



Data Ethics and Protection

Esame_20220623_Part_1_In-person



ANAM UR REHMAN
283909

Iniziato giovedì, 23 giugno 2022, 14:16

Terminato giovedì, 23 giugno 2022, 15:01

Tempo impiegato 45 min.

Valutazione 14,00 su un massimo di 15,00 (93%)

Domanda 1

Completo

Punteggio ottenuto 7,00 su 7,50

In an EU country, a company decides to use wearable robots for its employees. The robots have to fit the body and the company is considering several options, including the use of images generated by employees' body scans. In addition, the robots will be equipped with some sensors to collect certain parameters (body temperature, heart rate) during the work shift.

Can this technology be developed and used in a GDPR-compliant manner? Please provide arguments for your answer, considering different purposes, scenarios and possible technical solutions.

Subject-Matter

The company is collecting biometric data about employees such as body measurements via body scan images. This information can not only identify the Data subject, but also they cannot easily change their body shape and sizes. This fall under the GDPR.

For other measurements, if a unique identifier is used to collect temprature and heart rate, then the data is pseudonymous but Data subject can still be identified using additionall information, Hence it is also under consituency of GDPR.

The company is already in EU so the territorial scope aspect is already met.

Purpose, scenarios

If the company is working in this project to increase the productivity of employees then it is a different context w.r.t if they are trying to help disabled or old-age employees who cannot work long hours due to their physical nature condition. In the later case, we have different

proportionality and balance of interest is also different.

The company cannot rely (only) on the Data subject consent because there might be a conflict of interest between employee and their company.

It is also not mentioned where the data about body temperature and heart rate is stored and for how long they will keep it in the form which allows directly or indirectly identification of Data subject.

Possible technical solutions

As far as body shapes are concerned, company can avoid that by designing robots for different categories, (small, medium, large, Xlarge) and providing the possibility of adjusting some parts length, width to fit better the employee. Keep in mind that these adjustments should disappear after the shift is over and robot should turn back to a "Default" shape.

To build these categories efficiently, they can perform a survey from employee where participation is totally optional and data is collected for very short period of time (even for 1 day). This is useful in the case when company has employees from different part of the world and using national level statistics of body measure is not optimal. (Even if it is for 1 day, it is still Personal data and it falls under GDPR. So all the GDPR compliance principles should be considered prior to this survey)

For the measurements about body temperature and heart rate, the data should be collected at each work shift and destroyed as soon as the shift is over.

Commento:

Domanda 2

Completo

Punteggio ottenuto 7,00 su 7,50

What is a DPIA (Data Protection Impact Assessment) and why is it important?

What is DPIA?

DPIA is a document containing the following information:

- Description of the nature of personal data being collected, processed. The legal basis for Data Controller to perform these actions (if any).
- Describes if the consent of involved data subject is taken before performing any operation on their personal data in easily accessible manner. How Data subject can achieve his rights related to personal data such as right to rectification, erasure, portability, object etc.

- It assess kind of risk to data subject (to their privacy, fundamental human rights or freedom) are present and what is their severity. If any protected attributes about data subjects are being collected or processed. If there is a risk of any sort of discrimination based on protected attributes such as their Sex, ethnicity, Political preferences, Religion or biometric information etc.
- The legitimate interests of Data controller and their balance with Fundamental rights and freedom of data subject.
- What is the purpose of this data collection and processing (purpose limitation), For how long the personal data will be stored, processed or transmitted (Data retention policy), What other measures are taken to further safeguard any harmful impact on Data subject.
- Measures taken for data security such as encryption of user devices, pseudonymization.
- What is the impact on the society in terms of universal accessibility, environmental sustainability and physical safety.
- In case of Data Breach, what is the Incident Response plan.
- In summary, it assesses if given system, product is in compliance with GDPR.

Why is it important?

DPIA is fundamental to shape the design of product or system. Since it can shape the design, it must be done at the beginning of the project and not at the end.

It allows the seeker to mitigate any possible Bias and discrimination caused by their system by allowing them to make better subjective choices which are concentric on Public safety, freedom and fundamental human rights. Whenever there is a high Risk to Data subject rights or discrimination against them, the Data controller must perform DPIA.

Commento: