PIA information

PIA
EngSeg Grupo13

Author's name
Grupo

Assessor's name
13

Validator's name
Eng Seg

Creation date
18/04/2019

DPO's name
Self, Grupo 13

DPO's opinion
Apresenta uma boa segurança

Search of concerned people opinion
Concerned people opinion was requested.

Concerned people opinions
Self, Grupo 13

Concerned people statuses
The treatment could be implemented.

Concerned people opinions
Opiniões formadas aquando a analise da proposta

Context

Overview

Which is the processing under consideration?

Este projeto tem como objetivo uma aplicação identica ao _MB Way_, onde os clientes sao capazes de consultar o saldo, fazer transferencias e pagamentos bancarios ou pagar contas em estabelecimentos fisicos através da aplicação mobile.
Assim, a projeto fica com os dados bancarios dos seus clientes, bem como uma lista de transações por eles efetuadas.
Vai entao processar um numero elevado de dados pessoais referentes a uma margem considerável da população, já que qualquer proprietário de um cartão de multibanco, credito ou débito faz parte do alvo da aplicação.
Para apresentar a lista de tranferências, o sistema vai também monitorizar automaticamente todas as transações dos clientes.

What are the responsibilities linked to the processing?

A informação vai ser recolhida automaticamente a partir do momento que alguma acção é efetuada graças à API do sistema dos bancos. Essa informação vem protegida e fica armazenada no sistema da aplicação, e só é visualizada pelos clientes, que só podem ver a parte recorrente à sua informação.

Are there standards applicable to the processing?

GDPR

Evaluation : Acceptable

Data, processes and supporting assets

What are the data processed?

Informação: Nome do cliente, morada e dados da conta bancaria.
Duração: até cliente apagar conta
Acesso: Dados do cliente apenas acessiveias ao mesmo

How does the life cycle of data and processes work?

A informação guardada vai ser referente a tudo incluido numa conta bancária, seja referências, lista de transações, montante presente na conta e dados sobre o cliente, como nome, morada e idade.
A informação do cliente e da conta vai ser recolhida no momento da criação da conta na aplicação, e a informação das tranferências sempre que uma ocorrer.
O sistema deverá guardar todos estes dados até que o cliente decida anular a conta , podendo claro alterar os dados referentes a si próprio.

What are the data supporting assets?

API dos bancos que permitem receber as transações

Evaluation : Acceptable

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

A informação vai ser recolhida automaticamente a partir do momento que alguma acção é efetuada graças à API do sistema dos bancos. Essa informação vem protegida e fica armazenada no sistema da aplicação, e só é visualizada pelos clientes, que só podem ver a parte recorrente à sua informação.

Evaluation : Acceptable

What are the legal basis making the processing lawful?

Os clientes apresentam consenso na criação da conta

Evaluation : Acceptable

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

A informação vai ser recolhida automaticamente a partir do momento que alguma acção é efetuada graças à API do sistema dos bancos. Essa informação vem protegida e fica armazenada no sistema da aplicação, e só é visualizada pelos clientes, que só podem ver a parte recorrente à sua informação.

Evaluation : Acceptable

Are the data accurate and kept up to date?

Os clientes poderam mudar os seus dados pessoais, e as movimentações aceguradas pelas APIs

Evaluation : Acceptable

What are the storage duration of the data?

Até a conta ser anulada, de forma a possibilitar o cliente ver todas as suas movimentações

Evaluation : Acceptable

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Toda a informação relacionada com o tratamento dos dados será posta à disposição do publico, assegurando o bom tratamento do mesmo. Como a aplicação necessita de um cartão bancario, apenas adultos terão oportunidade de a usar.

Evaluation : Acceptable

If applicable, how is the consent of data subjects obtained?

Na criação da conta na aplicação

Evaluation : Acceptable

How can data subjects exercise their rights of access and to data portability?

Os clientes poderão modificar e/ou apagar os dados que se referem a eles próprios

Evaluation : Acceptable

How can data subjects exercise their rights to rectification and erasure?

Terão essa possibilidade na aplicação ou site principal

Evaluation : Acceptable

How can data subjects exercise their rights to restriction and to object?

Se apresentam consenso na criação permitem a não restrição dos dados, desde que só eles tenham visto esta.

Evaluation : Acceptable

Are the obligations of the processors clearly identified and governed by a contract?

Yes

Evaluation : Acceptable

In the case of data transfer outside the European Union, are the data adequately protected?

No

Evaluation : Acceptable

Risks

Planned or existing measures

Privacidade

Apenas o cliente será capaz de aceder á informação relativa à sua conta, através de encriptação dos dados.

Evaluation : Acceptable

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

Exposição de dados pessoais e da conta bancaria

What are the main threats that could lead to the risk?

Palavra passe pobre ou perdida.

What are the risk sources?

Cliente

Which of the identified controls contribute to addressing the risk?

Privacidade

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Muito grave se a pass for perdida ou adivinhada por um atacante

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, Basta assegurar a segurança da pass

Evaluation : Acceptable

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

erro na leitura dos dados

What are the main threats that could lead to the risk?

ataque aos dados cifrados no servidor ou falha na rede

What are the risk sources?

atacantes, má rede

Which of the identified controls contribute to addressing the risk?

Privacidade

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Limited, no máximo aparecem dados ilegiveis

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, muito dificil com um servidor seguro

Evaluation : Acceptable

Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

faz a aplicação inutil

What are the main threats that could lead to the risk?

ataque ao servidor

What are the risk sources?

atacantes

Which of the identified controls contribute to addressing the risk?

Privacidade

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Faz a aplicação não fazer nada

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, Seguro se o servidor for seguro

Evaluation : Acceptable

Action plan

Overview

Fundamental principles

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Information for the data subjects
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers

Planned or existing measures

Privacidade

Risks

Illegitimate access to data
Unwanted modification of data
Data disappearance

Improvable Measures
Acceptable Measures

Fundamental principles

No action plan recorded.

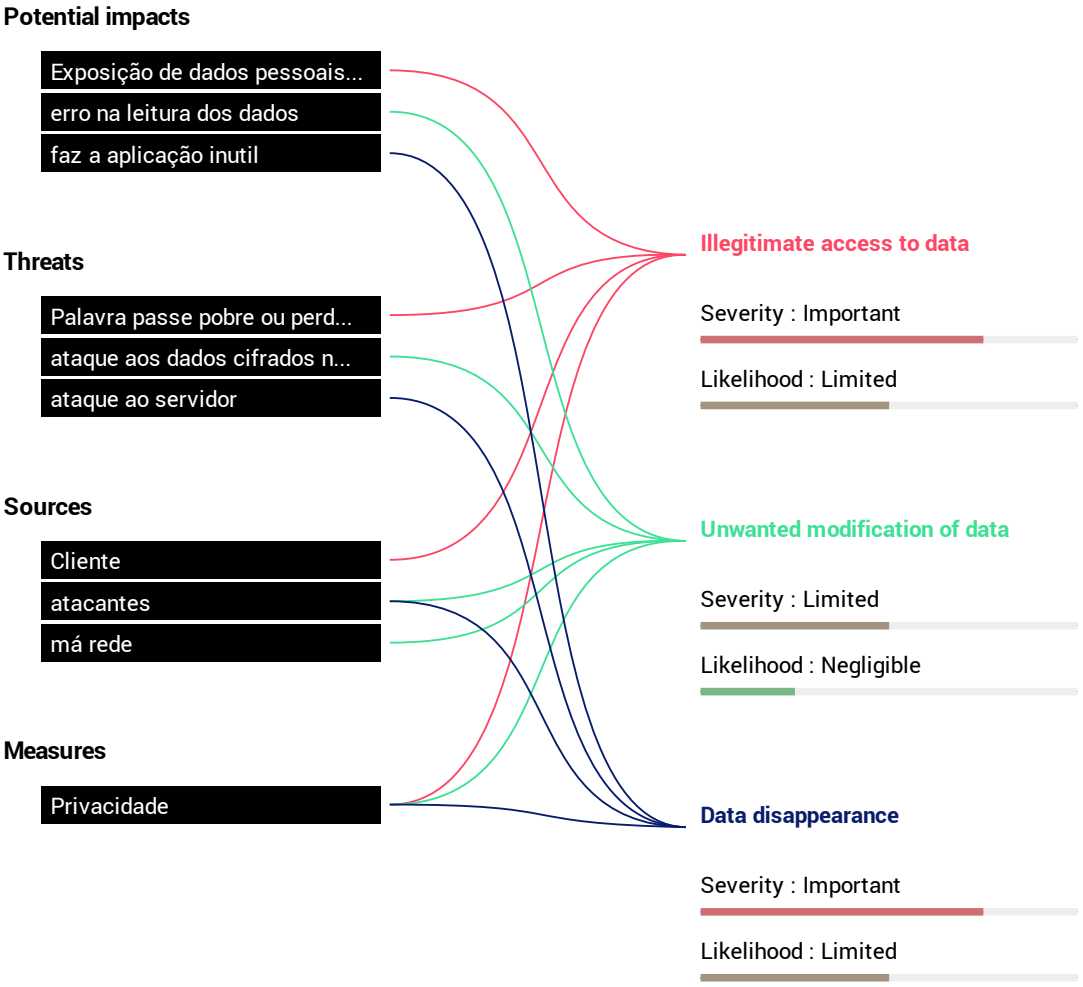
Existing or planned measures

No action plan recorded.

