VIGENT

Prospering Together

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

A - TRATAMENTO DE DADOS PESSOAIS – ÁREAS FUNCIONAIS

I – Recursos Humanos

II – Clientes e Fornecedores

III – Canal de Denúncias

B – RESPONSÁVEL PELO TRATAMENTO DE DADOS

1. Responsável pelo Tratamento de Dados

i) Comissão – Engenharia e Proteção do Aço
ii) Comissão – Produtos do Mar

1.1. Auditorias

1.2. Avaliação do Impacto de Proteção de Dados (AIPD)

1.3. Formação do Responsável pelo Tratamento de Dados e Comissões

C – EXERCÍCIO DOS DIREITOS DO TITULAR DE DADOS

1. Direitos do Titular de Dados

1.1 Direito de acesso

1.2. Direito de retificação

1.3. Direito ao apagamento

1.4. Direito à limitação de tratamento

1.5. Direito à portabilidade dos dados

1.6. Direito de oposição de tratamento

2. Exercício dos Direitos

D – PROCEDIMENTO EM CASO DE VIOLAÇÃO (“BREACH”)

E – ANEXOS:

- Regulamento (EU) 2016/697 do Parlamento Europeu e do Conselho de 27 de abril de 2016;
- Lei n.º 58/2019, de 8 de agosto;
- Lei n.º 93/2021, de 20 de dezembro.

I – RECURSOS HUMANOS

1. Recrutamento e Seleção

1.1. Candidaturas

Os candidatos podem submeter as suas candidaturas:

a) Diretamente no site do Grupo;

b) Via comunicação eletrónica para o *email*: recrutamento@vigent.pt

c) Pessoalmente, nas instalações do VigentGroup, mediante preenchimento da Fica de Inscrição.

1.2. Arquivo dos Currículos dos Candidatos

- Os currículos e/ou fichas de inscrição são reencaminhados para uma pasta digital no servidor central do VigentGroup – designada por pasta "**M**", à qual apenas tem acesso a equipa de recrutamento, seleção e admissão do Departamento de Recursos Humanos.
- São guardados pelo prazo de 2 (dois) anos, e destruídos automaticamente pelo sistema informático quando atingido aquele limite temporal.
- Para efeitos de monitorização do prazo de arquivo dos documentos, o software diariamente calcula o tempo de aquivo

dos currículos e, por sua vez, de modo automático procede ao seu *delete*.

1.3. Entrevistas

Em fase de entrevista não é solicitado qualquer documento adicional ao candidato.

Os candidatos, têm direito a igualdade de oportunidades e de tratamento no que se refere ao acesso ao emprego. O VigentGroup respeita esses direitos, desde logo não permitindo aos seus colaboradores/recrutadores, qualquer prática suscetível de privilegiar, beneficiar, prejudicar, privar de qualquer direito ou isentar de qualquer dever em razão, nomeadamente, de ascendência, idade, sexo, orientação sexual, estado civil, situação familiar, situação económica, instrução, origem ou condição social, património genético, capacidade de trabalho reduzida, deficiência, doença crónica, nacionalidade, origem étnica ou raça, território de origem, língua, religião, convicções políticas ou ideológicas e filiação sindical.

1.4. Seleção

1ª Fase – são selecionados entre dois a três candidatos pela equipa de recrutamento e seleção, cujos currículos, depois de anonimizados, são enviados para o responsável funcional.

Neste momento, o VigentGroup, encontra-se a diligenciar no sentido de adquirir um software que permita a anonimização efetiva dos currículos. Assim, nesta fase de transição, todos os responsáveis funcionais, subscreveram declaração de confidencialidade de onde resulta o seu conhecimento expresso da obrigação de cumprimento do R.G.P.D., bem com das consequências, nomeadamente pessoais em termos de

responsabilidade civil e criminal emergentes da violação do mesmo, bem como a obrigação de fazer prova de destruição dos restantes currículos. (*Mod.RGPD1_V1*).

2ª Fase – selecionado o candidato e com a aceitação da proposta apresentada pela empresa, é-lhe solicitada a documentação/informação necessária à sua admissão, bem como, à execução do contrato de trabalho. A saber:

- Preenchimento do Registo de Entrega de Documentos.
- Cartão de cidadão.
- Fotografia tipo passe.
- Certificado de habilitações.
- Preenchimento da declaração - Art.º 99º do Código do IRS;
- Declaração Bancária com identificação dos dados para pagamento da retribuição.

1.5. Medicina no Trabalho

A Lei n.º 102/2009 de 10 de setembro e suas alterações, introduzidas pela Lei n.º 42/2012, de 28 de agosto e pela Lei n.º 3/2014, de 28 de janeiro regulamentam o regime jurídico da promoção e prevenção da segurança e da saúde no trabalho, estabelecendo a obrigatoriedade dos empregadores organizarem as atividades de Segurança e Saúde no Trabalho, cabendo ao empregador a responsabilidade de assegurar aos trabalhadores as condições necessárias à prevenção e promoção da saúde em todos os aspetos relacionados com o trabalho. Neste sentido e, em cumprimento das obrigações legais impostas pelos diplomas acabados de citar, o VigentGroup dispõe de serviços médicos internos.

Porém, os dados recolhidos nos testes e exames médicos, e seu respetivo arquivo, efetuados em cumprimento da legislação relativa à segurança e saúde no trabalho são do acesso exclusivo do médico responsável. A entidade empregadora, que integra o universo do VigentGroup apenas tem acesso à declaração médica de onde resulta se o trabalhador está *apto* ou *não apto* a desempenhar as suas funções laborais.

1.6. Tratamento de Dados Biométricos

O recurso ao sistema biométrico tem vindo a apresentar-se como um meio tecnológico que visa substituir ou reforçar a segurança dos meios tradicionais de controlo de entradas e saídas, sendo ainda de extrema utilidade quando se pretende – por razões de segurança ou de segredo – restringir, nomeadamente, o acesso a locais cuja entrada é exceção para alguns.

Assim, em linha com as evoluções tecnológicas nestas matérias e em consequência da dimensão e dispersão geográfica das empresas do VigentGroup, foram implementados sistemas de controlo de assiduidade e acessos através da recolha de dados biométricos. Sistemas esses que se encontram legalmente autorizados pela entidade competente para o efeito – Comissão Nacional de Proteção de Dados (CNPD), nomeadamente através das autorizações n.ºs: 7480/2011; 9404/2013; 9091/2015; 9153/2015; 2399/2016; 11043/2016; 5992/2017 e 4172/2018.

1.7. Arquivo dos dados/documentos de Ex-Trabalhadores

Cessado, por qualquer razão o vínculo com um trabalhador, o VigentGroup procede ao arquivo dos seguintes documentos: contrato de trabalho; apólices de Seguros de Acidentes de Trabalho e doenças profissionais; formação profissional; documentos contabilísticos e fiscais.

O procedimento de arquivo é observado por duas vias distintas:

a) *Os documentos em suporte digital* ficam arquivados numa pasta digital especifica no servidor central do VigentGroup, denominada por pasta "M:\ARQUIVO_DRH\CESSAÇÕES CONTRATOS TRABALHO", à qual apenas têm acesso a equipa do Departamento de Recursos Humanos;

b) *Os documentos em suporte papel* ficam arquivados fisicamente no denominado "arquivo morto" sito nas instalações industriais denominada por METALOGAVA 3, sitas no lugar do Bicho, união das freguesias de Bougado e Santiago, concelho da Trofa, em espaço de acesso fechado e com acesso limitado em exclusivo à equipa do Departamento de Recursos.

