Código de Privacidade da ADP para Serviços de Processamento de Dados de Clientes

Código de Privacidade da ADP para Serviços de Processamento de Dados de Clientes

Introdução

A ADP disponibiliza uma ampla gama de serviços de gestão de capital humano aos seus clientes. A ADP comprometeu-se a proteger os Dados Pessoais no **Código de Conduta e Ética nos Negócios da ADP.**

Este Código de Privacidade da ADP para Serviços de Processamento de Dados de Clientes indica como este compromisso é implementado pela ADP para o Processamento de Dados Pessoais pertencentes a Funcionários do Cliente, em conexão com a prestação de Serviços ao Cliente e Atividades de Apoio ao Cliente. Neste contexto, os Dados do Cliente são processados pela ADP como Processador de Dados em nome dos seus Clientes.

Para as regras aplicáveis ao Processamento de Dados Pessoais da ADP como Controlador de Dados referentes àqueles indivíduos com os quais a ADP possui um relacionamento comercial (por exemplo, Indivíduos que representam Clientes da ADP, Fornecedores, Parceiros Comerciais, outros Profissionais e Consumidores) e outros Indivíduos cujos Dados Pessoais são processados pela ADP no contexto das suas atividades comerciais como um Controlador de Dados, consulte o ***Código de Privacidade da ADP para Dados Empresariais***.

Artigo 1 – Âmbito, Aplicabilidade e Implementação

Âmbito – Aplicabilidade aos dados do EEE

1.1 Este Código trata do Processamento de Dados Pessoais de Funcionários de Clientes pela ADP na sua função como Processador de Dados para Clientes no curso da prestação de Serviços ao Cliente, onde tais Dados Pessoais estão (a) sujeitos à Lei Aplicável do EEE (ou estavam sujeitos à Lei Aplicável do EEE antes da transferência de tais Dados Pessoais para uma Empresa do Grupo fora do EEE num país que não tenha sido considerado como capaz de fornecer um nível adequado de proteção dos dados pelas instituições competentes do EEE); e (b) processados de acordo com um Contrato de Serviço que especificamente determina que este Código se aplicará a tais Dados Pessoais.

Onde existirem dúvidas quanto à aplicabilidade deste Código, o respetivo Administrador de Privacidade deverá procurar o conselho da Equipa de Privacidade de Dados Globais e Governança antes do Processamento ocorrer.

Processamento eletrónico e em papel

1.2 Este Código aplica-se ao Processamento de Dados de Clientes pela ADP por meio eletrónico e em sistemas de arquivo em papel sistematicamente acessíveis.

Aplicabilidade da Lei Local

1.3 Nada neste Código deverá ser interpretado para eliminar quaisquer direitos ou recursos que os Funcionários do Cliente possam ter ao abrigo da Lei Aplicável. Quando a Lei Aplicável proporcionar mais proteção do que este Código,

deverão aplicar-se as respetivas disposições da Lei Aplicável. Quando este Código proporcionar mais proteção do que a Lei Aplicável, ou fornecer salvaguardas, direitos ou recursos adicionais para Indivíduos, o mesmo deverá ser aplicado.

Políticas e Diretrizes **1.4** A ADP pode complementar este Código por meio de políticas, normas, diretrizes e instruções que sejam consistentes com este Código.

Responsabilização **1.5** Este Código é vinculativo à ADP. Os Executivos Responsáveis serão responsáveis pela conformidade das suas organizações empresariais com este Código. O pessoal da ADP deve cumprir este Código.

Data Efetiva **1.6** Este Código foi aprovado pelo Consultor Geral, mediante apresentação pelo Diretor de Privacidade Global, e foi adotado pelo Comité Executivo da ADP. Este Código entrará em vigor em 11 de abril de 2018 (**Data Efetiva**). O Código (incluindo uma lista das Empresas do Grupo envolvidas no Processamento de Dados de Clientes) será publicado no site www.adp.com. Também deve ser disponibilizado aos Indivíduos mediante solicitação.

Este Código será implementado pelo Grupo ADP com base nos prazos especificados no Artigo 16.

Políticas Prévias **1.7** Este Código complementa as políticas de privacidade da ADP e substitui as declarações anteriores na medida em que elas entrem em contradição com este Código.

Função da Entidade Delegada da ADP **1.8** A Automatic Data Processing, Inc. nomeou a ADP Nederland BV, com sede social em Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Holanda, como Entidade Delegada da ADP, responsável pela aplicação deste Código no Grupo ADP, e a ADP Nederland BV aceitou esta nomeação.

Artigo 2 – Contrato de Serviço

Contrato de Serviço, Subprocessadores **2.1** A ADP processará os Dados do Cliente apenas com base num Contrato de Serviço que incorpora os requisitos obrigatórios de contratação do processador de dados sob a Lei Aplicável do Processador de Dados e para os Fins Legítimos especificados no Artigo 4.

A Entidade Contratante da ADP usa Subprocessadores, tanto Subprocessadores da ADP como Subprocessadores Externos, no desempenho regular dos Serviços ao Cliente. Os Contratos de Serviço da ADP autorizarão o

uso de tais Subprocessadores, desde que a Entidade Contratante da ADP permaneça responsável perante o Cliente pelo desempenho dos Subprocessadores, de acordo com os termos do Contrato de Serviço. As disposições do Artigo 7 regem ainda o uso de Subprocessadores.

Cessação do Contrato de Serviço

2.2 Mediante a cessação dos Serviços ao Cliente, a ADP cumprirá as obrigações do Contrato de Serviço com o Cliente em relação ao retorno dos Dados do Cliente, fornecendo ao Cliente os Dados do Cliente necessários para a continuidade das atividades comerciais do Cliente (se os dados não forem previamente fornecidos ou disponibilizados ao Cliente através da funcionalidade relevante do produto, como a capacidade de descarregar os Dados do Cliente).

Quando as obrigações da ADP nos termos do Contrato de Serviço forem cumpridas, a ADP destruirá de forma segura as restantes cópias dos Dados do Cliente e (mediante solicitação do Cliente) certificará o Cliente de que o fez. A ADP pode manter uma cópia dos Dados do Cliente na medida exigida pela Lei Aplicável, conforme autorizado pelo Cliente, ou conforme necessário para propósitos de resolução de litígios. A ADP não processará mais os Dados do Cliente, exceto na medida do necessário para as finalidades acima mencionadas. As obrigações de confidencialidade da ADP sob o respetivo Contrato de Serviço persistirão enquanto a ADP mantiver uma cópia de tais Dados do Cliente.

Auditoria de Medidas de Cessação

2.3 No prazo de 30 dias após a cessação do Contrato de Serviço (a menos que exigido por uma Autoridade de Proteção de Dados competente), a ADP permitirá, a pedido do Cliente ou da Autoridade de Proteção de Dados competente, que as suas instalações de Processamento sejam auditadas de acordo com os Artigos 11.2. ou 11.3 (conforme aplicável) para verificar se a ADP cumpre as suas obrigações relacionadas à cessação sob o Artigo 2.2.

Artigo 3 – Obrigações de Conformidade

Instruções do Cliente

3.1 A ADP processará os Dados do Cliente em nome do Cliente, apenas de acordo com o Contrato de Serviço, conforme as instruções documentadas recebidas do Cliente ou conforme necessário para cumprir a Lei Aplicável.

Conformidade com a Lei Aplicável

3.2 A ADP processará os Dados do Cliente de acordo com a Lei Aplicável do Processador de Dados.

A ADP responderá pronta e adequadamente às solicitações de assistência do Cliente, conforme exigido por lei, para permitir que o Cliente cumpra as suas

obrigações sob a Lei Aplicável do Controlador de Dados, de acordo com o Contrato de Serviço.

Incumprimento, Efeito Adverso Substancial

3.3 Se uma Empresa do Grupo tiver conhecimento de que a Lei Aplicável do Processador de Dados de um país não pertencente ao EEE, ou qualquer alteração na Lei Aplicável do Processador de Dados de um país não pertencente ao EEE ou uma instrução do Cliente, poderá ter um efeito adverso substancial sobre a capacidade da ADP cumprir as suas obrigações sob os artigos 3.1, 3.2 ou 11.3, tal Empresa do Grupo deverá notificar prontamente a Entidade Delegada da ADP e o Cliente, em tal caso o Cliente terá o direito sob este Código de suspender temporariamente a transferência de Dados do Cliente para a ADP, até ao momento em que o processamento seja ajustado para remediar o incumprimento. No caso de um ajuste não ser possível, o Cliente terá o direito de cessar a parte relevante do Processamento pela ADP, de acordo com os termos do Contrato de Serviço. Esses direitos e obrigações não se aplicam quando as circunstâncias ou a alteração na Lei Aplicável do Processador de Dados resultarem dos Requisitos Obrigatórios.

Pedido de Divulgação dos Dados do Cliente

3.4 Se a ADP receber um pedido de divulgação de Dados do Cliente de uma autoridade de aplicação da lei ou de um órgão de segurança de um país não pertencente ao EEE (Autoridade), será avaliado primeiro, caso a caso, se esse pedido é legalmente válido e vinculativo para a ADP. Qualquer pedido que não seja legalmente válido e vinculativo à ADP sofrerá resistência de acordo com a Lei Aplicável.

Sujeito ao parágrafo a seguir, a ADP informará prontamente o Cliente, a Autoridade de Proteção de Dados (DPA) principal e a DPA competente para o Cliente, nos termos do Artigo 11.3 de qualquer pedido da Autoridade, que seja juridicamente válido e vinculativo à ADP, e solicitará à Autoridade que o coloque em espera por um período razoável, a fim de permitir que a DPA principal emita um parecer sobre a validade do pedido de divulgação.

Se a suspensão da execução e/ou notificação à DPA principal de um pedido de divulgação juridicamente válido e vinculativo for proibido, como no caso de uma proibição sob o direito penal de preservar a confidencialidade de uma investigação em relação à aplicação da lei, a ADP solicitará à Autoridade que renuncie esta proibição e documentará que fez este pedido. A ADP fornecerá, anualmente, informações gerais sobre o número e tipo de pedidos de divulgação que recebeu no prazo anterior de 12 meses, das Autoridades à DPA principal.

Este Artigo não se aplica a pedidos recebidos pela ADP de autoridades no curso normal das suas atividades como fornecedor de serviços de GCH (como ordens judiciais para guarnição de salários), que a ADP pode continuar a fornecer de

acordo com a Lei Aplicável, o Contrato de Serviço e instruções dos Clientes.

Questões do Cliente **3.5** A ADP responderá pronta e adequadamente às questões do Cliente relacionadas com o Processamento dos Dados do Cliente de acordo com os termos do Contrato de Serviço.

Artigo 4 – Finalidades do Processamento de Dados

Finalidades Legítimas de Negócio **4.1** A ADP processa os Dados Pessoais (incluindo Categorias Especiais de Dados) referentes aos Funcionários do Cliente conforme necessário para fornecer os Serviços ao Cliente, Atividades de Apoio ao Cliente e para as seguintes finalidades adicionais:

(a) Alojamento, armazenamento e outros processamentos necessários para a continuidade dos negócios e recuperação de desastres, incluindo o backup e arquivo de cópias de dados pessoais;

(b) Administração e segurança de sistemas e redes, incluindo monitorização da infraestrutura, gestão de identidades e credenciais, verificação, autenticação e controlo de acesso;

(c) Monitorização e outros controlos necessários para salvaguardar a segurança e a integridade das transações (por exemplo, transações financeiras e atividades de movimentação de dinheiro), inclusive para a devida diligência (como a verificação da identidade do Indivíduo e a qualificação do Indivíduo para receber produtos ou serviços (como a verificação da contratação ou o estado da conta);

(d) Fazer cumprir os contratos e proteger a ADP, os seus Colaboradores, Clientes, Funcionários do Cliente e o público contra roubo, responsabilidade legal, fraude ou abuso, incluindo: (i) detetar, investigar, prevenir e mitigar os danos resultantes de fraudes financeiras e as suas tentativas, fraude de identidade e outras ameaças contra ativos financeiros e físicos, credenciais de acesso e sistemas de informações; (ii) participação em iniciativas externas de segurança cibernética, antifraude e lavagem de dinheiro; e (iii) conforme necessário para proteger os interesses vitais dos Indivíduos, por exemplo, alertando os Indivíduos para uma ameaça de segurança detetada;

(e) Execução e gestão de processos de negócios internos da ADP, que levam ao processamento incidental de Dados do Cliente para:

(1) Auditoria interna e relatórios consolidados;

(2) Conformidade legal, incluindo arquivamentos obrigatórios, utilizações e divulgações de informações exigidas pela Lei Aplicável;

(3) Desidentificação de dados e agregação de dados desidentificados para a minimização de dados e análise de serviços;

(4) Uso de dados desidentificados e agregados, conforme permitido pelos Clientes, para facilitar a análise, a continuidade e a melhoria dos produtos e serviços da ADP; e

(5) Facilitar a governança corporativa, incluindo fusões, aquisições, alienações e joint ventures.

Artigo 5 – Requisitos de Segurança

Segurança dos Dados **5.1** A ADP empregará medidas técnicas, físicas e organizacionais comercialmente razoáveis e apropriadas para proteger os Dados do Cliente contra o uso indevido ou acidental, ilegal ou destruição não autorizada, perda, alteração, divulgação, aquisição ou acesso durante o processamento, que atenderá aos requisitos da Lei Aplicável do EEE, ou quaisquer exigências mais rigorosas, conforme impostas pelo Contrato de Serviço. A ADP deve, em qualquer caso, adotar as medidas especificadas no Anexo 2 deste Código, cujas medidas podem ser modificadas pela ADP, desde que tais mudanças não diminuam substancialmente o nível de segurança fornecido aos Dados do Cliente de acordo com o Anexo 2.

Acesso aos Dados e Confidencialidade **5.2** O Pessoal só será autorizado a aceder aos Dados do Cliente na medida necessária para servir os fins de processamento de dados aplicáveis nos termos do Artigo 4. A ADP impõe obrigações de confidencialidade ao Pessoal que tenha acesso aos Dados do Cliente.

Notificação de Violação da Segurança dos Dados **5.3** A ADP notificará o Cliente sobre uma Violação da Segurança dos Dados imediatamente após tomar conhecimento de que tal violação ocorreu, a menos que um funcionário responsável pela aplicação da lei ou uma autoridade supervisora determine que a notificação impediria uma investigação criminal, ou causaria danos à segurança nacional ou uma violação da confiança no setor industrial relevante. Neste caso, a notificação será adiada conforme as instruções de tal funcionário responsável pela aplicação da lei ou autoridade supervisora. A ADP responderá prontamente às solicitações do Cliente relacionadas à referida Violação da Segurança dos Dados.

1) Artigo 6 – Transparência para os Funcionários do Cliente

Outras Solicitações dos Funcionários do Cliente **6.1** A ADP notificará imediatamente o Cliente sobre solicitações ou reclamações relacionadas ao Processamento de Dados Pessoais pela ADP que sejam recebidas diretamente dos Funcionários do Cliente sem responder a tais solicitações ou reclamações, a menos que seja estabelecido de outra forma no Contrato de Serviço ou instruído pelo Cliente.

Se instruído pelo Cliente a responder às solicitações do Funcionário do Cliente e reclamações no Contrato de Serviço, a ADP deve garantir que os Funcionários do Cliente recebem todas as informações razoavelmente necessárias (como o ponto de contacto e o procedimento) para que o Funcionário possa efetivamente fazer a solicitação ou apresentar a queixa.

As disposições deste Artigo 6.1 não se aplicarão a solicitações que sejam tratadas pela ADP no curso normal da prestação de Serviços ao Cliente e Atividades de Apoio ao Cliente.

Artigo 7 – Subprocessadores

Contratos de Subprocessamento Externo **7.1** Os Subprocessadores Externos só podem processar os Dados do Cliente de acordo com um Contrato de Subprocessador. O Contrato de Subprocessador deverá impor ao Subprocessador Externo condições semelhantes de Processamento relacionadas à proteção de dados, que não serão menos protetoras do que aquelas impostas à Entidade Contratante da ADP pelo Contrato de Serviço e por este Código.

Publicação da Descrição Geral dos Subprocessadores **7.2** A ADP publicará uma descrição geral das categorias de Subprocessadores envolvidos no desempenho dos Serviços ao Cliente no respetivo website da ADP. Esta descrição geral deve ser prontamente atualizada em caso de alterações.

Notificação de Novos Subprocessadores e Direito de Objeção **7.3** A ADP notificará o Cliente sobre quaisquer novos Subprocessadores contratados pela ADP para a prestação dos Serviços ao Cliente. Num prazo de 30 dias a contar da data da receção da notificação, o Cliente poderá contestar o Subprocessador ao fornecer uma notificação por escrito à ADP alegando motivos justificáveis e objetivos relacionados à incapacidade de proteção dos Dados do Cliente por parte de tal Subprocessador, de acordo com as respetivas obrigações do Contrato de Subprocessador, conforme mencionado no artigo 7.1. No caso de as partes não chegarem a uma solução mutuamente aceitável, a ADP deverá, a seu critério, abster-se de permitir que o Subprocessador tenha acesso aos Dados do Cliente ou permitir que o

Cliente rescinda os Serviços do Cliente relevantes de acordo com os termos do Contrato de Serviço.

Exceção **7.4** As disposições desta Secção 7 não se aplicarão na medida em que o Cliente instruir a ADP para permitir que um Terceiro processe os Dados do Cliente de acordo com um contrato que o Cliente tenha diretamente com o Terceiro (por exemplo, um fornecedor de benefícios externo).

Artigo 8 – Supervisão e Conformidade

Diretor de Privacidade Global

8.1 O Grupo ADP terá um Diretor de Privacidade Global, responsável por:

(a) Presidir o Conselho de Direção de Privacidade;

(b) Supervisionar a conformidade com este Código;

(c) Supervisionar, coordenar, comunicar e consultar os membros relevantes da Rede de Privacidade sobre questões de privacidade e proteção de dados;

(d) Fornecer relatórios de privacidade anuais sobre os riscos da proteção de dados e questões de conformidade ao Comité Executivo da ADP;

(e) Coordenar investigações ou averiguações oficiais sobre o Processamento dos Dados do Cliente por uma autoridade governamental, em conjunto com os membros relevantes da Rede de Privacidade e do Departamento Jurídico da ADP;

(f) Lidar com conflitos entre este Código e a Lei Aplicável;

(g) Monitorizar o processo pelo qual as Avaliações de Impacto na Privacidade (PIAs) são conduzidas e revisar as PIAs conforme apropriado;

(h) Monitorizar a documentação, notificação e comunicação de Violações da Segurança dos Dados;

(i) Emitir pareceres sobre os processos, sistemas e ferramentas de gestão de dados para implementar a estrutura de gestão da privacidade e proteção de dados, conforme estabelecido pelo Conselho de Direção de Privacidade, incluindo:

(1) Manter, atualizar e publicar este Código, respetivas políticas e normas;

(2) Emitir pareceres sobre as ferramentas para recolha, manutenção e atualização de inventários contendo informações sobre a estrutura e funcionamento de todos os sistemas que Processam os Dados do Cliente;

(3) Fornecer, dar assistência ou aconselhamento na formação de privacidade para o Pessoal, para que este entenda e cumpra as suas responsabilidades sob este Código;

(4) Coordenar com o departamento de Auditoria Interna da ADP e outros o desenvolvimento e manutenção de um programa de controlo apropriado para monitorizar, auditar e relatar a conformidade com este Código e para permitir que a ADP verifique e certifique essa conformidade conforme necessário;

(5) Implementar procedimentos conforme necessário para abordar questões, preocupações e reclamações sobre a privacidade e a proteção de dados; e

(6) Emitir pareceres sobre as sanções apropriadas para violações deste Código (por exemplo, normas disciplinares).

Rede de Privacidade

8.2 A ADP estabelecerá uma Rede de Privacidade apta para direcionar a conformidade com este Código no seio da organização global da ADP.

A Rede de Privacidade criará e manterá uma estrutura para apoiar o Diretor de Privacidade Global e para supervisionar as tarefas definidas no Artigo 8.1 e outras tarefas que sejam apropriadas para manter e atualizar este Código. Os membros da Rede de Privacidade, conforme relevante para a sua função na região ou na organização, devem executar as seguintes tarefas adicionais:

(a) Supervisionar a implementação dos processos, sistemas e ferramentas de gestão de dados que permitam a adesão ao Código pelas empresas do Grupo nas respetivas regiões ou organizações;

(b) Apoiar e avaliar a gestão geral da privacidade, proteção de dados e a conformidade das Empresas do Grupo nas suas regiões;

(c) Emitir pareceres regularmente aos seus Administradores de Privacidade e ao Diretor de Privacidade Global sobre os riscos regionais ou locais de privacidade e questões de conformidade;

(d) Verificar se os respetivos inventários dos sistemas que Processam os Dados do Cliente estão a ser preservados;

(e) Estarem disponíveis para responder a solicitações de aprovação da privacidade ou de aconselhamento;

(f) Fornecer informações necessárias ao Diretor de Privacidade Global para completar o relatório de privacidade anual;

(g) Dar assistência ao Diretor de Privacidade Global no caso de investigações ou averiguações oficiais pelas autoridades governamentais;

(h) Desenvolver e publicar políticas de privacidade e normas apropriadas para as suas regiões ou organizações;

(i) Aconselhar as Empresas do Grupo na retenção e destruição de dados;

(j) Notificar o Diretor de Privacidade Global sobre reclamações e ajudar na resolução dessas reclamações; e

(k) Auxiliar o Diretor de Privacidade Global, outros membros da Rede de Privacidade, Administradores de Privacidade e outros, conforme necessário para:

(1) Permitir que as empresas ou organizações do Grupo cumpram o Código, utilizando as instruções, ferramentas e formações que foram desenvolvidas;

(2) Partilhar as práticas recomendadas para a gestão da privacidade e proteção de dados dentro da região;

(3) Confirmar que os requisitos de privacidade e proteção de dados são tidos em conta sempre que novos produtos e serviços forem implementados nas empresas ou organizações do Grupo; e

(4) Auxiliar os Administradores de Privacidade, Empresas do Grupo, unidades de negócios, áreas funcionais e o pessoal de aquisições com o uso de subcontratantes.

Administradores de Privacidade

8.3 Os Administradores de Privacidade são executivos da ADP que foram nomeados por um Executivo Responsável e/ou pela Direção Executiva da ADP para implementar e aplicar o Código numa unidade de negócios ou área funcional da ADP. Os Administradores de Privacidade são responsáveis pela implementação efetiva do Código na respetiva unidade de negócios ou área funcional. Em particular, os Administradores de Privacidade devem verificar se os controlos de gestão de privacidade e proteção de dados estão integrados em todas as práticas de negócios que afetam os Dados do Cliente e se os recursos e orçamento adequados estão disponíveis para atender às obrigações deste Código. Os Administradores de Privacidade poderão delegar tarefas e deverão atribuir os recursos adequados conforme necessário para cumprir as suas responsabilidades e alcançar os objetivos de conformidade.

As responsabilidades do Administrador de Privacidade incluem:

(a) Monitorizar a gestão e a conformidade geral da privacidade e a proteção de dados na sua Empresa do Grupo, unidade de negócios ou área funcional e verificar se todos os processos, sistemas e ferramentas criados pela Equipa de Privacidade de Dados Globais e Governança foram implementados de forma eficaz;

(b) Confirmar se as tarefas de gestão e conformidade da privacidade e proteção de dados são apropriadamente delegadas no curso normal dos negócios, bem como durante e após a reestruturação organizacional, terceirização, fusões, aquisições e alienações;

(c) Colaborar com o Diretor de Privacidade Global e os membros relevantes da Rede de Privacidade para entender e tratar de quaisquer novos requisitos legais, e verificar se os processos de gestão da privacidade e proteção de dados são atualizados para tratar de circunstâncias em mudança e requisitos legais e regulamentares;

(d) Consultar o Diretor de Privacidade Global e os membros relevantes da Rede de Privacidade em todos os casos em que existir um conflito real ou potencial entre a Lei Aplicável e este Código;

(e) Monitorizar os Subprocessadores usados pela Empresa do Grupo, unidade de negócios ou área funcional para confirmar a conformidade contínua dos Subprocessadores com este Código e os Contratos de Subprocessadores;

(f) Confirmar se todo o Pessoal da Empresa do Grupo, unidade de negócios ou área funcional concluiu os cursos de formação de privacidade necessários; e

(g) Direcionar os Dados do Cliente armazenados para serem excluídos, destruídos, desidentificados ou transferidos conforme exigido pelo Artigo 2.2.

Executivos Responsáveis

8.4 Os Executivos Responsáveis, como responsáveis máximos das unidades de negócios ou áreas funcionais, são responsáveis por garantir que a gestão eficaz da privacidade e a proteção de dados é implementada nas suas organizações. Cada Executivo Responsável deve (a) nomear os Administradores de Privacidade apropriados, (b) assegurar que os recursos e orçamento estão disponíveis para a conformidade e (c) fornecer apoio ao Administrador de Privacidade conforme necessário para lidar com os pontos fracos da conformidade e gerir os riscos.

Conselho de Direção de Privacidade

8.5 O Diretor de Privacidade Global deve presidir um Conselho de Direção de Privacidade composto pelos Administradores de Privacidade, membros da Rede de Privacidade nomeados pelo Diretor de Privacidade Global, e outros que possam ser necessários para auxiliar na missão do Conselho. O Conselho de Direção de Privacidade criará e manterá uma estrutura para apoiar as tarefas que possam ser apropriadas para as Empresas do Grupo, unidades de negócios e áreas funcionais para cumprirem este Código, realizarem as tarefas aqui estabelecidas e apoiarem o Diretor de Privacidade Global.

Membros da Rede de Privacidade e Administradores de Privacidade

8.6 Se a qualquer momento não existir um Diretor de Privacidade Global nomeado ou capaz de desempenhar as funções atribuídas ao cargo, o Consultor Geral deverá nomear uma pessoa para atuar como Diretor de Privacidade Global. Se a qualquer momento não existir nenhum membro da Rede de Privacidade

designado para uma região ou organização em particular, o Diretor de Privacidade Global deverá assumir as tarefas de tal membro da Rede de Privacidade estabelecidas no Artigo 8.2.

Se a qualquer momento não existir um Administrador de Privacidade designado para uma Empresa do Grupo, unidade de negócios ou área funcional, o Executivo Responsável deve nomear uma pessoa apropriada para realizar as tarefas estabelecidas no Artigo 8.3.

Cargos Estatutários **8.7** Os membros da Rede de Privacidade, por exemplo, responsáveis pela proteção de dados ao abrigo da Lei Aplicável do EEE, que ocupam as suas funções nos termos da lei, devem desempenhar as suas responsabilidades de trabalho na medida em que não entrem em conflito com os seus cargos estatutários.

Artigo 9 – Políticas e Procedimentos

Políticas e Procedimentos **9.1** A ADP deve desenvolver e implementar políticas, normas, diretrizes e procedimentos para fazer cumprir este Código.

Informação do Sistema **9.2** A ADP deve manter informações prontamente disponíveis sobre a estrutura e o funcionamento de todos os sistemas e processos que processam os Dados do Cliente, tais como inventários de sistemas e processos que impactam os Dados do Cliente, juntamente com informações geradas no curso de Avaliações de Impacto na Proteção de Dados. Uma cópia desta informação será fornecida, mediante solicitação, à DPA principal ou a uma DPA competente para o Cliente nos termos do Artigo 11.3.

Artigo 10 – Formação

Formação **10.1** A ADP fornecerá formações sobre as obrigações e princípios estabelecidos neste Código, e outras obrigações de privacidade e segurança de dados para todo o Pessoal com acesso a Dados do Cliente ou responsabilidades associadas ao Processamento de Dados do Cliente.

Artigo 11 – Monitorização e Auditoria de Conformidade

Auditorias Internas **11.1** A ADP auditará, regularmente, os processos e procedimentos de negócios que envolvem o Processamento de Dados do Cliente para estarem em conformidade com este código. Em particular:

(a) As auditorias podem ser realizadas no curso das atividades regulares da Auditoria Interna da ADP (inclusive através do uso de Terceiros independentes), e outras equipas internas envolvidas em funções de garantia, e numa base ad-hoc, a pedido do Diretor de Privacidade Global;

(b) O Diretor de Privacidade Global também pode solicitar que uma auditoria seja conduzida por um auditor externo e informará o Executivo Responsável da respetiva unidade de negócios e/ou do Comité Executivo da ADP, conforme apropriado;

(c) As normas profissionais aplicáveis de independência, integridade e confidencialidade devem ser observadas durante o processo de auditoria;

(d) O Diretor de Privacidade Global e o membro apropriado da Rede de Privacidade devem ser informados sobre os resultados das auditorias;

(e) Na medida em que a auditoria revelar um incumprimento deste Código, essas descobertas serão relatadas aos Administradores de Privacidade e aos Executivos Responsáveis relevantes. Os Administradores de Privacidade cooperarão com a Equipa de Privacidade de Dados Globais e Governança para desenvolver e executar um plano de correção apropriado;

(f) Uma cópia dos resultados da auditoria relacionados à conformidade com este Código será fornecida, mediante solicitação, à DPA principal ou a uma DPA competente nos termos do Artigo 11.3.

Auditoria de Clientes

11.2 A ADP abordará os pedidos de auditoria do Cliente, conforme descrito neste Artigo 11.2. A ADP responderá às perguntas feitas pelo Cliente em relação ao Processamento de Dados do Cliente pela ADP. Caso o Cliente considere, de forma razoável, que as respostas fornecidas pela ADP justificam uma análise mais aprofundada, a ADP deverá, de acordo com o Cliente:

(a) Disponibilizar as instalações que utiliza no Processamento de Dados do Cliente para uma auditoria realizada por um avaliador independente e qualificado que seja razoavelmente aceitável para a ADP e vinculado por obrigações de confidencialidade satisfatórias para a ADP e contratado pelo Cliente. O Cliente fornecerá uma cópia do relatório da auditoria ao Diretor de Privacidade Global, que será tratada como informação confidencial da ADP. As auditorias não serão realizadas mais de uma vez por ano, por Cliente, durante o prazo do Contrato de Serviço, durante o horário normal de funcionamento, e estarão sujeitas a (i) um pedido, por escrito, enviado à ADP com pelo menos 45 dias de antecedência da data proposta para a auditoria; (ii) um plano detalhado da auditoria, por escrito, revisado e aprovado pela organização de segurança da ADP; e (iii) as políticas de segurança no local da ADP. Tais auditorias ocorrerão apenas

na presença de um representante do Departamento de Segurança Global da ADP, da Equipa de Privacidade de Dados Globais e Governança da ADP ou de tal pessoa designada pelo respetivo representante. As auditorias não poderão interromper as atividades de Processamento da ADP ou comprometer a segurança e a confidencialidade dos dados pessoais pertencentes a outros clientes da ADP; ou

(b) A ADP fornecerá uma declaração ao Cliente, emitida por um avaliador independente e qualificado, a certificar que os processos e procedimentos de negócio da ADP que envolvem o Processamento de Dados do Cliente estão em conformidade com este Código.

A ADP pode cobrar aos Clientes uma taxa razoável por tal auditoria.

Este Artigo 11.2 complementa ou esclarece os direitos de auditoria que os Clientes podem ter nos termos da Lei Aplicável e dos Contratos de Serviços. Em caso de contradição, as disposições da Lei Aplicável e dos Contratos de Serviços prevalecerão.

Auditorias pelas Autoridade de Proteção de Dados (DPAs)

11.3 Qualquer DPA de um país do EEA que seja competente para auditar um Cliente da ADP será autorizado a auditar a transferência de dados relevantes para a conformidade com este Código, sob as mesmas condições aplicáveis a uma auditoria feita pela DPA do próprio Cliente sob a Lei Aplicável do Controlador de Dados.

Para facilitar tal auditoria:

(a) A ADP e o Cliente colaborarão de boa-fé para tentar resolver o pedido, fornecendo informações à DPA, como relatórios de auditoria da ADP, e deverão facilitar as discussões entre a DPA, e os especialistas no assunto do Cliente e da ADP, que podem revisar a segurança, privacidade e controlos operacionais que estão em vigor. O Cliente terá acesso aos seus Dados de Cliente de acordo com o Contrato de Serviço e poderá delegar tal acesso a representantes da DPA;

(b) Se as informações disponíveis através desses mecanismos forem insuficientes para atender aos objetivos declarados da DPA, a ADP fornecerá à DPA a oportunidade de entrar em contacto com o auditor da ADP;

(c) Se isso parecer insuficiente, a ADP fornecerá à DPA o direito de examinar as instalações de processamento de dados da ADP usadas para Processar os Dados do Cliente com um aviso prévio razoável, durante o horário normal de funcionamento e com total respeito perante a confidencialidade das informações obtidas e os segredos comerciais da ADP. A DPA só pode aceder aos Dados de Clientes que pertencem ao Cliente.

Este Artigo 11.3 complementa ou esclarece os direitos de auditoria que as DPAs podem ter nos termos da Lei Aplicável e dos Contratos de Serviços. Em caso de contradição, as disposições da Lei Aplicável prevalecerão.

Relatório Anual **11.4** O Diretor de Privacidade Global deverá produzir um relatório anual para o Comité Executivo da ADP sobre a conformidade com este Código, privacidade, riscos de proteção de dados e outros assuntos relevantes. Este relatório refletirá as informações fornecidas pela Rede de Privacidade e outros sobre desenvolvimentos locais e questões específicas dentro das Empresas do Grupo.

Mitigação **11.5** A ADP tomará as medidas apropriadas para resolver quaisquer casos de incumprimento deste Código identificados durante as auditorias de conformidade.

Artigo 12 – Questões Jurídicas

Direitos dos Funcionários do Cliente **12.1** Se a ADP violar o Código em relação aos Dados Pessoais de um Funcionário do Cliente coberto por este Código, , o Funcionário do Cliente poderá, como terceiro beneficiário, aplicar os Artigos 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8 e 14.3 deste Código de Processador contra a Entidade Contratante da ADP.

Na medida em que o Funcionário do Cliente possa executar quaisquer desses direitos contra a Entidade Contratante da ADP, a Entidade Contratante da ADP não poderá invocar uma violação das suas obrigações por um Subprocessador para evitar a responsabilidade, exceto na medida em que a defesa de um Subprocessador também constituirá uma defesa da ADP. A ADP pode, no entanto, afirmar quaisquer defesas ou direitos que estariam disponíveis para o Cliente. A ADP também pode reivindicar quaisquer defesas que a ADP possa ter contra o Cliente (como negligência contributiva) na defesa contra a reivindicação do Indivíduo afetado.

