

Preview

GENERAL INFORMATION

Preview

Editing : Grupo 3
Evaluation : Grupo 3
Validation : Grupo 3

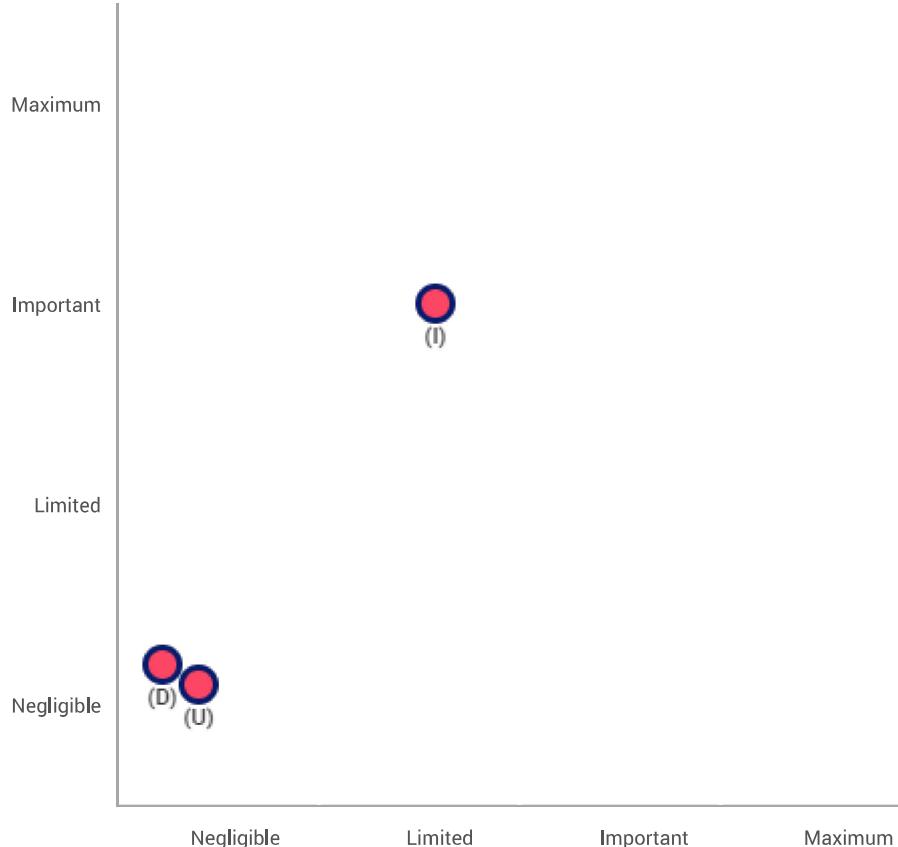
Status : Simple validation

100%

Validation

Risk mapping

Risk seriousness



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

11/05/2021

Validation

Action plan

Overview

Fundamental principles	Planned or existing measures
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Guardar o mínimo de dados possível, e do lado do utilizador CRSF Tokens
Risks	Improvable Measures Acceptable Measures
	<ul style="list-style-type: none"> Illegitimate access to data Unwanted modification of data Data disappearance

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 opinion

Por serem coisas simples, como a implementação de tokens CSRF, e práticas comuns da indústria, este tipo de mitigação deve ser implementado.

Search of concerned people opinion

Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested

Indisponibilidade

Context Overview

What is the processing under consideration?

O armazenamento de dados do utilizador para criação de assinaturas digitais utilizando o Cartão de Cidadão Português e a Chave Móvel Digital.

What are the responsibilities linked to the processing?

O processamento de dados irá ser realizado de modo a poder permitir a criação de uma assinatura digital de vários tipos de documentos. Assim, será necessário processar os dados relativos ao Cartão de Cidadão do utilizador, dados relativos à Chave Móvel Digital do utilizador, e relativos ao próprio documento em questão que deverá ser assinado.

Are there standards applicable to the processing?

O RGPD (Regulamento Geral da Proteção de Dados) tem de ser tido em conta neste projeto.

Evaluation : Acceptable

Context

Data, processes and supporting assets

What are the data processed?

Os dados processados para efeitos de autenticação são o número de telemóvel do utilizador, que não são armazenados do lado do servidor mas apenas do lado do cliente. Os documentos a assinar também são processados.

How does the life cycle of data and processes work?

Os documentos a assinar são carregados para o servidor, processados para gerar a respetiva assinatura, e são depois descartados, não sendo guardados no lado do servidor para além do tempo necessário para o cumprimento do pedido do utilizador.

O número de telemóvel do utilizador é guardado do lado do cliente, pelo que apenas é processado do lado do servidor apenas quando é necessário fazer a assinatura, tal como no ponto anterior.

What are the data supporting assets?

Este processo de assinatura está integrado na aplicação DSS Web App, da Comissão Europeia, pelo que utiliza os mesmos sistemas do que esta.

Evaluation : Acceptable

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Os documentos a assinar são processados para cumprir o pedido do utilizador, bem como os dados necessários para gerar a assinatura do documento. Assim o seu uso é legítimo, segundo o GDPR.