Os documentos são arquivados pelo prazo de 10 (dez) anos, e destruídos da seguinte forma:

a) *os digitais* – são automaticamente destruídos pelo software quando registado o limite do prazo de arquivo. Para efeitos de monitorização do prazo de arquivo dos documentos, o software diariamente calcula o tempo decorrido de arquivo dos documentos e, por sua vez, procede à destruição automática dos mesmos.

b) *em suporte papel* – são destruídas, anualmente, todas as pastas contendo documentos contratuais de âmbito laboral, cuja cessação tenha ocorrido há mais de 10 anos.

II – CLIENTES e FORNECEDORES

Com a implementação do RGPD, e com vista ao seu cumprimento, o VigentGroup reviu as cláusulas contratuais gerais.

Os dados recolhidos de Clientes e Fornecedores são os dados exclusivamente necessários para a execução dos contratos e/ou prestação de serviços.

Porém, todas as minutas contratuais, previamente existentes, foram revistas de modo a dar cumprimento às imposições resultantes do RGPD.

Em caso algum, são recolhidos de Clientes ou Fornecedores dados categorizados como sensíveis para efeitos de RGPD.

III – CANAL DE DENÚNCIAS

A Diretiva 2019/1937, foi transposta para o ordenamento jurídico português, através da Lei n.º 93/2021, de 20 de dezembro, que entrou em vigor a 20 de junho de 2022.

Estabelece o regime geral de proteção de denunciantes de infrações, transpondo a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União.

As entidades obrigadas a deter o referido canal devem garantia o anonimato das denúncias, e por seu turno a proteção da privacidade e dos dados pessoais inerentes às mesmas.

Assim, o VigentGroup no estrito cumprimento das obrigações legais decorrentes da Lei n.º 93/2021, de 10 de dezembro (Regime Geral de Proteção de Denunciantes de Infrações) e do Decreto-Lei n.º 109-E/2021, de 9 de dezembro (Regime Geral de Prevenção da Corrupção),

procederá ao tratamento de alguns dos seus dados pessoais, nomeadamente, dados identificativos e dados de contacto, bem como qualquer outra informação que o denunciante considere pertinente fornecer, para efeitos de receção e seguimento da/s denúncia/s que apresente.

Os dados serão conservados pelo prazo legal de 5 (cinco) anos e, independentemente desse prazo, durante a pendência de processos judiciais ou administrativos referentes à/s denúncia/s.

Os dados pessoais poderão ser transmitidos a terceiros (Subcontratantes) cuja participação se revele indispensável para assegurar o regular funcionamento deste canal ou o adequado tratamento das denúncias apresentadas.

Sempre que estes terceiros procedam ao tratamento dos dados pessoais, em nosso nome e por nossa conta, garantimos o mesmo nível de segurança, confidencialidade e privacidade no referido tratamento.

O VigenGroup poderá ter de transmitir alguns dos dados pessoais às Autoridades Competentes, por imposição legal e/ou judicial.

B RESPONSÁVEL PELOS DADOS

Política de Protecção de Dados Pessoais

1. A Organização deve orientar-se pelo princípio de *accountability*. Assim, o VigentGroup, nomeadamente através da sua participada *VIGENTGROUP SERVIÇOS CORPORATIVOS UNIPESSOAL LDA*, enquanto entidade responsável pelo tratamento dos dados pessoais do Grupo, implementou mecanismos internos para se certificar do cumprimento corporativo do RGPD, desde logo, pela criação de duas comissões de avaliação de risco para promoção de auditorias e avaliações de impacto (AIPD) para cada uma das áreas de negócio do Grupo: Produtos do Mar e Engenharia e Proteção do aço.

i. *Comissão de Auditoria – Produtos do Mar;*

ii. *Comissão de Auditoria – Engenharia e Proteção do Aço*

1.1 Auditorias

Caberá às comissões designadas para o efeito, sempre que necessário, a realização de auditorias com o objetivo de garantir que:

1º os dados pessoais são legítimos e limitados na sua recolha ao que é estritamente necessário;

2º os dados estão atualizados, seguros e confidenciais;

3º o VigentGroup tem políticas, procedimentos, códigos de conduta e instruções internas formalizados e implementados, suscetíveis de serem disponibilizados para efeitos de auditoria às entidades de supervisão;

4º o VigentGroup adotou sistemas de monitorização do cumprimento das políticas e procedimentos adotados nestas matérias.

