Associação Empresarial da Região de Viseu

newsletter

Viseu, 15 de maio de 2018

LEGISLAÇÃO

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

ENTRA JÁ EM VIGOR NO DIA 25 DE MAIO

Relembramos todos os nossos Associados que o RGPD (Regulamento Geral da Proteção de Dados - Regulamento (UE) 2016/79 do Parlamento Europeu e do Conselho, de 27 de abril de 2016) entra já em vigor no próximo dia **25 de maio de 2018**.
Apesar de ainda não existir no nosso País uma Lei sobre pontos específicos deste Regulamento, a verdade é que este entrará mesmo em vigor, pois não necessita de transposição.
Abordaremos de forma sumária os principais conceitos e efetuamos algumas sugestões para a aplicação do RGPD nas empresas.

A MINHA EMPRESA ESTÁ SUJEITA À APLICAÇÃO DO RGPD?
Estão sujeitas ao RGPD, todas as empresas (pessoas singulares ou coletivas) que realizem operações de tratamento de dados pessoais.
O RGPD também se aplica ao subcontratante (ex. contabilistas, revisores oficiais de contas, advogados, etc…) que trate dados pessoais por conta da empresa (ex. quando o contabilista processa os salários dos funcionários da empresa).
Neste caso, as empresas devem efetuar com os seus subcontratantes, um contrato de confidencialidade no âmbito da proteção dos dados pessoais.
O RGPD também se aplica às PME, pois a sua aplicação não depende da dimensão da empresa, mas sim do facto de esta tratar dados pessoais.
Se a empresa se situar dentro da União Europeia, o tratamento de dados pessoais está sujeito ao RGPD, independentemente de o tratamento ocorrer dentro ou fora da União Europeia.
No entanto, ainda que a empresa se situe fora da União Europeia, aplica-se o RGPD sempre que os titulares dos dados pessoais se encontrem na União Europeia e o tratamento esteja relacionado com:

- **Oferta de bens ou serviços aos residentes na UE.**
Ex: A existência de um mero site ou endereço eletrónico de uma empresa não é suficiente para determinar a aplicação do RGPD. No entanto, se no site é usada uma das línguas ou uma moeda de uso corrente na UE, revela que o titular do site pode pretender oferecer serviços ou produtos a um residente da UE e por isso está sujeito ao RGPD.

- Controlo do comportamento de residentes na UE.
Face ao referido, é praticamente impossível que uma empresa não esteja sujeita ao RGPD, pois basta ter funcionários ou emitir faturas a uma pessoa singular para que tal aconteça.

O QUE SÃO DADOS PESSOAIS?
São todas as informações relativas a uma **PESSOA SINGULAR** identificada ou identificável (titular dos dados).
Considera-se que é identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, designadamente: nome, morada, outras formas de localização, número de cartão de cidadão, número de contribuinte, número de utente dos serviços de saúde, número de identificação da segurança social, número de passaporte, situação familiar, hábitos de consumo, identificadores por via eletrónica, IP, som, imagem, elementos da identidade física, fisiológica, genética, mental, económica, cultural ou social, rendimento, entre outros.

Quando existir alguma dúvida se um dado é ou não pessoal deve consultar-se a CNPD (Comissão Nacional de Proteção de Dados) que é a autoridade de controlo em Portugal.

O RGPD só se aplica a pessoas singulares, não se aplicando aos dados das empresas e outras pessoas coletivas. No entanto, as informações respeitantes a empresários em nome individual ou sociedades unipessoais podem constituir dados pessoais, sujeitos à aplicação do RGPD, caso permitam a identificação de uma pessoa singular.

QUAIS SÃO OS DADOS SENSIVEIS?

Dentro dos dados pessoais existe uma categoria mais restrita de dados, a que o RGPD chama dados sensíveis.
São considerados dados sensíveis:
- A origem racial ou étnica;
- As opiniões políticas;
- As convicções religiosas ou filosóficas;
- A filiação sindical.
- Dados genéticos;
- Dados biométricos para identificar a pessoa de forma inequívoca;
- Dados médicos ou relativos à saúde.
- Dados relativos à vida sexual ou orientação sexual.