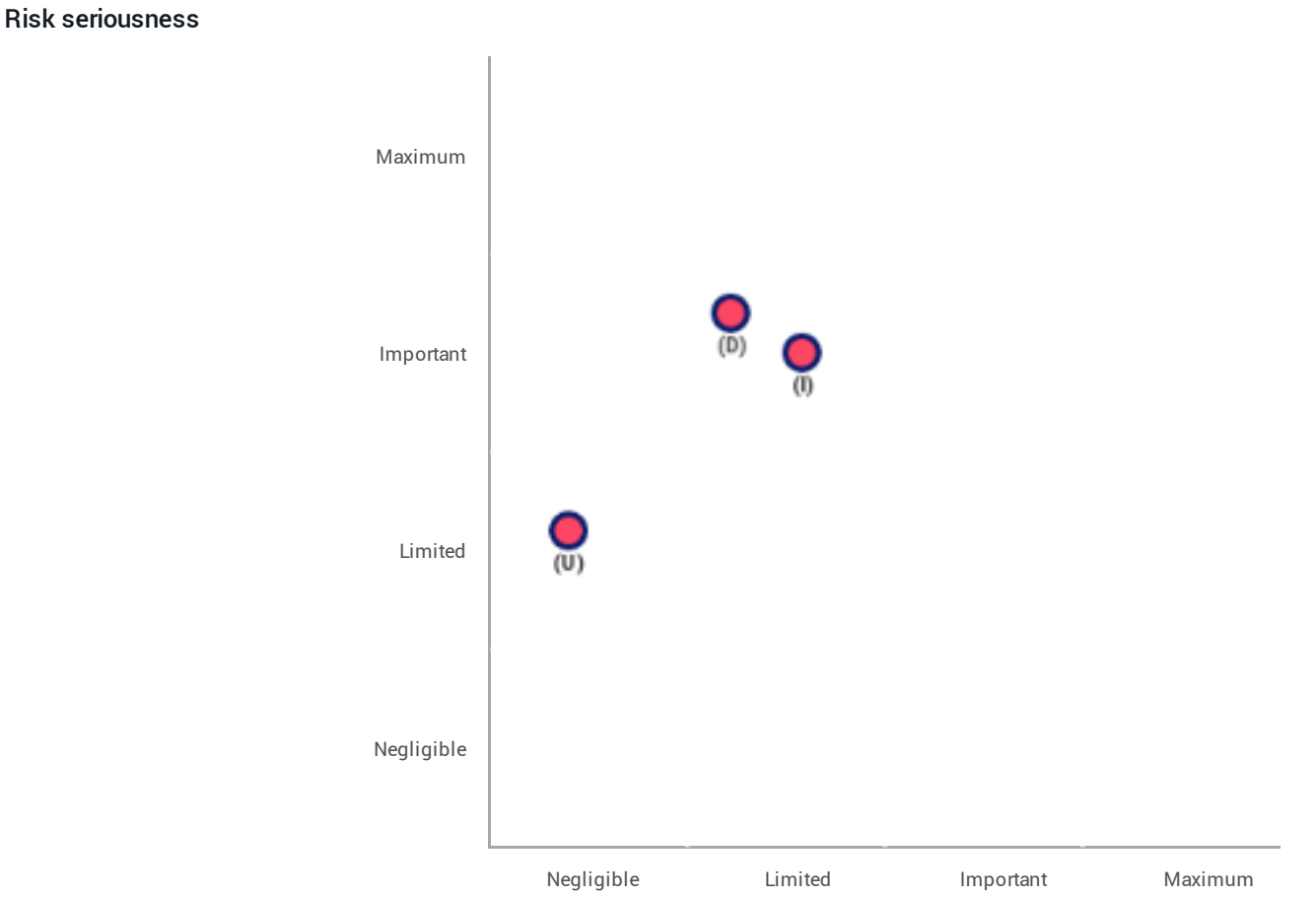
Risks

No action plan recorded.

Risks overview



Risk mapping



- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance