26 de junho de 2018

EXIDE TECHNOLOGIES
("Exide" ou "a Empresa")

Política de proteção de dados (a "Política")

É necessário que leia esta política visto que disponibiliza informações importantes sobre:

- os princípios de proteção de dados que a Exide deve cumprir;
- o que constitui informações pessoais (ou dados) e informações pessoais (ou dados) sensíveis;
- como a Exide recolhe, utiliza e (em última instância) elimina informações pessoais e informações pessoais sensíveis em conformidade com a Política;
- onde podem ser encontradas informações detalhadas adicionais relativas aos dados, por ex., as informações pessoais que a Exide recolhe e utiliza, como as informações pessoais são utilizadas, armazenadas e transferidas, para que objetivos, as medidas tomadas para manter essas informações pessoais seguras e durante quanto tempo são mantidas;
- as suas obrigações como funcionário da Exide em relação à proteção de dados; e
- as consequências do incumprimento desta Política.

1 Introdução

1.1 A Exide obtém, mantém e utiliza informações pessoais (também referidas como "dados pessoais") sobre terceiros para vários objetivos legais específicos, conforme estabelecido nos *avisos de privacidade da proteção de dados* da Exide.

1.2 Esta Política estabelece a forma como cumprimos as nossas obrigações de proteção de dados. O objetivo desta Política também é o de garantir que o pessoal, incluindo os funcionários, bem como trabalhadores temporários, compreende e cumpre as regras que governam a recolha, utilização e eliminação de informações pessoais às quais possam ter acesso no decorrer do seu trabalho.

1.3 A Exide empenha-se no cumprimento das nossas obrigações de proteção de dados e a ser concisa, clara e transparente sobre como obtemos e utilizamos informações pessoais, e como (e quando) eliminamos essas informações quando já não forem necessárias.

1.4 Se tiver quaisquer dúvidas ou comentários sobre o conteúdo desta Política ou se necessitar de informações adicionais, deve entrar em contacto com o Correspondente de RGPD local ou com o Departamento jurídico.

2 Âmbito

2.1 Os funcionários devem consultar os avisos de privacidade da proteção de dados da Exide e, quando apropriado, as suas restantes políticas relevantes incluindo as relacionadas com a *segurança da informação e retenção de registos,* que contêm informações adicionais relativas à proteção de informações pessoais nesses contextos.

2.2 A Exide irá rever e atualizar esta Política em conformidade com as nossas obrigações de proteção de dados. Esta Política não faz parte do contrato de trabalho de nenhum funcionário e podemos modificar, atualizar ou suplementar a Política periodicamente. Comunicamos qualquer política nova ou modificada ao pessoal quando for adotada.

3 Definições

registos criminais são informações pessoais relativas a condenações e ofensas criminais,

alegações, procedimentos e medidas relacionadas com segurança das **informações**;

violação de dados é uma violação de segurança que resulta em destruição, perda, alteração,

difusão ou acesso não autorizado às informações pessoais de forma acidental ou ilícita;

sujeito de dados é o indivíduo relacionado com as informações pessoais;

pessoais (por vezes conhecidas por dados pessoais) são informações relativas a dados

sujeito das **informações** que pode ser identificado (diretamente ou indiretamente) a partir dessas informações;

processamento é a obtenção, registo, organização, armazenamento, modificação, recuperação,

difusão de **informações** e/ou destruição de informações ou, de modo geral, utilizar ou fazer alguma coisa com estas;

Pseudonimização é o processo através do qual as informações pessoais são processadas de forma que não possam ser utilizadas para identificar um sujeito de dados sem a utilização de informações adicionais, que são mantidas em separado e sujeitas a medidas técnicas e organizacionais para garantir que as informações pessoais não podem ser associadas a um sujeito de dados identificável;

informações pessoais sensíveis (por vezes conhecidas por "categorias especiais de dados pessoais" ou "dados pessoais sensíveis") são as informações pessoais sobre a raça, etnia,

opiniões políticas, crenças religiosas ou filosóficas, filiação (ou não filiação) sindical, informações genéticas, informações biométricas (quando utilizadas para identificar um sujeito de dados) e informações relativas à saúde, vida sexual ou orientação sexual de um sujeito de dados.

