Mirror Room Clinic

What is the legal environment for the Mirror Room experiment? Is Stichting Autres Direction's legal policy in compliance with the GDPR?

Recommendations on the implementation of the GDPR's novelties

Anna Lytra
Aspasia Xirou
Eleftherios Chelioudakis
Karina Bittar Britto Arantes
Matus Mesarcik

2017

Table of Contents

Disclaimer

The following legal advice intends to adapt the Mirror Room Experience's current privacy policy to the new General Data Protection Regulation (hereinafter, GDPR). Due to administrative reasons, we could not have access to the experiment onsite beforehand, resulting in an analysis performed merely over the experiment's policy. The legal document was provided by the We Are Data team in Dutch language, non-officially and kindly translated by our colleague Maurits Jan Meeusem. Furthermore, we emphasize that the implementation of recommendations provided in this work to the Mirror Room Project does not ensure the actual compliance with the GDPR.

Introduction

"Autres Directions Foundation" (hereinafter AD), through its project "WE ARE DATA" is aiming to raise awareness regarding the intervention of technology to our private sphere. From the beginning of 2015, its traveling installation called the "Mirror Room" is moving from city to city across the Netherlands, in an attempt to make the subject of data protection and privacy tangible by confronting people with their own personal information. Through this project, AD wants to showcase the ease in which the new types of technology have the capacity to gather data about ourselves, and how far technology can penetrate to our private domain.[1]

Until the day this report was drafted (4th May 2017), over 3.400 individuals have participated to the Mirror Room experiment. Since the project was launched in 2015, the European Data Protection Law governing its functioning was the Directive 95/46/EC and the national Dutch Act which implemented it. However, as of May 2018 the new Regulation (EU) 2016/67[2] will apply, there will be a need for this project to be in compliance with the new regime. Therefore, the goal of this report is to examine what are the issues that emerge from the Mirror Room project with regard to privacy and data protection, and how these issues could be addressed under the new Regulation's requirements.

By investigating the existing privacy policy of the 'WE ARE DATA' project, we aim to underline possible faults that exist in the processing of the personal data involved and to showcase what are the steps that AD needs to take to comply with the GDPR. As a very first recommendation, we suggest that the policy should be provided in the English language also, in accordance with the aim of the experiment to gradually approach a greater public, while in compliance with the transparency of their data processing.

[1]Thomas Blom,TijlAkkermans, Hester Swaving,'The Mirror Room, Who do we see… when you look in the mirror?' (We Are Data,2015) <http://wearedata.nl/en/mirror-room/>accessed 4 May 2017.
[2]Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

Notion of personal data

The material scope of the GDPR is the processing of personal data. But what exactly qualifies as personal data and what type of data does AD process? The goal of this section is to offer clarification upon the notion of personal data and the special category of them, namely sensitive data. By virtue of the Article 4 (1) of the GDPR, personal data qualifies as "*any information relating to an identified or identifiable natural person".* Recital 26 offers further clarification to this definition, by stating that in order to determine whether a natural person is identifiable, "*account should be taken of all the means reasonably likely to be used*, *such as singling out, either by the controller or by another person to identify the natural person directly or indirectly"*. Therefore, it should be considered all objective criteria, namely the costs of and the amount of time required for identification, given the available technology at the time of the processing and technological developments.

Moreover, Recital 26 examines the notion of pseudonymous and anonymous data. Specifically, the data which have undergone *pseudonymization* "*could be attributed to a natural person by the use of additional information"*. These data are considered to be *information on an identifiable natural person* and consequently qualify as personal data, if the additional information can be accessed without disproportionate effort. Conversely, anonymous data, "*namely information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"*[3]*,* do not qualify as personal data. Therefore, truly and irreversibly anonymous data do not fall under the Data Protection regime.

The Article 29 Data Protection Working Party, with the WP 136 Opinion 4/2007[4] also cooperate with the notion of personal data. According to it, personal data are (i) any information regardless of the content (not have to concern private or family life), or

[3] *Ibid.*

[4] The Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', Analysis of the definition of Personal Data according to the Data Protection Directive [2007]WP 136.

the format / medium (video, voice recording, structured or unstructured information) (ii) relating to a data subject, (iii) who is an identified or identifiable person. The phrase "relating to the data subject" means that the information needs to be related to a living natural person (not a group) in content (regarding the data subject), in purpose (data processed with the purpose to evaluate or influence the data subject), or in result (data processing lead to an impact over the data subject).

Additionally, a person can be identified or identifiable directly, through a unique identifier such as a social number, or indirectly, through the combination of identifiers, which allows the recognition of the data subject by narrowing down the group to which the latter belongs (such as age, occupation, place of residence, etc.). The GDPR clarifies that a disproportionate effort to identify a natural person might not lead to personal data if the identification process requires unreasonable costs and time regarding the available technological resources and its development.[5] Finally, the Working Party 29 offers an additional explanation of the notion 'Identifiable'. Taking a step further from Recital 26, the Working Party 29 takes into consideration possible risks of data confidentiality and security breaches during the processing, which could ultimately lead to the identification of the data subject.