A Regra é a da proibição de tratamento de dados sensíveis.

O QUE É O TRATAMENTO DE DADOS PESSOAIS?

Considera-se tratamento de dados pessoais qualquer operação ou conjunto de operações, com ou sem recurso a meios automatizados, efetuada sobre dados pessoais, designadamente:
• Recolha de dados;
• Registo de dados;
• Organização de dados;
• Conservação;
• Adaptação ou alteração;
• Recuperação;
• Consulta;
• Utilização;
• Divulgação por qualquer forma de disponibilização dos dados;
• Limitação;
• Comparação ou interconexão;
• Apagamento;
• Destruição (Ex: deitar um papel ao lixo que contenha dados pessoais é considerado uma operação de tratamento de dados pessoais).

QUAIS SÃO AS REGRAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS?

O RGPD impõe um conjunto de princípios que, têm que ser obrigatoriamente observados no processo de tratamento de dados pessoais, e que são os seguintes:

Tratamento lícito, leal e transparente:

Os dados pessoais têm que ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados. Tal significa que este tem que perceber como é que os seus dados pessoais são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento.

Princípio da limitação das finalidades:

Os dados pessoais têm que ser recolhidos para fins determinados, explícitos e legítimos.
É proibido o tratamento de dados para fins diferentes daqueles para que foram recolhidos – Ex: não posso recolher dados para fins publicitários e posteriormente utilizá-los para venda de serviços de formação.
Uma empresa não pode simplesmente recolher dados pessoais para fins indefinidos.

As pessoas cujos dados são recolhidos e vão ser tratados, têm que ser informadas dos fins a que o tratamento se destina.

Princípio da minimização:

Os dados têm que ser adequados, pertinentes e limitados (pedir o menor nº de dados possíveis – Ex: não necessito da morada e do email, tenho que pedir um dos dois) aos que são necessários para os fins para os quais foram recolhidos e vão ser tratados.
A empresa deve recolher e tratar, apenas os dados pessoais que são estritamente necessários para cumprir os fins a que se destinam (ex: tenho uma loja. Se quiser oferecer um desconto no dia ou mês de aniversário dos meus cliente apenas preciso de saber o dia e o mês, pois para aquele fim não é necessário saber o ano do nascimento).

Exatidão:

Os dados têm que ser exatos e estar sempre atualizados.

Limitação da Conservação:

A empresa deve garantir que os dados pessoais são conservados apenas durante o tempo necessário às finalidades para as quais foram recolhidos, tal significa que os dados devem ser conservados durante o mínimo tempo possível
A empresa deve implementar um procedimento de manutenção, arquivo e apagamento dos dados de modo a que estes não sejam conservados durante um período de tempo superior ao necessário.
Na fixação de prazo de conservação ou manutenção dos dados, têm que ser cumpridos prazos legais de conservação de dados (ex: os dados genéticos têm que ser conservados por 40 anos/ os dados biométricos do trabalhador devem ser imediatamente apagados após a sua saída da empresa/ prazos fiscais, antifraude, período de garantia dos produtos e outros).
A empresa tem que estabelecer prazos para o apagamento ou revisão dos dados pessoais que detém.

Segurança, integridade e confidencialidade:

Os dados têm que ser tratados de uma forma que garanta a sua segurança, incluindo a sua proteção contra o seu tratamento não autorizado e contra a sua perda, destruição ou danificação acidental, adotando-se as medidas técnicas e organizativas adequadas.

