Informação PIA

PIA
Meteorologia Automática

Nome do autor
Diana

Nome do assessor
Adriana

Nome do validador
Diana

Data de criação
10/04/2019

Nome do DPO
Diana

Opinião do DPO
De acordo com a análise efetuada, o tratamento de dados pode ser implementado, uma vez que não causará nenhuma ameaça para os tais.

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

Opiniões de partes interessadas
Adriana

Status de pessoas em questão
O tratamento deve ser implementado.

Opiniões de partes interessadas
Tendo em conta toda a informação apresentada, o tratamento poderá ser implementada de acordo com as normas de segurança descritas.

Contexto

Visão geral

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

Imaginemos que estávamos a iniciar um projeto que tinha como principal intuito desenvolver um site que envolvia a utilização de dados pessoais cujo processamento resulta num risco elevado. O objetivo deste site seria informar os utilizadores que estivessem registados no mesmo sobre os estados da meteorologia. Para tal existem alguns dados que seriam necessário para o fornecimento da informação meteorológica, nomeadamente:

- Nome do utilizador;
- Morada do utilizador (região geográfica);
- Endereço de email;
- Dados bancários (A informação enviada iria ter custos);
- Pagamentos mensais através de paypal ou cartão de crédito

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

É da responsabilidade da empresa definir os mecanismos apropriados para alcançar a conformidade com as política, sendo a responsabilidade pela implementação operacional das equipa de desenvolvimento do site.
Contudo, vai ser necessário que o sistema seja desenvolvido por especialista na área de segurança devido a dados sensíveis de cliente, achando assim desnecessário de uma entidade externa para análise de segurança.

Quais são as normas aplicáveis à finalidade de tratamento?

Os dados pessoas poderão ser recolhidos e tratados pela empresa com as seguintes finalidades:

- Envio da informação meterológica;
- Calculo e pagamento da mensalidade do serviço prescrito

Avaliação : Aceitável
Comentário de avaliação :
De acordo com as informações disponíveis, as medidas impostas no serviço são adequadas para atender apropriadamente aos requisitos de proteção de dados.

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

- Dados pedidos: nome, email, informação geográfica e dados de pagamento;
- Estes dados só são pedidos no momento do registo;
- Não existe nenhuma relação com os clientes, desde que sejam com idade superior a 18 anos, qualquer pessoa pode-se registar no site;

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

- Todos os dados serão mantidos na base de dados até o cliente decidir terminar a conta.

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

- A informação geográfica e consultada todos os dias;
- A informação de pagamento é consultada mensalmente;
- O número de indivíduos são o número de pessoas que se registarem;
- A área que é abrangida correspondente aos utilizadores que se registam;
- Os dados não serão partilhados com mais nenhuma identidade;

Avaliação : Aceitável
Comentário de avaliação :
De acordo com a descrição os dados adquiridos são necessários ao bom funcionamento do serviço.

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

A finalidade de tratamento de dados é específica, explícita e legítima uma vez que:

● Os fins para os quais os dados pessoais podem ser utilizados pelas Partes Interessadas da empresa;

● Todos os dados recolhidos têm uma finalidade determinada, explícita e legítima e não são tratados posteriormente de uma forma incompatível com essa finalidade.

Avaliação : Aceitável

Comentário de avaliação :

É importante reduzir a gravidade dos riscos, minimizando o número de dados pessoais que serão processados, limitando esses dados ao estritamente necessário para os fins para os quais são processados (caso contrário, não devem ser recolhidos). Então, também é possível minimizar os dados por meio de controlos que visam reduzir sua sensibilidade.

Qual é o fundamento para tratamento de dados pessoais?

O fundamento para o tratamento de dados pessoais consiste:

- Consentimento;
- Interesse legítimo

Avaliação : Aceitável

Comentário de avaliação :

Os dados pessoais devem ser recolhidos para finalidades específicas, explícitas e legítimas e não processadas posteriormente de maneira incompatível com esses fins.

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

● Sim, os dados pessoais recolhidos são adequados, revelantes e limitados para o proposito do serviço a ser fornecido, uma vez que vamos adquirir os dados através de um formulário, no ato de registo.

