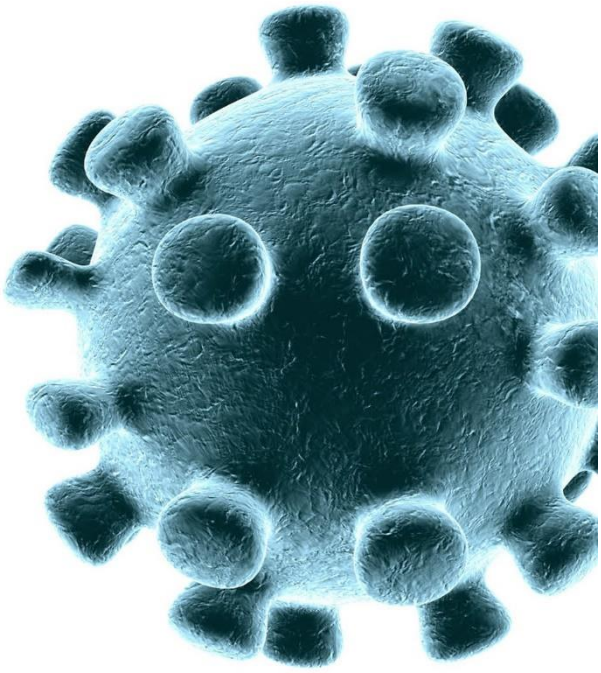
ADVOGADOS



GUIA JURÍDICO : COVID-19

O QUE PRECISA SABER

PROTECÇÃO DE DADOS

COMO PODEM AS EMPRESAS USAR DADOS PESSOAIS RECOLHIDOS NO ÂMBITO DO PLANO DE CONTINGÊNCIA DA INFECÇÃO PELO NOVO CORONAVIRUS?

A título introdutório, fazemos notar que a Comissão Nacional de Protecção de Dados (CNPD) ainda não se pronunciou especificamente sobre a matéria do impacto do COVID-19 nas empresas.

Dito isto, a resposta à questão é que as empresas podem usar esses dados no quadro da lei. É importante ter em conta que a legislação de proteção de dados não deve constituir uma barreira à saúde pública. Porém, mesmo nas atuais circunstâncias, essa legislação não pode ser negligenciada.

As empresas encontram-se a realizar tratamentos de dados pessoais para finalidades não anteriormente previstas e que envolvem, entre outros, dados sobre o paradeiro de trabalhadores, viagens profissionais e pessoais recentemente realizadas e sobre a manifestação de sintomas ou da própria doença no seio da empresa (dados de saúde).

Existe, assim a necessidade de encontrar um justo equilíbrio entre a proteção contra ameaças à saúde pública e a proteção dos dados dos indivíduos, procurando garantir que as empresas não promovem tratamentos de dados pessoais dos seus trabalhadores para lá do justificado pelas circunstâncias excecionais que vivemos.

Na sua Orientação 6/2020, intitulada “Infeção por SARS-CoV-2 (COVID-19) Procedimentos de prevenção, controlo e vigilância em empresas”, a Direção Geral de Saúde descreve as principais etapas que as empresas devem considerar para

estabelecer um Plano de Contingência no âmbito da infeção pelo novo Coronavírus, assim como os procedimentos a adotar perante um Trabalhador com sintomas desta infeção.

O cumprimento deste Plano de Contingência pelas empresas exige, assim o tratamento de dados de saúde de trabalhadores nos quais se manifestou a doença e em casos suspeitos, devendo esse tratamento respeitar um conjunto de regras essenciais. Nesse âmbito, devem as empresas tomar em consideração o seguinte:

■ Licitude do tratamento:

O tratamento de dados de saúde dos trabalhadores, em regra, proibido, encontra-se legitimado em certas circunstâncias relacionadas com o cumprimento de obrigações ao nível do direito laboral.

Por exemplo, no âmbito da medicina no trabalho e preventiva, de avaliação de capacidade de trabalho do empregado, ou ainda para prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde, quando as empresas ajam no quadro de instruções recebidas das autoridades de saúde pública ou de outras autoridades competentes.

