



ACORDO DE TRATAMENTO DE DADOS

1. OBJETO DO ACORDO

- (1) A Konica Minolta (doravante, também designada por: “subcontratante”) presta serviços ao Cliente (de ora em diante, também designado por: “responsável pelo tratamento”), de acordo com os termos e condições expressas no contrato de aluguer e manutenção (doravante designado por “Acordo Principal”). Na medida em que a prestação dos aludidos serviços implica o tratamento de dados pessoais por conta do Responsável pelo Tratamento, tal como referido no Regulamento Geral sobre a Proteção de Dados, que entrou em vigor em 25 de maio de 2018 (doravante: RGPD), as Partes estabelecem os seus respetivos direitos e obrigações no presente Acordo de Tratamento de Dados (doravante designado por: “ATD”).
- (2) Os dados pessoais tratados podem ser dados provenientes do responsável pelo tratamento ou dos subcontratantes associados ao responsável pelo tratamento, ao abrigo do disposto nos artigos 26º e 28º do RGPD, ou dados pessoais recolhidos pelo subcontratante em nome dos mesmos (todos os dados pessoais serão doravante designados conjuntamente por “dados pessoais do responsável pelo tratamento”).
- (3) O tipo de dados pessoais do responsável pelo tratamento e as categorias de titulares de dados pessoais afetados pelo tratamento, bem como a natureza e a finalidade do tratamento, são especificados no Anexo 1 do presente ATD.
- (4) A duração do presente ATD coincidirá com a do Acordo Principal, salvo no que diz respeito às disposições que impõem obrigações ou direitos de cessação que vão para além do prazo de vigência do Acordo Principal.

2. DIREITO A EMITIR INSTRUÇÕES

- (1) O Subcontratante só pode recolher, tratar ou utilizar dados no âmbito do acordo principal, conforme as instruções do Responsável pelo Tratamento.
- (2) As instruções do Responsável pelo Tratamento são inicialmente estabelecidas no presente ATD e podem ser posteriormente alteradas, complementadas ou substituídas por instruções individuais por escrito ou em texto (instruções individuais). As instruções



verbais são confirmadas pelo Responsável pelo Tratamento sem demora (pelo menos em forma de texto). O Responsável pelo Tratamento tem o direito de emitir instruções em qualquer altura. Isto inclui instruções relativas à eliminação, retificação e restrição do tratamento de dados. Para os produtos cuja utilização o exija, as pessoas autorizadas a dar ou receber instruções estão definidas no respetivo anexo 1 do presente ATD.

- (3) Caso o Subcontratante considere que uma instrução do Responsável pelo Tratamento viola disposições regulamentares ou legais de proteção de dados, o responsável pelo tratamento deve ser informado o mais rapidamente possível. O Subcontratante tem o direito de suspender a execução da instrução em causa até que a mesma seja confirmada ou alterada pelo responsável pelo tratamento. O Subcontratante pode recusar a execução de uma instrução manifestamente ilegal.
- (4) O Subcontratante receberá uma remuneração separada com base ou de acordo com a lista atual de preços dos serviços do Subcontratante para quaisquer serviços baseados nas instruções do Cliente que não estejam cobertas pelo Contrato Principal, ou que não sejam legalmente exigidas ao Subcontratante.

3. MEDIDAS DE SEGURANÇA DO SUBCONTRATANTE

- (1) O Subcontratante obriga-se a cumprir as disposições legais e regulamentares relativas à proteção de dados. O Subcontratante concorda em estruturar a organização interna na sua esfera de responsabilidade para levar em conta os requisitos especiais de proteção de dados. O Subcontratante implementará todas as medidas técnicas e organizacionais necessárias para a proteção adequada dos dados do Responsável pelo Tratamento, de acordo com o Artigo 32.º do Regulamento Geral de Proteção de Dados (RGPD). O Subcontratante poderá alterar as medidas de segurança implantadas, mas estas deverão assegurar que o nível de segurança acordado no Anexo 1, do presente ATD seja mantido.
- (2) O Subcontratante nomeou um responsável pela proteção de dados da empresa. Os dados de contacto do responsável pela proteção de dados estão publicados no site do Subcontratante.
- (3) O Subcontratante imporá uma obrigação de confidencialidade (Artigo 28.º, n.º 3, al. b) do RGPD) a todas as pessoas autorizadas a tratar dados pessoais ao abrigo do presente acordo (doravante referidos como “funcionários”), e assegurará o cumprimento da referida obrigação, com o devido cuidado.



4. DEVERES DO SUBCONTRATANTE

- (1) O Subcontratante informará o Responsável pelo Tratamento no mais curto espaço de tempo possível, mediante comunicação escrita, de qualquer violação de dados pessoais de que tenha conhecimento. A notificação de uma violação da segurança dos dados pessoais deve conter pelo menos as seguintes informações:
- (2) (a) uma descrição sobre a natureza da violação da segurança dos dados pessoais, na medida do possível, com menção das categorias, do número de titulares de dados em causa e das categorias e do número de registos de dados pessoais em causa;
- (3) (b) o nome e os dados de contacto do responsável pela proteção de dados, ou de outro ponto de contacto onde possam ser obtidas mais informações;
- (4) (c) as consequências prováveis da violação da segurança dos dados pessoais;
- (5) (d) uma descrição das medidas tomadas ou propostas pelo Subcontratante para eliminar a violação e, se for o caso, medidas para mitigar quaisquer efeitos desvantajosos.
- (6) O Subcontratante adotará as medidas consideradas necessárias para garantir os dados e mitigar quaisquer possíveis implicações desvantajosas para os titulares de dados, informará o Responsável pelo Tratamento em conformidade e solicitará instruções.
- (7) O Subcontratante informará ainda o Responsável pelo Tratamento sempre que os dados deste forem afetados por uma violação de que tenha conhecimento.
- (8) No caso de os dados do Responsável pelo Tratamento, enquanto estejam na posse do Subcontratante, serem ameaçados por penhora ou confisco, através de processos de insolvência ou de liquidação ou através de outros eventos ou medidas de terceiros, o Subcontratante informará o Responsável pelo Tratamento em conformidade, a menos que tal seja proibido, sem prejuízo de informar, no mais curto espaço de tempo possível, todas as autoridades jurisdicionais que o poder de decisão final sobre os dados é exclusivamente do Cliente na sua capacidade de “Responsável pelo Tratamento” no âmbito da aceção dada pelo RGPD.
- (9) O Subcontratante manterá um registo de todas as categorias de atividades de tratamento realizadas em nome do Responsável pelo Tratamento, a qual contém todas as informações de acordo com o Artigo 30.º, n.º 2, do RGPD.
- (10) O Responsável pelo Tratamento e o Subcontratante, se assim for solicitado, ajudarão a Comissão Nacional de Proteção de Dados no cumprimento das suas obrigações.



5. DIREITOS DO RESPONSÁVEL PELO TRATAMENTO

- (1) O Subcontratante, antes do início do tratamento de dados e em intervalos regulares, estabelece as medidas técnicas e organizacionais a serem implementadas pelo Subcontratante. Para este efeito, o Responsável pelo Tratamento pode, por exemplo, obter informações do Subcontratante, solicitar que lhe sejam apresentadas certificações ou atestados de peritos ou, após coordenação atempada (com pelo menos três semanas de antecedência), inspecionar as medidas técnicas e organizativas do Subcontratante. As inspeções podem ser efetuadas durante as horas normais de expediente, pessoalmente ou por um terceiro competente. As inspeções por terceiros devem ser efetuadas com o acordo do Subcontratante, os terceiros que se encontrem numa relação de concorrência podem ser rejeitados pelo Subcontratante. O Responsável pelo Tratamento efetua as inspeções apenas na medida do necessário e não perturba desproporcionadamente as operações do Subcontratante. Cada parte suportará os seus próprios custos de auditorias e inspeções.
- (2) O Subcontratante compromete-se a fornecer ao Responsável pelo Tratamento, a pedido escrito deste último e num prazo razoável, todas as informações e elementos de prova necessários para a realização de uma auditoria ou de uma inspeção das medidas técnicas e organizativas adotadas pelo Subcontratante.
- (3) O Responsável pelo Tratamento documenta o resultado da auditoria ou da inspeção e transmite-o ao Subcontratante. Em caso de erros ou irregularidades detetados pelo Responsável pelo Tratamento, nomeadamente nos resultados do tratamento de dados encomendado, o Subcontratante é informado, no mais curto espaço de tempo possível. Se a auditoria ou inspeção revelar problemas que, para serem evitados no futuro, exijam alterações ao tratamento encomendado, o Responsável pelo Tratamento informará, por escrito, o Subcontratante dos resultados e das alterações solicitadas.

