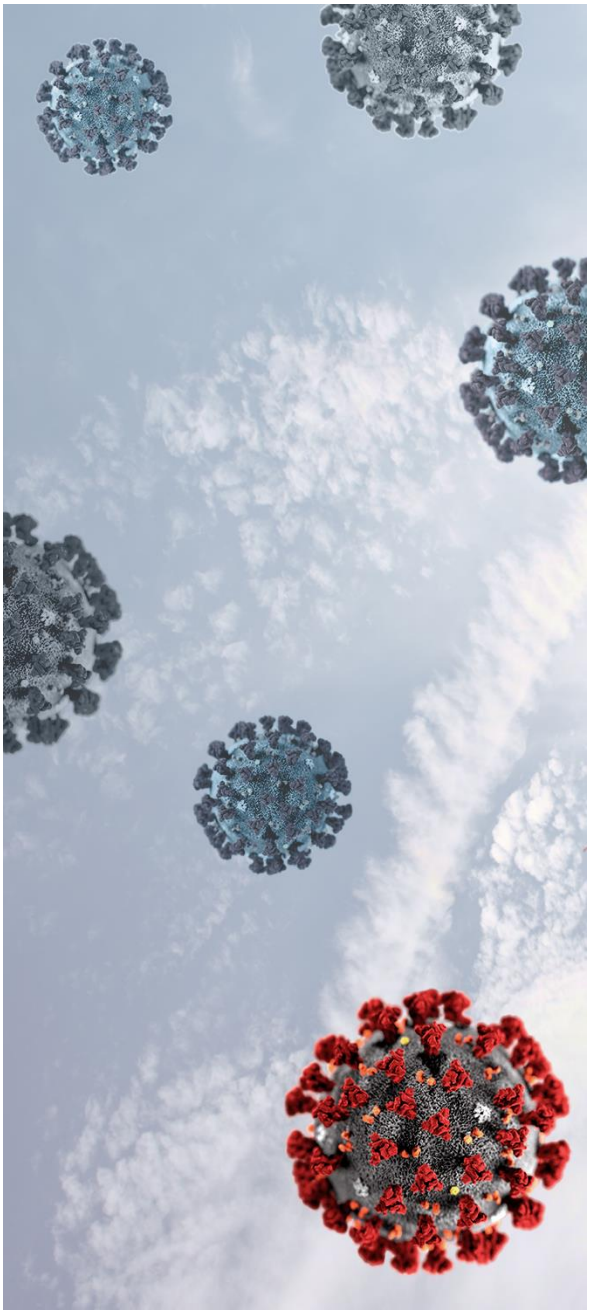
CUATRECASAS

COVID-19: Novidades em matéria de proteção de dados

Newsletter | Portugal

20 de maio de 2020



- Orientações da CNPD sobre o controlo à distância em regime de teletrabalho
- Orientações da CNPD sobre a divulgação de informação relativa a infetados por Covid-19
- Orientações da CNPD sobre a recolha de dados de saúde dos trabalhadores
- Orientações da CNPD para a utilização de tecnologias de suporte ao ensino à distância
- Orientações da CNPD sobre a recolha dos dados de saúde dos alunos
- Orientações da CEPD sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19
- Boas Práticas de Cibersegurança em Teletrabalho publicadas pelo Centro Nacional de Cibersegurança de Portugal

I. Orientações da CNPD sobre o controlo à distância em regime de teletrabalho

Na sequência das medidas de confinamento e de isolamento social, generalizou-se o recurso ao teletrabalho.

Em circunstâncias normais, os instrumentos de trabalho utilizados pelo trabalhador em teletrabalho pertencem ao empregador. Nesse caso, os trabalhadores devem observar as regras de utilização e funcionamento dos instrumentos de trabalho que lhe forem disponibilizados, apenas podendo utilizá-los para a prestação do seu trabalho, salvo acordo em contrário.

Porém, o carácter excecional da situação atual determinou a impossibilidade de as entidades empregadoras disponibilizarem recursos tecnológicos para a generalidade dos seus trabalhadores. Assim, frequentemente os meios utilizados são propriedade dos colaboradores.

Independentemente da propriedade dos instrumentos de trabalho, em teletrabalho o empregador continua a manter os seus poderes de direção e de controlo da execução da prestação laboral. Porém, uma vez que este regime não regula o controlo à distância, a CNPD relembra que «*a regra geral de proibição de utilização de meios de vigilância à distância, com a finalidade de controlar o desempenho profissional do trabalhador, é plenamente aplicável à realidade de teletrabalho*». Conclusão esta a que sempre se chegaria pela aplicação dos princípios da proporcionalidade e da minimização dos dados pessoais.

Deste modo, a CNPD enfatizou que não são admitidas soluções tecnológicas para controlo à distância do desempenho do trabalhador, tais como «*softwares que, para além do rastreamento do tempo de trabalho e de inatividade, registam as páginas de Internet visitadas, a localização do terminal em tempo real, as utilizações dos dispositivos periféricos (ratos e teclados), fazem captura de imagem do ambiente de trabalho, observam e registam quando se inicia o acesso a uma aplicação, controlam o documento em que se está a trabalhar e registam o respetivo tempo gasto em cada tarefa*».

Na opinião da CNPD, estas ferramentas recolhem excessivamente dados pessoais dos trabalhadores, promovendo o controlo do trabalho num grau muito mais detalhado do que aquele que é legitimamente realizado no trabalho presencial nas instalações da entidade empregadora. Nessa medida, a recolha e o tratamento destes dados violam o princípio da minimização dos dados pessoais.

Não obstante, a CNPD recorda que o empregador pode exercer de outros modos o seu poder de controlo da atividade do trabalhador, como mediante a fixação de objetivos, criação de obrigações de reporte com a periodicidade que entenda, marcação de reuniões em teleconferência, etc.

Em relação à necessidade de registo de tempos de trabalho, as soluções que tal o permitam devem limitar-se a reproduzir o registo efetuado quando o trabalho é prestado nas instalações da entidade empregadora (i.e., registar o início e fim da atividade laboral e pausa para almoço). Não estando tais ferramentas disponíveis, excecionalmente é legitimo ao empregador fixar a obrigação de envio de

email, SMS ou qualquer outro meio que lhe permita, para além de controlar a disponibilidade do trabalhador e os tempos de trabalho, demonstrar que não foram ultrapassados os tempos máximos de trabalho permitidos por lei.

II. Orientação da CNPD sobre a divulgação de informação relativa a infetados por Covid-19

Assistimos diariamente à divulgação e disponibilização de informação, efetuada pelas autoridades de saúde, relativa aos totais nacionais de casos suspeitos, confirmados, recuperados e óbitos devido à Covid-19.

Os dados publicados pela Direcção-Geral de Saúde ("DGS") são uma fonte de informação para os municípios, que têm publicado informação relativa à sua área territorial, com vista à tranquilização das suas populações.

Em relação a estas publicações, a CNPD tem recebido queixas de cidadãos, dado que os seus dados pessoais, de identificação e contacto, incluindo de crianças, têm sido publicados nas páginas e nas redes sociais da responsabilidade da autarquia local, após a confirmação do diagnóstico de COVID-19.

Face a esta situação, a CNPD veio informar que as autarquias locais não têm poderes para licitamente publicar dados de saúde com identificação das pessoas a quem os mesmos dizem respeito.

Com efeito, «*esta informação está sujeita a um regime jurídico especialmente protegido, por corresponder a uma categoria de dados pessoais que é suscetível de gerar ou promover a estigmatização e a discriminação dos respetivos titulares*». Ainda que as autarquias locais aleguem a necessidade de conhecer e divulgar dados de saúde para a sua missão de garantir a saúde e a proteção civil da população, esse tratamento dos dados depende de uma norma legal habilitante que o previsse e que especificamente acautelasse os direitos e interesses dos titulares dos dados, sendo que tal previsão legal não existe.

Outra base de legitimidade em que se poderia fundamentar este tratamento corresponde ao consentimento dos titulares dos dados pessoais, o qual será, no entanto, dificilmente verificável neste contexto. De facto, face à situação de vulnerabilidade das pessoas contaminadas pelo vírus, bem como a sua situação de dependência da intervenção das autoridades públicas, não estão verificadas as condições para a emissão de consentimentos livres.

De qualquer modo, a CNPD refere que «*uma tal divulgação pública sempre se terá por desproporcionada, pelo impacto negativo que tem na vida das pessoas contaminadas – reitera-se, algumas das quais crianças –, com restrição excessiva dos seus direitos fundamentais, sem que se possa afirmar que a vantagem diretamente decorrente dessa divulgação, a existir, não é alcançável por outras vias menos lesivas e intrusivas da vida privada das pessoa*s».