Só é lícito o tratamento de dados pessoais que cumprem, pelo menos, uma das seguintes condições:

1) Obtenção do consentimento para o tratamento
Um das regras previstas no RGPD é a necessidade de consentimento do titular dos dados pessoais, para que os mesmos sejam tratados.
O consentimento para ser válido, tem que ser:
• Dado de livre vontade;
• Deve ser dado para uma finalidade específica;
• Informado (dos motivos para a recolha e tratamento dos dados);
• Explicito;
Prestado por ato inequívoco (a empresa tem que conseguir demonstrar que o titular dos dados deu o seu consentimento. Pelo que se aconselha a que o consentimento seja sempre dado por escrito. Aconselha-se ainda, que os formulários eletrónicos contenham toda a informação necessária para que se possa obter um consentimento formal).
O consentimento dado antes do dia 25 de maio de 2018 (data em que entra em vigor o RGPD), só é válido se estiver em conformidade com as regras do RGPD. Se assim for não é necessário pedir novo consentimento.
No entanto, alertam-se as empresas para o facto de que devem rever todos os consentimentos que têm, e as datas em que foram pedidos, pois se, por exemplo, forem muito antigos e não foram atualizados, a sua validade é duvidosa.

2)O tratamento dos dados é necessário para a execução de um contrato ou para diligências pré-contratuais
Se o titular dos dados pessoais for parte no contrato ou, se as diligências pré-contratuais forem realizadas a seu pedido, é lícito o tratamento dos seus dados, mas apenas e só para os fins relacionados com o contrato ou com as diligências.

Ex: A empresa vende produtos pela internet. Pode tratar dos dados fornecidos pela pessoa que sejam necessários para lhe vender o produto solicitado, antes de celebrar o contrato e durante a sua execução. Pode efetuar o tratamento do nome, da morada de entrega, do nº de contribuinte, do cartão de crédito, porque está no âmbito de um contrato de compra e venda.

3)O tratamento dos dados é necessário para o cumprimento de uma obrigação legal a que a empresa está sujeita.

Enquadra-se neste caso o envio, por parte da entidade empregadora à seguradora dos dados do trabalhador para efeitos de realização de seguro de acidentes de trabalho, o envio dos dados dos trabalhadores para a Segurança Social, para a Autoridade Tributária ou para os serviços de medicina no trabalho.

Nestes casos a empresa não está a praticar qualquer ato ilícito, porque é obrigada por leia a fornecer os dados pessoais dos seus trabalhadores àquelas entidades.

4)O tratamento é feito para o interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento

Enquadra-se aqui o caso de sermos interpelados pela polícia para efeitos de aplicação de uma multa.

5)O tratamento de dados é necessário para a defesa de interesses vitais do seu titular ou de outra pessoa singular.

É o caso de o titular entrar na urgência do hospital e o médico necessitar dos seus dados para o poder tratar.

6)O tratamento é necessário para efeitos de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial, se for uma criança.

Existe por exemplo um interesse legítimo em transmitir dados pessoais no âmbito de um grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários ou quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas.

As crianças têm uma proteção especial quanto aos seus dados pessoais. É necessário o consentimento do titular das responsabilidades parentais, para o tratamento de dados pessoais de crianças com idade inferior a 16 anos.

COMO SE FAZ O TRATAMENTO DE DADOS SENSIVEIS?

A regra prevista no RGPD é que o tratamento dos dados sensíveis é proibido. No entanto, existem exceções que permitem o tratamento de dados sensíveis, e que são as constantes do seguinte quadro:

EXCEÇÃO	OBSERVAÇÕES
Existe CONSENTIMENTO EXPLICITO pelo titular para o tratamento dos seus dados sensíveis	EX: O trabalhador pede à empresa que lhe retire do salário a quota para o sindicato e a pague.
O tratamento é necessário para efeitos de medicina preventiva ou do trabalho, para avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamento de saúde ou de ação social, ou a gestão de sistemas ou serviços de saúde ou de ação social.	Para a medicina no trabalho não é preciso o consentimento do trabalhador, pois a recolha de dados é feita para o cumprimento de uma obrigação legal a que estão sujeitas as empresas. No entanto, como são dados ligados à saúde, só o médico do trabalho é que pode fazer a recolha e tratamento dos dados. A empresa não o pode fazer. O médico apenas pode informar a empresa se o trabalhador está apto ou não, uma vez que está proibido de revelar dados de saúde ou doenças de que o trabalhador padeça.
Tratamento necessário para efeitos do cumprimento de obrigações e, do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social.	Ex: Processamento de salários, comunicação dos dados à segurança social, atribuição de pensões, etc….
Quando esteja em causa a proteção de interesses vitais do titular	O titular entra na urgência inconsciente, estando por isso incapacitado para dar o consentimento.
Tratamento necessário à declaração, exercício ou à defesa de um direito num processo judicial sempre que os tribunais estejam no exercício da sua função.	
Tratamento necessário por motivos de interesse público importante	O tratamento deve ser proporcional ao objetivo visado, respeitar a proteção de dados pessoais e prever medidas adequadas e específicas que salvaguardem os interesses fundamentais ou os direitos do seu titular.
Tratamento efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais.	Apenas quando o tratamento respeita a membros ou antigos membros do organismo ou, pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos e, desde que os dados pessoais não sejam divulgados a terceiros sem o consentimento do seu titular.
Dados manifestamente tornados públicos pelo titular	Tem que se verificar bem a publicidade dos mesmos.
Tratamento necessário por motivos de interesse público no domínio da saúde pública	Ex: Assegurar um elevado nível na prestação de cuidados de saúde, dos medicamentos, etc…
Tratamento necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos	O tratamento deve ser proporcional ao objetivo visado, respeitar a proteção de dados pessoais e prever medidas adequadas e específicas que salvaguardem os interesses fundamentais ou os direitos do seu titular.

OBRIGAÇÕES DAS EMPRESAS

As empresas são as responsáveis pelo tratamento dos dados. De acordo com o RGPD, a empresa é responsável por cumprir a suas normas e também para demonstrar esse cumprimento. Pelo que, em matéria de implementação do RGPD, devem pautar-se pelo PRINCIPIO DA ACCOUNTABILLITY, nos termos do qual não basta ter a garantia de que não existirá fuga ou violação dos dados pessoais, sendo também indispensável provar, através de evidências, de que cumprem o RGPD, nomeadamente:

•Que os dados pessoais que a empresa possui foram recolhidos de forma legítima;
•Que os dados pessoais estão limitados ao fim para o qual foram recolhidos;
•Que os dados estão atualizados, seguros e são confidenciais;
•Que a empresa tem politicas, procedimentos, códigos de conduta, regulamentos ou outros documentos formais e que possam ser disponibilizados à CNPD (Comissão Nacional de Proteção de dados);
•Que tem sistema para monitorizar se as politicas e procedimentos implementados estão a ser cumpridos;
•Tem um sistema permanente e dinâmico que verifica a conformidade da empresa com o RGPD;
•Efetuar auditorias internas de controlo do cumprimento do RGPD;
•Efetuar o registo de todas as atividades relacionadas com o tratamento de dados pessoais, de modo a que possa demonstrar junto da CNPD que está a cumprir o RGPD. Este Regulamento prevê que as empresas com menos de 250 trabalhadores não estão sujeitas à manutenção do registo. No entanto, uma vez que todas têm que ter provas de que estão a cumprir o RGPD, aconselha-se a que todas efetuem e atualizem os registos da atividade de tratamento de dados pessoais;
•Efetuar o reforço das políticas e procedimentos de segurança de dados;
•Efetuar a notificação da violação dos dados pessoais;

O RGPD prevê que as empresas e outras entidades estão obrigadas a notificar a entidade de controlo (CNPD) de todas as violações de

dados com riscos para o seu titular.
Esta comunicação tem que ser realizada no prazo de 72 horas a contar da deteção da violação.
•Se a empresa tem um subcontratante que efetua tratamento de dados em seu nome (ex: contabilista que processa os salários), tem que efetuar um contrato com este onde especifique quais são os seus deveres perante os dados pessoais que lhe são fornecidos, que só pode tratar estes dados com base em instruções da empresa, quais as medidas técnicas e organizativas que deve adotar para a sua proteção, a fixação de um dever de confidencialidade do subcontratante e de todas as pessoas que com ele colaboram, entre outras.