Procedimento de Reclamação **12.2** Os Funcionários do Cliente podem registar uma reclamação por escrito em relação a qualquer reivindicação que tenham, de acordo com o Artigo 12.1, com a Equipa de Privacidade de Dados Globais e Governança por correio ou e-mail no endereço indicado no final deste Código. O Funcionário do Cliente também pode registar uma reclamação ou reivindicação junto às autoridades ou aos

tribunais, de acordo com o Artigo 12.3 deste Código.

A Equipa de Privacidade de Dados Globais e Governança será responsável pelo tratamento das reclamações. Cada reclamação será atribuída a um membro apropriado do Pessoal (seja na Equipa de Privacidade de Dados Globais e Governança ou na respetiva unidade de negócios ou na área funcional). Este Pessoal irá:

(a) Confirmar imediatamente a receção da reclamação;

(b) Analisar a reclamação e, se necessário, iniciar uma investigação;

(c) Se a reclamação for bem fundamentada, informar o Administrador de Privacidade aplicável e o membro relevante da Rede de Privacidade para que um plano de correção possa ser desenvolvido e executado; e

(d) Manter registos de todas as reclamações recebidas, respostas dadas e ações corretivas tomadas pela ADP.

A ADP utilizará esforços necessários para resolver as reclamações sem atrasos, de modo a que seja dada uma resposta ao Funcionário do Cliente dentro de quatro semanas da data em que a reclamação foi apresentada. A resposta será dada por escrito e enviada ao Funcionário do Cliente através dos meios que o Funcionário do Cliente usou originalmente para contactar a ADP (*por exemplo*, via correio ou e-mail). A resposta descreverá as etapas que a ADP tomou para investigar a reclamação e indicará a decisão da ADP em relação a quais etapas (se existirem algumas) serão tomadas como resultado da reclamação.

No caso de a ADP não poder concluir razoavelmente a sua investigação e dar resposta dentro de quatro semanas, deverá informar o Funcionário do Cliente, dentro de quatro semanas, que a investigação está a decorrer e que uma resposta será fornecida dentro de um prazo de oito semanas.

Se a resposta da ADP à reclamação for insatisfatória para o Funcionário do Cliente (por exemplo, a solicitação for negada) ou a ADP não observar as condições do procedimento de reclamações estabelecido neste Artigo 12.2, o Funcionário do Cliente poderá registar uma reclamação ou reivindicação junto às autoridades ou nos tribunais, de acordo com o Artigo 12.3.

Jurisdição para Reivindicações de Funcionários do Cliente

12.3 Os Funcionários do Cliente são encorajados a seguir, em primeiro lugar, o procedimento de reclamações estabelecido no Artigo 12.2 deste Código antes de apresentar qualquer reclamação ou reivindicação junto às autoridades ou tribunais.

Os Funcionários do Cliente podem, à sua escolha, submeter reivindicações de

acordo com o Artigo 12.1 apresentando uma reclamação
(i) à DPA no país da sua residência habitual, local de trabalho ou local onde ocorreu a infração, contra a Entidade Contratante da ADP ou a Entidade Delegada da ADP; ou
(ii) à DPA principal ou aos tribunais da Holanda, mas, nesse caso, apenas contra a Entidade Delegada da ADP.

Os Funcionários do Cliente podem, à sua escolha, submeter reivindicações de acordo com o Artigo 12.1 apresentando uma reclamação:
(i) aos tribunais do país da sua residência habitual, ou do país de origem da transferência de dados ao abrigo do presente Código, contra a Entidade Contratante da ADP ou a Entidade Delegada da ADP; ou
(ii) à DPA principal ou aos tribunais da Holanda, mas, nesse caso, apenas contra a Entidade Delegada da ADP.

As DPAs e os tribunais devem aplicar as suas próprias leis substantivas e processuais aos litígios. A escolha tomada pelo Funcionário do Cliente não prejudicará os direitos substantivos ou processuais que as partes possam ter sob a Lei Aplicável.

Direitos dos Clientes

12.4 O Cliente poderá fazer cumprir este Código contra (i) a Entidade Contratante da ADP ou, (ii) a Entidade Delegada da ADP perante a DPA principal ou os tribunais da Holanda, mas apenas se a Entidade Contratante da ADP não estiver estabelecida num país do EEE. A Entidade Delegada da ADP deve garantir que são tomadas as medidas necessárias para lidar com as violações deste Código pela Entidade Contratante da ADP, ou qualquer outra Empresa do Grupo envolvida.

A Entidade Contratante da ADP e a Entidade Delegada da ADP não podem invocar uma violação das suas obrigações por outra Empresa do Grupo ou um Subprocessador para evitar a responsabilidade, exceto na medida em que a defesa de tal Empresa do Grupo ou Subprocessador constituiria também uma defesa da ADP.

Medidas Corretivas Disponíveis, Ónus da Prova para Funcionários do Cliente

12.5 No caso de um Funcionário do Cliente ter uma reivindicação de acordo com o Artigo 12.1, o Funcionário do Cliente terá direito a uma indemnização por quaisquer danos, na medida prevista pela lei aplicável do EEE.

Se os Funcionários do Cliente apresentarem reivindicações por danos nos termos do Artigo 12.1, os Funcionários do Cliente terão o ónus de demonstrar que sofreram danos e de estabelecer factos plausíveis que demonstrem que os danos ocorreram devido a uma violação deste Código. Posteriormente, a

Entidade Contratante da ADP (ou a Entidade Delegada ADP, conforme aplicável) terá o ónus de provar que os danos sofridos pelos Funcionários do Cliente devido a uma violação deste Código não são imputáveis à respetiva Empresa do Grupo ou ao Subprocessador, ou de reivindicar outras defesas aplicáveis.

Compensação do Cliente

12.6 Em caso de violação deste Código, e sujeito aos termos do Contrato de Serviço, os Clientes terão direito a uma compensação de danos diretos, de acordo com as disposições do Contrato de Serviço.

Assistência Mútua

12.7 Todas as Empresas do Grupo deverão, conforme necessário, cooperar e auxiliar, na medida do razoavelmente possível, com (a) o tratamento de um pedido, reclamação ou reivindicação feita por um Cliente ou um Funcionário do Cliente ou (b) o cumprimento de uma investigação ou averiguação por uma autoridade governamental competente.

A Empresa do Grupo que receber um pedido de informação nos termos do Artigo 6.1, ou uma reclamação ou reivindicação nos termos do Artigo 12.2 ou 12.3, é responsável por tratar de toda a comunicação com o Cliente ou com o Funcionário do Cliente em relação ao pedido ou reivindicação, exceto em circunstâncias que ditem o contrário, ou conforme indicado pela Equipa de Privacidade de Dados Globais e Governança.

Conselhos da DPA e Decisões Vinculativas

12.8 A ADP cooperará de boa-fé e realizará todos os esforços razoáveis para seguir os conselhos da DPA principal e da DPA competente, conforme o Artigo 12.3, sobre a interpretação e aplicação deste Código. A ADP respeitará as decisões vinculativas das DPAs competentes.

Lei Aplicável a este Código

12.9 Este Código será regido e interpretado de acordo com a lei holandesa.

Artigo 13 – Sanções por Incumprimento

Incumprimento

13.1 O incumprimento deste Código, por parte do Pessoal, poderá resultar em medidas adequadas de natureza disciplinar ou contratual, de acordo com a lei aplicável e as políticas da ADP, até e incluindo o término da relação de emprego ou contratual.

Artigo 14 – Conflitos entre este Código e a Lei Aplicável do Processador de Dados

Conflito entre este Código e a Lei

14.1 Quando existir um conflito entre a Lei Aplicável do Processador de Dados e este Código, o Executivo Responsável ou o Administrador de Privacidade deverá consultar o Diretor de Privacidade Global, o(s) membro(s) relevante(s) da Rede de Privacidade (conforme apropriado) e o departamento jurídico da unidade de negócios para determinar como fazer cumprir este Código, e para resolver o conflito na medida do razoavelmente possível, dados os requisitos legais aplicáveis à ADP.

Novos Requisitos Legais Contraditórios

14.2 Os membros do departamento jurídico, os Responsáveis pela Segurança da Empresa da ADP e os Administradores de Privacidade informarão imediatamente a Equipa de Privacidade de Dados Globais e Governança sobre quaisquer novos requisitos legais dos quais tenham conhecimento que possam interferir na capacidade da ADP para cumprir este Código.

Os Administradores de Privacidade relevantes, em consulta com o departamento jurídico, deverão informar imediatamente os Executivos Responsáveis sobre qualquer novo requisito legal que possa interferir na capacidade da ADP para cumprir este Código.

Reportar à DPA principal

14.3 Se a ADP tiver conhecimento de que a Lei Aplicável do Processador de Dados ou qualquer alteração na Lei Aplicável do Processador de Dados possa ter um efeito adverso substancial na capacidade da ADP para cumprir as suas obrigações sob os Artigos 3.1, 3.2 ou 11.3, a ADP reportará isso à DPA principal.

Artigo 15 – Alterações a este Código

Aprovação para Alterações

15.1 Quaisquer alterações materiais a este Código exigem a aprovação prévia do Diretor de Privacidade Global e do Consultor Geral, e a adoção pelo Comité Executivo da ADP e, serão depois comunicadas às Empresas do Grupo. Alterações imateriais ao Código podem ser feitas mediante a aprovação prévia do Diretor de Privacidade Global. A Entidade Delegada da ADP deve notificar, anualmente, a DPA principal sobre as alterações feitas a este Código.

Quando uma alteração a este Código tiver um impacto significativo nas condições de Processamento dos Serviços ao Cliente, a ADP informará prontamente a DPA principal, dando inclusive uma breve explicação para tal alteração, como também notificará o Cliente sobre tal alteração. No prazo de 30 dias após a receção da notificação, o Cliente poderá opor-se a tal alteração, fornecendo uma notificação, por escrito, à ADP. No caso de as partes não conseguirem chegar a uma solução mutuamente aceitável, a ADP implementará uma solução alternativa de transferência de dados. No caso de nenhuma solução alternativa de transferência de dados poder ser implementada, o Cliente terá o direito, de acordo com este Código, de suspender a respetiva transferência dos seus Dados para a ADP. Caso não seja possível a suspensão das transferências de dados, a ADP permitirá que o Cliente cesse os respetivos Serviços do Cliente de acordo com os termos do Contrato de Serviço.

Aprovação para Alterações

15.1 Quaisquer alterações materiais a este Código exigem a aprovação prévia do Diretor de Privacidade Global e do Consultor Geral, e a adoção pelo Comité Executivo da ADP e, serão depois comunicadas às Empresas do Grupo. Alterações imateriais ao Código podem ser feitas mediante a aprovação prévia do Diretor de Privacidade Global. A Entidade Delegada da ADP deve notificar, anualmente, a DPA principal sobre as alterações feitas a este Código.

Quando uma alteração a este Código tiver um impacto significativo nas condições de Processamento dos Serviços ao Cliente, a ADP informará prontamente a DPA principal, dando inclusive uma breve explicação para tal alteração, como também notificará o Cliente sobre tal alteração. No prazo de 30 dias após a receção da notificação, o Cliente poderá opor-se a tal alteração, fornecendo uma notificação, por escrito, à ADP. No caso de as partes não conseguirem chegar a uma solução mutuamente aceitável, a ADP implementará uma solução alternativa de transferência de dados. No caso de nenhuma solução alternativa de transferência de dados poder ser implementada, o Cliente terá o direito, de acordo com este Código, de suspender a respetiva transferência dos seus Dados para a ADP. Caso não seja possível a suspensão das transferências de dados, a ADP permitirá que o Cliente cesse os respetivos Serviços do Cliente de acordo com os termos do Contrato de Serviço.

Data Efetiva das Alterações

15.2 Qualquer alteração entrará em vigor com efeito imediato após a sua aprovação, de acordo com o Artigo 15.1, publicada no website www.adp.com e comunicada aos Clientes.

Versões Anteriores **15.3** Qualquer pedido, reclamação ou reivindicação de um Funcionário do Cliente envolvendo este Código será julgado de acordo com a versão deste Código que está em vigor no momento em que é feito o pedido, reclamação ou reivindicação.

Artigo 16 – Implementação e Períodos de Transição

Implementação **16.1** A implementação deste Código deve ser supervisionada pelos Administradores de Privacidade, com a assistência da Equipa de Privacidade de Dados Globais e Governança. Exceto conforme indicado abaixo, haverá um período de transição de dezoito meses a partir da Data Efetiva (conforme estabelecido no Artigo 1.6) para a conformidade com este Código.

Consequentemente, exceto quando indicado de outra forma, dentro de dezoito meses da Data Efetiva, todo o Processamento de Dados do Cliente deverá ser realizado em conformidade com este Código, e o Código deverá estar plenamente em vigor. Durante o período de transição, o Código entrará em vigor para uma Empresa do Grupo, assim que a Empresa do Grupo completar as tarefas necessárias para a implementação total e assim que tenha fornecido uma notificação apropriada ao Diretor de Privacidade Global.

Novas Empresas do Grupo **16.2** Qualquer entidade que se torne uma Empresa do Grupo após a Data Efetiva deverá cumprir este Código dentro de dois anos após se tornar uma Empresa do Grupo.

Entidades Desvinculadas **16.3** Uma Entidade Desvinculada permanecerá coberta por este Código após a sua desvinculação por tal período como é exigido pela ADP para desembaraçar o Processamento de Dados do Cliente relacionado a essa Entidade Desvinculada.

Período de Transição para Contratos em Vigor **16.4** Quando existirem contratos em vigor com Subprocessadores ou outros Terceiros que sejam afetados por este Código, as disposições dos contratos prevalecerão até que os contratos sejam renovados no curso normal dos negócios; desde que, no entanto, todos esses contratos em vigor estejam em conformidade com este Código dentro de 18 meses a partir da Data Efetiva.

Dados de Contacto

Equipa de Privacidade de Dados Globais e Governança da ADP:
privacy@adp.com

Entidade Delegada da ADP
ADP Nederland B.V.

Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
HOLANDA

Interpretações

INTERPRETAÇÕES DESTE CÓDIGO:

(i) A menos que o contexto exija o contrário, todas as referências a um determinado Artigo ou Anexo são referências a esse Artigo ou Anexo no presente documento ou a este documento, uma vez que podem periodicamente ser alteradas;

(ii) Os títulos são incluídos apenas por conveniência e não devem ser usados na interpretação de qualquer disposição deste Código;

(iii) Se uma palavra ou frase é definida, as suas outras formas gramaticais têm um significado correspondente;

(iv) A forma masculina deve incluir a forma feminina;

(v) As palavras "incluir", "inclua", "incluindo" e quaisquer palavras que as sigam devem ser interpretadas sem limitação à generalidade de quaisquer palavras ou conceitos precedentes e vice-versa;

(vi) A palavra “escrita” deve incluir qualquer comunicação documentada, escrita, contrato, registo eletrónico, assinatura eletrónica, cópia fac-símile ou outro instrumento legalmente válido e exequível, sem ter em conta o formato;

(vii) Uma referência a um documento (incluindo, sem limitação, uma referência a este Código) é para o documento como emendado, variado, suplementado ou substituído, exceto na medida proibida por este Código ou pelo documento referenciado; e

(viii) Uma referência à lei inclui qualquer requisito regulamentar, recomendação setorial e práticas recomendadas emitidas pelas autoridades de supervisão nacionais e internacionais relevantes ou outros órgãos.

ANEXO 1 – Definições BCR

Decisão de Adequação	DECISÃO DE ADEQUAÇÃO significa qualquer determinação por uma Autoridade de Proteção de Dados ou outro órgão competente, de que um país, uma região ou um destinatário de uma transferência de dados é considerado como fornecendo um nível adequado de proteção dos Dados Pessoais. Entidades abrangidas por uma Decisão de Adequação incluem destinatários localizados em países que, de acordo com a Legislação Aplicável, são considerados como fornecendo um nível adequado de proteção de dados, bem como aqueles vinculados por outro instrumento (como um conjunto de Regras Corporativas Vinculativas), que foram aprovadas pela Autoridade de Proteção de Dados aplicável ou outro órgão competente. Em relação aos Estados Unidos, as empresas que se tornarem certificadas para qualquer estrutura de privacidade dos EUA-EEE e/ou EUA-Suíça seriam abrangidas por uma Decisão de Adequação.
ADP (Grupo ADP)	ADP (o GRUPO ADP) significa, coletivamente, a Automatic Data Processing, Inc. (a Empresa-Mãe) e as Empresas do Grupo, incluindo a ADP, Inc.
Entidade Contratante da ADP	ENTIDADE CONTRATANTE da ADP significa a Empresa do Grupo que celebrou um contrato exigido pelos Códigos, como o Contrato de Serviço, o Contrato de Subprocessador ou o contrato de transferência de dados.
Entidade Delegada da ADP	ENTIDADE DELEGADA DA ADP significa a ADP Nederland, B.V., com sede social em Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Holanda.
Comité Executivo da ADP	COMITÉ EXECUTIVO DA ADP significa o comité de diretores composto pelo (i) diretor executivo (CEO) da Automatic Data Processing, Inc., e (ii) os outros diretores que reportam diretamente ao CEO e que, coletivamente, têm responsabilidade pelas Operações do grupo ADP.
Subprocessador da ADP	Para o efeito do Código de Privacidade para Serviços de Processamento de Dados de Clientes, um SUBPROCESSADOR da ADP significa qualquer Empresa do Grupo contratada por outra Empresa do Grupo como um Subprocessador para os Dados do Cliente.
Lei Aplicável do Controlador de Dados	Para o efeito do Código de Privacidade para Serviços de Processamento de Dados de Clientes, LEI APLICÁVEL DO CONTROLADOR DE DADOS significa quaisquer leis de privacidade ou proteção de dados que se apliquem a um Cliente da ADP, como o Controlador de Dados de tais Dados do Cliente.

Lei Aplicável do Processador de Dados	Para o efeito do Código de Privacidade para Serviços de Processamento de Dados de Clientes, LEI APLICÁVEL DO PROCESSADOR DE DADOS significa quaisquer leis de privacidade ou proteção de dados que se apliquem à ADP como o Processador de Dados, em nome de um Cliente que é um Controlador de Dados.
Lei Aplicável	LEI APLICÁVEL significa qualquer lei de privacidade ou proteção de dados que seja aplicável a qualquer atividade de Processamento específica.
Candidato	CANDIDATO significa qualquer Indivíduo que forneça Dados Pessoais à ADP no contexto de candidatura a uma posição com a ADP como um Colaborador.
Arquivo	ARQUIVO significa uma coleção de Dados Pessoais que não são mais necessários para atingir as finalidades para as quais os Dados foram originalmente recolhidos ou que não são mais usados para as atividades gerais da empresa, mas são potencialmente usados apenas para fins históricos, científicos ou estatísticos, resolução de disputas, investigações ou finalidades gerais do arquivo. O acesso a um Arquivo é limitado aos administradores do sistema e a outras pessoas cujas tarefas exigem um acesso específico ao arquivo.
Colaborador	COLABORADOR significa um Candidato, um funcionário atual da ADP ou um ex-funcionário da ADP, com a exceção de um Indivíduo Colaborador. NOTA: o Código de Privacidade do Local de Trabalho da ADP não se aplica, portanto, ao Processamento de Dados Pessoais de Indivíduos Colaboradores.
Automatic Data Processing, Inc.	A AUTOMATIC DATA PROCESSING, INC. é a empresa-mãe do Grupo ADP, e é uma corporação registada no Delaware (EUA) com o seu principal local de negócios na One ADP Boulevard, Roseland, Nova Jérsia, 07068-1728, EUA.
Regras Corporativas Vinculativas	REGRAS CORPORATIVAS VINCULATIVAS significam uma política de privacidade de um grupo de empresas consideradas para fornecer um nível adequado de proteção da transferência de Dados Pessoais dentro desse grupo de empresas sob a Lei Aplicável.
Dados de Contacto Comercial	DADOS DE CONTACTO COMERCIAL significam todos os dados pertencentes a um profissional que se encontram normalmente num cartão de visita ou numa assinatura de e-mail.
Parceiro Comercial	PARCEIRO COMERCIAL significa qualquer terceiro, que não seja um Cliente ou Fornecedor que tem ou teve um relacionamento comercial ou uma aliança estratégica com a ADP (*por exemplo*, parceiro de

	marketing conjunto, joint venture ou parceiro de desenvolvimento conjunto).
Finalidade de Negócio	FINALIDADE DE NEGÓCIO significa um fim legítimo para Processar Dados Pessoais, conforme especificado nos Artigo 2, 3 ou 4 de qualquer Código da ADP, ou para Processar Categorias Especiais de Dados, conforme especificado no Artigo 4 de qualquer Código da ADP.
Crianças	Para fins de recolha de dados e marketing da ADP, CRIANÇAS significa Pessoas abaixo da idade determinada pela lei aplicável como capazes de consentir com tal recolha de dados e/ou marketing.
Cliente	CLIENTE significa qualquer Terceiro que utilize um ou mais produtos ou serviços da ADP no curso do seu próprio negócio.
Dados do Cliente	DADOS DO CLIENTE significam Dados Pessoais pertencentes a Funcionários do Cliente (incluindo possíveis funcionários, ex-funcionários e dependentes de funcionários) Processados pela ADP em relação à prestação de Serviços ao Cliente.
Funcionário do Cliente	FUNCIONÁRIO DO CLIENTE significa qualquer Indivíduo cujos Dados Pessoais são Processados pela ADP como um Processador de Dados para um Cliente de acordo com um Contrato de Serviços. Por uma questão de clareza, FUNCIONÁRIO DO CLIENTE refere-se a todos os Indivíduos cujos Dados Pessoais são processados pela ADP na prestação de Serviços ao Cliente (independentemente da natureza jurídica da relação entre o Indivíduo e o Cliente). Não inclui Profissionais cujos Dados Pessoais são Processados pela ADP em conexão com o relacionamento direto da ADP com o Cliente. Por exemplo, a ADP pode Processar Dados Pessoais de um Profissional de RH para celebrar um contrato com o Cliente - estes Dados estão sujeitos ao Código de Privacidade para Dados Empresariais. No entanto, quando a ADP fornece serviços de Processamento salariais ao Cliente (por exemplo, emissão de folhas de pagamento, fornecimento de assistência sobre o uso de um sistema da ADP), os dados do Indivíduo seriam Processados como Dados do Cliente.
Serviços ao Cliente	SERVIÇOS AO CLIENTE significam os serviços de gestão de capital humano que são fornecidos pela ADP aos Clientes, tais como serviços de recrutamento, salariais e compensação, benefícios dos funcionários, gestão de talentos, administração de RH, consultoria, análise e serviços de reforma.
Atividades de Apoio ao Cliente	ATIVIDADES DE APOIO AO CLIENTE significam aquelas atividades de Processamento realizadas pela ADP para apoiar a entrega dos seus produtos e serviços. As Atividades de Apoio ao Cliente podem incluir, por exemplo, formação de profissionais, respostas a perguntas

	sobre os serviços, abertura e resolução de pedidos de apoio, fornecimento de informações sobre produtos e serviços (incluindo atualizações e alertas de conformidade), controlo e monitorização da qualidade e respetivas atividades que facilitem o uso efetivo dos produtos e serviços da ADP.
Código	CÓDIGO significa (conforme aplicável) o Código de Privacidade da ADP para Dados Empresariais, o Código de Privacidade do Local de Trabalho da ADP (interno à ADP) e o Código de Privacidade para Serviços de Processamento de Dados do Cliente; coletivamente referidos como os Códigos.
Indivíduo Colaborador	INDIVÍDUO COLABORADOR significa um funcionário de um Cliente dos EUA que é associado de uma filial indireta dos EUA da Automatic Data Processing, Inc. como parte da oferta de serviço da organização do empregador profissional nos EUA.
Consumidor	CONSUMIDOR significa um Indivíduo que interage diretamente com a ADP a título pessoal. Por exemplo, Consumidores incluem indivíduos que participam em programas de desenvolvimento de talentos ou utilizam produtos e serviços da ADP para uso pessoal (*ou seja*, fora de uma relação laboral com a ADP ou com um Cliente da ADP).
Trabalhador Contingente	TRABALHADOR CONTINGENTE significa um Indivíduo que presta serviços à ADP (e que está sujeito à supervisão direta da ADP) numa base provisória ou não permanente, como trabalhadores temporários, trabalhadores contratados, prestadores de serviços independentes ou consultores.
Controlador de Dados	CONTROLADOR DE DADOS significa a entidade ou pessoa singular que sozinha, ou em conjunto com outras pessoas, determina os propósitos e meios do Processamento de Dados Pessoais.
Processador de Dados	PROCESSADOR DE DADOS significa a entidade ou pessoa física que processa dados pessoais em nome de um controlador de dados.
Autoridade de Proteção de Dados ou DPA	AUTORIDADE DE PROTEÇÃO DE DADOS OU DPA significa qualquer autoridade reguladora ou supervisora que supervisiona a proteção de dados ou a privacidade num país no qual uma Empresa do Grupo é estabelecida.
Avaliação de Impacto na Proteção de Dados (DPIA)	AVALIAÇÃO DE IMPACTO NA PROTEÇÃO DE DADOS (DPIA) significa um procedimento para conduzir e documentar uma avaliação prévia do impacto que um determinado Processamento possa ter na proteção de Dados Pessoais, quando tal Processamento pode resultar num risco elevado para os direitos e liberdades dos Indivíduos, em

	especial quando são utilizadas novas tecnologias. Uma DPIA deverá conter: (i) uma descrição: (a) do âmbito e contexto do Processamento; (b) da Finalidade de Negócio para os quais os Dados Pessoais são Processados; (c) das finalidades específicas para as quais Categorias Especiais de Dados são Processadas; (d) das categorias de destinatários de Dados Pessoais, incluindo destinatários não abrangidos por uma Decisão de Adequação; (e) dos períodos de armazenamento de Dados Pessoais; (ii) Uma avaliação: (a) da necessidade e proporcionalidade do Processamento; (b) dos riscos para os direitos de privacidade dos Indivíduos; e das medidas para mitigar esses riscos, incluindo salvaguardas, medidas de segurança e outros mecanismos (tais como a privacidade na conceção) para garantir a proteção dos Dados Pessoais.
Violação da Segurança dos Dados	VIOLAÇÃO DA SEGURANÇA DOS DADOS significa qualquer incidente que afeta a confidencialidade, integridade ou disponibilidade dos Dados Pessoais, tais como o uso ou acesso não autorizado ou divulgação de Dados Pessoais, que comprometa a privacidade ou segurança dos Dados Pessoais.
Dependente	DEPENDENTE significa o cônjuge, parceiro, filho ou beneficiário de um Colaborador, ou o contacto de emergência de um Colaborador ou Trabalhador Contingente.
Entidade Desvincula	ENTIDADE DESVINCULADA significa uma Empresa do Grupo que deixou de ser propriedade da ADP como resultado da venda de ações e/ou ativos da empresa, ou outra alienação, na medida em que a empresa não se classifica mais como uma Empresa do Grupo.
EEE	EEE ou ESPAÇO ECONÓMICO EUROPEU significa todos os Estados Membros da União Europeia, mais a Noruega, a Islândia e o Liechtenstein e, para efeitos dos Códigos, a Suíça e o Reino Unido após sua saída da União Europeia. Por decisão do Conselho Geral – a ser publicado em www.adp.com pode incluir outros países com leis de proteção de dados com restrições de transferência de dados semelhantes às Restrições de Transferência de Dados do EEE.

Lei Aplicável do EEE	LEI APLICÁVEL DO EEE significa os requisitos previstos pelas Leis Aplicáveis do EEE, que são aplicáveis a quaisquer Dados Pessoais originalmente recolhidos no contexto das atividades de uma Empresa do Grupo estabelecida no EEE (também após a transferência para outra Empresa do Grupo estabelecida fora do EEE).
Restrição de Transferência de Dados do EEE	RESTRIÇÃO DE TRANSFERÊNCIA DE DADOS DO EEE significa qualquer restrição relativa a transferências internacionais de Dados Pessoais sob as leis de proteção de dados de um país do EEE.
Data Efetiva	DATA EFETIVA significa a data em que os Códigos entram em vigor, conforme estabelecido no Artigo 1 dos Códigos.
Consultor geral	CONSULTOR GERAL significa o Consultor Geral da Automatic Data Processing, Inc.
Diretor de Privacidade Global	DIRETOR DE PRIVACIDADE GLOBAL significa o Colaborador da ADP que ocupa este cargo na Automatic Data Processing, Inc.
Empresa do Grupo	EMPRESA DO GRUPO significa qualquer entidade legal que seja uma filial da Automatic Data Processing, Inc. e/ou da ADP, Inc, se a Automatic Data Processing, Inc. ou a ADP, Inc. deter, direta ou indiretamente, mais de 50% do capital social emitido, detém 50% ou mais do poder de voto nas assembleias gerais de acionistas, tem o poder de nomear a maioria dos diretores ou de outra forma dirigir as atividades de tal entidade legal.
Indivíduo	INDIVÍDUO significa qualquer pessoa física identificada ou identificável cujos Dados Pessoais são Processados pela ADP como um Processador de Dados ou um Controlador de Dados, com a exceção de Indivíduos Colaboradores. NOTA: o Código de Privacidade da ADP para Dados Empresariais e o Código de Privacidade do Local de Trabalho da ADP não se aplicam, portanto, ao Processamento de Dados Pessoais de Indivíduos Colaboradores.
Processador Interno	PROCESSADOR INTERNO significa qualquer Empresa do Grupo que Processe Dados Pessoais em nome de outra Empresa do Grupo, sendo o Controlador de Dados.
DPA principal	DPA PRINCIPAL significa a Autoridade de Proteção de Dados Holandesa.
Requisitos Obrigatórios	REQUISITOS OBRIGATÓRIOS significam aquelas obrigações sob qualquer Lei Aplicável do Processador de Dados que requerem o Processamento de Dados Pessoais para (i) segurança nacional ou defesa; (ii) segurança pública; (iii) a prevenção, investigação, deteção

	ou repressão de infrações penais ou de violações da ética para profissões regulamentadas; ou (iv) a proteção de qualquer Indivíduo, ou os direitos e liberdades dos Indivíduos.
Equipa de Privacidade de Dados Globais e Governança	EQUIPA DE PRIVACIDADE DE DADOS GLOBAIS E GOVERNANÇA significa o Departamento de Privacidade e Governança de Dados da ADP. O Departamento de Privacidade e Governança de Dados é dirigido pelo Diretor de Privacidade Global e é composto pelos diretores de privacidade, gestores de privacidade e outro Pessoal com relações profissionais com o Diretor de Privacidade Global ou com os diretores privacidade e gestores de privacidade.
Interesse Primordial	INTERESSE PRIMORDIAL significa os interesses prementes estabelecidos no Artigo 13.1 do Código de Privacidade do Local de Trabalho da ADP e do Código de Privacidade da ADP para Dados Empresariais, com base no qual, as obrigações da ADP ou os direitos dos Indivíduos estabelecidos nos Artigos 13.2 e 13.3 dos Códigos podem, sob circunstâncias especificas, ser anulados se este interesse premente superar o interesse do Indivíduo.
Dados Pessoais ou Dados	DADOS PESSOAIS ou DADOS significam qualquer informação relacionada a um Indivíduo identificado ou identificável. Os Dados Pessoais também podem ser referidos como informações pessoais em políticas e normas que implementam os Códigos.
Conselho de Direção de Privacidade	CONSELHO DE DIREÇÃO DE PRIVACIDADE significa o conselho liderado pelo Diretor de Privacidade Global e composto pelos Administradores de Privacidade, membros da Rede de Privacidade selecionados pelo Diretor de Privacidade Global, e outros que possam ser necessários para auxiliar na missão do Conselho.
Rede de Privacidade	REDE DE PRIVACIDADE significa os membros da Equipa de Privacidade de Dados Globais e Governança e outros membros do Departamento Jurídico, incluindo profissionais de conformidade e oficiais de proteção de dados responsáveis pela conformidade da privacidade nas suas respetivas regiões, países, unidades de negócios ou áreas funcionais.
Administrador de Privacidade	ADMINISTRADOR DE PRIVACIDADE significa um executivo da ADP que foi nomeado por um Executivo Responsável e/ou pela Direção Executiva da ADP para implementar e fazer cumprir os Códigos de Privacidade numa Unidade de Negócios da ADP.
Processamento	PROCESSAMENTO significa qualquer operação executada nos Dados Pessoais, seja ou não por meios automáticos, como recolha, registo, armazenamento, organização, alteração, uso, divulgação (incluindo a concessão de acesso remoto), transmissão ou exclusão

	de Dados Pessoais.
Contrato de Processador	CONTRATO DE PROCESSADOR significa qualquer contrato para o Processamento de Dados Pessoais celebrado entre a ADP e um Processador Externo.
Profissional	PROFISSIONAL significa qualquer indivíduo (que não seja um funcionário) que interage diretamente com a ADP numa capacidade profissional ou comercial. Por exemplo, os Profissionais incluem a equipa de RH do cliente que se envolve com a ADP como utilizadores dos produtos ou serviços da ADP. Os Profissionais também incluem representantes de contas de Clientes, Fornecedores e Parceiros Comerciais, contactos comerciais, contactos de associações de comércio, reguladores, contactos dos meios de comunicação e outras pessoas que interagem com a ADP numa capacidade comercial.
Executivo Responsável	EXECUTIVO RESPONSÁVEL significa o Diretor Administrativo de uma Empresa do Grupo, ou chefe de uma unidade de negócios ou área funcional, que possui propriedade orçamentária primária para a Empresa do Grupo, unidade de negócios ou área funcional.
Finalidade secundária	FINALIDADE SECUNDÁRIA significa qualquer finalidade diferente da Finalidade Original para a qual os Dados Pessoais são processados.
Contrato de Serviços	CONTRATO DE SERVIÇOS significa qualquer contrato, acordo ou termos segundo os quais a ADP fornece Serviços a um Cliente.
Categorias Especiais de Dados	CATEGORIAS ESPECIAIS DE DADOS significam Dados Pessoais que revelam a origem racial ou étnica de um Indivíduo, opiniões políticas ou filiação em partidos políticos ou organizações semelhantes, crenças religiosas ou filosóficas, participação num organização profissional, comercial ou sindicato, saúde física ou mental incluindo qualquer parecer sobre isso, deficiências, código genético, vícios, vida sexual, ofensas criminais, antecedentes criminais ou processos relativos a um comportamento criminoso ou ilegal.
Pessoal	PESSOAL significa, coletivamente, os Colaboradores da ADP atualmente empregados e os Trabalhadores Contingentes que estão atualmente a trabalhar para a ADP.
Contrato de Subprocessador	CONTRATO DE SUBPROCESSADOR significa um contrato por escrito ou eletrónico entre a ADP e um Subprocessador Externo de acordo com o Artigo 7.1 do Código de Privacidade para Serviços de Processamento de Dados do Cliente.

Subprocessadores	SUBPROCESSADORES significam, coletivamente, Subprocessadores da ADP e Subprocessadores Externos.
Fornecedores	FORNECEDOR significa qualquer terceiro que forneça bens ou serviços à ADP (por exemplo, como um fornecedor de serviços, agente, Processador de Dados, consultor ou vendedor).
Terceiro	TERCEIRO significa qualquer pessoa, organização privada ou órgão governamental que não seja uma Empresa do Grupo.
Controlador Externo	CONTROLADOR EXTERNO significa um Terceiro que Processa Dados Pessoais e determina as finalidades e os meios do Processamento.
Processador Externo	PROCESSADOR EXTERNO significa um Terceiro que Processa Dados Pessoais em nome da ADP e que não está sob a autoridade direta da ADP.
Subprocessador Externo	SUBPROCESSADOR EXTERNO significa qualquer Terceiro contratado pela ADP como Subprocessador.

ANEXO 2 - **Medidas de Segurança**

Presented by:	**ADP - Global Security Organization**
Version:	**2.0**
Released:	**September 2019**

Contents

Terms and Definitions

The following terms may appear throughout the document:

Term or Acronym used	Definition
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Overview

ADP maintains a formal information security program containing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of client information. This program is reasonably designed to (i) safeguard the security and confidentiality of client information, (ii) protect against anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information.

This document contains an overview of ADP's information security measures and practices, as of the release date and which are subject to change by ADP. These requirements and practices are designed to be consistent with the ISO/IEC 27001:2013 information security standards. ADP periodically assesses its security policies and standards. Our goal is to help ensure that the security program effectively and efficiently operates to protect all the information entrusted to us by our clients and their employees.

.

Section 1 - Information Security Policies

Independence of Information Security Function

ADP's Chief Security Officer oversees ADP's Global Security Organization (GSO) and reports to the General Counsel (GC), instead of to the Chief Information Officer, which gives GSO the necessary independence from IT. The GSO is a cross-divisional, converged security team that has a multi-disciplinary approach in cyber and information security and compliance, operational risk management, client security management, workforce protection, and business resilience. GSO senior management, under our Chief Security Officer, are responsible for managing security policies, procedures, and guidelines.

Formal Definition of an Information Security Policy

ADP has developed and documented formal information security policies that set out ADP's approach to managing information security. Specific areas covered by this policy include, but are not limited to:

- **Security Management Policy –** Outlines the responsibilities of the Global Security Organization (GSO) and the Chief Security Officer (CSO), including the information security responsibilities and controls on hiring process from a security perspective.
- **Global Privacy Policy -** Discusses the collection of personal information, access to, accuracy, disclosures, and privacy statement to clients.
- **Employees Acceptable Use of Electronic Communications and Data Protection Policy** – Describes acceptable use, different electronic communications, encryption, and key management.
- **Information Handling Policy –** Provides requirements for the classification of ADP information and establishes protection controls.
- **Physical Security Policy–** Defines the security requirements of ADP facilities and subsequently our employees and visitors who work there.
- **Security Operations Management Policy –** Provides minimum controls for maintaining system patches, effectively addresses the threat from malware, and maintains backups and database security controls.
- **Security Monitoring Policy –** Provides controls for intrusion detection systems (IDS), logs, and data loss prevention (DLP).
- **Investigations and Incident Management Policy –** Defines standards for incident response, electronic discovery, workforce protection, and access to employees electronic stored information.
- **Access & Authentication Policy –** Outlines requirements for authentication (e.g. user ID and password), remote access, and wireless access.
- **Network Security Policy –** Security architecture of routers, firewalls, AD, DNS, email servers, DMZ, cloud services, network devices, web proxy, and switched network technology.
- **Global Third-Party Risk and M&A Policy –** Defines minimum security controls for engaging any third party to assist ADP in achieving its business objectives.
- **Application Management Policy –** Establishes appropriate security controls into each stage of the system development lifecycle.
- **Business Resiliency Policy –**Governs the protection, integrity and preservation of ADP by establishing the minimum requirements to document, implement, maintain, and continually improve Business Resiliency Programs
- **Converged Security Risk Management Policy –** Identification, monitoring, response, analysis, governance, and new business initiatives.

Policies are published in the ADP intranet and are accessible to all employees and contractors from within the ADP network.

Information Security Policy Review

ADP reviews its information security policies at least once per year or whenever there are major changes impacting the functioning of ADP's information systems.

Section 2 - Organization of Information Security

Information Security Roles and Responsibilities

The GSO consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined for all members of the GSO. The GSO is charged with the design, implementation and oversight of our information security program based on corporate policies. The GSO's activities are overseen by the Executive Security Committee, whose members include ADP's Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer, and General Counsel.

Mobile Computing and Teleworking Policy

ADP requires all confidential information to be encrypted on mobile devices, to prevent data leakage, which could result from theft or loss of a computer / device. Advanced end-point protection and two-factor authentication over VPN is also required to access the corporate networks remotely. All remote devices are required to be password protected. ADP employees are required to report lost or stolen remote computing devices immediately through a Security Incident Reporting Process.

All employees and contractors, as a condition of employment with ADP, must comply with the Acceptable Use of Electronic Communications and Data Protection Policy and other relevant policies.

Section 3 - Human Resource Security

Background Checks

Consistent with applicable legal requirements in the individual's jurisdiction, ADP conducts appropriate background checks commensurate with the duties and responsibilities of its employees, contractors and third parties. These checks confirm the candidate's suitability for handling clients' information prior to engaging or hiring such individuals.

Background screening may include the following components:

- Identity/employment eligibility verification
- Employment history
- Educational history and professional qualifications
- Criminal records (where legally authorized and depending on local country regulations)

Confidentiality Agreements with Employees and Contractors

ADP employment contracts and contracts with contractors contain terms that indicate obligations and responsibilities related to client information to which they will have access. All ADP employees and contractors are bound by confidentiality obligations.

Information Security Training Program

All employees are required to complete information security training as part of their onboarding plan. In addition, ADP delivers annual security training to remind employees of their responsibilities when performing their day-to-day duties.

Employees' Responsibilities and Disciplinary Processes

ADP has published a security policy that all ADP employees must comply with. Violations of security policies may lead to revocation of access privileges and/or disciplinary actions up to and including termination of consulting contracts or employment.

Termination of Employment Responsibilities

Responsibilities upon termination of employment have been formally documented and include, at minimum:

- Return all ADP information and assets in the possession of the respective employee, on whatever medium it is stored
- Termination of access rights to ADP facilities, information and systems
- Change of passwords for remaining active shared accounts, if applicable
- Transfer of knowledge, if applicable.

Section 4 - Asset Management

Acceptable Use of Assets

Acceptable use of assets is explained in several policies, applicable to ADP employees and contractors, to help ensure that ADP's and clients' information are not exposed by use of such assets. Examples of areas described in these policies are: use of electronic communications, use of electronic equipment, and use of information assets.

Classification of Information

Information acquired, created or maintained by or on behalf of ADP is assigned, as applicable, a security classification of:

- Public- Example: Marketing brochures, published annual reports
- ADP Internal Use Only- Example: Interoffice communications, operating procedures
- ADP Confidential- Example: Personal and Sensitive Personal Information
- ADP Restricted- Example: Financial forecasts, strategic planning information

Requirements for handling information are directly correlated to the information security classification. Personal Information and Sensitive Personal Information are always considered ADP Confidential. All client information is classified as confidential.

ADP employees are accountable for protecting and handling information assets in accordance with their security classification level, which provides protection of information and applicable handling requirements for each classification level. The ADP confidentiality classification is applied to all information stored, transmitted, or handled by third parties.

Equipment and Media Disposal

When ADP equipment, documents, files, and media are disposed of or reused, appropriate measures are taken to prevent subsequent retrieval of client's information originally stored in them. All information on computers or electronic storage media, regardless of classification, is securely disposed of, unless the media is physically destroyed, before being released outside ADP facilities or repurposed. The procedures for the secure destruction/erasure of ADP information held on equipment, in documents, files, and media are formally documented.

Physical Media in Transit

Organizational safeguards have been implemented to protect printed materials containing clients' information against theft, loss, and/or unauthorized access/modification (i) during transit e.g. sealed envelopes, containers and hand delivery to authorized user; and (ii) during review, revision or other processing where removed from secure storage.

Section 5 - Access Control

Business Requirements of Access Control

ADP's Access Control Policy is based on business-defined requirements. The policies and control standards are articulated into access controls that are enforced in all components of the provided service and are based on a "least-privilege" and "need to know" principle.

Access to Infrastructure - Access Control Management

Access requests to move, add, create, and delete are logged, approved and periodically reviewed.

A formal review is performed, at least yearly, to confirm that individual users accurately correspond to the relevant business role and would not have continued access after a position change. This process is audited and documented in a SOC1[1] type II report. From within an Identity Management System, a dedicated ADP team is responsible for granting, denying, cancelling, terminating and decommissioning/deactivating access to ADP facilities and information systems. ADP uses a centralized identity and access management (IAM) tool that is managed centrally by a dedicated GETS team. According to the access rights requested through the centralized IAM tool, a validation workflow will be triggered that could involve the users' supervisor. Access is provided on a temporary basis and workflows exist to prevent such access from remaining permanent. An employee's access to a facility is decommissioned immediately after the last day of employment by deactivating their access card (employee badge). The employee's user IDs are immediately deactivated. All employee's assets are returned and checked by the competent line manager and are compared against the asset list in the configuration management data base. Following a job position change, or organizational changes, user profiles or user access rights are required to be modified by the applicable business unit management and the IAM Team. Additionally, a formal review of access rights is performed every year to verify that individual users' rights correspond to their relevant business role and that there are no remaining irrelevant access rights after a position transfer.

Password Policy

ADP associate password policies are enforced in servers, databases and network devices and applications, to the extent the device/application allows it. The password complexity is derived from a risk-based analysis of the protected data and content. The policies meet prevailing industry standards for strength and complexity, including but not limited to the use of step-up, two-factor, or biometric authentication where appropriate.

Client application authentication requirements vary by product, and federated services (SAML 2.0) are available on specific ADP applications using a unified network and security layer managed by GETS.

Session Timeouts

ADP enforces automatic timeouts to all servers, workstations, applications and VPN connections based upon a risk-based approach consistent with industry standards. Re-establishment of sessions may take place only after the user has provided a valid password.

[1] In the case of certain US Services offered by ADP, this is audited in a SOC 2 Type 2 report.

Section 6 - Cryptography

Cryptographic Controls

ADP requires that sensitive information exchanged between ADP and ADP third parties must be encrypted (or transport channel must be encrypted) using industry accepted encryption techniques and strengths. Alternatively, a private leased line may be used.

Key Management

ADP has an internal Encryption Security Standard that includes well-defined key management and key escrow procedures, including both symmetric and asymmetric keys management.