O número de telemóvel, como tem o objetivo de facilitar o início de sessão do utilizador, está apenas a ser guardado do lado do utilizador. Assim sendo, não são colocadas questões de incumprimento do GDPR.

Evaluation : Acceptable

What are the legal basis making the processing lawful?

A base legal para o processamento dos dados é o processamento para um propósito específico para o qual o utilizador dá o seu consentimento implícito (pedir para assinar um documento implica, obrigatoriamente, o uso do documento).

A base legal para o processamento do número de telemóvel é o consentimento explícito do utilizador (o número apenas é armazenado se o mesmo o pedir).

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')?

Os documentos a assinar são necessários para cumprir o pedido do utilizador.

O número de telemóvel é recolhido, com o consentimento explícito do utilizador, para facilitar a assinatura futura de documentos.

Evaluation : Acceptable

Are the data accurate and kept up to date?

Como não existem dados guardados do lado do servidor por um período de tempo extendido, não é necessário manter os dados atualizados, pois estes são "refreshed" sempre que o utilizador pretende assinar um novo documento.

Evaluation : Acceptable

What are the storage duration of the data?

Os dados ficam guardados do lado do utilizador durante o tempo que este desejar.

Evaluation : Acceptable

Fundamental principles

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Os utilizadores são informados do processamento na página principal da aplicação, bem como nas páginas onde podem pedir a assinatura dos documentos.

Evaluation : Acceptable

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

Para a assinatura digital de documentos, é necessário que estes façam upload dos documentos, e autorizem o login com o seu Cartão de Cidadão/Chave Móvel Digital, pelo que, estes atos, constituem consentimento para o processamento dos dados.

Relativamente ao número de telemóvel, o consentimento é obtido com uma "checkbox", que não está pré-preenchida.

Evaluation : Acceptable

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

Não aplicável, visto que não são guardados dados do lado do servidor.

Evaluation : Acceptable

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

Não aplicável, novamente, pois não são guardados dados do lado do servidor.

Evaluation : Acceptable

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

Não aplicável, novamente, pois não são guardados dados do lado do servidor.

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

Guardar o mínimo de dados possível, e do lado do utilizador

Guardas o número de telemóvel em cookies (apenas do lado do utilizador). Assim, não existe risco de divulgação dos dados.

Evaluation : Acceptable

CRSF Tokens

Utilizar tokens CSRF para prevenir ataques baseados XSS.

Evaluation : Acceptable

Risks

Illegitimate access to data

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

Possivelmente o roubo de identidade, através do número de telemóvel do utilizador.

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

Cross-Site Scripting (XSS) poderá permitir o roubo do número de telemóvel do utilizador, pelo que medidas de mitigação standard deverão ser cumpridas.

What are the risk sources?

Hackers a fazer target de um utilizador.

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

Guardar o mínimo de dados possível, e do lado do utilizador, CSRF Tokens

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

Important, O roubo do número de telemóvel pode ter impacto alto na vida de um utilizador, incluindo o potencial para roubo de identidade. No entanto, com as técnicas de mitigação anteriormente descritas (que são prática comum em web development), o risco é minimizado.

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

Limited, O potencial do risco é baixo, considerando as mitigações a implementar.

Evaluation : Acceptable

Risks

Unwanted modification of data

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

Reintrodução do número de telemóvel correto

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

Cross-Site Scripting (XSS) poderá permitir o roubo do número de telemóvel do utilizador, pelo que medidas de mitigação standard deverão ser cumpridas.

What are the risk sources?

Hackers a fazer target de um utilizador.

Which of the identified controls contribute to addressing the risk?

CRSF Tokens, Guardar o mínimo de dados possível, e do lado do utilizador

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

Negligible, O risco de modificação de dados é negligível pelo seu impacto limitado.

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

Negligible, O risco de modificação de dados, por ser negligível por não ter utilidade prática, é limitado.

Evaluation : Acceptable

Risks

Data disappearance

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

Reintrodução do número de telemóvel correto

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

Cross-Site Scripting (XSS) poderá permitir o roubo do número de telemóvel do utilizador, pelo que

medidas de mitigação standard deverão ser cumpridas.

What are the risk sources?

Hackers a fazer target de um utilizador.

Which of the identified controls contribute to addressing the risk?

CRSF Tokens, Guardar o mínimo de dados possível, e do lado do utilizador

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

Negligible, O risco de apagar dados, por não ter utilidade prática, e pelo seu limitado impacto, é negligível.

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

Negligible, O risco de apagar dados, por não ter utilidade prática, e pelo seu limitado impacto, é negligível.

Evaluation : Acceptable

Risks

Risks overview

Potential impacts

Possivelmente o roubo de id...
Reintrodução do número de t...

Threats

Cross-Site Scripting (XSS) ...

Sources

Hackers a fazer target de u...

Measures

Guardar o mínimo de dados p...
CRSF Tokens

Illegitimate access to data

Severity : Important

Likelihood : Limited

Unwanted modification of data

Severity : Negligible

Likelihood : Negligible

Data disappearance

Severity : Negligible

Likelihood : Negligible

