PIA information

PIA
Grupo 8

Author's name
Bruno, Pereira

Assessor's name
Bruno, Pereira

Validator's name
Bruno, Pereira

Creation date
18/04/2019

Context

Overview

Which is the processing under consideration?

O processamento de dados corresponde à coleta de informações de computadores pessoais e dispositivos móveis, tendo em vista coletar dados de aplicações em ambos os dispositivos para uma aplicação de gestão de agenda, onde os dados serão usados para identificar atividades que possam ser inferidas como de determinado(s) projeto(s). O processo de coleta é todo automatizado.

O alcance da recolha de dados está no âmbito de atividades como chamadas telefónicas, SMS, localização geográfica (GPS ou outra), atividades de desenvolvimento de software (IDEs, Git, editores de texto, janelas abertas).

What are the responsibilities linked to the processing?

Os controladores dos dados serão a empresa da aplicação a desenvolver, bem como todos os intervenientes na coleção e classificação dos dados (programadores/admistradores/operadores) da empresa e sub-contratados à empresa, bem como aplicações e/ou serviços de terceiros para tratamento dessa classificação, seja por machine-learning, seja por normalização de dados.

Are there standards applicable to the processing?

De acordo com o Art. 40 e o Art. 42, deverá existir um contrato entre o controlador e sujeito dos dados com base no seu consentimento da participação da coleta ou outro vínculo legal. Esse contrato deverá demonstrar de forma clara que o sujeito dos dados deu consentimento e o mesmo contrato é de fácil acesso, inteligível, contendo a identidade do controlador.

Data, processes and supporting assets

What are the data processed?

Atividades de janelas abertas num sistema operativo Linux, atividades com o sistema de controlo de versões Git, chamadas e SMS efetuados com um smartphone Android Nougat, bem como localizações geográficas de grande precisão (GPS), precisão ponderada (Wifi, Bluetooth), como também contagem de passos. Os dados pessoais dos utilizadores para a aplicação de gestão de agenda também serão guardados, tais como nome, número de contato telefónico, email, morada, função na empresa como também dados relativos a projetos que os clientes estejam envolvidos, como nome de projetos, pessoas associadas a esse projeto (stakeholders).

How does the life cycle of data and processes work?

Os dados serão transferidos através de uma aplicação REST dos vários clientes para bases de dados centrais - uma relacional para os dados pessoais e outra não relacional para os dados da coleta das atividades. A aplicação mobile possui uma base de dados SQLite, no entanto os dados guardados serão eliminados após dados periodo de coleta sendo enviados automáticamente para o servidor onde os dados serão guardados nas duas bases de dados. A destruição de dados pessoais é após término do projeto e os dados de atividades serão guardados a mais longo prazo, para processamento e classificação para serem catalogados para futuro processamento numa base de conhecimento.

What are the data supporting assets?

Base dados Postgres, base de dados MongoDB, Android Nougat, Linux genérico para uso diário de trabalho, servidor CentOS alojado na Google Cloud e acessos via browser e smartphone à aplicação no servidor na nuvem - ambos acessos por uma API REST.

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Todos os dados serão coletados apenas para classificação e consequente identificação de determinada atividade no âmbito de um projeto empresarial.

What are the legal basis making the processing lawful?

Todos os utilizadores da aplicação dão o seu consentimento após leitura e concordância de uma notificação na forma de contrato antes do registo na aplicação, sendo que os dados são necessários para identificar tempo gasto em dado projeto, uma vez que é a base do modelo de negócio da empresa que desenvolve a aplicação.

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 dados relacionados diretamente com dados pessoais e projetos da empresa são estritamente necessário para contatos e identificação mínima perante a aplicação. Os dados coletados para processamento, classificação e identificação das atividades do projeto são necessários para inferir que atividades de projeto pertencem, sendo possível remover dados através de filtros, anonimização dos dados, desde que seja possível indentificar qual a altura da atividade, o tempo gasto com essa atividade em determinado projeto (não incluindo a atividade em si, apenas um marcador de atividade genérico - como "Chamada no âmbito do projeto X às 15:00" - sendo o tempo gasto inferido por um conjunto de atividades onde se possa dizer que essas atividades todas são do projeto X).

Are the data accurate and kept up to date?

Os utilizadores podem alterar os seus dados pessoais e os projetos que estão a realizar, bem como as pessoas associadas a esse projeto, bem como pode remover a sua conta. Os dados das atividades coletadas são processados e classificados de forma a que apenas em que alturas e tempo gasto com as mesmas em determinado projeto, de forma a que sejam independentes de quem gerou os dados, durante a sua participação no projeto X.

What are the storage duration of the data?

Os dados serão mantidos até ao final do projeto se forem dados relacionados com atividades recolhidas, sendo depois catalogados para futuro processamento, sem associação com o utilizador que gerou os dados e devidamente anomizados até que já não sirva para uma base de conhecimento. Os dados pessoais são mantidos durante todo o registo na aplicação até remoção da conta.

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Os utilizadores são informados no contrato antes do registo na aplicação.

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

O registo na aplicação apenas é efetuado se o sujeito dos dados concordar com a recolha dos dados, caso contrário a aplicação não pode funcionar.

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

Os sujeitos dos dados podem pedir explicitamente na aplicação a confirmação de que os dados do sujeito estão a ser processados e onde podem aceder a esses dados pessoais.

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

Os sujeitos dos dados podem utilizar a área explicitamente criada para esse efeito na aplicação.

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

Todos os dados pessoais são apagados após remoção de conta.

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

Os controladores dos dados serão a empresa da aplicação a desenvolver, bem como todos os intervenientes na coleção e classificação dos dados (programadores/admistradores/operadores) da empresa e sub-contratados à empresa, bem como aplicações e/ou serviços de terceiros para tratamento dessa classificação tem um contrato legal de não-divulgação de dados e acesso aos dados e a que tipo de dados terá acesso.

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

A conta da Google Cloud está nos Estados Unidos e os dados da nuvem são adequadamente protegidos.

Risks

Planned or existing measures

Encryption

Anonymisation

Partitioning data

Logical access control

Archiving

Traceability (logging)

Paper document security

Minimising the amount of personal data

Operating security

Clamping down on malicious software

Managing workstations

Website security

Backups

Maintenance

Processing contracts

Network security

Physical access control

Monitoring network activity

Hardware security

Avoiding sources of risk

Protecting against non-human sources of risks

Organisation

Policy

Managing privacy risks

Integrating privacy protection in projects

Managing personal data violations

Personnel management

Relations with third parties

Supervision

Illegitimate access to data

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

Descoberta de padrões de atividade, roubo de identidade e outros crimes relaciados com compromisso de dados pessoais, Perda de lucro para a empresa

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

What are the risk sources?

Which of the identified controls contribute to addressing the risk?

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

Important

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

Important

Unwanted modification of data

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

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

What are the risk sources?

Which of the identified controls contribute to addressing the risk?

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

Important

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

Important

Data disappearance

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

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

What are the risk sources?

Which of the identified controls contribute to addressing the risk?

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

Important

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

Important

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

Encryption
Anonymisation
Partitioning data
Logical access control
Archiving
Traceability (logging)
Paper document security
Minimising the amount of personal data
Operating security
Clamping down on malicious software
Managing workstations
Website security
Backups
Maintenance
Processing contracts
Network security
Physical access control
Monitoring network activity
Hardware security
Avoiding sources of risk
Protecting against non-human sources of risks
Organisation
Policy
Managing privacy risks
Integrating privacy protection in projects
Managing personal data violations
Personnel management
Relations with third parties
Supervision

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

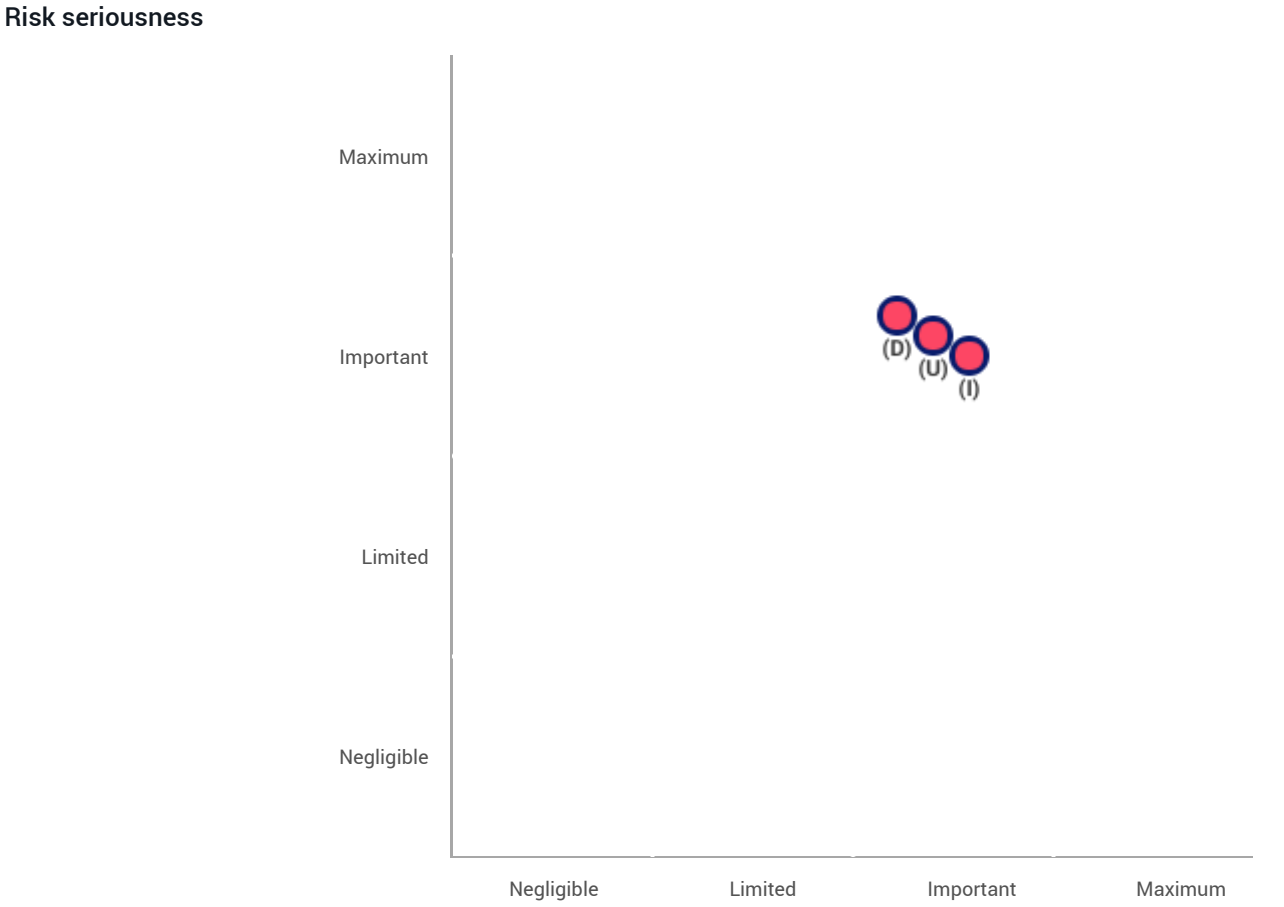
No action plan recorded.

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

18/04/2019