Privacy Assessment Doneasy

Author: Marie-José Bonthuis (Privacy1)
Date: 10-10-2021
Version: draft

About Doneasy
Doneasy offers visitors in public spaces an interactive experience (using an interactive pillar) that allows the public to explore the world of NGO's and other fundraising initiatives, through engaging stories and videos. The videos are shown when a visitor appears in front of the column. Doneasy uses A.I. camera systems. Visitors are scanned during the session based on physical characteristics (height and skeletal structure) to determine whether they are a child, young person, adult or an elderly person and what their gender is. It also recognises which emotion belongs to the person (neutral, angry, happy, etc.). In the future, it may also be possible to recognise how this emotion changes during the session.

These interactive pillars encourage users to donate/purchase on the spot, by tapping or swiping their debit card directly at the terminal. The financial data processed through the payment terminal is completely separated from the data processed during the visit (e.g. gender, age group, emotion) and the processing of personal data that the visitor can leave behind through a QR code. Doneasy informs visitors by a privacy statement about these processings.

Doneasy creates interaction between content, users and donation/purchase, stimulates the audience with content that adapts accordingly. These services are based on recognition of the body/person and the moment of the donation.

Research questions
Doneasy wants to comply with the principles of the General Data Protection Regulation (GDPR) and any additional legislation regarding the use of the interactive pillars. Specifically, Doneasy requires answers to the following questions:
1. Does Doneasy process personal data?
2. Does Doneasy use profiling?
3. Does Doneasy use facial recognition?
4. Under what conditions can Doneasy share visitor data with NGOs and any third parties?
5. Are there any (different) legal aspects that apply in the UK that Doneasy should take into account if they want to offer their service in the UK?
6. Can Doneasy resell the email addresses that are processed after visitors fill them in by using the QR code to third parties?

Method
Interviews were conducted with several employees of Doneasy, addressing the above issues.

1. Does Doneasy process personal data?
To answer this question, it is important to distinguish the various processing operations:
i. the processing of data during the session, i.e. recognition of gender, age category and emotion;
ii. the processing of transaction data;
iii. the processing of data generated as a result of the QR code entered by visitors.

These three processes operate completely separate from each other.

Session data
Based on an existing algorithm, the software of the pillars can recognize a person by means of a camera/scanner and classify them into an age category (child, young person, adult or elderly). In addition, the software can recognize gender and emotions. The software also distinguishes active visitors from bystanders. It could be argued that this involves the processing of biometric data, which is designated as special personal data in the GDPR (article 9 GDPR) to which a stricter regime applies.

The “Guidelines on processing of personal data through video devices” state in recital 74:

"In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed “for the purpose of uniquely identifying a natural person”.

Recital 79 from the Guidelines says:

"However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under Article 9.”

Doneasy therefore does not process special personal data for the purpose of uniquely identifying a person. After all, they classify individuals based on categories. Since the data (gender, age category) cannot be related to the payment data nor to the data entered through the QR code, this data cannot be direct of indirectly identified to a natural person in any way.

Transaction data
The transaction data is processed by Sepay in which Doneasy does not play a role. All transactions are created between the NGO and the visitor. Even if the transactions are created between the visitor and Doneasy , therefore Doneasy does not process any transaction data of the visitors and is not able to trace visitors with this data.

Visitor data (QR code)
Through a QR code, visitors can choose to leave their data with Doneasy, to stay informed about collaborations with NGO’s. For this question it is important in which role Doneasy operates, as a processor of the NGO or as a data controller. This depends on who determines the purpose and means of the processing and how this is communicated to the visitor. It is assumed that the purpose and means are determined by Doneasy. This will need to be transparent to visitors, for example by clearly stating the name and a QR code that refers to the privacy statement.

In addition, Doneasy, in the role of data controller, offers the most marketing opportunities.

2. Profiling
If Doneasy displays certain content based on characteristics of a person this could be considered as profiling.

Article 4(4) GDPR defines profiling as follows:

"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Profiling consists of three elements:

i. it must be an automated form of processing;
ii. It must involve personal data; and
iii. the purpose of profiling must be to evaluate personal aspects relating to a natural person.

According to the Guidelines, profiling is a procedure that may involve a series of statistical inferences. Profiling is often used to make predictions about people by using data from different sources to assign characteristics to an individual based on the characteristics of others who are statistically similar. The GDPR defines profiling as “the automated processing of personal data for the purpose of evaluating personal aspects, in particular, in order to analyse or predict things about individuals.” The use of the word "evaluate" suggests that profiling involves some kind of *assessment* about an individual. A simple classification of persons based on characteristics such as age, gender and height does not necessarily lead to profiling. That depends on the purpose of that classification. For example, a company may want to categorise its customers by age or gender for statistical purposes and produce a list of its customers without making predictions or drawing conclusions about a particular person. In this case, as well as in the case of Doneasy, the aim is not to evaluate individual characteristics and therefore there is no profiling involved.

3. Face recognition vs. body detection
It has been investigated whether the software that uses an algorithm (A.I.) can be considered as any kind of face recognition. This is important in order to assess whether Doneasy needs to take into account additional conditions.

Facial recognition is a method of discovering or verifying the identity of persons by means of their face. The face of a person is analysed and converted into templates. These templates are then stored. When the same person's face appears again, the system automatically recognises it. Based on this, for example access can be granted.
Face detection is literally detecting a face. The purpose of Doneasy is in no way to identify people, for instance by recognising them when they appear in front of a column for a second time. After all, the session data is not stored. Instead, only physical characteristics of persons are detected, with the aim of classifying them in a certain age category and thus displaying certain content. No templates are captured or stored in the process. Based on this definition, it can be concluded that Doneasy does not use facial recognition, but: *body detection*.

4. Direct marketing with personal data
Assuming that Doneasy is the data controller of the data collected by the visitors through the QR code, it will have to be assessed whether Doneasy has a legitimate interest in being able to use the data for direct marketing purposes. This processing must then be included in the privacy statement on the website and those involved must be given the opportunity to opt out (unsubscribe) in every communication.

If the processing of personal data is based on a legitimate interest of Doneasy, Doneasy should weigh up its own interest against the interest of the visitor's right to privacy. The existence of a preponderance in favour of Doneasy can be demonstrated more easily when a relationship already exists between Doneasy and the data subject. For example, sending direct marketing to an existing customer and sending advertising for related products may fall under the legitimate interest, but sending an e-mail to someone who has only liked a Doneasy social media page will not.

In the second case, when there is no existing customer relationship, Doneasy must ask the visitor for consent before sending the direct marketing. This consent should be free and specific. Doneasy should therefore clearly specify what the visitor is giving consent for. The recipient of the direct marketing must also be able to withdraw his consent easily. With an e-mail, offering the option to

withdraw consent is easy. For instance, every direct marketing e-mail should contain a link that offers the recipient the option to unsubscribe from the mailing in question.

NGO's may also have a legitimate interest if they are designated as a data controller. Sharing (reselling) personal data with third parties is only possible with the active consent of the data subject. This consent can be given on the website.

5. Conditions United Kingdom
The provisions of the GDPR apply throughout Europe, the UK received an adequacy decision from the European Commission after the Brexit. This means that this country can be considered as having a comparable level of data protection. As far as direct marketing is concerned, the Dutch Telecom Act (Telecommunicatiewet) has been compared with a comparable law that applies in the U.K.

Use of electronic mail for direct marketing purposes

22.—(1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers.
(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

In the UK too, consent (opt-in) must therefore be given before direct marketing mail can be sent, unless the following exception for existing customers applies.

(3) A person may send or instigate sending of electronic mail for the purpose of direct marketing where—
(a) that a person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;
(b) direct marketing is in respect of that person's similar products and services only; and
(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

The exception for existing customers who are offered direct marketing relating to similar products or services - also applies in the UK (soft opt-in). In this case, existing customers are persons who, in the context of a selling a product or service or negotiations concerning that product or service, have provided their contact details to the sender of the marketing.

The recipient of the marketing does not have to have actually purchased something before a soft opt-in can be obtained. It is sufficient if negotiations for the sale of a product or service have taken place. This means that the recipient must have shown an active interest. This is the case, for instance, when a quotation is requested or when the potential customer asks for more details about a certain product or service. This is also different from the situation in the Netherlands. In the Netherlands, someone is only an existing customer if a product or service has been purchased by that person. There has to be a sales agreement or service agreement in which someone is or was obliged to supply something and the customer has to pay for it. The requirements to be regarded as an existing customer are therefore less strict in the UK than in the Netherlands.

The soft opt-in exception only applies to commercial marketing. Charities, political parties or other non-profit organisations cannot rely on the soft opt-in when sending marketing to existing customers. Such organisations therefore require prior consent for existing customers as well. In the Netherlands no distinction is made between idealistic, charitable and commercial purposes as far as the existing customer relationship is concerned. It is therefore important that Doneasy presents itself as a commercial organisation in the UK.

23. A person shall neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail—
(a)where the identity of the person on whose behalf the communication has been sent has been disguised or concealed; or
(b)where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided.

The sender of the marketing must not conceal or disguise his identity and must provide a valid contact address so that the recipients of the marketing may unsubscribe or opt out.

6. Other points of interest

Children's data
Children (up to the age of 16) are a vulnerable group of society and are less aware of the risks, consequences and their rights in relation to the processing of their personal data. Organisations must therefore, according to the EDPB, take specific protection measures when processing personal data of children. This specific protection must especially apply to the use of children's personal data for marketing purposes. After all, children are easy to influence with personalised advertising. Because of their age and immaturity, children may not fully understand the reasons for such marketing and the consequences it may have for them.

Considering the above, the consent of the parents of the child concerned is required before direct marketing messages may be sent.

Transparency
With regard to the use of a QR code by Doneasy, it is important that first the web address of the web page - to which one is being directed - is shown, before the link is automatically forwarded to the relevant web page. After all, one does not know what is behind it (think of phishing sites that also use these kinds of techniques). This is already shown in the QR code on most phones.

Appendix Privacy statement

Doneasy BV, located at Herengracht 136, 1015 BV, Amsterdam, is responsible for the processing of personal data as shown in this privacy statement.

Contact details:
https://www.doneasy.com
Herengracht 140, 1015 BW, Amsterdam
+31619832720

Personal data that we process

Doneasy processes your personal data because you make use of our services and/or because you provide us with this data yourself. Below you will find an overview of the personal data that we process:

- First and last name
- Telephone number
- E-mail address
- IP address

Special and/or sensitive personal data that we process

Our website and/or service does not intend to collect data on website visitors who are under the age of 16. Unless they have permission from their parents or guardian. However, we cannot verify whether a visitor is over 16. We therefore recommend that parents be involved in the online activities of their children, in order to prevent data being collected on children without parental permission. If you are convinced that we have collected personal data on a minor without such consent, please contact us at info@doneasy.com and we will delete this information.

For what purpose and on which lawful basis we process personal data

Doneasy processes your personal data for the following purposes:

- Sending you our newsletter and/or advertising folder
- To be able to call you or send you an e-mail if this is necessary to provide our services
- To inform you about changes to our services and products

Doneeasy BV processes your personal data on the following lawful bases:

- Legitimate interest: if we mail or call you for marketing purposes (only in the case of existing customers)

- Consent: if you give us permission to call or email you for informational or marketing purposes

Automated decision-making

Doneasy does not make any decisions about matters that could have (significant) consequences for people, based on automated processing. These decisions are made by computer programs or systems, without the involvement of a person (for example an employee of Doneasy).

How long we keep/store personal data
Doneasy will not keep your personal data longer than is strictly necessary to realise the goals for which your data is collected. We use the following retention periods for all categories of personal data: 1 year.

Sharing personal data with third parties
Doneasy will only provide your personal data to third parties if this is necessary for the implementation of our agreement or to comply with a statutory obligation.

Cookies, or similar techniques, which we use
Doneasy does not use cookies or similar techniques.

Access, amending or deleting data
You have the right to access, correct or erase (delete) your personal data. You also have the right to withdraw your consent for data processing or to object to the processing of your personal data by Doneasy and you have the right to data portability. This means that you can request us to send (in a computer file) the personal data that we process about you to you or another organization named by you. You can send a request for access, correction, erasure, data portability or a request to withdraw your consent or to object to the processing of your personal data to info@doneasy.com.

To make sure that the request was made by you, we ask you to send a copy of your identity document with the request. Please make sure that your passport photo, MRZ (machine readable zone), passport number and Citizen Service Number are blackened in this copy. This is to protect your privacy. We will respond to your request as soon as possible, but within four weeks at the latest. Doneasy would also like to point out that you have the possibility to lodge a complaint with the national supervisory authority, the Autoriteit Persoonsgegevens. You can do so via the following link:
https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons

How we protect personal data
Doneasy takes the protection of your data seriously and will take appropriate measures to prevent abuse, loss, unauthorized access, unwanted disclosure and unauthorized changes. If you feel that your data is not properly protected or if there are indications of abuse, please contact our customer service or send an e-mail to info@doneasy.com.