

Preview

GENERAL INFORMATION

Preview

Editing : Paulo Gameiro
Evaluation : Pedro Rodrigues
Validation : Rafaela Soares

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

22/03/2020

Validation

Action plan

Overview

Fundamental principles	Planned or existing measures
Purposes	Encryption
Legal basis	Anonymization
Adequate data	Logical access control
Data accuracy	Traceability (logging)
Storage duration	Minimising the amount of personal data
Information for the data subjects	Website security
Obtaining consent	Backups
Right of access and to data portability	Network security
Right to rectification and erasure	Physical access control
Right to restriction and to object	Monitoring network activity
Subcontracting	Hardware security
Transfers	Avoiding sources of risk
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

Rafaela Soares

DPO's opinion

easy to do

Search of concerned people opinion

Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested

Context

Overview

What is the processing under consideration?

O projeto escolhido consiste num programa de gestão de utilização de tempo, onde todos os dados de utilização do sistema operativo como programas de email, editores de texto, IDE's, git, chamadas, sms e localizações GPS são guardadas para inferir quando é que o utilizador esteve a trabalhar e em actividades de lazer.

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 utilização de tempo, onde os dados serão usados para identificar atividades que possam ser inferidas como de determinado(s) projeto(s) ou lazer.

What are the responsibilities linked to the processing?

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 utilização de tempo 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). 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). 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 subcontratados 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.

Evaluation : Acceptable

Context

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 utilização de tempo 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?

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

What are the data supporting assets?

Base dados Postgres, MongoDB, Android , 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.

Evaluation : Acceptable

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.

Evaluation : Acceptable

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.

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 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 são necessários para categorizar as atividades, sendo possível remover dados através de filtros, anonimização dos dados, desde que seja possível identificar qual a altura da atividade, o tempo gasto com essa atividade (não incluindo a atividade em si, apenas um marcador de atividade genérico como "Chamada no âmbito do projeto X às 10:00" - sendo o tempo gasto inferido por um conjunto de atividades onde se possa dizer que essas atividades todas são do projeto X).

Evaluation : Acceptable

Are the data accurate and kept up to date?

Os utilizadores podem alterar os seus dados pessoais , 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.

Evaluation : Acceptable

What are the storage duration of the data?

Os dados serão mantidos até ao final do ano 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.

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 no contrato antes do registo na aplicação.

Evaluation : Acceptable

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.

Evaluation : Acceptable

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.

Evaluation : Acceptable

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.

Evaluation : Acceptable

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

Todos os dados pessoais são apagados após remoção de conta.

Evaluation : Acceptable

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/administradores/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.

Evaluation : Acceptable

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.

Evaluation : Acceptable

Risks

Planned or existing measures

Encryption

Evaluation : Acceptable

Anonymization

Evaluation : Acceptable

Logical access control

Evaluation : Acceptable

Traceability (logging)

Evaluation : Acceptable

Minimising the amount of personal data

Evaluation : Acceptable

Website security

Evaluation : Acceptable

Backups

Evaluation : Acceptable

Network security

Evaluation : Acceptable

Physical access control

Evaluation : Acceptable

Monitoring network activity

Evaluation : Acceptable

Hardware security

Evaluation : Acceptable

Avoiding sources of risk

Evaluation : Acceptable

Risks

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 relacionados com compromisso de dados pessoais

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

What are the risk sources?

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

Encryption

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, -

Evaluation : Acceptable

Risks

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?

Encryption

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

Limited, -

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

Limited, -

Evaluation : Acceptable

Risks

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?

Encryption

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

Limited, -

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

Limited, -

Evaluation : Acceptable

Risks

Risks overview

Potential impacts

Descoberta de padrões de at...

—

Threats

—

—

Illegitimate access to data

Severity : Important

Likelihood : Important

Sources

