Preview

GENERAL INFORMATION

edit

100%

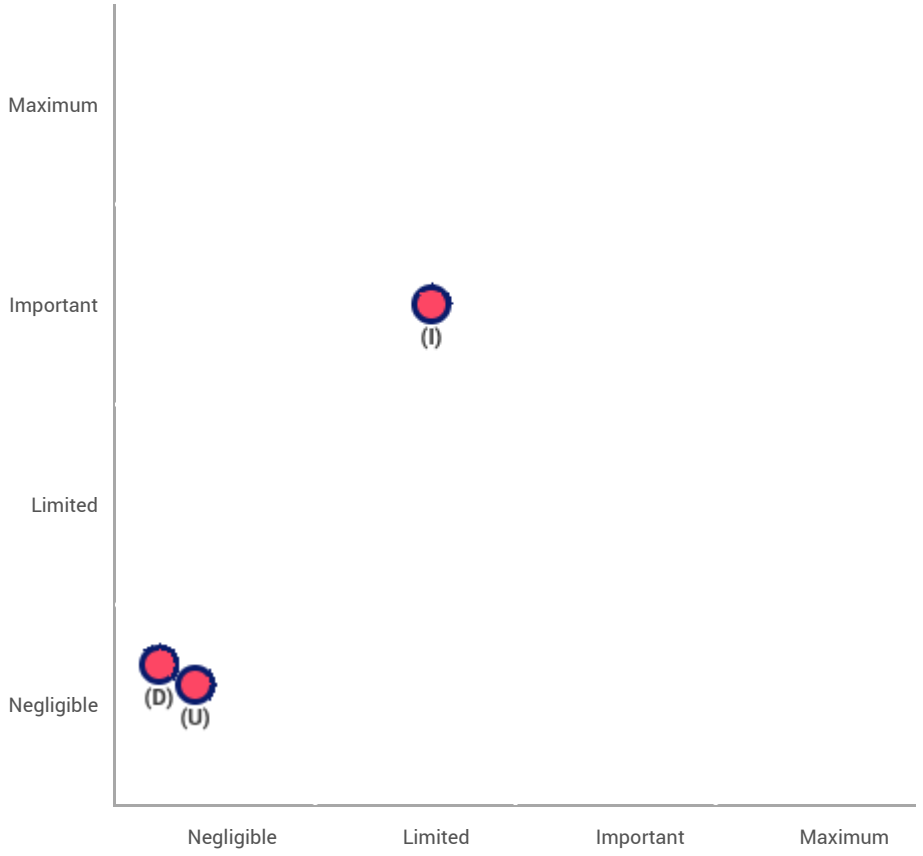
Preview

Editing :	Grupo 8	**Status :**	Simple validation
Evaluation :	Grupo 8		
Validation :	Grupo 8		

Validation

Risk mapping

Risk seriousness



Risk likelihood

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

5/20/22

Validation

Action plan

Overview

Fundamental principles | Planned or existing measures

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

Redução da acumulação de dados pessoais
Cifragem

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.

Validation

TO TRANSLATE - DPO and data subjects opinion

DPO's name

DPO

DPO's status

The treatment could be implemented.

DPO's opinion

Por respeitar todas as normas, este tratamento pode ser implementado

Search of concerned people opinion

Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested

Indisponibilidade

indisponibilidade

Context
Overview

What is the processing under consideration?

Armazenamento dos dados do utilizador para a criação de assinaturas digitais utilizando o Cartão de Cidadão e/ou a Chave Móvel Digital.

What are the responsibilities linked to the processing?

O tratamento de dados vai ser realizado para permitir a criação de assinaturas digitais de documentos, então, é necessário tratar dados do Cartão de Cidadão e da Chave Móvel Digital do utilizador e ainda do documento a ser assinado.

Are there standards applicable to the processing?

As normas descritas pelo Regulamento Geral da Proteção de Dados.

Evaluation : Acceptable

Context
Data, processes and supporting assets

What are the data processed?

Número de telemóvel, sem prazo definido. Os documentos a assinar também são processados e esses dados são conservados apenas durante o tempo de processamento necessário para a realização da assinatura digital.

How does the life cycle of data and processes work?

O número de telemóvel é guardado e consultado e processado quando é necessário realizar a assinatura de um documento. O documento é carregado, os seus dados são processados para realizar a assinatura e depois desta estar gerada, o documento e respetivos dados são descartados.

What are the data supporting assets?

O tratamento feito é integrado numa aplicação da Comissão Europeia, a DSS Web App, por isso, todos os ativos utilizados são os mesmo utilizados por essa aplicação.

Evaluation : Acceptable

Fundamental principles
Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Os dados são tratados apenas para possibilitar a geração da assinatura digital do utilizador, que é a razão pela qual o utilizador os submete à aplicação, então, a finalidade do tratamento é específica, explícita e legítima.

Evaluation : Acceptable

What are the legal basis making the processing lawful?

O fundamento é o consentimento do utilizador para o tratamento dos dados que submete, há um consentimento implícito do tratamento dos dados do documento a assinar visto que, para o assinar,

é necessário utilizá-lo e processá-lo.

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')?

Sim, todos os dados recolhidos são usados para questões de assinatura ou de autenticação, não são recolhidos nem tratados mais dados do que os estritamente necessários.

Evaluation : Acceptable

Are the data accurate and kept up to date?

Sim, os dados não são guardados por um longo período de tempo, pelo que aquando da utilização da aplicação pelo utilizador, os dados são sempre atualizados.

Evaluation : Acceptable

What are the storage duration of the data?

Os dados são conservados apenas durante o tempo necessário para o processamento e realização da assinatura. Depois disso, do lado do utilizador, os dados são cosnervados pelo tempo desejado.

Evaluation : Acceptable

Fundamental principles

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

As informações osbre o tratamento dos dados estão disponíveis na página principal da aplicação e nas páginas onde o utilizador pede a assinatura do documento.

Evaluation : Acceptable

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

O consentimento é obtido quando o utilizador submete o documento na aplicação e efetua login com o Cartão de Cidadão ou Chave Móvel Digital, sendo que estes últimos já pedem o consentimento ao utilizador para a partilha dos dados com a aplicação. O consentimento para o número de telemóvel é obtido quando o utilizador preenche uma caixa de verificação.

Evaluation : Acceptable

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

Os dados não são guardados no lado do servidor, pelo que a garantia de acesso e portabilidade não é aplicável.

Evaluation : Acceptable

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

Os dados não são guardados no lado do servidor, pelo que a garantia de atualização e apagamento não é aplicável.

Evaluation : Acceptable

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

Não aplicável.

Evaluation : Acceptable

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

Não aplicável.

Evaluation : Acceptable

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

Não aplicável.

Evaluation : Acceptable

Risks

Planned or existing measures

Redução da acumulação de dados pessoais

Guardar (mesmo que apenas no lado do utilizador) o mínimo de dados possível, pelo menor tempo possível.

Evaluation : Acceptable

Cifragem

Guardar a "hash" dos dados e não os dados em plaintext.

Evaluation : Acceptable

Risks

Illegitimate access to data

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

Possibilidade de assinaturas de documentos com vantagens para o atacante e implicações sérias legais para o utilizador., Roubo de identidade

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

Um ataque de Cross-Site Scripting, Um acesso à página fonte da WebApp que possa ser caminho para encontrar uma vulnerabilidade de codificação

What are the risk sources?

Pessoas com conhecimento suficiente e que queiram atacar um utilizador da aplicação.

Which of the identified planned controls contribute to addressing the risk?

Cifragem, Redução da acumulação de dados pessoais

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

Important, Um acesso ilegítimo aos dados, neste caso, ao número de telemóvel do utilizador pode ter um impacto sério muito significativo na vida do mesmo, assim, mesmo com as técnicas de mitigação usadas baixarem a probabilidade de um ataque sucedido, considera-se que o risco é ainda significativo.

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

Limited, Devido às técnicas de mitigação implementadas, considera-se que a probabilidade de risco é limitada.

Evaluation : Acceptable

Risks

Unwanted modification of data

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

O utilizador teria que introduzir o número de telemóvel correto, A autenticcação não é sucedida enquanto o utilizador não efetuar a correção dos dados

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

Um ataque de Cross-Site Scripting, Um acesso à página fonte da WebApp que possa ser caminho para encontrar uma vulnerabilidade de codificação

What are the risk sources?

Pessoas com conhecimento suficiente e que queiram atacar um utilizador da aplicação.

Which of the identified controls contribute to addressing the risk?

Redução da acumulação de dados pessoais

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

Negligible, Dado um ataque suedido que explore este risco não tem grande impacto para o utilizador, considera-se que a gravidade de risco é insignificante.

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

Negligible, Pelo pouco impacto que tem, considera-se a probabilidade deste risco insignificante.

Evaluation : Acceptable

Risks

Data disappearance

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

O utilizador teria que introduzir o número de telemóvel correto, A autenticc não efetuar a correção dos dados, A autenticcação não é sucedida enquanto o utilizador não efetuar a correção dos dados

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

Um acesso à página fonte da WebApp que possa ser caminho para encontrar uma vulnerabilidade de codificação, Um ataque de Cross-Site Scripting

What are the risk sources?

Pessoas com conhecimento suficiente e que queiram atacar um utilizador da aplicação.

Which of the identified controls contribute to addressing the risk?

Redução da acumulação de dados pessoais

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

Negligible, Este risco tem um impacto muito baixo e pouca utilidade prática para um atacante, por isso, considera-se um risco de gravidade insignificante.

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

Negligible, Devido ao seu baixo impacto e pouca utilidade prática, considera-se a probabilidade deste risco insignificante.

Evaluation : Acceptable

Risks

Risks overview