Encryption keys used for ADP information are always classified as confidential information. Access to such keys is strictly limited to those who have a need to know and, if an exception approval is provided. Encryption keys and key lifecycle management followed industry standard practices.

Section 7 - Physical and Environmental Security

ADP's approach to physical security has two objectives – creating a safe work environment for ADP associates and protecting Personal Information held in ADP data centers and other strategic ADP locations.

ADP security policy requires ADP management to identify those areas requiring a specific level of physical security. Access to those areas is provided only to authorized associates for authorized purposes. ADP secured areas employ various physical security safeguards, including video surveillance systems, use of security badges (identity-controlled access) and security guards stationed at entry and exit points. Visitors may only be provided access where authorized and are supervised at all times.

Section 8 - Operations Security

Formalization of IT Operations Procedures

GETS is the ADP unit responsible for IT infrastructure operations and maintenance. GETS formally maintains and documents IT operations policies and procedures. These procedures include, but are not limited to the following:

- Change management
- Back-up management
- System error handling
- System restart and recovery
- System monitoring
- Jobs scheduling and monitoring

Infrastructure Change Management

A periodic Change Advisory Board (CAB), including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings discuss impacts deployment windows and promotions to production, as well as to coordinate any other change in the production infrastructure.

System Capacity Planning and Acceptance

Capacity requirements are continuously monitored and regularly reviewed. Following these reviews, systems and networks are scaled up or down accordingly. When significant changes must be made due to a change in capacity or a technological evolution, the GETS benchmarking team may perform stress tests to the relevant application and/or system. At the conclusion of stress testing, the team provides a detailed report of performance evolution by gauging the changes in (i) components, (ii) system configuration or version, or (iii) middleware configuration or version.

Protection Against Malicious Code

Industry standard endpoint protection technologies are leveraged to protect ADP assets in accordance with industry standard best practices.

Back-Up Management Policy

ADP has policies in place that require all production hosting operations to back-up production information. The scope and the frequency of back-ups are executed in accordance with the business requirements of relevant ADP services, the security requirements of the information involved, and the criticality of the information with respect to disaster recovery. Monitoring of scheduled back-ups is performed by GETS, to identify back-up issues or exceptions.

Security Logging and Monitoring

ADP has implemented a central and read-only logging infrastructure (SIEM) and a log correlation and alerting system (TPSI). Log alerts are monitored and treated in a timely manner by the CIRC.

All of these systems are synchronized using a unique Network Time Protocol (NTP)based clock reference.

Each individual log contains, at minimum:

- Timestamp
- Who (identity of the operator or administrator)

- What (information about the event)

Audit trails and system logging for ADP applications are designed and set up to track the following information:

- Authorized access
- Privileged operations
- Unauthorized access attempts
- Systems alerts or failures
- Changes to systems security settings, when the system allows such logging

These logs are only available to ADP authorized personnel and are sent in live mode to prevent data from being tampered with before being stored in the secure logging appliances.

Infrastructure Systems and Monitoring

ADP uses appropriate measures to provide infrastructure monitoring 24 hours per day, 7 days per week. Disruption alerts are managed by different teams according to their severity level and the skills required to resolve them.

ADP hosting center facilities employ monitoring applications that are constantly running on all related processing systems and on the network components to provide ADP staff proactive notification of issues and warnings in anticipation of possible problems.

Technical Vulnerability Management

All computers installed in the hosting infrastructure must comply with the installation of a specialized security hardened operating system (or secure build process). Hosted operations employ a hardened, approved, and standardized build for every type of server used within our infrastructure. Out-of-the-box installation of operating systems is prohibited since these installations may create vulnerabilities, such as generic system account passwords, that would introduce an infrastructure risk. These configurations reduce the exposure of hosted computers running unnecessary services that can lead to vulnerabilities.

ADP has a documented methodology for conducting release and periodic vulnerability assessments and compliance reviews of Internet facing web-based applications and their corresponding infrastructure components, which include at least 15 primary categories of testing. Assessment methodology is based on both internal and industry best practices, including, but not limited to, Open Web Application Security Project (OWASP), SANS Institute and Web Application Security Consortium (WASC).

Section 9- Communications Security

Network Security Management

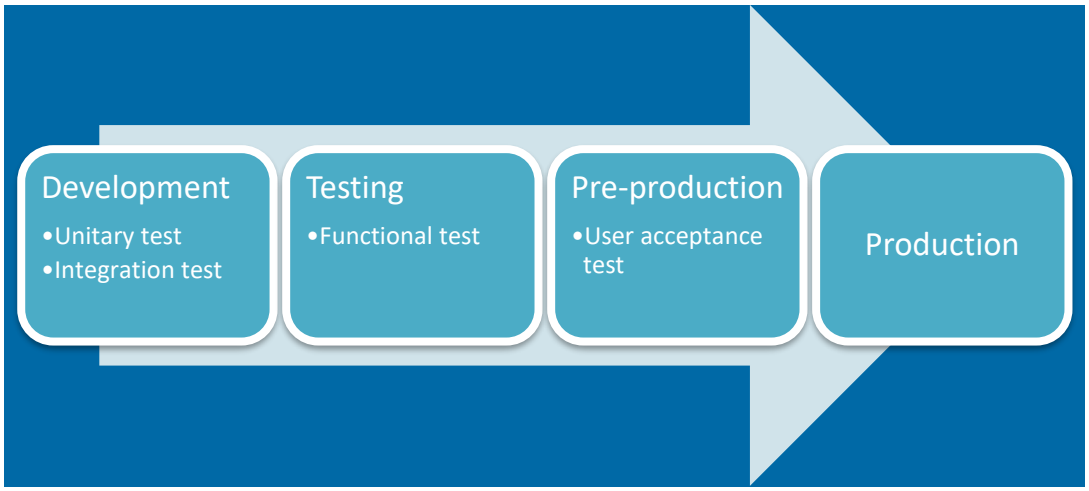
ADP employs a network-based intrusion detection system that monitors traffic at the network infrastructure level (24 hours a day, 7 days a week) and identifies suspicious activity or potential attacks.

Exchange of Information

ADP implements appropriate controls so that ADP clients' information sent to third parties is transferred between authorized information systems and resources only and is only exchanged through ADP’s secure and authorized transfer mechanisms.

Security in Development and Support Processes

During the development cycle, applicable documentation is generated, and testing plans are built for the testing phase. Different stages are defined for each environment with relevant approval at each phase:



- To move from Testing to Pre-production environment, approval from ADP's Quality team is required.
- To move from Pre-production to Production, approval from IT Operations is required.

Development teams are required to utilize secure coding methods. Application changes are tested in development and regression environments before they reach the production systems. Tests are performed and documented. Upon approval, changes are deployed into production. Penetration testing is performed after significant changes.

A periodic CAB, including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings take place on a regular basis, and are meant to discuss impacts, to agree on deployment windows and to approve the promotion of software packages to production, as well as to inform about any other changes in production infrastructure.

ADP's IT Operations team provides the final approval before promotion to production environment of the software packages.

Security in Development Environment

Production and development environments are segregated and independent from each other. Appropriate access controls are employed to enforce proper segregation of duties. Software packages are accessible at each stage of the development process and only by the teams involved in that stage.

Test Data

Per ADP's Application Management Policy, the use of real or un-sanitized data in development and testing is not permitted unless explicitly requested and authorized by client.

Section 11 - Supplier Relationships

Identification of Risks Related to External Parties

Risk assessments of third parties who require access to ADP and/or client information are periodically performed to determine their compliance with ADP security requirements for third parties, and to identify any gaps in the applied controls. If a security gap is identified, new controls are agreed upon with such external parties.

Information Security Agreements with External Parties

ADP enters into agreements with all third parties which include appropriate security commitments to meet ADP’s security requirements.

Section 12 - Information Security Incident Management

Management of Information Security Incidents and Improvements

ADP has a documented methodology for responding to security incidents timely, consistently, and effectively.

Should an incident occur, a predefined team of ADP employees activates a formal incident response plan that addresses areas such as:

- Escalations based on the classification of incident or incident severity
- Contact list for incident reporting/escalation
- Guidelines for initial responses and follow up with involved clients
- Compliance with applicable security breach notification laws
- Investigation log
- System recovery
- Issue resolution, reporting, and review
- Root Cause and Remediation
- Lessons learned

ADP policies define a security incident, incident management, and all employees' responsibilities regarding the reporting of security incidents. ADP also conducts regular training for ADP employees and contractors to help ensure awareness of reporting requirements. Training is tracked to ensure completion.

Section 13- Information Security Aspects of Business Resiliency Management

ADP Business Resiliency Program

ADP is committed to keeping our services and operations running smoothly, so that we can provide our clients with the best service possible. It's our priority to identify — and mitigate — the technology, environmental, process, and health risks that may get in the way of providing our business services. ADP has created an integrated framework that lays out our mitigation, preparedness, response, and recovery processes and includes:

- Risk Assessment
- Risk Threat Analysis
- Business Impact Analysis
- Plan Development
- Business Continuity Planning
- Disaster Recovery Planning
- Health and Safety Planning
- Real-World Response
- Crisis Management
- Emergency Response
- Testing and Validation
- Review
- Revise
- Exercise

Section 14- Compliance

Compliance with Security Policies and Standards

ADP employs a process to internally perform compliance reviews on a periodic basis. Additionally, ADP performs a SOC1[2] type II audit on a periodic basis. These audits are conducted by a well-known third-party audit firm and audit reports are available on a yearly basis for clients upon request, when applicable.

Technical Compliance

To enforce technical compliance with best practices, ADP performs regularly scheduled network vulnerability scans. The scan results are then prioritized and developed into corrective action plans with the hosting teams and their management.

Vulnerability scans are performed on a regular basis of both internal and external environments. Additionally, source code scans and penetration testing are performed on a product-by-product basis. Utilizing specialized application scanning tools, application level vulnerabilities, if any, are identified, shared with the product development management teams, and incorporated into the quality assurance processes for corrective action. The results are analyzed, and corrective action plans developed and prioritized.

Retention of Data

ADP's data retention policy regarding client information is designed to comply with applicable laws. At the end of a client contract, ADP complies with its contractual obligations related to the client's information. ADP will return or allow the client to retrieve (by data download), all client information required for the continuity of the client's business activities (if not previously provided). Then, ADP will securely destroy remaining client information, except to the extent required under applicable law, authorized by the client or needed for dispute resolution purposes.

[2] In the case of certain US Services offered by ADP, there would be also SOC 2 Type II exec. reports

ANEXO 3 - Lista de Empresas do Grupo vinculadas pelo Código de Processador

ADP (Filipinas), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Filipinas, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Suíça
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontário M8X 2X9, Canadá
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Bruxelas, Bélgica
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, República Checa
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Alemanha
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelona, Espanha
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milão, Itália
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunes, Tunísia
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, França
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, França
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Holanda
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, França
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 Índia
ADP International Services B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Holanda
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Roterdão
ADP Outsourcing Italia SRL	Viale G. Richard 5/A – 20143 Milão, Itália
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Varsóvia, Polónia
ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, Índia – 500082
ADP RPO UK Limited	22 Chancery Lane, Londres, Inglaterra, WC2A 1LS

ADP RPO, LLC	3401 Technology Drive, Findlay, OH, USA 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Eslováquia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Turim, Itália
ADP Sverige AB	Östermalmstorg 1, 114 42 Stockholm, Suécia
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1º – 6º andar, Distrito 2, Bucareste, Romênia 020334
Automatic Data Processing Limited (Austrália)	6 Nexus Court, Mulgrave, VIC 3170, Austrália
Automatic Data Processing Limited (Reino Unido)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Condado de Cambridge, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugal
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068