6. CONTRATAÇÃO DE SUBCONTRATADOS PELA KONICA MINOLTA

- (1) Com a assinatura do presente ATD, a Konica Minolta recebe uma autorização geral para nomear Subcontratantes para a execução do Acordo Principal. Os Subcontratantes nomeados são enumerados no Anexo 1.
- (2) O Subcontratante está autorizado a alterar as relações de subcontratação existentes ou a estabelecer novas relações. O Subcontratante informará o mais rapidamente possível o Responsável pelo Tratamento desse facto. O responsável pelo tratamento pode opor-se à contratação de novos subcontratantes. O responsável pelo tratamento deve levantar



imediatamente qualquer objeção; as objeções não podem basear-se em considerações alheias.

- (3) O Subcontratante é obrigado a selecionar cuidadosamente os subcontratantes em função da sua adequação e fiabilidade. Se recorrer a subcontratantes, o Subcontratante deve contratá-los em conformidade com as disposições do presente ATD. Se forem envolvidos subcontratantes de um país terceiro, o Subcontratante deve assegurar que é garantido um nível adequado de proteção de dados para o respetivo subcontratante (por exemplo, acordando as cláusulas contratuais-tipo da UE).
- (4) Uma relação de subcontratação no âmbito das disposições supra não será considerada como tal se o Subcontratante contratar terceiros para executar serviços que devem ser considerados de natureza secundária. Tais serviços incluem, por exemplo, os serviços postais, de transporte, expedição, serviços de limpeza e serviços de telecomunicações, bem como os serviços de segurança, que não se encontram diretamente relacionados com os serviços que o Subcontratante presta ao Responsável pelo Tratamento.

7. CONSULTA E DIREITOS DOS TITULARES DOS DADOS

- (1) O Subcontratante apoiará o Responsável pelo tratamento, na medida do possível, implementando medidas técnicas e organizacionais apropriadas relacionadas com o cumprimento das suas obrigações nos termos dos Artigos 12.º a 22.º, e 32.º a 36.º do RGPD.
- (2) No caso de um titular de dados se dirigir diretamente à Subcontratante para o exercício dos respetivos direitos, incluindo, mas não limitado aos direitos de informação, retificação ou eliminação, a mesma não reagirá de forma independente, dando conhecimento de tal pedido ao Responsável pelo Tratamento e aguardando instruções.

8. RESPONSABILIDADE

- (1) O Responsável pelo Tratamento concorda em assumir total responsabilidade – dentro dos limites do Acordo Principal – por quaisquer reclamações feitas contra o Subcontratante em razão de qualquer perda ou dano sofrido por um titular de dados como resultado do tratamento de dados ou do uso de dados, no curso de tratamento que seja proibido ou incorreto, de acordo com a legislação de proteção de dados, desde que o tratamento de dados ou o uso de dados proibidos ou incorretos seja baseado em instruções emitidas pelo Responsável pelo Tratamento.



- (2) Cada uma das Partes eximirá a outra Parte da respetiva de responsabilidade se essa outra Parte puder provar que não foi de forma alguma responsável pela circunstância que levou à perda ou dano sofrido pelo titular dos dados.

9. CESSAÇÃO DO ACORDO PRINCIPAL

- (1) Após a cessação do Acordo Principal, ou a qualquer momento a pedido da parte responsável, o Subcontratante devolverá à parte responsável todos os documentos, dados e suportes de dados fornecidos pelo Responsável pelo Tratamento ou – a pedido do Responsável pelo Tratamento – exceto se existir uma obrigação de armazenar dados pessoais ao abrigo da legislação aplicável – apagá-los-á ou substituí-los-á. Isto também se aplica a quaisquer cópias de segurança de dados nas instalações do Subcontratante. O Subcontratante tem o direito de faturar ao Responsável pelo Tratamento a eliminação ou a substituição dos dados pessoais armazenados no disco rígido de uma fotocopiadora multifunções.
- (2) O Subcontratante é obrigado a tratar confidencialmente os dados de que tenha tido conhecimento no âmbito do Acordo Principal durante e após o termo do mesmo. O presente ATD mantém-se em vigor para além do termo do Acordo Principal, enquanto o Subcontratante tiver à sua disposição dados pessoais fornecidos pelo Responsável pelo Tratamento ou recolhidos pelo Subcontratante em nome do Responsável pelo Tratamento.

10. DISPOSIÇÕES GERAIS

- (1) As alterações e emendas ao presente DPA devem ser efetuadas por escrito.
- (2) O presente ATD é parte integrante do Acordo Principal. Por conseguinte, todos os direitos e obrigações previstos no Acordo Principal, incluindo as limitações de responsabilidade, aplicam-se igualmente ao presente ATD. Em caso de contradição, incoerência ou dúvida entre os termos e condições do presente ATD e os termos e condições do Acordo Principal, as condições do Acordo Principal prevalecerão sobre as condições do ATD.
- (3) Se determinadas disposições do presente ATD forem ou se tornarem inválidas ou inaplicáveis, no todo ou em parte, tal não afetará a validade das restantes disposições.
- (4) O presente Acordo será regido pela lei portuguesa e, em caso de litígio, o tribunal competente será o Tribunal Judicial da Comarca de Loures.



ANEXO AO ATD DA KONICA MINOLTA

Descrição das medidas de segurança técnicas e organizativas

1. DESCRIÇÃO DA NATUREZA E DA FINALIDADE DO TRATAMENTO

Os sistemas de impressão multifuncionais e/ou de produção da Konica Minolta processam documentos em papel e eletrónicos para efeitos de impressão, digitalização, cópia e fax.

O tratamento de dados pessoais do responsável pelo tratamento ou de terceiros (doravante designados conjuntamente por "*dados pessoais do responsável pelo tratamento*") pela Konica Minolta é efetuado exclusivamente no âmbito da prestação de serviços e manutenção aos sistemas Konica Minolta. Os dados pessoais serão tratados apenas com o objetivo de prestar serviços e manutenção. A Konica Minolta não procede a qualquer outra recolha ou utilização dos dados pessoais do responsável pelo tratamento. A natureza específica do tratamento dependerá das opções de serviço e dos serviços remotos descritos no presente anexo que tenham sido escolhidos pelo Responsável pelo Tratamento.

O tratamento dos dados pessoais do responsável pelo tratamento pode ocorrer no decurso do fornecimento e da instalação dos sistemas Konica Minolta (especialmente no contexto de uma ligação em rede) e no decurso de trabalhos físicos de assistência e manutenção do equipamento.

Os sistemas multifuncionais e de impressão de produção da Konica Minolta são capazes de registar processos técnicos em ficheiros de registo encriptados. A Konica Minolta não inicia a criação de ficheiros de registo até que a análise de erros se torne necessária. Os ficheiros de registo podem ser acedidos por um técnico da Konica Minolta no local, no entanto, no procedimento padrão, os ficheiros de registo são transferidos para servidores pertencentes e operados pela Konica Minolta Europe (localização do servidor na Alemanha) como parte dos serviços remotos da Konica Minolta (Konica Minolta "*Remote Service Platform*" – "*RSP*").

Adicionalmente, os serviços remotos podem ser utilizados para criar cópias de segurança da configuração do equipamento, que podem ser armazenadas de forma encriptada e protegida por palavra-passe nos próprios servidores do Responsável pelo Tratamento, ou nos servidores da Konica Minolta Europe (localização do servidor na Alemanha).

Tanto os ficheiros de registo como as cópias de segurança da configuração do dispositivo não contêm quaisquer conteúdos de impressão, digitalização, cópia ou operações semelhantes efetuadas nos Sistemas.



O serviço remoto e a manutenção dos sistemas Konica Minolta serão efetuados de acordo com as opções de serviço escolhidas pelo Responsável pelo Tratamento. Para este efeito, a Konica Minolta opera a "Konica Minolta Remote Service Platform" (RSP), ligações ao painel remoto, a solução "Konica Minolta Remote Support Tool", ou soluções funcionalmente comparáveis. Ao efetuar a manutenção remota, não é possível eliminar completamente a possibilidade de visualizar e, assim, processar dados pessoais do Responsável pelo Tratamento.

