Validação

Mapeamento de riscos

Validação

Plano de ação

Princípios fundamentais

Nenhum plano de ação registado.

Medidas existentes e planeadas

Nenhum plano de ação registado.

Riscos

Nenhum plano de ação registado.

Validação

Opinião do DPO e dos titulares dos dados

Nome do DPO

DPO

Estado do DPO

O tratamento deve ser implementado.

Opinião do DPO

Considera-se que não há contra-indicações à implementação do tratamento.

Procura da opinião de partes interessadas

A opinião das partes em questão foi solicitada.

Opiniões de partes interessadas

Partes Interessadas

Status de pessoas em questão

O tratamento deve ser implementado.

Opiniões de partes interessadas

Considera-se que não há contra-indicações à implementação do tratamento.

Contexto

Visão geral

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

A aplicação tem a finalidade de emitir certificados para os seus utilizadores e permitir manter uma plataforma a partir das quais os seus utilizadores consigam aceder a estes e verificar as suas validades.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

É importante manter os certificados apenas acessíveis a quem os emite e é também importante manter as contas de cada utilizador inacessíveis a terceiros.

Quais são as normas aplicáveis à finalidade de tratamento?

A informação dos utilizadores que é mantida pela aplicação é protegida a partir da utilização de protocolos criptográficos.
A informação de cada conta é também associada unicamente a esta.

Avaliação : Aceitável

Contexto

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Os dados pessoais tratados são o nome dos utilizadores, informações de contacto, morada e nacionalidade, não havendo um prazo de conservação definido para estes. São também tratados os certificados e timestamps de cada utilizador.

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

Os nomes dos utilizadores e passwords são mantidos numa base de dados, assim como informações de certificados e timestamps de cada utilizador. Todas as outras informações são utilizadas atomicamente para a emissão de certificados por parte de um software terceiro, o OpenSSL. São mantidas num ficheiro que é criado, utilizado e posteriormente removido.

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

Os dados são utilizados pelo software OpenSSL.

Avaliação : Aceitável

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

Sim, a finalidade é a emissão de certificados e consulta destes, assim como a verificação da sua validade.

Avaliação : Aceitável

Qual é o fundamento para tratamento de dados pessoais?

São necessários para identificar utilizadores e para associar os seus certificados a estes, e são também necessários para a emissão de novos certificados.

Avaliação : Aceitável

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

Sim, apenas os dados necessários para a emissão de certificados são recolhidos, e são usados atomicamente.

Avaliação : Aceitável

Os dados pessoais estão atualizados e são fidedignos?

Sim, estão sempre atualizados sendo que são requeridos no momento em que serão utilizados pela aplicação.

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

Não está estabelecido.

Avaliação : Aceitável

Princípios fundamentais

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?

Os titulares dos dados são informados do propósito da utilização dos seus dados (emissão de certificados).

Avaliação : Aceitável

Como é obtido o consentimento dos titulares de dados?

O consimento é obtido pois os dados têm que ser fornecidos voluntariamente pelos utilizadores.

Avaliação : Aceitável

Como é garantido o acesso e portabilidade de dados pessoais?

Cada utilizador consegue aceder a qualquer momento às suas informações mantidas na aplicação, a partir do momento que se autentique nesta (consegue aceder aos seus certificados/timestamps).

Avaliação : Aceitável

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

Atualização/retificação é mantida porque os dados devem ser introduzidos de cada vez que são necessários.
O apagamento é garantido porque os dados são utilizados atomicamente.

Avaliação : Aceitável

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

O utilizador tem a opção de não introduzir todos os dados que lhe são requeridos.

Avaliação : Aceitável

As obrigações dos subcontratantes são claramente identificadas e reguladas por contrato ou outro ato normativo?

Os dados utilizados por terceiros são utilizados no momento de emissão de novos certificados e não são mantidos.

Avaliação : Aceitável

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

Não está estabelecido que se faça transferência de dados.

Avaliação : Aceitável

Riscos

Medidas planeadas ou existentes

Cifragem

Os dados que são mantidos pela aplicação são cifrados com uma função de hash.

Avaliação : Aceitável

Controlo de acesso lógico

A aplicação implementa um sistema de controlo de acesso, sendo que um utilizador tem que se autenticar para aceder à aplicação, e ainda voltar a autenticar-se para executar determinadas ações.

Avaliação : Aceitável

de dados pessoais

Os dados pessoais que são mantidos pela aplicação são os mínimos necessários para o seu funcionamento.

Avaliação : Aceitável

Relações com terceiros

É utilizado software de terceiros (OpenSSL) sendo que este é software open source, utilizado na versão mais recente, sem vulnerabilidades conhecidas até à data.

Avaliação : Aceitável

Riscos

Acesso ilegítimo dos dados

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

Podiam ser tornados públicos, mas a informação estaria cifrada., Podiam ser eliminados ou alterados.

Quais são os principais ameaçasque poderiam levar ao risco?

SQL Injection, Spoofing, Tampering, DoS

Quais são as fontesde risco?

Hackers, Negligência dos utilizadores, Falha no software de terceiros

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

Cifragem, Controlo de acesso lógico, de dados pessoais, Relações com terceiros

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

Limitado, Se o risco ocorresse, a informação a que se chegaria estaria cifrada, no caso de se acederem às informações mantidas pela aplicação.
O maior risco seria a potencial perda desta informação.

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

Insignificante, O risco considera-se insignificante, pois há medidas de proteção contra os potenciais riscos que podem ocorrer.

Avaliação : Aceitável

Riscos

Modificação indesejada dos dados

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

Podiam ser eliminados ou alterados., Podiam ser tornados públicos, mas a informação estaria cifrada.

Quais são as principais ameaças que poderiam levar ao risco?

SQL Injection, Spoofing, Tampering

Quais são as fontesde risco?

Falha no software de terceiros, Hackers, Negligência dos utilizadores

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

Cifragem, Controlo de acesso lógico, de dados pessoais, Relações com terceiros

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

Limitado, Se o risco ocorresse, a informação a que se chegaria estaria cifrada, no caso de se acederem às informações mantidas pela aplicação.
O maior risco seria a potencial perda desta informação.

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

Insignificante, O risco considera-se insignificante, pois há medidas de proteção contra os potenciais riscos que podem ocorrer.

Avaliação : Aceitável

Riscos

Desaparecimento de dados

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

Podiam ser eliminados ou alterados.

Quais são as principais ameaças que poderiam levar ao risco

Tampering

Quais são as fontesde risco?

Hackers, Negligência dos utilizadores

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

Controlo de acesso lógico, de dados pessoais

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

Limitado, Se o risco ocorresse, a informação a que se chegaria estaria cifrada, no caso de se acederem às informações mantidas pela aplicação.
O maior risco seria a potencial perda desta informação.

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

Insignificante, O risco considera-se insignificante, pois há medidas de proteção contra os potenciais riscos que podem ocorrer.

Avaliação : Aceitável

Riscos

Visão geral dos riscos