Medidas Técnicas e Organizacionais Worldline Financial Services (Europe) S.A.

(EU PT)

1 Finalidade deste Documento

Este documento contém uma lista das medidas técnicas e operacionais que são aplicáveis como padrão. As medidas reais tomadas dependem do Serviço e do local de processamento em questão, pois nem todas as medidas são relevantes para todos os Serviços e locais. A Worldline garante ter, relativamente a todos os Serviços e localizações, as medidas técnicas e operacionais necessárias e adequadas incluídas na lista abaixo, na sequência de uma Avaliação de Impacto sobre a Protecção de Dados. As medidas destinam-se a:

- garantir a segurança e confidencialidade dos Dados Pessoais;
- proteger contra quaisquer ameaças ou perigos à segurança e integridade dos Dados Pessoais;
- proteger contra qualquer processamento, perda, utilização, divulgação ou aquisição ou acesso não autorizados a quaisquer Dados Pessoais

A página também contém uma lista de subcontratantes utilizados pela Worldline para a prestação dos seus serviços. A Worldline garante que todos os seus subcontratantes tenham fornecido garantias adequadas sobre a protecção dos dados pessoais por eles processados em nosso nome, mediante o controlo da subcontratação: não deve haver qualquer processamento de dados encomendado na acepção do artigo da GDPR. 28 sem instruções adequadas do comitente, por exemplo, uma concepção contratual clara, uma gestão formalizada da subcontratação e uma selecção rigorosa dos processadores (certificação ISO, ISMS), demonstração prévia de competência, controlo de acompanhamento.
A Worldline compromete-se a monitorizar continuamente a eficácia das suas salvaguardas de informação e a realizar uma auditoria anual de conformidade por parte de um terceiro, a fim de fornecer garantias sobre as medidas e controlos em vigor.

2 Medidas Técnicas e Organizacionais

A Pessoas, sensibilização e RH:

- Todos os recrutamentos seguem um processo de rastreio em conformidade com os princípios da política de verificação de antecedentes da Worldline;
- Em cada contrato, cada empregado tem cláusulas de Acordos de Não Divulgação;
- A formação de sensibilização para o Código de Ética (incluindo um teste) é uma obrigação anual para todos os funcionários e deve ser realizada através de um módulo de aprendizagem electrónica dedicado;
- A Política de Utilização Aceitável ou a versão local do Grupo IT são compartilhadas com todos os empregados;
- A declaração de política de segurança assinada pela Direcção é partilhada com todos os funcionários;
- O pessoal da Worldline é obrigado anualmente a seguir a política de Protecção de Dados da Worldline, formação em Segurança da Informação e Segurança (incluindo um teste);
- Formação regular de sensibilização acerca do RGPD para todos os empregados (para além da política de Protecção de Dados Worldline, formação em Segurança e Protecção da Informação);
- O acesso aos sistemas é fornecido numa base de «necessidade de ter em conta» a separação de funções;
- São realizadas auditorias internas regulares de segurança para verificar as práticas de segurança.

B Segurança física e registos em papel:

Conformidade com a política de Segurança Física e Ambiental do Grupo Worldline:

- Sistemas de controlo de acesso e gestão de visitantes implementados para todos os visitantes/convidados;
- Controlo de acesso físico (protecção contra o acesso não autorizado ao processamento de dados ou locais de arquivo): particularmente por meio de cartões magnéticos ou inteligentes, abridores de portas eléctricos, porteiro, pessoal de segurança, sistemas de alarme, sistemas de vídeo;
- Revisões de acesso físico de acordo com a periodicidade definida;
- Secretária limpa, ecrã limpo e impressão de tipo «follow me», processo implementado;
- A informação, que inclui documentos em papel, tratados pelo importador de dados é classificada, etiquetada, protegida e tratada de acordo com a política de classificação de informação Worldline;
- Excepto com prévia autorização específica, os computadores fixos não são retirados do local;
- Vigilância CCTV para proteger áreas restritas;
- Sistemas de alarme e combate a incêndios implementados para segurança dos funcionários;
- Realizam-se simulacros de evacuação em caso de incêndio com frequências especificadas.

C O dispositivo remoto do utilizador final está protegido:

Os utilizadores remotos estão a trabalhar com computadores portáteis e de secretária na rede protegida Worldline sujeita a manutenção pela Global IT para o Grupo Worldline. Além disso, são incorporadas as seguintes medidas de segurança:

- Criptografia do disco rígido nos computadores portáteis concedidos pela empresa;
- Autenticação de 2 Fatores (PKI/Alternativa);
- Gestão centralizada e protecção anti-vírus;
- Gestão e monitorização do software para controlar uma instalação de software autorizada;
- Os controlos de ID de login e palavra-passe são implementados para aceder à informação;
- Implementação de revisão periódica do acesso;
- Os e-mails são automaticamente verificados por programas anti-vírus e anti-spam.