DIREITOS DOS TITULARES DE DADOS PESSOAIS

DIREITO À INFORMAÇÃO

O RGPD determina que deve ser fornecido aos titulares dos dados pessoais um conjunto de informações tanto nos casos em que os dados são recolhidos diretamente junto do titular, como nos casos em que a recolha não se realize na sua presença (ex. cedência de dados pela internet).

• Quando deve ser dada a informação?

Na recolha direta junto do titular dos dados a informação é dada nesse momento.
No caso de recolha indireta, pode ser no momento da recolha quando esta tenha sido efetuada através do preenchimento de um formulário eletrónico on-line. Nos outros casos tem que se enviar a informação no prazo de 30 dias a contar da receção dos dados.

• Qual a informação a dar?

Tem que ser obrigatoriamente dada a seguinte informação:
a) Identidade e contactos da empresa/responsável pelo tratamento dos dados ou do seu representante.
b) No caso de a recolha ser direta, tem que se dizer se irá existir comunicação de dados a entidades terceiras e, se a mesma constitui ou não uma obrigação legal ou contratual e as consequências do não fornecimento dos dados.
c) Categoriais dos dados pessoais.
d) Quais são os fins a que se destinam os dados.
e) Prazo de conservação dos dados.
f) A existência do direito de acesso, retificação, apagamento e limitação do tratamento.
g) A existência do direito de se opor ao tratamento.
h) Se o tratamento dos dados se basear no consentimento do seu titular, tem que se informar que este pode retirar o consentimento a qualquer momento.
i) A existência do direito de não sujeição a decisões automatizadas, incluindo a definição de perfis.
j) O direito à portabilidade dos dados.
k) O direito ao conhecimento da existência de uma violação de dados.
l) O direito a reclamar para CNPD.
m) No caso de a recolha ser indireta, além disto é necessário informar quais são as categorias de dados que vão ser recolhidos e as fontes dos dados.

• Como deve ser dada a informação:

Estas informações podem ser dadas por escrito ou oralmente.
A informação deve ser dada de forma concisa, clara, transparente e precisa.
No entanto, como a empresa tem que comprovar que prestou a informação, aconselha-se a que a mesma seja sempre dada por escrito, existindo sempre um documento que comprove que o titular dos dados foi informado.

DIREITO DE ACESSO

Os titulares dos dados têm o direito de saber se os seus dados pessoais estão ou não a ser tratados, se foram transmitidos para outras entidades, qual o destino que lhe foi dado, bem como aceder aos seus dados e a todas as informações respeitantes às atividades de tratamento.
Este direito de acesso deve ser tendencialmente gratuito, não obstante poder ser criada uma taxa para permitir tal acesso no caso de pedidos infundados ou excessivos.

DIREITO DE RETIFICAÇÃO

Os titulares dos dados têm direito a obterem a retificação dos mesmos sempre que estejam desatualizados, incorretos ou incompletos.

DIREITO AO APAGAMENTO

Este direito é uma das grandes novidades do RGPD, e também é referido como o “direito a ser esquecido”.
O mesmo confere ao titular dos dados pessoais o direito a solicitar às empresas/responsáveis pelo tratamento o pagamento dos seus

dados.
Assim, os titulares dos dados pessoais têm o direito a obter a sua eliminação, mas desde que:
• Os dados sejam desnecessários para as finalidades para as quais foram recolhidos e tratados;
• O titular retire o seu consentimento, quando o tratamento for fundamentado neste e não exista outro fundamento legal para o tratamento de dados;
• O titular se oponha ao tratamento de dados pessoais utilizados para fins automatizados;
• Quando os dados pessoais tenham sido tratados de forma ilícita.
Por exemplo, não se podem apagar dados que a empresa esteja legalmente obrigada a conservar.

DIREITO À LIMITAÇÃO DO TRATAMENTO
O titular dos dados pessoais 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 mesmos 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.

DIREITO DE PORTABILIDADE DOS DADOS
Esta é outra das novidades introduzidas pelo RGPD e que consiste no facto de o titular dos dados poder solicitar ao responsável pelo tratamento os seus dados pessoais, num formato de uso comum, ou solicitar a sua transferência para outra empresa/responsável pelo tratamento dos dados.
No entanto, o titular dos dados apenas poderá exigir que os seus dados sejam entregues a outro responsável pelo tratamento, quando tal for tecnicamente possível.
Este direito está limitado aos casos em que o tratamento é feito por meios automatizados e depende do consentimento do titular ou da execução de um contrato.

DIREITO DE OPOSIÇÃO E DECISÕES INDIVIDUAIS AUTOMATIZADAS
As decisões individuais exclusivamente automatizadas, ocorrem quando são tomadas decisões sobre a pessoa por meios tecnológicos e sem envolvimento humano. Pode não haver definição de perfis.
O titular dos dados tem o direito de não ser sujeito a este tipo de decisões automatizadas, podendo-se opor, a qualquer momento, ao tratamento dos dados pessoais que lhe respeitem, incluindo a definição de perfis.
Se uma empresa avaliar as suas caraterísticas (ex: idade, altura, sexo, etc.) ou o classificar numa categoria, tal significa que está a definir o seu perfil.

DIREITO A RETIRAR O CONSENTIMENTO
O consentimento deve ser tão fácil de retirar como de dar. Se o titular dos dados retirar o seu consentimento, a empresa fica impedida de efetuar o tratamento de dados e, deve apagá-los rapidamente.
No entanto, não está obrigada a apagar os dados, se a sua conservação for obrigatória por Lei (ex. Imposições da Autoridade Tributária, da Segurança, Social, etc…) ou necessária para a execução de um contrato.
Se o consentimento for dado para tratar dados para vários fins, este pode ser retirado apenas para um desses fins, mantendo-se para os restantes.

Exercício dos direitos e deveres de resposta das empresas
Os titulares dos dados podem exigir o acesso, a retificação, o apagamento, a correção, a portabilidade dos dados ou a oposição ao tratamento através de qualquer forma, pedido escrito, eletrónico ou verbal.
A empresa é obrigada a responder o mais rapidamente possível, tendo o prazo máximo de 30 dias para o fazer.
Na eventualidade de necessitar de mais prazo (pode ir até 3 meses no caso de grande complexidade), tem que o comunicar ao titular dos dados e invocar os fundamentos para a prorrogação.
A empresa deve responder de uma forma clara, concisa e suficiente.
Em caso de indeferimento da pretensão deve comunicar as razões que a fundamentam e informar o titular dos dados que pode apresentar uma reclamação junto da CNPD.

Por último, há que referir que não há limite de prazo para os titulares dos dados poderem exercer quaisquer uns destes direitos.

INCUMPRIMENTO DO RGPD:

O Artigo 83º do RGPD determina que o seu incumprimento está sujeito a aplicação de medidas ou coimas, designadamente, prevê o seguinte:

- Probabilidade de existência de uma infração – Aplicação de uma advertência;
- Infração - Podem ser aplicadas sanções de repreensão, proibição temporária ou definitiva de tratamento de dados ou aplicação de coimas até € 20.000.000,00 de euros ou, no caso das empresas, até 4% do seu volume de negócios.

No entanto, a legislação nacional irá também dispor sobre esta matéria, esperando-se que fixe critérios para determinação objetiva do valor das coimas a aplicar.

SUGESTÕES DE APLICAÇÃO DO RGPD

Passa-se a dar uma indicação e sugestão do que podem e devem fazer neste sentido.

1º PASSO – FAZER UM LEVANTAMENTO/DIAGNÓSTICO DO EXISTENTE:

a) Identificar os meus titulares de dados:

•Trabalhadores;
•Fornecedores que sejam pessoas singulares ou empresários em nome individual;
•Prestadores de serviços
•Clientes, se forem pessoas singulares;
•Formadores;
•Formandos
•Candidatos a emprego. Neste caso e no que respeita aos currículos, há que fazer uma distinção: Quando estes são pedidos pela empresa no âmbito de um processo de recrutamento, os dados pessoais estão sujeitos a tratamento.

Quando são enviados por iniciativa das pessoas e não são pedidos pela empresa, esta pode optar por fazer o tratamento ou não. Aconselha-se a que, por uma questão de salvaguarda, conste sempre no site a expressão " não estamos a recrutar".

•Estagiários;
•Subcontratantes a quem transmito dados (contabilistas, revisores oficiais de contas, advogados, serviços de medicina no trabalho, serviços de higiene e segurança no trabalho, seguradoras, autoridade tributária, segurança social, etc.)
•Outros.

Os dados dos gerentes, administradores ou membros da direção, enquanto estes atuarem nessa qualidade, não estão sujeitos ao RGPD, uma vez que são dados públicos.

b) Verificar se tenho bases de dados, que dados têm, onde estão guardadas e que tem acesso às mesmas.
c) Como foram recolhidos os dados? Tenho dados sensíveis?
d)Que tratamento de dados faço e se o mesmo é ou não licito?
e) Quem tem acesso aos dados?
f) Transmito dados pra terceiros (Ex: contabilistas, medicina no trabalho…)?
g) Que medidas de segurança tenho implementadas para a proteção dos dados?
h)Prestei informações aos titulares dos dados?
i) Os dados foram recolhidos para fins específicos?
j)Tenho os dados necessários para os fins que foram recolhidos ou tenho dados a mais?
k) O meu site cumpre as políticas de privacidade exigidas pelo RGPD?

2º PASSO – IMPLANTAÇÃO DO RGPD

Depois de efetuado o diagnóstico, as empresas devem corrigir o que estiver incorreto e eliminar os dados que não necessitem. De seguida, a melhor forma de implementar o RGPD é através da criação de procedimentos operacionais internos, que estabeleçam os passos, as regras, as questões que cada pessoa da empresa que tenha a seu cargo o tratamento de dados tem que dar, cumprir, verificar e responder, de modo a que o RGPS seja rigorosamente cumprido.

Os procedimentos Operacionais internos devem prever os seguintes pontos:

1 – Recolha de dados:

Tenho que assegurar e ter evidências que:

•A forma de recolha é adequada (tenho consentimento, contrato ou estou a cumprir uma obrigação legal);

•A base legal para o tratamento está correta;
•São transmitidas todas as informações aos titulares dos dados e arranjar evidências do conhecimento por parte destes;
•O consentimento foi prestado e foi guardada evidência do mesmo.

2 – Registo das atividades de tratamento:

A empresa e os subcontratantes devem manter um registo de todas as atividades de tratamento de dados sob a sua responsabilidade que, entre outros, deve prever:
•Fins do tratamento;
•Categorias de titulares dos dados;
•Categorias de dados;
•Categorias de destinatários dos dados;
•Transferências internacionais;
•Prazo de apagamento de dados;
•Descrição das medidas de segurança;

3 – Exercício dos direitos dos titulares dos dados

A empresa deve elaborar um procedimento que aborde duas situações:
•Forma e meio do titular dos dados exercer os seus direitos;
•Forma e prazos de resposta a um pedido de exercício de qualquer um dos direitos que o titular tem.
Não esquecer que a resposta é obrigatória, deve ser feita por escrito (para se ter a evidencia) e o prazo é de 30 dias seguidos.
Caso não se consiga responder dentro deste prazo é necessários comunicá-lo por escrito ao titular dos direitos e informá-lo de que pode reclamar para a CNPD.
Não esquecer também que o sistema informativo deve estar preparado para a portabilidade dos dados.

4 – Subcontratantes e Destinatários

O procedimento deve prever um modelo de contrato a celebrar com os subcontratantes. O contrato deve prever:
•Identificação dos dados que se vão transmitir e identificação do seu titular;
•Âmbito e finalidade da transmissão de dados;
•Extensão da vinculação das obrigações em matéria de proteção de dados aos trabalhadores e terceiros com que o subcontratante contacte;
•Fixação de cláusula penal a aplicar em caso de fuga, violação ou roubo de dados.