Avaliação : Aceitável

Comentário de avaliação :

Os dados pessoais devem ser precisos e, quando necessário, mantidos atualizados.

Os dados pessoais estão atualizados e são fidedignos?

● Apesar dos esforços em manter os conteúdos atualizados e fidedignos, estes podem apresentar incorreções, erros de tipografia ou estar desatualizados, podendo ser alterados em qualquer momento.

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

● Todos os dados serão mantidos na base de dados até o cliente decidir terminar a 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?

Através da declaração de proteção de dados, a organização informa ao público em geral a natureza, a intenção e a finalidade dos dados pessoais que são recolhidos, usados e tratados.

Avaliação : Aceitável

Como é obtido o consentimento dos titulares de dados?

O consentimento dos titulares é obtido no ato do registo no site.

Avaliação : Aceitável

Como é garantido o acesso e portabilidade de dados pessoais?

O acesso e portabilidade de dados pessoais é garantido a partir do formulário de inscrição no serviço.

Avaliação : Aceitável

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

No ato do registo será garantido o facto de caso seja necessário atualizar/retificar ou apagar os dados pessoais pedido pelo titular dos mesmos.

Avaliação : Aceitável

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

No ato do registo será garantido a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos. Não havendo necessidade de contrariar o pedido do mesmo.

Avaliação : Aceitável

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

Não existem subcontratantes neste sistema.

Avaliação : Aceitável

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

Os dados não vão ser tranferidas para fora da União Europeia.

Avaliação : Aceitável

Riscos

Medidas planeadas ou existentes

Cifração dos dados

Através de tecnicas criptográficas serão cifrados todos os dados relativos aos utlizadores.

Avaliação : Aceitável

Acesso ilegítimo dos dados

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

Acesso a dados bancários o que poderia levar a débitos que não correspoderiam ao valor real do serviço.

Quais são os principaisameaçasque poderiam levar ao risco?

Software vulnerável

Quais são as fontesde risco?

Fontes humanas internas

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

Cifração dos dados

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

Limitado, Como o serviço é demasiadamente simplista a gravidade do risco acaba por ser limitada, não havendo um perigo constante do sistema.

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

Insignificante, Como o serviço é demasiadamente simplista a probabilidade de risco é insignificante.

Avaliação : Aceitável

Modificação indesejada dos dados

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

Os impactos nos dados dos titulares caso o reisco ocorresse seriam inumeros, mas nomeadamente a perda do serviço seria um desses impactos.

Quais são as principais ameaças que poderiam levar ao risco?

O facto do software possuir vulnerabilidades poderia levar a um risco.

Quais são as fontesde risco?

Fontes humanas internas, Fontes humanas externas, Fontes não humanas, Fontes de risco

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

Cifração dos dados

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

Limitado, A gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados é estimada devido ao utilidade do sistema desenvolvido.

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

Insignificante, Não será do interesse dos atacantes explorarem os dados dos utilizadores deste tipo de serviço, assim sendo, estimamos a probabilidade do risco como insignificante.

Avaliação : Aceitável

Desaparecimento de dados

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

Os principais impactos nos dados dos titulares se o risco ocorrer são o facto dos utilizadores deixarem de receber as informaçoes meteorológicas.

Quais são as principais ameaças que poderiam levar ao risco

As principais ameaças que poderiam levar ao risco são o facto de o software desenvolvido não ter segurança adequada ao tipo de dados.

Quais são as fontesde risco?

Fontes humanas internas, Fontes humanas externas, Fontes não humanas

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

Cifração dos dados

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

Limitado, A gravidade do risco classifica-se como limitada, uma vez que neste caso, os titulares podem sofrer apenas a perda do serviço.

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

Insignificante, A probabilidade do risco torna-se insignificante uma vez que os dados não serão de interesse direto para os atacantes.

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

Cifração dos dados

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

- Acesso a dados bancários o ...
- Os impactos nos dados dos t...
- Os principais impactos nos ...

Ameaças

- Software vulnerável
- O facto do software possuir...
- As principais ameaças que p...