D Segurança de Acesso Remoto

A autenticação de 2 factores é utilizada em geral para o acesso remoto aos sistemas-alvo críticos da Worldline. Se a fonte da ligação remota for um sistema controlado pela Worldline, então a autenticação do dispositivo com base num certificado no dispositivo é implementada.
Qualquer outra configuração de ligações tem de ser previamente aprovada pelo departamento de segurança.

E As medidas genéricas de segurança são nomeadamente:

- Os dados são armazenados nos Centros de Dados da UE e da Suíça ou no caso de computadores portáteis encriptados no dispositivo local;
- Terminação da ligação de acesso na Zona Desmilitarizada;
- Todas as ligações até à zona protegida (zona PCI) são encriptadas;
- O acesso à zona PCI só é possível através de uma autenticação forte por meio de um cliente de segurança fornecido;
- Múltiplos níveis de «firewalls» e detecção de intrusão precisam de ser aprovados;
- Acesso gerido de acordo com princípios de controlo de acesso baseados em funções;
- Gestão da privacidade, incluindo formação regular dos empregados;
- Gestão da resposta a incidentes;
- Configurações padrão para protecção da privacidade.

F Controlo de acesso aos dados pessoais

Os empregados com acesso a dados privados só podem aceder aos dados necessários para a realização das actividades sob a sua responsabilidade. A autorização de acesso é concedida com base na «necessidade de saber» e na «necessidade de aceder» e é baseada na função ou no nome. Os registos de acesso estão em vigor e atribui-se a responsabilidade pelo controlo de acesso.

As seguintes medidas estão em vigor:

- Obrigação de os empregados cumprirem as políticas da Worldline e as políticas locais de segurança e protecção de dados;
- Instruções de trabalho sobre o tratamento de dados privados;
- Controlo de acesso electrónico (protecção contra utilização não autorizada de sistemas de processamento ou armazenamento de dados): especialmente através de palavras-passe (incluindo a política correspondente), mecanismos de bloqueamento automático, autenticação de dois factores, encriptação de suportes de dados;
- Controlo de acesso interno (prevenção de leitura, cópia, modificação ou remoção não autorizadas de dados dentro da Worldline): nomeadamente, utilizando perfis de autorização padrão numa base de «necessidade de saber», um processo padrão para atribuição de direitos de utilizador, registo de acesso, revisão periódica dos direitos atribuídos, especialmente de contas de administrador;

110.0788.17 EU_PT/04.2022

- Destruição controlada dos suportes de informação;
- Existem procedimentos para verificar o cumprimento de procedimentos e instruções de trabalho.

G Segurança e confidencialidade dos dados pessoais

Com base numa avaliação de risco (e, se necessário, num AIPD adicional) a Worldline garantirá um nível de segurança adequado ao risco, incluindo, nomeadamente, se for caso disso:

- Esquema de classificação de dados: categorização de dados pessoais de acordo com o grau de confidencialidade com base em obrigações legais ou auto-avaliação;
- Leitura, cópia, modificação ou remoção não autorizadas durante a transmissão ou condução electrónica: em particular através de encriptação e Redes Privadas Virtuais (VPN);
- a capacidade de assegurar a permanente confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de processamento;
- Protecção contra destruição ou perda acidental ou intencional, tais como estratégia de backup (online/offline; on-site/off-site), alimentação ininterrupta (UPS, grupo gerador diesel), antivírus, firewall, canais de alerta e planos de emergência; verificações de segurança nas infra-estruturas e níveis de aplicação, plano de segurança multinível com externalização de backups para centros de backup de dados, processos padrão em caso de mudança/despedimento de funcionários;
- A capacidade de restaurar a disponibilidade e o acesso aos Dados Pessoais de forma atempada em caso de um incidente físico ou técnico;
- Um processo para testar, avaliar e determinar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento (auditoria interna, PCI-DSS, ISO27001, instituições supervisoras nacionais);
- Registos de processamento de acordo com os requisitos do RGPD;
- Utilização de sistemas de registo de acesso com relevância para efeitos de poder detectar tentativas de acesso não autorizadas;
- Os dados e metadados do cliente principal (incluindo cópias de segurança, arquivos, ficheiros de registo, etc.) só serão armazenados enquanto servirem as finalidades para as quais os dados foram recolhidos, a menos que exista uma obrigação legal ou contratual de conservar os dados durante um período de tempo mais longo.

H Controlo organizacional

O Processador de Dados deve manter a sua organização interna de forma a cumprir os requisitos da legislação aplicável e os requisitos do responsável pelo tratamento de dados em matéria de segurança de dados. Isto deve ser realizado por:

Políticas e procedimentos internos de tratamento de dados, directrizes, instruções de trabalho, descrições de processos e regulamentos de programação, testes e divulgação, na medida em que estejam relacionados com os Dados Pessoais transferidos pelo responsável pelo tratamento;

Implementação de um quadro normativo de protecção de dados que é auditado anualmente e considerado conforme;

Ter um plano de emergência com procedimentos e atribuição de responsabilidades em vigor (plano de contingência de reserva).