4 Princípios de proteção de dados

4.1 A Exide irá cumprir os seguintes princípios de proteção de dados no processamento de informações pessoais:

4.1.1 iremos processar informações pessoais de forma legal, justa e transparente;

4.1.2 iremos recolher informações pessoais apenas para objetivos especificados, explícitos e legítimos e não iremos processá-las de forma incompatível a estes objetivos legítimos;

4.1.3 apenas iremos processar as informações pessoais que são adequadas, relevantes e necessárias para os objetivos relevantes;

4.1.4 iremos manter informações pessoais precisas e atualizadas, e tomar medidas razoáveis para garantir que informações pessoais imprecisas são eliminadas ou corrigidas sem atraso;

4.1.5 iremos manter informações pessoais sob uma forma que permita a identificação de sujeitos de dados durante um período não superior ao necessário para os objetivos para os quais as informações são processadas; e

4.1.6 iremos tomar as medidas técnicas e organizacionais apropriadas para garantir que as informações pessoais são mantidas de forma segura e protegida contra processamento não autorizado e ilícito e contra perda, destruição ou danos acidentais.

5 Bases para processamento de informações pessoais

5.1 Em relação a qualquer atividade de processamento, a Exide irá, antes de iniciar o processamento pela primeira vez e, em seguida, regularmente enquanto continua:

5.1.1 rever os objetivos da atividade de processamento em particular e selecionar as bases legais mais adequadas para esse processamento, ou seja:

(a) se o sujeito de dados consentiu o processamento;

(b) se o processamento é necessário para realizar o contrato no qual o sujeito de dados constitui uma das partes, ou para tomar medidas a pedido do sujeito de dados antes de entrar num contrato;

(c) se o processamento é necessário para cumprir uma obrigação legal à qual a Empresa está sujeita;

(d) se o processamento é necessário para proteger os interesses vitais do sujeito de dados ou outra pessoa singular; ou

(e) se o processamento é necessário para os interesses legítimos da Exide, da Empresa ou de terceiros, exceto quando esses interesses são anulados pelos interesses e direitos e liberdades fundamentais do sujeito de dados—consulte a cláusula 5.2 abaixo.

5.1.2 exceto quando o processamento se basear no consentimento, verificar se o processamento é necessário para cumprir as bases legais relevantes (ou seja, verificar se não existe outra forma razoável de cumprir esse objetivo);

5.1.3 documentar a nossa decisão em relação a qual base legal aplicar, para auxiliar na demonstração do cumprimento dos princípios de proteção de dados;

5.1.4 incluir informações acerca dos objetivos do processamento e da base legal para tal nos nossos avisos de privacidade relevantes;

5.1.5 onde forem processadas informações pessoais sensíveis, identificar também uma condição legal especial para o processamento dessas informações (consulte o parágrafo 6.2.2 abaixo) e documente (apenas para o Reino Unido); e

5.1.6 onde forem processadas informações sobre ofensas criminais em conformidade com a legislação da União ou do Estado-membro, identificar também uma condição legal para o processamento dessas informações e documentá-las.

5.2 Ao determinar se os interesses legítimos da Empresa são a base mais adequada para o processamento legal, iremos:

5.2.1 realizar uma avaliação de interesses legítimos (LIA) adequada e guardar um registo da mesma, para nos certificarmos de que conseguimos justificar a nossa decisão;

5.2.2 se a LIA identificar um impacto significativo de privacidade, considerar se também é necessário realizar uma avaliação de impacto de proteção de dados (DPIA); e

5.2.3 incluir informações acerca dos nossos interesses legítimos nos nossos avisos de privacidade relevantes.

6 Informações pessoais sensíveis

6.1 As informações pessoais sensíveis, por vezes, são referidas como "categorias especiais de dados pessoais" ou "dados pessoais sensíveis".

6.2 A Empresa pode precisar, periodicamente, de processar informações pessoais sensíveis. Apenas iremos processar as informações pessoais sensíveis se:

6.2.1 temos uma base legal para o fazer como definido no parágrafo 5.1.1 acima, por ex., se for necessário para realizar o contrato de trabalho, para cumprir as obrigações legais da Exide ou para os interesses legítimos da Empresa; e

6.2.2 se se aplicar uma das condições especiais para o processamento de informações pessoais sensíveis, por ex.:

(a) o sujeito de dados consentiu explicitamente;

(b) o processamento é necessário para exercer os direitos ou obrigações da legislação laboral da Exide ou do sujeito de dados;

(c) o processamento é necessário para proteger os interesses vitais do sujeito de dados e este encontra-se fisicamente incapaz de dar consentimento;

(d) o processamento relaciona-se com os dados pessoais que são, manifestamente, tornados públicos pelo sujeito de dados;

(e) o processamento é necessário para estabelecer, exercer ou defender ações judiciais; ou

(f) o processamento é necessário por motivos de interesse público substancial.

6.3 As informações pessoais sensíveis não serão processadas pela Exide até:

6.3.1 o sujeito de dados ter sido informado devidamente (através de aviso de privacidade

ou outros meios) da natureza do processamento, da finalidade do mesmo e a base legal.

6.4 A Empresa não realizará a tomada de decisão automatizada (incluindo a criação de perfis) com base nas informações pessoais sensíveis do sujeito de dados.

6.5 O *aviso de privacidade da proteção de dados* da Empresa define os tipos de informações pessoais sensíveis que a Exide processa, para que são utilizadas e a base legal do processamento.

6.6 Relativamente às informações pessoais sensíveis, a Empresa cumprirá os procedimentos definidos nos parágrafos 6.7 e 6.8 abaixo para se certificar de que cumpre os princípios de proteção de dados definidos no parágrafo 4 acima.

6.7 **Durante o processo de recrutamento**: O Departamento de Recursos Humanos da Exide certificar-se-á de que (salvo indicação em contrário da legislação):

6.7.1 durante as etapas de pré-seleção, entrevista e tomada de decisão, não serão colocadas relativamente a informações pessoais sensíveis, por ex., a raça ou a etnia, filiação sindical ou questões relacionadas com a saúde;

6.7.2 qualquer formulário de monitorização de igualdade de oportunidades é mantido separado do formulário de candidatura do sujeito de dados, e não é visualizado pela pessoa que realiza a pré-seleção, as entrevistas ou a tomada de decisão de recrutamento;

6.7.3 as verificações de "direito ao trabalho" são realizadas antes de uma oferta de emprego ser considerada incondicional, e não durante as etapas iniciais de pré-seleção, entrevista ou tomada de decisão;

6.8 **Durante a contratação**: o Departamento de Recursos Humanos irá processar:

6.8.1 informações de saúde para administrar os subsídios de baixa, manter registos de faltas por motivo de doença, monitorizar a assiduidade do pessoal e facilitar os benefícios de saúde e de doença;

6.8.2 informações pessoais sensíveis para fins de monitorização de igualdade de oportunidades. Se possível, estas informações serão anonimizadas; e

6.8.3 informações de filiação sindical para fins de administração de pessoal e pagamento de "quotas".

7 Informações de registos criminais

As informações de registos criminais serão processadas em conformidade com a legislação da União ou do Estado-membro.

8 Avaliações de impacto de proteção de dados (DPIA)

8.1 Uma vez que o processamento tem a probabilidade de apresentar um alto risco à proteção de dados do sujeito de dados (por ex., onde a Exide planeie utilizar uma nova tecnologia), antes de iniciar o processamento, iremos realizar uma DPIA para avaliar:

8.1.1 se o processamento é necessário e proporcional em relação à sua finalidade;

8.1.2 os riscos para os sujeitos de dados; e

8.1.3 que medidas podem ser tomadas para fazer face a esses riscos e proteger as informações pessoais.

8.2 Antes de ser introduzida qualquer tecnologia nova, o gestor responsável deve entrar em contacto com o Departamento de Tecnologias da Informação, de modo a realizar-se uma DPIA.

8.3 Durante a realização de qualquer DPIA, a Empresa irá procurar aconselhamento e os pontos de vista de quaisquer outras partes interessadas relevantes.