Fontes

- Fontes humanas internas
- Fontes humanas externas
- Fontes não humanas
- Fontes de risco

Medidas

- Cifração dos dados

Acesso ilegítimo dos dados

Gravidade : Limitado

Probabilidade : Insignificante

Modificação indesejada dos dados

Gravidade : Limitado

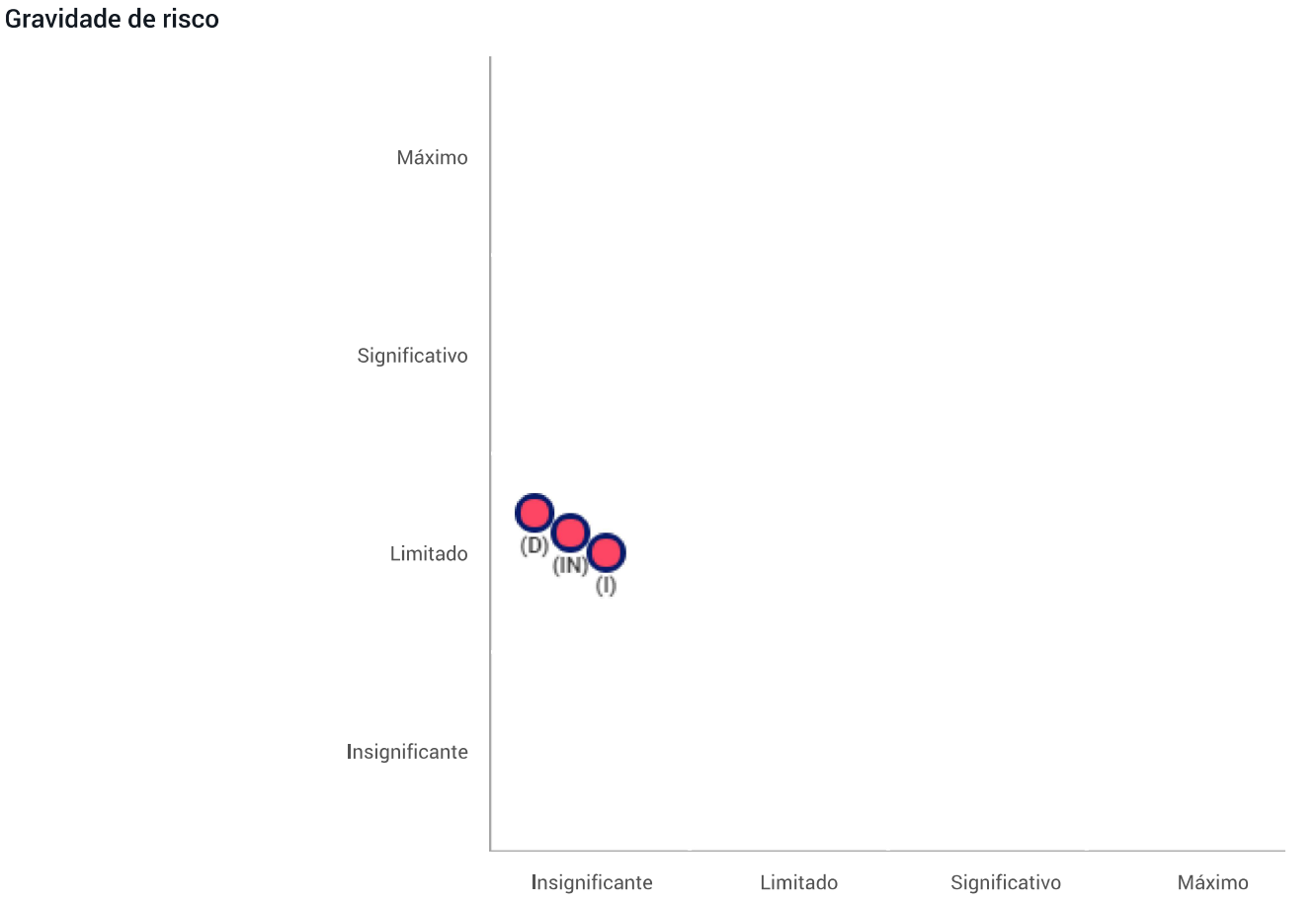
Probabilidade : Insignificante

Desaparecimento de dados

Gravidade : Limitado

Probabilidade : Insignificante

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

10/04/2019