5 – Avaliação de Impacto

Quando um certo tipo de tratamento de dados, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e fins, for suscetível de implicar um elevado risco para os direitos e liberdade das pessoas singulares, a empresa/responsável pelo tratamento de dados deve fazer, antes de iniciar o tratamento, uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. O procedimento interno deve indicar as situações em que deve ser feita a avaliação de impacto.

7 – Medidas de segurança do tratamento

O procedimento deve descrever todas as medidas de segurança, informáticas, técnicas e organizativas, que devem ser respeitadas na empresa.
A título de exemplo:
•Pseudonimização (Substituição de material pessoalmente identificável por identificadores artificiais – Ex: números);
•Cifragem (codificação de mensagens para que apenas as pessoas autorizadas as possam ler);
•Inserção de passwords;
•Bloqueio de telemóveis;
•Bloqueio de acesso a dados por departamentos da empresa que não necessitem dos mesmos;
•Introdução do sistema de hibernação nos computadores quando não estiverem a ser usados;
•Minimização;
•Instalação no sistema informático de todas as medidas de proteção;

8 – Informação a prestar aos trabalhadores

Nos termos do RGPD a informação aos trabalhadores deve incluir:
•A identidade e contactos da empresa e do seu representante legal;
•Os contactos do Encarregado de Proteção de Dados (DPO) se este existir;
•As finalidades do tratamento dos dados pessoais, bem como o fundamento jurídico para o tratamento;
•Os destinatários ou entidades a quem vão ser transmitidos os seus dados pessoais;
•Se existem transferência dos seus dados pessoais para países fora da UE;
•Qual o prazo de conservação de dados;

•Informação sobre os direitos dos titulares: acesso, retificação, apagamento, portabilidade, limitação e oposição;
•Se o tratamento se basear no consentimento, deve informar-se que pode retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no mesmo;
•Se a comunicação dos dados pessoais constitui ou não uma obrigação legal, ou um requisito necessário para celebrar um contrato.
•Se o titular dos dados os está obrigado a fornecer e, as eventuais consequências do não fornecimento;
•A existência de decisões automatizadas, nomeadamente a definição de perfis.

9 – Notificação de violação

O procedimento tem que prever a forma de atuação em caso de violação/roubo, etc de dados pessoais.
A empresa tem que notificar a CNPD, sem demora injustificada e sempre que possível até 72 horas após ter tido conhecimento da violação de dados, a menos que da mesma não haja a suscetibilidade de resultar um risco para os direitos e liberdades dos titulares.
Quando a violação implicar este risco, a empresa/responsável pelo tratamento dos dados pessoais deve também comunicar a violação de dados ao titular dos mesmos, sem demora injustificada.

10 – Documentos a elaborar e prova do cumprimento do RGPD

Perante todas estas obrigações e a necessidade de comprovar, a todo o tempo, o cumprimento do RGPD, aconselha-se que as empresas elaborem os seguintes documentos:
•Manual de acolhimento, onde constem os direitos e obrigações em matéria de proteção de dados pessoais;
•Regulamento Interno onde constem todas as regras em matéria de proteção de dados;
•Fazer contratos com os subcontratantes ou adendas ao contrato caso estes já existam;
•Fazer adendas aos contratos dos trabalhadores inserindo cláusulas em matéria de proteção de dados pessoais;
•Inserir a informação nos seus sites;
•Inserir uma politica de privacidade nos sites;
•Elaborar uma folha de registo de todas as atividades de tratamento de dados;
•Implementar um sistema de arquivo com regras;
•Fazer modelos de recolha do consentimento;
•Fazer modelos de prestação de informação;
•Avaliação de impacto.
•Deve implementar-se um mecanismo permanente e dinâmico da verificação de conformidade e cumprimento do RGPD;
•Promover auditorias internas de controlo.

Estamos ao dispor para esclarecimentos que os nossos Associados pretendam.

AIRV – Associação Empresarial da Região de Viseu
Edíficio Expobeiras – Parque Industrial de Coimbrões – 3500 618 Viseu
Tel: 232470290 Fax: 232470299 Email: chenriques@airv.pt www.airv.pt