9 Documentação e registos

9.1 A Exide irá conservar registos escritos de atividades de processamento, incluindo:

9.1.1 o nome e os detalhes da entidade legal da Exide (e, quando aplicável, de outros

controladores);

9.1.2 os objetivos do processamento;

9.1.3 uma descrição das categorias dos sujeitos de dados e das categorias de dados pessoais;

9.1.4 categorias de recetores de dados pessoais;

9.1.5 quando relevante, detalhes de transferências para países terceiros, incluindo a documentação das salvaguardas do mecanismo de transferência existentes;

9.1.6 quando possível, calendários de retenção; e

9.1.7 quando possível, uma descrição de medidas de segurança técnicas e organizacionais.

9.2 Como parte do nosso registo de atividades de processamento, documentamos, ou fornecemos ligação a documentação, sobre:

9.2.1 informações necessárias para avisos de privacidade;

9.2.2 registos de consentimentos;

9.2.3 contratos de controlador-processador;

9.2.4 a localização das informações pessoais;

9.2.5 as DPIA; e

9.2.6 registos de violação de dados.

9.3 Se processarmos informações pessoais sensíveis ou informações de registos criminais, conservaremos registos escritos:

9.3.1 dos objetivos relevantes do processamento, incluindo (quando necessário) o motivo pelo qual é necessário;

9.3.2 da base legal para o nosso processamento; e

9.3.3 se retemos ou eliminamos as informações pessoais em conformidade com o nosso documento de política e, se não for o caso, os motivos para não seguir a nossa política.

9.4 Iremos realizar revisões regulares das informações pessoais que processamos e atualizar a nossa

documentação em conformidade.

10 Direitos dos sujeitos de dados

10.1 Os sujeitos de dados têm os seguintes direitos em relação às suas informações pessoais:

10.1.1 a serem informados sobre a forma, o motivo e a base nos quais as informações são processadas—consulte o *[aviso de privacidade da proteção de dados] da Exide;*

10.1.2 a obterem a confirmação de que as suas informações estão a ser processadas e a obterem acesso às mesmas e a determinadas outras informações, efetuando uma solicitação de acesso do sujeito;

10.1.3 a correção dos dados se estiverem imprecisos ou incompletos;

10.1.4 a eliminação dos dados se já não forem necessários para a finalidade para a qual foram recolhidos/processados, ou se não existirem motivos legítimos superiores para o processamento (isto é, por vezes, conhecido como "o direito ao esquecimento");

10.1.5 restringir o processamento das informações pessoais se a precisão das informações for contestada, ou o processamento for ilegal; e

10.1.6 restringir o processamento das informações pessoais temporariamente onde julgue serem imprecisas, ou onde apresentaram objeções ao processamento;

10.1.7 onde for exigido por lei definir orientações para a retenção, eliminação e

comunicação dos seus dados pessoais após a morte.

11 Obrigações dos sujeitos de dados

11.1 Os indivíduos são responsáveis por ajudar a Exide a manter as suas informações pessoais atualizadas. Poderá ter acesso às informações pessoais de outros funcionários, fornecedores e clientes no decorrer do seu contrato de trabalho ou participação. Se tal for o caso, a Empresa espera o seu auxílio para cumprir as obrigações de proteção de dados a esses sujeitos de dados. Se tiver acesso a informações pessoais, deve:

11.1.1 aceder apenas a informações pessoais às quais tem autorização de acesso, e apenas para fins autorizados;

11.1.2 permitir o acesso a outro pessoal da Exide a informações pessoais apenas se este possuir uma autorização apropriada;

11.1.3 permitir o acesso a outro pessoal que não pertença à Empresa a informações pessoais apenas se tiver autoridade específica para o fazer dos Recursos Humanos ou os Departamentos jurídicos;

11.1.4 manter as informações pessoais em segurança (por ex., cumprir as regras de acesso a instalações, acesso aos computadores, proteção de palavras-passe e armazenamento e destruição seguras de ficheiros e outras precauções definidas na Política de Segurança de Informações Globais da Empresa);

11.1.5 não remover informações pessoais ou dispositivos que contenham informações pessoais (ou que podem ser utilizados para aceder às mesmas), das instalações da Empresa a não ser que sejam tomadas medidas de segurança adequadas (tais como a pseudonimização, encriptação ou proteção por palavra-passe) para proteger as informações e o dispositivo; e

11.1.6 não armazenar informações pessoais em discos locais ou em dispositivos pessoais que são utilizados para fins profissionais.

