíveis em <https://dataprotection.group.issworld.com>. Contate o seu DPM Local ou o departamento jurídico para ter acesso ao website, se aplicável.

## 1.4 Definições aplicadas nesta Política

**Regras Vinculativas Aplicáveis às Empresas (RVAE ou BCR):** De forma a permitir a transferência contínua de Dados Pessoais entre as nossas entidades, a ISS subscreveu, a nível mundial, um conjunto de Regras Vinculativas Aplicáveis às Empresas (RVAE ou BCR), aprovadas pelas Autoridades em matéria de Proteção de Dados da União Europeia. Uma lista de países da ISS que subscreveram as RVAE/BCR está disponível em <https://dataprotection.group.issworld.com>.

**Direção Nacional:** Em cada país da ISS, o Country Manager e todos os Diretores que lhe reportam diretamente, tais como, entre outros, o Diretor Financeiro (CFO Nacional), o Diretor de Pessoas & Cultura, o Diretor Comercial, o Diretor de Assessoria Legal e Diretores das Divisões.

**Responsável Pelo Tratamento de Dados:** Refere-se à pessoa singular ou coletiva, autoridade pública, serviço ou outro organismo que, individualmente ou em conjunto com outros, define as finalidades e meios para o tratamento de Dados Pessoais. Por exemplo, a ISS será normalmente considerada a Responsável pelo Tratamento de Dados Pessoais dos nossos funcionários.

**Mapa de Dados:** Cada país ou entidade da ISS é responsável por manter uma lista dos Dados Pessoais tratados, onde está mencionado como e onde são tratados e quem tem acesso a esses Dados Pessoais. O Mapa de Dados é assegurado pelo DPM Local e deve ser atualizado regularmente.

**Subcontratante:** O Subcontratante refere-se à pessoa singular ou coletiva, autoridade pública, serviço ou qualquer outro organismo que trate os Dados Pessoais em nome do Responsável pelo Tratamento de Dados. Por exemplo, os fornecedores da ISS serão normalmente considerados Subcontratante ao tratarem os Dados Pessoais dos funcionários da ISS. Quando a ISS trata os Dados Pessoais dos funcionários dos nossos clientes, a ISS será o Subcontratante.

**Acordo do Subcontratante:** As atividades do Subcontratante deverão ser regulamentadas por um acordo vinculativo entre o Responsável pelo Tratamento de Dados e o Subcontratante. Esse acordo deverá estabelecer a duração e a finalidade do tratamento, os tipos de Dados Pessoais tratados e os deveres e direitos do Responsável pelo Tratamento de Dados. Os Dados Pessoais só podem ser tratados com base em instruções documentadas do Responsável pelo Tratamento de Dados. O Subcontratante tem a obrigação de informar o Responsável pelo Tratamento de Dados se considerar que uma instrução para tratar os dados do Responsável pelo Tratamento de Dados viola o RGPD ou outra legislação local aplicável.

**Titular dos Dados:** O Titular dos Dados é uma pessoa singular identificável que pode ser reconhecida direta ou indiretamente, através de um elemento identificador como um nome, um número de identificação, dados de localização, um identificador online ou através de um ou mais fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

**Avaliação de Impacto Sobre a Proteção de Dados (AIPD):** Uma avaliação de impacto em matéria de privacidade pretende identificar e registar os componentes essenciais de qualquer sistema proposto que contenha quantidades significativas de Dados Pessoais ou de Categorias Especiais de Dados Pessoais e estabelecer de que forma os riscos de privacidade associados a esse sistema podem ser geridos.

**EEE:** O Espaço Económico Europeu (EEE) reúne os Estados-membros da UE e outros três estados (Islândia, Liechtenstein e Noruega) num mercado interno regulado pelas mesmas regras básicas. Os Estados-membros da UE são: Áustria, Bélgica, Bulgária, Croácia, República do Chipre, República Checa, Dinamarca, Estónia, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal, Roménia, Eslováquia, Eslovénia, Espanha, Suécia e Reino Unido.

**RGPD:** O Regulamento Geral de Proteção de Dados (RGPD) é a referência comum ao Regulamento da UE 2016/679 que substitui a Diretiva sobre proteção de dados e as legislações locais de proteção de dados na UE. O RGPD foi adotado no dia 27 de abril de 2016. Entra em vigor no dia 25 de maio de 2018. Ao contrário de uma Diretiva, não exige que

os governos nacionais aprovem qualquer legislação de aplicação e é, por isso, diretamente vinculativo e aplicável.

**DPO do Grupo:** O Encarregado pela Proteção de Dados do Grupo ISS. O DPO do Grupo supervisiona o cumprimento global das regras de proteção de dados a nível mundial, realiza as formações dos DPM locais e fornece orientações para todas as questões respeitantes a esta Política e à sua implementação.

**Política de Segurança da Informação:** Refere-se à Política de Segurança de Informação da ISS, incluindo todas as subpolíticas. As políticas estão disponíveis em <https://dataprotection.group.issworld.com>.

**Políticas do Grupo ISS:** Políticas e diretrizes emitidas e atualizadas, periodicamente, pelo Grupo ISS disponíveis em <https://governance-policies.group.issworld.com>.

**DPM Local:** Na maioria dos países, a Direção Nacional da ISS designou um gestor local da proteção de dados (se exigido pela legislação ou direção local) ou um responsável local pelo cumprimento em matéria de dados pessoais, conforme o caso.

**Dados Pessoais:** Refere-se a quaisquer informações relacionadas com uma pessoa singular identificada ou identificável ("Titular dos Dados").

**Categorias Especiais:** Refere-se aos Dados Pessoais que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical, dados genéticos e biométricos com o objetivo de identificar exclusivamente um Titular dos Dados, dados relativos à saúde ou à vida sexual ou orientação sexual de uma pessoa singular. Além destas categorias, podem existir requisitos locais adicionais de tipos específicos de dados que serão classificados como Categoria Especial. Se tiver dúvidas sobre os requisitos locais, contate o DPM Local ou o DPO do Grupo.

**Subcontratado:** Refere-se ao fornecedor de um Subcontratante nos casos em que tal fornecedor tenha acesso aos Dados Pessoais recebidos do Responsável pelo Tratamento de Dados.

## 1.5 Questões – Revisão da Política

Quaisquer questões que possam surgir relativamente à presente Política ou em relação a um aspeto concreto da mesma, deverão ser colocadas ao DPO do Grupo (telefone: +45 38 17 00 00 ou e-mail: [dpo@group.issworld.com](mailto:dpo@group.issworld.com)). Se tiver dúvidas, pergunte sempre ou solicite orientações antes de agir.

A Política será analisada pela EGM como e quando for necessário e, pelo menos, uma vez por ano.



De forma a cumprir as regras de proteção de dados aplicáveis, a ISS deverá ser capaz de documentar e demonstrar que os seguintes seis princípios são respeitados.

Sempre que a ISS recolher ou tratar Dados Pessoais, estes processos deverão ser feitos em conformidade com as disposições legais relevantes.

A ISS implementou processos e procedimentos para assegurar que os funcionários da ISS que trabalhem com Dados Pessoais saibam que os Dados Pessoais só podem ser tratados se a ISS tiver um fundamento legal para o fazer. Ao tratar Dados Pessoais em nome dos nossos clientes, a ISS deverá sempre assegurar-se que recebeu instruções para tratar os Dados Pessoais e que os Dados Pessoais somente são tratados de acordo com tais instruções.

A ISS não tratará Dados Pessoais para outros fins que não sejam aqueles para os quais os dados foram recolhidos originalmente, salvo se os Titulares dos Dados tiverem dado o seu consentimento ou na medida do permitido pela legislação aplicável.

A ISS é obrigada a cumprir a(s) finalidade(s) original(is) para a recolha de dados aquando do tratamento ou utilização ulterior de Dados Pessoais, incluindo quando os Dados Pessoais são recebidos de outra entidade da ISS. A finalidade do tratamento de dados apenas pode ser alterada com o consentimento do Titular dos Dados ou na medida do permitido pela legislação aplicável.

A ISS irá tratar os Dados Pessoais de uma forma transparente e responderá aos pedidos de informação dos Titulares dos Dados.



## **Como procedemos**

Ao tratar os Dados Pessoais enquanto Responsável pelo Tratamento de Dados, a ISS assegurará que as informações exigidas nos termos da legislação aplicável são fornecidas aos Titulares dos Dados. Se solicitado por um Titular dos Dados, a ISS deverá confirmar se os Dados Pessoais são tratados pela ISS e, se for o caso, fornecer informações sobre os Dados Pessoais tratados conforme exigido nos termos da legislação aplicável.

A ISS deverá assegurar que os Titulares dos Dados serão encaminhados para um único ponto de contato responsável por fornecer as informações acima mencionadas. Esse ponto de contato único deverá ser o DPM Local ou o DPO do Grupo para países sem um DPM Local.

Se uma solicitação se referir a Dados Pessoais de um cliente (ou de terceiros), o DPO do Grupo deverá ser informado imediatamente, para garantir que o cliente é notificado o mais breve possível.

### **2.1.4 Qualidade e proporcionalidade dos dados**

#### **Política da ISS**

A ISS assegurará que todos os Dados Pessoais tratados pela ISS enquanto Responsável pelo Tratamento de Dados são precisos, adequados, relevantes e limitados ao que é necessário em relação aos fins para os quais os Dados Pessoais são tratados.

## **Como procedemos**

O tratamento de Dados Pessoais na ISS é orientado pelo princípio da proporcionalidade. Isto significa que a ISS deverá recolher, tratar e utilizar apenas os Dados Pessoais necessários para os fins relevantes do tratamento.

A ISS poderá anonimizar os Dados Pessoais, desde que os dados não sejam pertinentes para efeitos da proteção de dados.

A ISS assegurará que os Dados Pessoais estão corretos e se mantêm atualizados. Serão tomadas medidas adequadas para assegurar que os Dados Pessoais incorretos ou incompletos sejam corrigidos, bloqueados ou apagados.

### **2.1.5 Transferência dos Dados Pessoais e utilização de Subcontratados**

#### **Política da ISS**

Um aspeto fundamental da proteção dos Dados Pessoais é assegurar que um nível adequado de proteção é mantido aquando da transferência de Dados Pessoais entre as entidades do Grupo ISS ou da ISS para terceiros. A ISS assegurará que os Dados Pessoais serão apenas transferidos entre entidades da ISS ou para terceiros, desde que haja uma base legal para a transferência.

## **Como procedemos**

### Transferência de Dados Pessoais entre as entidades do Grupo ISS

A ISS implementou as Regras Vinculativas Aplicáveis às Empresas (RVAE/BCR) que regulam a transferência dos Dados Pessoais entre as entidades da ISS. De acordo com as RVAE/BCR, todas as entidades signatárias da ISS comprometeram-se a assegurar uma proteção adequada dos Dados Pessoais recebidos de outras entidades da ISS. Quando a ISS atua enquanto Subcontratante poderá transferir Dados Pessoais para um subcontratado da ISS de acordo com as RVAE/BCR na medida em que uma entidade da ISS é Responsável pelo Tratamento de Dados dos dados pessoais que estão a ser transferidos.

### Transferência de Dados Pessoais da ISS para terceiros no EEE

Ao transferir Dados Pessoais da ISS para terceiros localizados no EEE ou na Suíça, a ISS assegurará que as partes celebraram um Acordo sobre o Tratamento de Dados e que uma das seguintes condições é cumprida:

- (a) O modelo do Acordo sobre Tratamento de Dados da ISS foi usado pela ISS e pela entidade terceira recetora, ou
- (b) A lista de verificação do Acordo do Subcontratante foi seguida e todos os requisitos ali incluídos foram abordados.

### Transferência de Dados Pessoais da ISS para terceiros fora do EEE

Ao transferir Dados Pessoais da ISS para terceiros localizados fora do EEE, a ISS assegurará que uma das seguintes condições é cumprida:

- (a) que tenha sido celebrado o contrato-tipo da UE (cláusulas contratuais-tipo para Subcontratantes 2010/87/UE ou cláusulas contratuais-tipo entre Responsáveis pelo Tratamento de Dados 2001/497/CE ou 2004/915/CE) entre a ISS e a entidade terceira recetora, ou
- (b) que a transferência é permitida nos termos da legislação aplicável.

### Utilização de um Subcontratante e/ou de um Subcontratado

Se a ISS, atuando enquanto Responsável pelo Tratamento de Dados ou Subcontratante, incumbir uma entidade terceira de tratar Dados Pessoais, deverá assegurar-se que os seguintes requisitos serão cumpridos:

- (a) a referida entidade terceira (que atuará como Subcontratante ou Subcontratado) é cuidadosamente avaliada e selecionada pela ISS com base na sua capacidade de assegurar a implementação e manutenção das medidas de segurança técnicas e organizativas necessárias para o cumprimento da legislação aplicável relativa ao tratamento de dados;

- (b) a ISS assegurará e verificará regularmente se a entidade terceira que atua como Subcontratante ou Subcontratado mantém o cumprimento dos requisitos de segurança técnicos e organizativos estabelecidos;
- (c) a ISS assegurará que a realização do tratamento de dados atribuído é regulada por um Acordo escrito relativo ao Subcontratante, no qual os direitos e deveres do Subcontratante são claramente definidos; e
- (d) a ISS assegurará que o Subcontratante está vinculado por um contrato para tratar os Dados Pessoais recebidos da ISS ou recolhidos em nome desta, somente se estiver em conformidade com o acordo e com respeito pelas instruções da ISS.

#### 2.1.6 Categorias Especiais de Dados Pessoais

##### **Política da ISS**

Ao tratar **Categorias Especiais de Dados Pessoais** tais como registos criminais, testes de personalidade, sanções disciplinares e respetiva motivação, informação relativa à saúde e acidentes de trabalho **devem ser tomadas precauções especiais**.

##### **Como procedemos**

Se for exigido à ISS tratar Categorias Especiais de Dados Pessoais, deverá ser obtido o consentimento explícito do Titular dos Dados, salvo se o tratamento for expressamente permitido pela legislação aplicável.

O DPM Local ou o DPO do Grupo deverá ser sempre consultado antes do tratamento das Categorias Especiais de Dados Pessoais. Além disso, este tratamento deverá ser incluído no Mapa de Dados local. Além disso, ao transmitir Categorias Especiais de Dados Pessoais, os anexos contendo tais informações devem ser encriptados.

Se se considerar que o tratamento de Categorias Especiais de Dados Pessoais está associado a um elevado risco para os Titulares dos Dados, deverá ser realizada uma Avaliação de Impacto sobre a Proteção de Dados (AIPD).

## 3 SEGURANÇA DOS DADOS



### 3.1 Política da ISS

A ISS deverá assegurar que são adotadas medidas de segurança técnicas e organizativas para proteger os Dados Pessoais da destruição, perda ou alteração accidental ou ilícita, divulgação ou acesso não autorizados, utilização fraudulenta ou outro tratamento que infrinja a legislação aplicável.

Tendo em conta o custo da sua implementação, tais medidas deverão assegurar um nível de segurança adequado aos riscos associados ao tratamento e à natureza dos Dados Pessoais a serem protegidos. As Categorias Especiais de Dados Pessoais deverão estar sujeitas a medidas de segurança e proteção específicas.

### 3.2 Como procedemos

De forma a cumprir estes requisitos, a ISS adotou uma Política de Segurança da Informação, estabeleceu e documentou uma organização de segurança de informática e integrou a segurança dos dados nos processos da sua organização.

Apenas os funcionários que estejam autorizados e tenham sido especificamente instruídos em conformidade com os requisitos da proteção de dados poderão recolher, tratar ou utilizar Dados Pessoais. A autorização de acesso do funcionário individual deverá ser restrita de acordo com a natureza e âmbito do campo de atividade específico desse funcionário. Os funcionários estão proibidos de utilizar Dados Pessoais para fins privados, de transferir ou de disponibilizar de alguma outra forma os Dados Pessoais a pessoas não autorizadas. As pessoas não autorizadas neste contexto incluem, por exemplo, outros funcionários da ISS, na medida em que não precisem dos Dados Pessoais para realizar as suas tarefas especializadas. O dever de confidencialidade continua a vigorar após o termo do contrato de trabalho do funcionário em questão com a ISS.

Entre as medidas específicas utilizadas para assegurar a proteção adequada dos Dados Pessoais incluem-se os controlos de admissão, de acesso ao sistema, de acesso aos dados, de transmissão, de introdução de dados, de postos de trabalho, de disponibilidade e de discriminação, bem como a encriptação manual de dados pessoais sensíveis.

Todos os computadores e dispositivos móveis estão protegidos por senha/código de acesso. A rede interna da ISS possui um sistema de firewall para proteger os conteúdos internos da empresa do acesso externo não autorizado. A transmissão de Dados Pessoais na própria rede da empresa é normalmente encriptada, na medida em que a natureza e a finalidade pretendida dos Dados Pessoais assim o exija e as Categorias Especiais de Dados Pessoais são encriptadas manualmente quando necessário.

## 4 VIOLAÇÃO DA PROTEÇÃO DE DADOS



### 4.1 Política da ISS

No caso da segurança do tratamento de Dados Pessoais ter sido comprometida ou ser suscetível de ser comprometida ou se tiver havido de qualquer outra forma uma divulgação ou acesso não autorizado ou acidental dos Dados Pessoais, o DPM Local ou o DPO do Grupo deverá ser imediatamente notificado.

A ISS dispõe de um processo específico, descrito no Modelo de Violação de Dados, que define de que forma a ISS lida com os incidentes de violação da proteção de dados de forma a atenuar quaisquer impactos adversos nos Titulares dos Dados, nos nossos clientes e na nossa atividade empresarial, a fim de cumprir os requisitos de notificação aplicáveis pela legislação local e/ou com os nossos deveres contratuais para com os nossos clientes.

### 4.2 Como procedemos

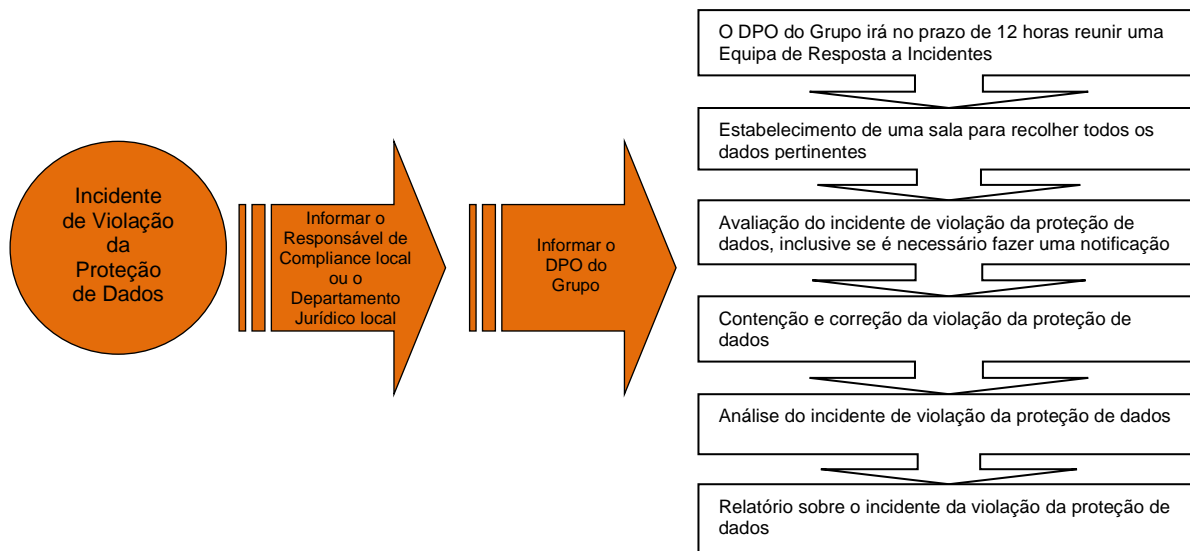
De forma a sensibilizar e a formar os nossos funcionários para identificar e divulgar situações de violação de proteção de dados, a ISS desenvolveu um módulo de formação sobre violações da proteção de dados. Este módulo de formação está disponível na plataforma de formação MyLearning@ISS. Para mais orientações sobre formação e sensibilização, consulte a Secção 5 da presente Política.

Se algum funcionário da ISS tomar conhecimento de uma divulgação não autorizada de Dados Pessoais ou de que a segurança em torno dos Dados Pessoais foi comprometida ou corre o risco de ser comprometida, por exemplo, devido a uma violação de segurança, o DPO do Grupo e o DPM Local deverão ser imediatamente contactados.

As seguintes informações deverão ser fornecidas utilizando o Formulário de Violação da Proteção de Dados:

- (a) que entidade da ISS está a lidar com a violação da proteção de dados;
- (b) resumo do incidente que provocou a violação da proteção de dados;
- (c) data e hora da violação da proteção de dados;
- (d) tipo(s) de Dados Pessoais que foi(ram) comprometido(s); e
- (e) o número de Titulares dos Dados afetados pela violação da proteção de dados.

Após ter recebido informação sobre um incidente de violação da proteção de dados, o DPO do Grupo deverá assegurar-se de que o seguinte processo é respeitado:



De forma a assegurar que os departamentos relevantes em cada entidade da ISS possuem o conhecimento e experiência necessários para reagir adequadamente a um incidente de violação da proteção de dados, o DPM Local deverá coordenar com o DPO do Grupo um exercício de simulação de incidente de violação de dados, pelo menos de dois em dois anos.

Como parte das obrigações da ISS (legais e contratuais) de documentar a formação de proteção de dados dos funcionários relevantes, a ISS utilizará a plataforma de formação MyLearning@ISS disponível em cada país.