De igual modo, também não podem ser publicados dados de saúde, mesmo sem identificação dos doentes, quando o reduzido número de casos de um determinado território, em função da respetiva dimensão populacional, permita a identificação das pessoas contaminadas.

Deste modo, as autarquias locais deverão abster-se de adotar iniciativas que impliquem a recolha e a divulgação de dados pessoais dos seus cidadãos quando as mesmas não tenham base legal, nem sejam execução de orientações da autoridade nacional de saúde.

III. Orientações da CNPD sobre a recolha de dados de saúde dos trabalhadores

As entidades empregadoras têm vindo a adotar medidas com vista à prevenção do contágio entre os seus trabalhadores, tais como, a recolha e o registo de dados relativos à saúde e à vida privada dos trabalhadores suscetíveis de indiciar infeção pelo vírus, como a temperatura corporal dos trabalhadores.

A CNPD recorda que «*os dados pessoais relativos à saúde são dados sensíveis, reveladores de aspetos da vida privada do trabalhador que, em princípio, não têm que ser do conhecimento da entidade empregadora, nem devem sê-lo por poderem gerar ou potenciar discriminação*», estando esta categoria de dados sujeita a um regime especialmente reforçado de proteção de dados, do qual resulta que o empregador não conhece, nem pode recolher ou registar diretamente dados de saúde dos seus trabalhadores.

Apesar de a situação excecional em que vivemos ter provocado alterações profundas no contexto da prestação do trabalho e da relação empregador–trabalhador, a necessidade de prevenção de contágio pelo vírus não legitima, sem mais, a adoção de toda e qualquer medida por parte da entidade empregadora.

Com efeito, a prevenção de contaminação pode justificar a intensificação de cuidados de higiene, bem como a adoção de medidas organizativas quanto à distribuição no espaço dos trabalhadores ou à sua proteção física. Porém, esta «*não justifica a realização de atos que, nos termos da lei nacional, só as autoridades de saúde ou o próprio trabalhador, num processo de auto-monitorização, podem praticar*».

Assim, a CNPD considera que as entidades empregadoras não podem recolher e registar a temperatura corporal dos trabalhadores ou outra informação relativa à saúde ou a eventuais comportamentos de risco dos seus trabalhadores.

Não obstante, mantém-se a possibilidade de um profissional de saúde, no âmbito da medicina do trabalho, avaliar o estado de saúde dos trabalhadores, nomeadamente, mediante a recolha, através de preenchimento de questionários pelo trabalhador, de informação relativa à saúde ou à vida privada do mesmo relacionada com a sua saúde.

Em resposta à publicação destas Orientações, a Assembleia da República dirigiu um requerimento parlamentar pedindo esclarecimentos à CNPD. Na sua resposta, a CNPD reiterou a sua posição sobre medição da temperatura dos trabalhadores e enfatizou os seguintes pontos:

- Reafirma que o tratamento de dados de saúde no âmbito de relações laborais, com fundamento no consentimento do trabalhador, é incompatível com o direito fundamental à proteção e dados e privacidade protegidos pela Constituição da República Portuguesa e pela Carta dos Direitos Fundamentais da União Europeia.
- Considera que a disposição contida no Artigo 13.º-C do Decreto-Lei n.º 10-A/2020, de 13 de março, alterado pelo Decreto-Lei n.º 20/2020, de 1 de maio, que prevê a possibilidade de os empregadores procederem à leitura da temperatura corporal dos seus trabalhadores, não prevê as medidas adequadas à proteção dos direitos, liberdades e garantias dos titulares de dados que o RGPD obriga os Estados-membros a prever.
- Entende que o tratamento de dados de saúde com fundamento na invocação de interesse público assente no artigo 9.º, n.º 1, alíneas i) e h), do Regulamento Geral sobre a Proteção de Dados (aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016), tem que ser antecedida por disposição de direito nacional ou direito da União Europeia, que defina os pressupostos legais para o tratamento e determine as medidas adequadas para a proteção dos direitos e liberdades dos titulares de dados.

IV. Orientações da CNPD para a utilização de tecnologias de suporte ao ensino à distância

A CNPD publicou orientações dirigidas a todos os intervenientes no tratamento de dados realizados em ambiente escolar, sejam professores, alunos e pais ou encarregados de educação, assim como às entidades que agem nas condições de responsáveis pelo tratamento e subcontratantes.

A CNPD identifica um vasto leque de dados pessoais tratados pelas tecnologias de suporte ao ensino à distância: gravação de voz e imagem de todos intervenientes e terceiros, imagens do interior da habitação, dados inseridos em documentos partilhados ou em declarações verbais proferidas em videochamada, informação em *instante messaging* e fóruns.

No tocante às plataformas de ensino, verifica-se que são ou podem ser recolhidos dados relativos à utilização das plataformas (*metadados*), tais como tempo despendido na plataforma, número de cursos frequentados, aprovação, etc., e dados pessoais deduzidos dos dados anteriormente referidos: aptidões intelectuais, dificuldades de aprendizagem, traços de personalidade, dados de saúde associados ao intelecto e concentração.

Segundo a CNPD, a utilização destas plataformas importa vários riscos, em especial:

- Risco de utilização indevida dos dados recolhidos pelas plataformas, quer pelos responsáveis pelo tratamento, quer pelos subcontratantes, nomeadamente os fornecedores de serviços de computação em nuvem;
- Falta de transparência no armazenamento dos dados, no âmbito de eventuais subcontratações com fornecedores de serviços de computação em nuvem, que leva a uma perda de controlo pelos titulares dos dados;
- Tratamento discriminatório com base na definição de perfis ou avaliações, nomeadamente através de tomada de decisões automatizadas, assentes em sistemas *learning analytics*, que analisem o desempenho do aluno;
- A utilização de plataformas de comunicação que não garantam a segurança das comunicações ou cuja incorreta configuração resulte na divulgação ou acesso não autorizado;
- Risco de confidencialidade na partilha de computadores;
- Risco de desresponsabilização das escolas e das plataformas, na ausência de uma atribuição clara das responsabilidades no contexto do uso destas tecnologias;
- Risco de vigilância à distância, com a finalidade de controlar o desempenho profissional dos professores (a este respeito, *vide supra* Orientações sobre o controlo à distância em regime de teletrabalho);
- Risco de inviabilização do exercício dos direitos pelos titulares dos dados junto das plataformas.

Assim, para mitigar os riscos enunciados, a CNPD recomenda que se adotem medidas adequadas às tecnologias empregues, nomeadamente:

- A adoção de cada plataforma de suporte ao ensino à distância deve ser precedida de uma avaliação de impacto na proteção de dados, de forma a identificar corretamente os riscos para a privacidade e permitir que sejam adotadas medidas mitigadoras desses riscos. A avaliação pode ser feita pelas entidades que disponibilizam e gerem as plataformas;
- Os professores devem ser devidamente informados relativamente à utilização das plataformas. Em particular, devem conseguir identificar as corretas configurações para garantir que da utilização não decorrem riscos para a privacidade dos utilizadores, com especial enfoque nos alunos;
- Sempre que possível, deve optar-se por tecnologias que impliquem a menor exposição possível do titular e do seu ambiente familiar (e.g., fóruns de discussão por oposição a videoconferência);

A utilização de quaisquer algoritmos de análise de desempenho (*learning analytics*) deve sempre ser criteriosa e feita de forma justa e transparente para com os titulares e apenas se estiver preenchida alguma das condições de licitude desse tratamento.

Importa aqui reforçar que nenhum estabelecimento de ensino pode impor a utilização desta específica tecnologia de inteligência artificial aos seus alunos, dependendo essa utilização de uma vontade informada, livre, específica e explícita do aluno ou, quando menor, de quem o representa.

Deve ser dada clara informação aos titulares acerca do funcionamento dos algoritmos de análise, nomeadamente quando estiverem em causa decisões automatizadas. E deve ser sempre garantido o direito do titular dos dados de obter intervenção humana nesse processo.

V. Orientações da CNPD sobre a recolha dos dados de saúde dos alunos

A reabertura das escolas e o recomeço das aulas levou vários estabelecimentos de ensino a recolherem a temperatura dos alunos à entrada das suas instalações.

Na linha das várias posições públicas que já assumiu sobre o tratamento de dados de saúde, no âmbito da pandemia COVID-19, a CNPD relembra que os estabelecimentos de ensino, enquanto responsáveis pelo tratamento de dados, têm que cumprir os requisitos estritos para o tratamento de dados de saúde (dados sensíveis).

A CNPD afirma ainda que a reabertura das escolas, em conformidade com o Decreto-Lei n.º 20-H/2020, de 14 de maio, não obriga à medição de temperaturas, uma vez que não há qualquer orientação da Direção-Geral de Saúde sobre a necessidade e utilidade da medição de temperatura dos alunos.

Deste modo, a CNPD enfatiza a necessidade de cumprir os princípios gerais em matéria de tratamento de dados, nomeadamente a verificação de uma base de licitude adequada para o tratamento, nos seguintes termos:

- Os estabelecimentos de ensino têm que demonstrar a existência de um fundamento de licitude, nos termos dos artigos 5.º e 9.º do RGPD, para o tratamento de dados sensíveis. Não será suficiente a mera invocação de interesse legítimo de terceiros, uma vez que se terá de demonstrar que estes prevalecem sobre os direitos dos titulares de dados, nomeadamente, de menores.

- Com os mesmos fundamentos aduzidos acima, os estabelecimentos de ensino público não poderão invocar que o tratamento é necessário ao exercício de funções de interesse público, a que se refere a alínea e) do n.º 1 do artigo 9.º.

- Relativamente a basear o tratamento de dados no consentimento, considera a CNPD que a «*declaração de vontade eventualmente manifestada pelo aluno, ou pelo encarregado de educação, só é relevante para fundamentar o tratamento se não houver ameaça ou comunicação de que a recusa de sujeição ao procedimento de leitura da temperatura corporal implica a consequência negativa para o aluno de ser impedido de entrar numa sala de aula e, portanto, de obter os ensinamentos necessários à sua preparação para a avaliação*».

- A invocação da licitude do tratamento não se poderá basear em regulamento escolar, uma vez que a autonomia dos estabelecimentos não permite a restrição de direitos, liberdade e garantias, sem ato legal habilitante, nomeadamente o direito à proteção de dados pessoais e privacidade, protegidos pela Constituição da República Portuguesa e pelo RGPD.

- Ainda que se demonstre haver um fundamento de licitude, os responsáveis pelo tratamento deverão demonstrar que o tratamento é necessário, na medida em que seja o meio menos intrusivo para os direitos dos titulares, por relação a outras alternativas disponíveis.

VI. Orientações da CEPD sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19

Segundo as palavras da Comissária Europeia da Saúde, Stella Kyriakides, no combate à pandemia COVID-19 através de aplicações digitais não se prescindirá do «*padrão de ouro global*», que são os valores e legislação europeia que protegem os direitos fundamentais, nomeadamente à privacidade e proteção de dados.

Nesse sentido, o Comité Europeu de Proteção de Dados ("CEPD") emitiu a Diretriz 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19, a 21 de abril de 2020.

As orientações emitidas visam clarificar as *«condições e princípios de utilização proporcionada dos dados de localização e dos instrumentos de localização, para dois fins específicos:*

- *para apoiar a resposta à pandemia, modelando a propagação do vírus, de modo a avaliar a eficácia global das medidas de confinamento; e*

- *para rastrear contactos, notificando os indivíduos que estiveram próximos de alguém que foi confirmado como portador do vírus, a fim de, rapidamente, quebrar as cadeias de contaminação.»*

O CEPD relembra que já tinha tomado anteriormente posição relativamente ao tratamento de dados de geolocalização, recolhidos por prestador de serviços de comunicações eletrónicas, afirmando que deveriam ser previamente anonimizados.

Já relativamente aos dados de localização recolhidos diretamente dos dispositivos dos utilizadores, o seu tratamento só será lícito com a obtenção do consentimento prévio dos utilizadores ou quando o tratamento for estritamente necessário para o serviço da sociedade de informação explicitamente solicitado pelo utilizador (por ex., o uso de uma aplicação móvel).

O CEPD reflete sobre o conceito de anonimização de dados, as suas implicações jurídicas e técnicas, acabando por concluir que «*[e]xistem muitas opções para anonimização eficaz, mas sempre com uma ressalva. Os dados não podem ser anonimizados por si próprios, o que significa que apenas conjuntos de dados como um todo podem ser tornados anónimos. Neste sentido, qualquer intervenção num único padrão de dados (por meio de criptografia, ou qualquer outra transformação matemática) pode, na melhor das hipóteses, ser considerada uma pseudonimização*».