11.2 Deve contactar o Departamento de Recursos Humanos ou o Departamento jurídico se suspeitar que ocorreu, está a ocorrer ou é provável que ocorra uma das seguintes situações:

11.2.1 processamento de dados pessoais sem uma base legal para o processamento ou, no caso de informações pessoais sensíveis;

11.2.2 qualquer violação de dados como definido no parágrafo 15.1 abaixo;

11.2.3 acesso a informações pessoais sem a autorização adequada;

11.2.4 informações pessoais não conservadas ou eliminadas em segurança;

11.2.5 remoção de informações pessoais, ou dispositivos que contenham informações pessoais (ou que podem ser utilizados para aceder às mesmas) das instalações da Empresa sem tomar medidas de segurança adequadas;

11.2.6 qualquer outra violação desta política ou de qualquer um dos princípios de proteção de dados definidos no parágrafo 4.1 acima.

12 Acesso dos sujeitos de dados

12.1 Um sujeito de dados pode fazer um pedido ("SAR") a qualquer momento para saber mais sobre os dados pessoais que a Empresa conserva sobre o mesmo. Normalmente, a Empresa deve responder aos SAR até um mês após a receção (este prazo pode ser alargado até dois meses em caso de pedidos complexos e/ou numerosos e, nesses casos, o sujeito de dados deve ser informado da necessidade de extensão).

12.2 Todos os pedidos de acesso do sujeito recebidos devem ser reencaminhados para o Correspondente de RGPD local.

12.3 A Empresa não cobra uma taxa pelo processamento dos SAR normais. A Exide reserva-se o direito de cobrar taxas razoáveis para cópias adicionais de informações que já tenham sido dadas a um sujeito de dados, ou para pedidos manifestamente infundados ou excessivos, particularmente se esses pedidos são repetitivos.

13 Segurança de informações

13.1 A Empresa irá utilizar as medidas técnicas e organizacionais apropriadas para manter as informações pessoais seguras e, em particular, para proteger contra processamento não autorizado e ilícito e contra perda, destruição ou danos acidentais. Estas podem incluir:

13.1.1 certificar-se que, onde possível, as informações pessoais são pseudonimizadas ou encriptadas;

13.1.2 garantir a continuidade de confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de processamento;

13.1.3 garantir que, caso ocorra um incidente físico ou técnico, a disponibilidade e o acesso às informações pessoais podem ser restaurados rapidamente; e

13.1.4 um processo para testar, avaliar e examinar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento.

13.2 Nas situações em que a Empresa utilizar organizações externas para processar as informações pessoais em seu nome, é necessário implementar medidas de segurança adicionais para salvaguardar a segurança das informações pessoais. Em particular, os contratos com organizações externas devem estipular que:

13.2.1 a organização pode agir apenas sob as instruções escritas da Exide;

13.2.2 quem efetuar o processamento dos dados está sujeito a um dever de confidencialidade;

13.2.3 são tomadas medidas apropriadas para garantir a segurança do processamento;

13.2.4 os subcontratantes apenas estão envolvidos com o consentimento prévio da Exide e ao abrigo de um contrato por escrito;

13.2.5 a organização irá auxiliar a Exide a disponibilizar o acesso do sujeito e a permitir que os sujeitos de dados exerçam os seus dados em relação a proteção de dados;

13.2.6 a organização irá auxiliar a Exide a cumprir as suas obrigações em relação à segurança do processamento, à notificação de violações de dados e às avaliações de impacto de proteção de dados;

13.2.7 a organização irá eliminar ou devolver todas as informações pessoais à Exide como solicitado no fim do contrato;

13.2.8 a organização irá submeter-se a auditorias e inspeções, fornecer à Exide quaisquer informações que a Empresa necessite para assegurar que tanto a Exide como a organização cumprem as suas obrigações de proteção de dados; e

13.2.9 a organização irá notificar a Exide de imediato se lhe for pedido algo que infrinja a lei da proteção de dados.