1.2 Avaliação do Impacto de Proteção de Dados (AIPD)

Serão realizadas **AIDP** nos seguintes casos:

1º tratamento de dados com elevada probabilidade de risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades;

2º tratamento de dados que implique um elevado risco para os direitos e liberdades dos titulares desses dados, em especial quando os procedimentos internos adotados dificultem aos titulares o exercício dos seus direitos;

3º tratamento de dados que visa a tomada de decisões relativas a determinadas pessoas singulares na sequência de qualquer avaliação sistemática e completa dos seus aspetos pessoais, nomeadamente baseada na definição de perfis; na sequência do tratamento de categorias especiais de dados pessoais, biométricos e/ou sobre condenações penais, infrações e/ou medidas de segurança conexas;

4º violação de dados (“Data Breach”)

1.3 Formação dos Responsáveis pelo Tratamento de Dados e Comissões

O VigentGroup assegura que a entidade Responsável pelo Tratamento de Dados e comissões de auditoria têm formação adequada para o efeito.

1. Direitos do Titular de Dados

O RGPD confere aos titulares de dados pessoais, objeto de tratamento, um conjunto de direitos que devem ser salvaguardados pelo responsável pelo tratamento de dados.

1.1Direito de acesso/informação

Os titulares de dados têm direito:

- de saber se estão, ou não, a ser tratados dados pessoais que lhe digam respeito;
- se os dados foram transmitidos para outra entidade ou o destino que lhes foi dado;
- aceder aos seus dados e a todas as informações respeitantes às respetivas operações de tratamento.

1.2Direito de retificação

É assegurado aos titulares dos dados o direito a obterem a retificação dos seus dados pessoais que estejam desatualizados, incorretos e/ou incompletos.

Sempre que o organismo responsável pelo tratamento dos dados seja uma entidade pública, este direito é, simultaneamente, um dever por parte do administrador de manter atualizados os dados que lhe digam respeito.

1.3Direito ao apagamento ("o direito a ser esquecido")

Uma das grandes novidades do RGPD reside neste direito, também referido como "direito a ser esquecido", que confere aos titulares dos dados o direito de solicitar ao responsável pelo tratamento dos dados o apagamento dos seus dados.

Garante-se, assim, aos titulares dos dados, dentro das limitações estabelecidas por lei, o direito de obter a eliminação dos seus dados pessoais, desde que:

- Os dados se revelem desnecessários para as finalidades para as quais foram recolhidos ou tratados;
- O titular retire o seu consentimento, quando o tratamento for necessariamente fundamentado neste e não exista outro fundamento legal parta o tratamento dos dados;
- O titular se oponha ao tratamento de dados pessoais utlizados para fins automatizados e/ou de *profiling*;
- Quando os dados pessoais tenham sido tratados de forma ilícita.

Limitações a este direito:

- Conservação dos dados por razões de interesse público, segurança nacional, de faturação, comerciais, fiscais ou outros;
- Durante a vigência de um contrato, os necessários a sua execução.

1.4Direito à limitação de tratamento

Em paralelo ao direito ao apagamento, o legislador introduziu o direito à limitação do tratamento ao prever que o titular dos dados tem o direito de exigir a limitação do tratamento nas seguintes situações:

- Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
- O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

- O responsável pelo tratamento deixar de precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
- Se se tiver oposto ao tratamento até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

1.5Direito à portabilidade dos dados

Outra novidade introduzida pelo RGPD consiste no reconhecimento do direito de portabilidade dos dados, sendo conferido aos titulares o direito a solicitarem ao responsável pelo seu tratamento, os seus dados pessoais, num formato de uso comum e mesmo a sua transferência para outro responsável pelo tratamento.