No que concerne ao rastreamento de contactos (*contact tracing*), o CEDP enfatiza que o acompanhamento sistemático e em larga escala da localização e/ou de contactos entre pessoas «*só pode ser legitimado se contar com uma adoção voluntária pelos utilizadores*». Deste modo, não se contempla como lícita a hipótese de se impor o uso desta tecnologia aos cidadãos. O CEDP relembra a necessidade de estas *apps* serem desenvolvidas numa lógica de privacidade por defeito, com respeito pelos princípios da limitação das finalidades e da minimização de dados.

Os intervenientes envolvidos deverão também ter em consideração que poderá haver causas de legitimidade para o tratamento dos dados que se sobreponham ao consentimento, tais como a prossecução de um interesse público, pelas autoridades públicas, estabelecidas na legislação a União Europeia na dos Estados-membros.

Finalmente, o CEPD sublinha que os «*procedimentos e processos, incluindo os respetivos algoritmos implementados pelas aplicações de rastreamento de contactos, devem funcionar sob a estrita supervisão de pessoal qualificado, a fim de limitar a ocorrência de falsos positivos e negativos*», relembrando que o encaminhamento de potenciais infetados «*não deve basear-se unicamente no processamento automatizado*».

O CEDP ainda disponibiliza um conjunto de recomendações e orientações, de índole técnica, sobre o desenvolvimento de aplicações que cumpram o princípio de privacidade por defeito.

VII. Boas Práticas de Cibersegurança em Teletrabalho publicadas pelo Centro Nacional de Cibersegurança de Portugal

Informamos ainda que o Centro Nacional de Cibersegurança de Portugal publicou as "Boas Práticas de Cibersegurança em Teletrabalho" que devem ser tomadas em conta pelas organizações e empresas que tenham ainda os seus trabalhadores em teletrabalho.

https://www.cncs.gov.pt/recursos/boas-praticas/

Contactos

Cuatrecasas, Gonçalves Pereira & Associados,
Sociedade de Advogados, SP, RL
Sociedade profissional de responsabilidade limitada

Lisboa
Praça Marquês de Pombal, 2 (e 1-8º) I 1250-160 Lisboa I Portugal
Tel. (351) 21 355 3800 I Fax (351) 21 353 2362
cuatrecasasportugal@cuatrecasas.com I www.cuatrecasas.com

Porto
Avenida da Boavista, 3265 - 5.1 I 4100-137 Porto I Portugal
Tel. (351) 22 616 6920 I Fax (351) 22 616 6949
cuatrecasasporto@cuatrecasas.com I www.cuatrecasas.com

A Cuatrecasas criou a *Task Force Coronavírus*, uma equipa multidisciplinar que analisa em permanência a atual situação de crise emergente da pandemia de COVID-19. Para obter informações adicionais sobre o conteúdo deste documento, poderá contactar a nossa *Task Force* através do email TFcoronavirusPT@cuatrecasas.com ou dirigir-se ao seu contacto habitual na Cuatrecasas. Poderá ler as nossas publicações ou assistir aos nossos *webinars* através do nosso *website*.

Informação sobre o tratamento dos seus dados pessoais

Responsável pelo Tratamento: Cuatrecasas, Gonçalves Pereira & Associados, Sociedade de Advogados, SP, RL ("Cuatrecasas Portugal").
Finalidades: gestão da utilização do website, das aplicações e/ou da sua relação com a Cuatrecasas Portugal, incluindo o envio de informação sobre novidades legislativas e eventos promovidos pela Cuatrecasas Portugal.
Legitimidade: o interesse legítimo da Cuatrecasas Portugal e/ou, quando aplicável, o próprio consentimento do titular dos dados.
Destinatários: terceiros aos quais a Cuatrecasas Portugal esteja contratualmente ou legalmente obrigada a comunicar os dados, assim como a empresas do seu grupo.
Direitos: aceder, retificar, apagar, opor-se, pedir a portabilidade dos seus dados e/ou limitar o seu tratamento, conforme descrevemos na informação adicional.
Para obter informação mais detalhada, sobre a forma como tratamos os seus dados, aceda à nossa política de proteção de dados.

Caso tenha alguma dúvida sobre a forma como tratamos os seus dados, ou caso não deseje continuar a receber comunicações da Cuatrecasas Portugal, pedimos-lhe que nos informe através do envio de uma mensagem para o seguinte endereço de e-mail data.protection.officer@cuatrecasas.com.