O material de formação é assegurado e atualizado pelo DPO do Grupo.



## 6 CONTROLO E AUDITORIA



### 6.1 Política da ISS

Os princípios de proteção de dados desta Política contribuem de forma notável para gerir o nosso negócio de forma prudente e fiável. Contudo, não são suficientes por si só. O controlo e auditoria do cumprimento desta Política são importantes e necessários para documentar as responsabilidades e assegurar que possíveis lacunas são analisadas e seguidas de forma adequada.

### 6.2 Como procedemos

A implementação e o funcionamento dos processos e procedimentos destinados a assegurar o cumprimento dos requisitos da proteção de dados deverão ser realizados de forma a permitir o controlo e auditoria adequados. Isto significa que os processos e procedimentos relacionados com o tratamento dos Dados Pessoais deverão ser documentados e qualquer alteração a tais processos e procedimentos deverá ser atualizada no Mapa de Dados local.

#### 6.2.1 Auditoria interna

O DPO do Grupo supervisiona as atividades de auditoria interna realizadas pela Auditoria Interna do Grupo e fornece orientações para assegurar que as atividades de auditoria abordam o tratamento de Dados Pessoais da ISS, incluindo os métodos para assegurar que serão efetuadas ações corretivas e preventivas.

As entidades da ISS serão auditadas regularmente o que incluirá a auditoria do cumprimento com a legislação de proteção de dados aplicável e com a presente Política. A auditoria é realizada pela Auditoria Interna do Grupo, por outros especialistas internos ou por auditores externos.

O DPO do Grupo é responsável por alertar o Diretor Financeiro e o Diretor Legal Corporativo do Grupo ISS sobre quaisquer irregularidades detetadas no âmbito das auditorias, os quais estão incumbidos de assegurar que são realizadas ações corretivas para sanar o incumprimento o mais breve possível.

#### 6.2.2 Auditoria solicitada pelo cliente da ISS

Os clientes da ISS poderão, de acordo com a legislação aplicável ou com as disposições do contrato celebrado entre as partes, ter o direito de auditar ou solicitar uma auditoria a uma entidade da ISS que trate Dados Pessoais em nome dos clientes.

A ISS ajudará os clientes a realizar as auditorias de forma a assegurar a tais clientes que podem confiar que a ISS cumpre a legislação aplicável em matéria de proteção de dados e os deveres contratuais estabelecidos.

### 6.2.3 Auditoria aos fornecedores da ISS

Para assegurar o cumprimento com a legislação aplicável em matéria de proteção de dados, a ISS procederá regularmente a auditorias ao tratamento de Dados Pessoais realizados pelos seus fornecedores em nome da ISS. As auditorias poderão ser realizadas fisicamente nas instalações dos fornecedores ou através da análise de relatórios de auditorias realizadas por entidades terceiras independentes em nome do fornecedor.

Honestidade  
Respeitamos

Empreendedorismo  
Agimos

# Os valores da ISS

Responsabilidade  
Preocupamo-nos

Qualidade  
Entregamos

A ISS adotou uma Política de Denúncia (Speak Up Policy) para permitir que os funcionários, parceiros comerciais e outras partes interessadas da ISS denunciem qualquer caso grave e ou sensível de uma forma segura e confidencial.

Está disponível um Guia de Denúncia (Speak Up Guide) em <https://www.pt.issworld.com/carreira/empregador/politica-de-denuncias/guia-denuncia> para o ajudar a determinar, se a sua questão é (a) um caso local que deverá ser comunicado ao seu supervisor, gestor, diretor de Pessoas & Cultura, diretor jurídico local ou CFO local ou (b) um caso grave e sensível que deverá ser comunicado ao Grupo através de um sistema de comunicação seguro e alojado externamente disponível no website da ISS no seu país ou em <https://www.pt.issworld.com/carreira/empregador/politica-de-denuncias> ou através de uma linha telefónica + 44 2036301701.

Pode também contactar diretamente:

Dan Otzen

Diretor da Auditoria Interna do Grupo

ISS World Services, A/S

Buddingevej 197, DK-2860 Søborg, Dinamarca

E-mail: [Dan.Otzen@group.issworld.com](mailto:Dan.Otzen@group.issworld.com)

Telefone: +45 38 17 68 00

Todos os inquéritos serão tratados de forma confidencial e de acordo com a Política de Denúncia.

ISS A/S dezembro 2016