Todavia, o titular dos seus dados apenas poderá exigir que os seus dados sejam entregues a outro responsável pelo tratamento quando tal for tecnicamente possível. Esse direito encontra-se limitado aos casos em que o tratamento é efetuado por meios automatizados e depende do consentimento do titular da execução de um contrato.

1.6Direito de oposição de tratamento

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito que tenham por base interesses legítimos ou interesse público, incluindo a definição de perfis com base nessas disposições.

Perante a oposição do titular dos dados, o responsável pelo tratamento deve cessar o tratamento destes, a menos que apresente razões imperiosas e legitimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

2. Como pode o titular de dados exercer estes direitos?

a) Devem enviar um email para dataprotection@vigent.pt e/ou reportar diretamente às autoridades responsáveis – Comissão Nacional de Proteção de Dados através do endereço geral@cnpd.pt ;

b) O direito de acesso às informações pessoais dos Colaboradores do VigentGroup poderá ser exercido presencialmente junto do Departamento de Recursos Humanos. A retificação e/ou atualização dos dados poderá ser solicitada junto do mesmo departamento, ou por qualquer meio escrito, incluindo correio eletrónico para o endereço dataprotection@vigent.pt .

c) O responsável pelo tratamento deve responder o mais rapidamente possível, tendo no máximo 30 dias para o fazer. Na eventualidade de precisar de estender o prazo para além do período de 30 dias, o responsável deverá informar o titular dos dados dos fundamentos para a prorrogação;

d) O responsável deve responder de forma clara, concisa e suficiente. Em caso de indeferimento da pretensão do titular, o responsável pelo tratamento deve comunicar as razões que sustentam a decisão e informar da possibilidade de recorrer da decisão junto da entidade de controlo ou das instâncias jurisdicionais;

e) O responsável não pode exigir nenhum pagamento para a satisfação da pretensão do titular, podendo apenas, e no caso de pedidos excessivos, exigir o pagamento de uma taxa que visa suportar os encargos administrativos.

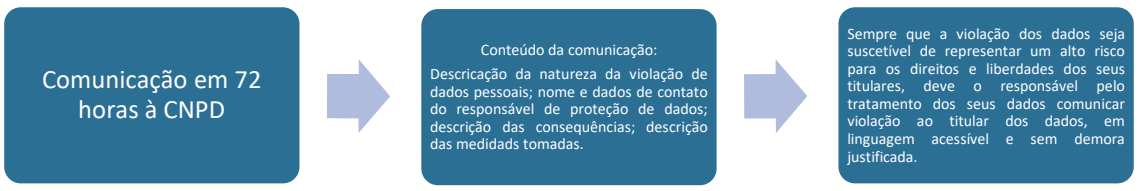
O que é uma violação de dados pessoais?

"[…] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento» - **artigo 4.º n.º 12 RGPD.**

Um dos requisitos do RGPD é que, através da adoção de medidas técnicas e organizativas adequadas, os dados pessoais sejam tratados, por forma a garantir a segurança adequada dos mesmos, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

Por conseguinte, um elemento fundamental de qualquer política em matéria de segurança de dados é conseguir, sempre que possível, prevenir uma violação e, quando esta aconteça, dar uma resposta em tempo útil.

Registada qualquer violação de dados, o responsável pelo tratamento de dados, dará cumprimento ao seguinte procedimento:



ANEXOS

Política de Protecção de Dados Pessoais

- Regulamento (EU) 2016/697 do Parlamento Europeu e do Conselho de 27 de abril de 2016;
- Lei n.º 58/2019, de 8 de agosto;
- Lei n.º 93/2021, de 20 de dezembro.


VIGENT
Prospering Together