No caso de uma eventual devolução dos sistemas Konica Minolta após o termo do Acordo Principal, os dados pessoais no disco rígido do equipamento e na memória interna serão destruídos, apagados, substituídos ou entregues ao responsável pelo tratamento.

2.1 TIPO DE DADOS PESSOAIS

Geral: Dados dos Titulares a que a Konica Minolta terá acesso ao abrigo do Contrato Principal outorgado com o Cliente.

Tipo de dados pessoais que podem ser incluídos nas cópias de segurança da configuração do dispositivo: Livro de endereços interno do equipamento (nomes de utilizador de TI e endereços de correio eletrónico), endereços IP, endereços MAC, número de série.

Categorias de dados pessoais eventualmente contidas nos ficheiros de registo: Nomes de utilizadores de TI (por exemplo, nomes de utilizadores Windows dos utilizadores do dispositivo), endereços de correio eletrónico dos utilizadores, endereços IP, endereços MAC, número de série, histórico do navegador de Internet do dispositivo (URLs acedidos), histórico do estado de energia do dispositivo, histórico dos últimos 150 trabalhos de impressão (proprietário do trabalho de impressão, carimbo de data/hora, nome do documento).

Todos os dados registados nos ficheiros de registo só são recolhidos a partir do início do registo de eventos.

Dados pessoais que podem ser tratados durante o serviço e a manutenção no local: [O tipo de dados pessoais eventualmente acessíveis aos técnicos da Konica Minolta depende dos dados processados nos Sistemas. Estes conteúdos só podem ser avaliados pelo Responsável pelo Tratamento].

- Dados pessoais de base (por exemplo, nome próprio e apelido)
- Dados de comunicação (por exemplo, telefone, correio eletrónico)
- Dados mestre do contrato (por exemplo, relação contratual, produto/interesse contratual)
- Histórico do cliente (por exemplo, dados CRM)
- Dados de faturação e pagamento de contratos
- Dados de cartões de crédito e dados bancários (números de contas bancárias)
- Dados de planeamento e controlo
- Informações obtidas de terceiros (por exemplo, agências de crédito, listas públicas)
- Endereços IP, Endereços MAC



Outros:

2.2 CATEGORIAS DE TITULARES DE DADOS

Categorias de titulares de dados afetados pelo tratamento:

[As seguintes categorias de titulares de dados pessoais só podem ser avaliadas pelo Responsável pelo Tratamento.]

- Funcionários (Art. 88.º do RGPD)
- Clientes
- Potenciais clientes
- Subscritores
- Fornecedores
- Contactos comerciais
- Menores (por exemplo, aprendizes, formandos, estagiários)
- Outros:

3. SUBCONTRATADOS PELA KONICA MINOLTA

A lista de subcontratados pela Konica Minolta Business Solutions Portugal envolvidos na prestação do serviço contratado, assim como a descrição do tratamento encontra-se disponível no website, através da seguinte hiperligação <https://www.konicaminolta.pt/pt-pt/informacoes-corporativas/subcontratados-pela-konica-minolta>.

4. MEDIDAS TÉCNICAS E ORGANIZACIONAIS

1. Confidencialidade

a) Controlo de acesso físico:

- Definição das pessoas autorizadas a entrar por meio de especificações organizacionais;
- Documentação da atribuição e revogação de direitos de entrada;
- Auditoria regular dos direitos de entrada;
- Controlo de entrada com identificação fotográfica personalizada e cartão de entrada com código PIN;
- Documentação de presença nas salas de servidores;



- Regulamentos de entrada para pessoas externas.

b) Controlo de acesso ao sistema:

São adotadas as seguintes medidas para impedir a intrusão de pessoas não autorizadas nos sistemas de tratamento de dados:

- A admissão aos sistemas é possível após autenticação com um nome de utilizador e uma palavra-passe individuais;
- Utilização de palavras-passe complexas, no mínimo com oito caracteres, que preencham pelo menos três de quatro critérios (letra maiúscula, letra minúscula, número, caractere especial) e alteração obrigatória da palavra-passe de 90 em 90 dias;
- Proibição da divulgação de palavras-passe;
- Registo das atribuições de direitos de acesso;
- Limitação do acesso da administração ao mínimo;
- Proteção dos sistemas de tratamento de dados contra o acesso não autorizado através de sistemas de firewall adequados;
- Bloqueio automático dos sistemas após um período definido de inatividade.

c) Controlo de acesso aos dados:

- As atividades não autorizadas nos sistemas de tratamento de dados fora do âmbito dos direitos atribuídos serão proibidas através de direitos de acesso e de um conceito de autorização baseado nas necessidades, bem como através da respetiva inspeção;
- Limitação dos direitos de admissão aos domínios de atividade;
- Separação das autorizações de direitos (organizacionais) das atribuições de direitos (técnicas);
- Registo de alterações de direitos;
- Controlos de tentativas de acesso não autorizado (IDS/IPS).

d) Controlo de separação:

- Especificação de diferentes perfis de utilizador (níveis de administrador/utilizador);
- Direitos de acesso específicos correspondentes aos requisitos de acesso aos dados;
- Separação dos ambientes de produção e de teste através de medidas técnicas (servidores virtuais, sistemas separados, segmentação de endereços IP).

2. Integridade

a) Controlo de transmissão:

- Encriptação da transferência de dados, especialmente quando a transferência é efetuada através de redes públicas (por exemplo, SSL, TLS);
- Erradicação e/ou destruição de dados, dispositivos de armazenamento de dados e cópias impressas em conformidade com a proteção de dados, de acordo com um conceito de classe de proteção;
- Encriptação de dispositivos de armazenamento de dados;
- Opção de passagem remota para dispositivos móveis.

**b) Controlo de entrada:**

- Os direitos de acesso são regularmente verificados e atualizados;
- O registo do tratamento de dados permite uma inspeção posterior e a determinação de se e por quem os dados pessoais foram introduzidos, alterados ou removidos (por exemplo, registos de alteração de dados em sistemas ERP centrais);
- Registo e conservação, em função das necessidades, das ações correspondentes realizadas nos sistemas (por exemplo, ficheiros de registo);
- Identificação única e etiquetagem do armazenamento de dados de dispositivos MFP/PP para devolução.

3. Disponibilidade e capacidade de carga: Controlo da disponibilidade e da capacidade de restabelecimento:

- Utilização de dois centros informáticos certificados e distantes um do outro, evitando assim a interrupção do serviço por espelhamento (ou seja, pela retenção de dados redundantes);
- Precauções técnicas sob a forma de sistemas de alerta precoce para proteção contra perturbações causadas por fogo/calor, água ou sobreaquecimento;
- Medidas de proteção contra perdas de energia e sobrecargas de corrente, por exemplo, sistemas de alimentação ininterrupta (UPS);
- Realização programada de cópias de segurança de dados e utilização adicional de procedimentos de espelhamento;
- Arquitetura de antivírus/firewall com várias camadas;
- Processo estabelecido para a aquisição central de hardware e software;
- Capacidade de restabelecimento atempado (art. 32.º, n.º 1, alínea c), do RGPD) através de um conceito de cópia de segurança global relacionado com o sistema;
- Governança de TI de acordo com o Cobit;
- Atualizações regulares de todos os sistemas em utilização, quando aplicável;
- Protocolos para medidas de emergência e recuperação de dados em vigor.

4. Controlo de encomendas:

- Nomeação de um responsável pela proteção de dados;
- Acordos de nível de serviço com os prestadores de serviços externos e contratação destes em conformidade com o RGPD;
- Instrução dos trabalhadores no tratamento de dados pessoais;
- Obrigação de os trabalhadores respeitarem o sigilo dos dados;
- Salvaguarda técnica através de medidas de acesso, separação e controlos de entrada.



5. Controlo da organização (verificação, valoração e avaliação):

- São estabelecidos processos contínuos de verificação e, se necessário, de adaptação das medidas de proteção de dados;
- Processos para lidar com um caso de proteção de dados em vigor;
- Diretrizes da empresa sobre o tratamento de dados pessoais, bem como a utilização de sistemas informáticos em vigor;
- Formação correspondente dos funcionários no que respeita à segurança informática e ao RGPD;
- Gestão de resposta a incidentes.

Assinaturas

Data:
Pelo Responsável pelo Tratamento:

Data:
Pela Konica Minolta:

Nome:
Cargo:

Nome: Vasco Manuel Pereira Falcão
Cargo: Diretor Geral