13.3 Antes de efetuar qualquer novo acordo que envolva o processamento de informações pessoais por uma organização externa, ou alterar um acordo já existente, o pessoal relevante deve pedir a aprovação dos seus termos pelo Departamento jurídico da Exide.

14 Armazenamento e retenção de informações pessoais

14.1 As informações pessoais (e informações pessoais sensíveis) serão conservadas em segurança em conformidade com a Política de Segurança de Informações Globais da Empresa.

14.2 As informações pessoais (e informações pessoais sensíveis) não devem ser retidas mais tempo do que o necessário. O período de tempo em que os dados devem ser retidos irá depender das circunstâncias, incluindo os motivos pelos quais as informações pessoais foram obtidas. Os funcionários devem seguir a Política de Retenção de Registos da Empresa que define o período de retenção relevante ou os critérios que devem ser utilizados para determinar o período de retenção. Se existirem quaisquer dúvidas, o pessoal deve consultar o Correspondente de RGPD local ou o Departamento jurídico.

15 Violações de dados

15.1 Uma violação de dados pode ter várias formas diferentes, como por exemplo:

15.1.1 perda ou roubo de dados ou equipamento no qual estejam armazenadas informações pessoais;

15.1.2 acesso não autorizado ou utilização de informações pessoais quer por um membro do pessoal ou por terceiros;

15.1.3 perda de dados resultante de uma falha num equipamento ou sistema (incluindo hardware e software);

15.1.4 erro humano, tal como eliminação ou alteração acidental de dados;

15.1.5 circunstâncias imprevistas, tais como incêndio ou cheias;

15.1.6 ataques deliberados a sistemas de TI, tais como pirataria, vírus ou phishing; e

15.1.7 se as informações forem obtidas enganando a organização que as armazena.

15.2 A Empresa irá:

15.2.1 comunicar o relatório necessário de violação de dados à Autoridade de supervisão ou Information Commissioner's Office (UK) sem atraso injustificado e, quando possível, dentro de 72 horas após tomar conhecimento da ocorrência, se for provável que resulte num risco aos direitos e liberdades dos sujeitos de dados; e

15.2.2 notificar os sujeitos de dados afetados se houver a possibilidade de uma violação de dados resultar num alto risco para os seus direitos e liberdades e a legislação obriga a que sejam notificados.

16 Transferências internacionais

16.1 A Empresa poderá transferir informações para fora do Espaço Económico Europeu (EEE) (que inclui os países da União Europeia e a Islândia, o Liechtenstein e a Noruega) para a empresa-mãe da Empresa, a Exide Technologies nos Estados Unidos da América sob a base em que a Exide Technologies é designada como detentora de cláusulas padrão de proteção de dados**.**

17 Formação

A Empresa irá certificar-se de que o pessoal tem a formação adequada em relação às suas responsabilidades de proteção de dados. Os indivíduos cujas funções requerem acesso regular a informações pessoais ou que são responsáveis pela implementação desta política ou de responder a pedidos de acesso dos sujeitos ao abrigo desta política, receberão formação adicional para ajudá-los a compreender as suas obrigações e como cumpri-las.

18 Consequências do incumprimento

18.1 A Empresa dá extrema importância ao cumprimento desta política. O incumprimento desta política:

18.1.1 põe em risco os sujeitos de dados cujas informações pessoais estão em processamento; e

18.1.2 apresenta o risco de sanções civis e criminais significativas para o indivíduo e para a Empresa; e

18.1.3 pode, nalgumas circunstâncias, ser considerada uma ofensa criminal para o indivíduo.

18.2 Devido à importância desta política, o incumprimento por parte de um funcionário em cumprir qualquer exigência da mesma, poderá levar a uma ação disciplinar sob os nossos procedimentos, e esta ação pode resultar em despedimento por conduta grave. Se se tratar de uma pessoa que não seja um funcionário, poderá ver o seu contrato terminado com efeito imediato.

18.3 Se tiver alguma questão ou preocupação em relação a algo nesta política, não hesite em contactar o Representante do país da RGPD ou o Departamento jurídico.