Informação PIA

PIA
Vinyl Store

Nome do autor
Francisco Matos

Nome do assessor
Carlos Pedrosa

Nome do validador
Sofia Pereira

Data de criação
25/03/2019

Nome do DPO
Francisco Pedrosa

Opinião do DPO
A empresa tem em consideração a segurança no processamento de dados

Procura da opinião de partes interessadas
A opinião das partes em questão foi solicitada.

Opiniões de partes interessadas
Carlos Matos

Status de pessoas em questão
O tratamento deve ser implementado.

Opiniões de partes interessadas
Entrevistas

Contexto

Visão geral

Qual é a finalidade de tratamento considerada no âmbito da análise?

Vender vinis

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

Manter os dados privados e impossíveis de ler

Quais são as normas aplicáveis à finalidade de tratamento?

RGPD

Avaliação : Aceitável

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Moradas e cartões de crédito

Como funciona o ciclo de vida dos dados pessoais e dos processos inerentes?

Criados, guardados, acedidos no momento de compra, removidos quando o cliente desejar

Quais são os ativos de informação utilizados na finalidade de tratamento?

Servidores de alto desempenho

Avaliação : Aceitável

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

Sim, é necessário estes dados para realizar transações

Avaliação : Aceitável

Qual é o fundamento para tratamento de dados pessoais?

Consentimento do utilizaor

Avaliação : Aceitável

Os dados pessoais recolhidos são adequados, relevantes e limitados para o propósito de tratamento realizado (princípio da minimização de dados)?

Sim, para ser possível vender o produto

Avaliação : Aceitável

Os dados pessoais estão atualizados e são fidedignos?

Opção de editar morada e cartão de crédito

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

Depois de 1 ano da última atividade na conta, ou quando o cliente remover a sua conta

Avaliação : Aceitável

Controlos para proteger os direitos pessoais dos titulares dos dados

Como é que os titulares dos dados são informados sobre o tratamento dos seus dados?

No momento de registo de conta

Avaliação : Aceitável

Como é obtido o consentimento dos titulares de dados?

No momento de registo eles serão questionados.

Avaliação : Aceitável

Como é garantido o acesso e portabilidade de dados pessoais?

Através de permissões de acessos à base de dados

Avaliação : Aceitável

Como é garantida a atualização/retificação e apagamento dos dados pessoais pedida pelo titular dos mesmos?

Através do apagamento de todos os dados relativos a este

Avaliação : Aceitável

Como é garantida a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos?

Secções críticas estarão bloqueadas

Avaliação : Aceitável

As obrigações dos subcontratrantes são claramente identificadas e regulados por contrato ou outro ato normativo?

Um contrato é assinado no momento de registo

Avaliação : Aceitável

No caso de transferência de dados fora da União Europeia, os dados são adequadamente protegidos?

Sim.

Avaliação : Aceitável

Riscos

Medidas planeadas ou existentes

Acesso não autorizado

Pedir aos utilizadores para realizarem uma verificação/alteração das suas palavras passes e emails

Avaliação : Aceitável

Acesso ilegítimo dos dados

Quais poderiam ser os principaisimpactos nos dados dos titulares se o risco ocorrer?

Uso de cartão de crédito sem consentimento

Quais são os principaisameaçasque poderiam levar ao risco?

Roubo de dinheiro

Quais são as fontesde risco?

Adversários que pretendam usar contas que não lhes pertencem

Quais são os controlos identificados que contribuem para abordar o risco?

Acesso não autorizado

Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados?

Significante, O roubo de contas põe em causa as contas dos clientes

Como estimas a probabilidade de risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Limitado, Hoje em dia, roubo de passwords é bastante comum

Avaliação : Aceitável

Modificação indesejada dos dados

Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer?

Alterar as moradas dos clientes

Quais são as principais ameaças que poderiam levar ao risco?

Adversários que intercetam as entregas dos produtos

Quais são as fontesde risco?

Adversários com conhecimentos informáticos

Quais são os controlos identificados que contribuem para abordar o risco?

Acesso não autorizado

Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados?

Insignificante, O cliente consegue identificar este risco

Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Insignificante, Não é muito comum intercetar o produto desta forma

Avaliação : Aceitável

Desaparecimento de dados

Quais são os principaisimpactos nos dados dos titulares se o risco ocorrer?

Perda de dados pessoais

Quais são as principais ameaças que poderiam levar ao risco

Adverários que pretenda realizar uma DoS

Quais são as fontesde risco?

Adversários com bons conhecimentos informáticos

Quais são os controlos identificados que contribuem para abordar o risco?

Acesso não autorizado

Como estimas a gravidade de risco, especialmente de acordo com impactos potenciais e controlos planeados?

Limitado, Perda de dados é mais grave para a empresa que para os clientes

Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Significante, Concorrência pode tentar impedir o funcionamento da empresa

Avaliação : Aceitável

Plano de ação

Visão geral

Princípios fundamentais

Objetivos
Base legal
Dados adequados
Precisão de dados
Duração dos dados
Informação para os titulares dos dados
Obtenção do consentimento
Informação para os titulares dos dados
Direito à retificação e apagamento
Direito à restrição e à oposição
Subcontratação
Transferências

Medidas existentes ou planeadas

Acesso não autorizado

Riscos

Acesso ilegítimo de dados
Modificação indesejada de dados
Desaparecimento de dados

Medidas Improváveis
Medidas Aceitáveis

Princípios fundamentais

Nenhum plano de ação registado.

Medidas existentes e planeadas

Nenhum plano de ação registado.

Riscos

Nenhum plano de ação registado.

Visão geral dos riscos

Impactos potenciais

- Uso de cartão de crédito se...
- Alterar as moradas dos clie...
- Perda de dados pessoais

Ameaças

- Roubo de dinheiro
- Adversários que intercetam ...
- Adverários que pretenda rea...

Fontes

- Adversários que pretendam u...
- Adversários com conheciment...
- Adversários com bons conhec...

Medidas

- Acesso não autorizado

Acesso ilegítimo dos dados

Gravidade : Significativo

Probabilidade : Limitado

Modificação indesejada dos dados

Gravidade : Insignificante

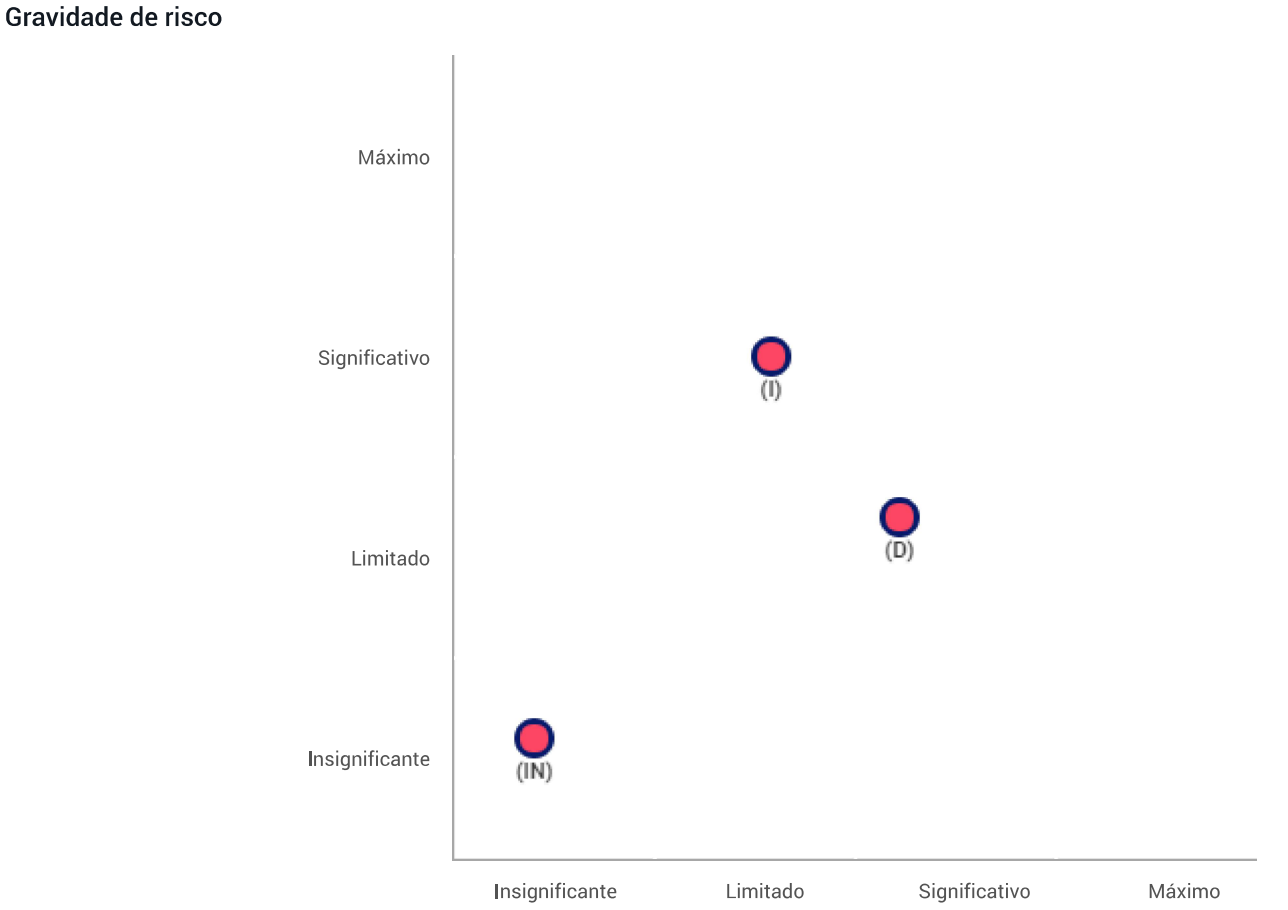
Probabilidade : Insignificante

Desaparecimento de dados

Gravidade : Limitado

Probabilidade : Significativo

Mapeamento de riscos



- Medidas existentes ou planeadas
- Com as medidas corretivas implementadas
- Acesso (i)legítimo aos dados
- Modificação (in)desejada dos dados
- Desaparecimento dos dados

25/03/2019