Neste último caso, o Regulamento Geral sobre a Proteção de Dados ("RGPD") permite o tratamento de dados de saúde quando "*necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde* (…)" (Artigo 9.º, n.º 2, al. i) e Considerando (46)), devendo entender-se enquadrado neste âmbito o tratamento para execução do Plano de Contingência.

■ Transparência:

As organizações devem ser transparentes quanto às medidas que implementem, incluindo quanto à finalidade de tratamento e aos prazos de conservação dos dados.

A informação a prestar, nomeadamente através das politicas de privacidade, deve ser concisa, facilmente percetível, acessível e clara.

Devem as politicas ser atualizadas logo que possível em ordem a contemplarem os tratamentos relacionados com a execução do Plano de Contingência.

■ Confidencialidade:

Qualquer tratamento de dados no contexto de prevenção da propagação do COVID-19 deve ser realizado de maneira a garantir a segurança dos dados, principalmente no que diz respeito aos dados de saúde.

A identidade dos indivíduos afetados não deve ser divulgada a terceiros, exceto às autoridades competentes, em cumprimento de uma determinação nesse sentido.

Acresce que na Lei n.º 58/2019, de 8 de agosto, o legislador português impõe que os tratamentos de dados de saúde, em circunstâncias como a execução de um Plano de Contingência, devem ser efetuados por um profissional obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação (Artigo 29.º, n.º2).

Devem, assim, as empresas limitar o seu tratamento ao perímetro da Direção de Recursos Humanos e no âmbito desta, apenas a responsáveis sujeitos a um dever de confidencialidade, os quais devem abster-se de revelar a outros colegas quem são os infetados, a menos que exista uma justificação clara nesse sentido (ex.: se tiver havido um contacto relevante entre o trabalhador infetado e colega(s), suscetível de gerar contaminação).

■ Proporcionalidade e Minimização dos dados:

As empresas devem garantir que tratam apenas os dados verdadeiramente necessários para a implementação das medidas preventivas ou de mitigação do COVID-19 que tenham adotado e, em particular aqueles que sejam solicitados pelas autoridades competentes.

Deve, assim, ser evitado um zelo excessivo. Por exemplo, não será proporcional a organização de um questionário dirigido a todos os trabalhadores solicitando a comunicação das respetivas temperaturas ou outros sintomas da doença.

Assim, os tratamentos de dados realizados devem abranger um conjunto mínimo de categorias de dados necessárias para as finalidades de saúde pública aqui em causa, nomeadamente:

- Os elementos de identificação do trabalhador infetado ou exposto ao vírus;

- As medidas tomadas pela empresa, incluindo a comunicação ao serviço de medicina no trabalho e o reporte a autoridades de saúde pública, se for o caso.

■ Prazos do Exercício de Direitos:

As circunstâncias excecionais em que ocorrem os tratamentos de dados relacionados não apenas com o Plano de Contingência, mas também com a operação geral da empresa não alteram os prazos (rígidos) de resposta a pedidos de exercício de direitos por parte dos titulares dos dados.

Assim, um pedido deve ser respondido sem demora injustificada e no prazo de um mês a contar da data de receção do pedido.

Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de receção do pedido.

Dadas as dificuldades acrescidas que a pandemia coloca na vida das empresas e nessa medida, as circunstâncias excecionais em que se encontram a laborar, consideramos admissível a prorrogação do prazo de um mês por dois meses adicionais, num total de até três meses para resposta ao pedido de exercício de direitos, se se verificarem na empresa em causa aquelas dificuldades e estas tiverem um impacto direto na capacidade de resposta aos pedidos de exercício de direitos.

Tais dificuldades devem ser explicadas ao titular e documentadas, para futura justificação perante a autoridade de controlo, se for o caso.

O QUE DEVE SER FEITO PARA PROTEGER OS DADOS PESSOAIS DURANTE ESTE PERIODO EXCEPCIONAL?

É importante tem em conta que o recurso ao trabalho remoto não deve comprometer o dever de sigilo e de segurança a que as empresas se encontram sujeitas, devendo evitar-se a circulação de informação pessoal, incluindo ficheiros de trabalhadores, clientes ou fornecedores em dispositivos não protegidos por palavras passe ou medidas de encriptação. Uma proteção equivalente deve ser adotada quanto ao transporte e manuseamento de documentação em papel fora do perímetro da empresa.

Assim, na medida do possível e com razoabilidade, devem as empresas garantir medidas de segurança lógica e física que assegurem uma adequada proteção dos dados, procurando estender para o perímetro das casas dos seus trabalhadores os cuidados que normalmente são dispensados aos dados no contexto da organização.

Por fim, é essencial não descurar a segurança da informação que permaneça nas organizações depois do respetivo encerramento, em particular arquivos e servidores que contenham quantidades mais significativas de dados pessoais e dados sensíveis.

A este respeito, devem as empresas assegurar-se junto de prestadores de serviço e subcontratantes de que têm os meios adequados de resposta para permitir um acesso continuo aos dados pessoais e a minimização do impacto das atuais circunstancias na segurança dos dados.

O momento excecional que vivemos não desobriga as empresas de assegurar os cuidados de sempre com a segurança da informação e de ter em prática as

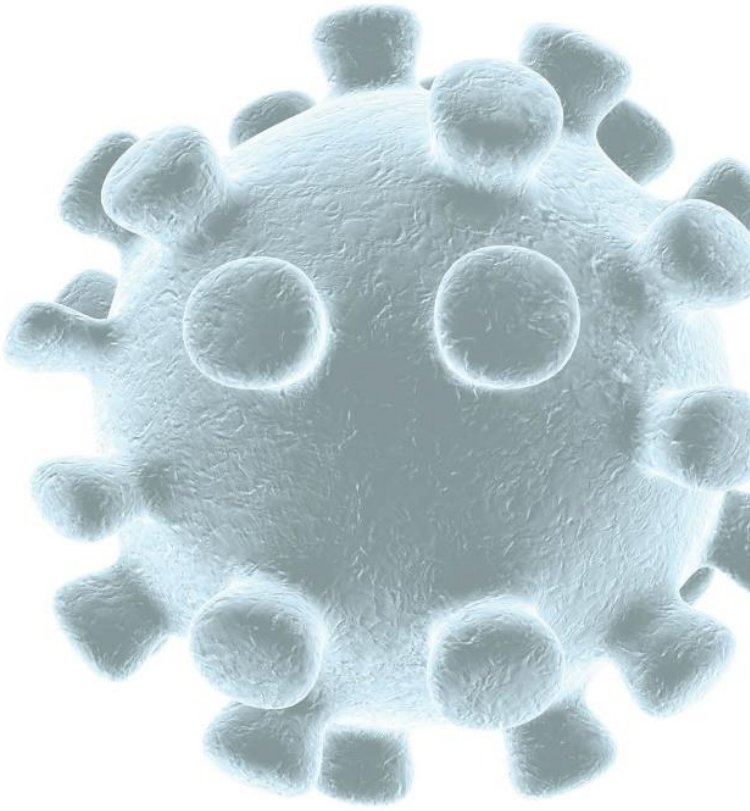
necessárias adaptações a um contexto de trabalho remoto, de maneira a manter uma capacidade de resposta adequada, nomeadamente em caso de violação de dados pessoais.

SE PRECISAR DE MAIS INFORMAÇÃO, CONTACTE-NOS:

TEL:+351 21 313 20 00 | EMAIL: geral.portugal@srslegal.pt

CONTACTO

Luís Neto Galvão
SÓCIO
luis.galvão@srslegal.pt



SRS GLOBAL
CONNECTED LEGAL EXPERIENCE

PORTUGAL • ANGOLA • BRASIL • MACAU • MALTA • MOÇAMBIQUE • SINGAPURA