When information qualifies as personal data the GDPR sets the legal framework for its processing. However, there is a specific category of personal data for which processing is prohibited, in principle. This specific category, namely sensitive data, encompasses all "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".*[6] Such a prohibition does not apply when, amongst other occasions, the

[5]Marc Dautlich, Information should not be regarded as Personal Data if it is too burdensome to confirm its status, (Out-law.com, 2012) <http://www.out-law.com/en/articles/2012/june/information-should-not-be-regarded-as-personal-data-if-it-is-too-burdensome-to-confirm-its-status-council-of-ministers-says/>accessed 4 May 2017.
[6]GDPR (n 2) art 9(1)

data subject has given explicit consent to the processing of these personal data for one or more specific purposes.[7]

Bearing in mind the above analysis of the legal framework that governs the notion of personal data and sensitive data, the next step of our assessment is to examine what type of data the AD processes for the purposes of its project. According to the Privacy Policy of the "WE ARE DATA" project, the personal data that AD processes are the data subject's first name, age, visitor's ID, skin color, time and location, facial photograph, heartbeat, length, weight and Body Mass Index (BMI). Specifically, as regards to the last three types of data collected, the Privacy Policy refers to them as "health-related personal data"[8].

"What personal data does AD collect?
AD collects and processes, after explicit consent of the ones involved, the following (personal) data:
- Personal (First name and age)
- Participation details (i.e. time, location, visitor'sID)
- Specific personal data (skin colour, heartbeat, facial photograph)
- Health-related personal data (length, weight, BMI)
The specific personal data and health-related personal data will be collected and processed
through use of the following measuring devices and programming:
- Body weight scale (Weight in KG)
- Camera 3d image - Kinect (Length, posture and position)
- Camera's - optical sensors (FaceReader, FacePiRes, FaceSwap)
An info-profile is created based on the participant's (personal) data".

Current Policy and Recommendations

As a first observation, the AD does not include into the abovementioned list all the personal data that it processes. One example is the gender of the data subject, which is one of the basic personal details which are being processed during the Mirror Room session. The profile report of AD includes in its results the gender of the data subject, so this information shall also be included in their data processing list, as the

[7] *Ibid*, art 9(2a)
[8] AD Privacy policy (Non-official translation).

gender is an information which, aligned with other data, *indirectly* contributes to make the data subject *identifiable*[9]. Therefore, we recommend reconsidering the listing of the referenced clause, in respect to the transparency principle provide for article 5 (1) of the GDPR, which will further be developed in this report. Furthermore, the negligent or intentional infringement of the GDPR principles and provisions triggers the application of fines and penalties, according to the GDPR's article 83 (3).

Regarding the processing of personal data, there are four categories which can be collected, namely provided data, observed data, derived data and inferred data.[10] This categorization of data in not provided by law, but it is still relevantly linked to the Mirror Room's setting, operation and aim to raise awareness over individuals' '*datalization*'. Examples of personal data that can be observed are the data generated by sensors or passively created by cameras.[11] In the AD's profile reports, there are information described as the "Fear Factor" and the "Prejudice Factor".

Under the first cluster there is data which indicates what the data subject is most afraid of, and under the second cluster there is information that showcases what race the data subject consider as the most threatening one. Such data derives from some scenarios that the data subject is submitted to during the Mirror Room session, but are not considered to be personal data according to the Privacy Policy of the AD. However, this observed data could qualify as personal data since it is information related to a data subject (personal fears and prejudices) which can corroborate with one's identifiability when linked to the rest of the personal data processed.

Moreover, another observation to be pointed out is that AD does not define heartbeat and facial pictures as health-related data. Having in mind the definition of the special category of personal data above, it could be concluded that both the heartbeat and the facial photograph qualify as data concerning health. Specifically,

[9] GDPR (n 2) art 4 (1).
[10] Carl Kalapesi, Rethinking Personal Data: Strengthening Trust, World Economic Forum, (Weforum.org, 2012), <http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf> accessed 4 May 2017.
[11] Ronald Leenes, Accountability and transparency in Big Data land, DSC/t Blog, (Tilburguniversity.edu, 2016), <https://www.tilburguniversity.edu/research/institutes-and-research-groups/data-science-center/blogs/data-sience-blog-ronald-leenes/> accessed 4 May 2017.

since the data subjects are submitted to stressful conditions during the Mirror Room experience, the variations to their heartbeat, both at normal and stressful conditions, can reveal their risk of suffering a heart attack in the future (data concerning physical health),[12] or their capacity to control their fears and remain composed under stressful incidents (data concerning mental health).

In addition, the facial picture of the data subjects can reveal important sensitive information regarding their health status. Specifically, diseases such as Periorbital Cellulitis, Cyanosis, and Cervical Adenopathy, or genetic disorders such as the Down syndrome, the Pierre Robin Sequence or the Moebius syndrome can be detected through facial pictures (bones structure, skin appearance, deformities, etc.). Combining this potential discrimination risk with the increasing interest over the last years in the application of machine learning to clinical informatics and healthcare systems, machine vision algorithms could be used to observe health symptoms which could negatively affect the data subjects.[13] Thus, both categories of data shall be treated as health-related data, and consequently sensitive data.

Therefore, we consider that, in respect to the guiding principles for processing data – fairness and transparency - one important improvement to be performed in the revised privacy policy of AD is to clearly provide data subjects with all the different types of the data that are being processed, both directly or indirectly: which personal data are being processed, where are they derived from and the means used process them are questions that demand clear answers and should be embedded to AD's policy.

Personal scope: Controller and Processors

[12] Paula Johnson , What your heart rate is telling you, Harvard Health Publications, Harvard Medical School, 2015, <http://www.health.harvard.edu/heart-health/what-your-heart-rate-is-telling-you>, accessed 4 May 2017.
[13] Kuan Wang and Jiebo Luo, Detecting Visually Observable Disease Symptoms from Faces, Springer Online, 2016, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5007273/> accessed 4 May 2017.

"Processors
AD ***might hire private contractors to have them take over part of the process, on behalf of a contractual obligation****. AD will ensure confidential and careful conduct with the personal data through contractual clauses, in so called '****processors contracts'.****"*

The concepts of controller and processor governed by the currently applicable data protection Directive and GDPR are very similar in their definitions. Controller is defined "as natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[14] On the other hand, processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." [15] Therefore, the relationship between the key actors of the data processing results from a supervisory relation of association and legal dependency.[16]

What shall be noted towards the relationship between controller and processor is that GDPR contains certain shift in the areas of security and responsibility. Unlike the current data protection law, the processor *jointly* with the controller shall implement appropriate safeguards to ensure an adequate level of security.[17] Hence, if the data subject suffers damages, he/she can claim compensation either from the controller or the processor.[18]

Recommendations

According to the legislative framework the controller shall bear in mind the following steps:

1. <u>Due diligence while searching for processors</u>

[14] GDPR (n 2) art 4 (7).
[15] *Ibid*, art 4 (8).
[16] The Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"'[2010] WP169.
[17] GDPR (n2) art 32.
[18] *Ibid,* art. 81.

The GDPR requires from controller **and processors** to have specific security safeguards in place when conducting processing of personal data. Therefore, the AD should carefully check beforehand if their potential processors are also capable of fulfilling the GDPR's requirements for security before contracting with them.

2. Conclusion of the contract

Initially, it must be clear from the contract that the controller determines the purpose of the processing, but the means may be left to the processors. GDPR requires that the pertinent relationship shall be governed by contract.[19] The legislation also provides guidance with regard to the content of such contract.[20] According to the nature of the Mirror Room we emphasize the need for careful drafting the clauses in connection with having sufficient security measures at place and division of responsibilities in case of data breach. The detailed procedure should be addressed encompassing the details, like providing notices to parties involved, time of reaction, measures taken immediately after the data breach etc.

3. Transparency & Data flow

Another issue that has to be taken into account when it comes to the relationship among the AD and its processors is fostering transparency. This is relevant especially in case of the software used for collecting the data. It should be clear if the software is provided by the Mirror Room team or third parties. If the latter is the case, it means that the data is accessed by a third party, since it is processed by them. AD then should consider having appropriate safeguards and transparent communication to their public about the layered processing. Details of the processing phases should be clearly addressed in the privacy policy.

4. Reaction & Aftercare

[19] *Ibid*, art. 28 (3).
[20] *Ibid.*

During the contractual relationship, the AD and processors shall keep their records and documents relating to the data processing activities. The latter shall reflect the principles of transparency and accountability. Efficiently drafted clause in the contract also governs appropriate reactions to sensitive situations that can occur during the processing of personal data.

Legal Ground

Chapter II of the GDPR provides for the legal grounds for lawful processing of general personal data and the guiding principles. The recently released provision underlines the lawfulness for processing the special categories of personal data, which are subjected to a stricter regime. The lawful processing of non-sensitive personal data is grounded on the individual's consent, the protection of one's vital interest, the performance of a contract or of a task carried out in the public interest and the legitimate interest of the controller or third parties.[21] Since the Mirror Room experience indicates the processing of both non-sensitive and sensitive (health) data, the adoption of the more rigorous regime should prevail in analogy to the specialty principle (*lex specialis derogate legi generali*).

The processing of sensitive data is, *a priori*, not allowed.[22] However, exemptions are provided for in order to make the processing of health data legitimate. Unlike the processing of non-sensitive data, the processing of sensitive data cannot rely on a general contractual relationship, unless there is a clear and explicit individual's request to a service or a product in which the revealing of sensitive data are embedded.[23] Consequentially, only explicit consent, vital interest of the data subject, public interest and legitimate activities (e.g. employment, social security) are held as a lawful processing basis for sensitive data.[24] The GDPR also provides for a special case where an implicit consent is also acknowledged as a legal ground for processing:

[21] *Ibid*, art 6.
[22] *Ibid,* art 9.
[23] Handbook On European Data Protection Law (1st edn, Publ Office of the European Union [ua] 2014).
[24] GDPR (n 2) art 9 (2).

when the data is manifestly made public by the data subject, the permission to use it is presumed.[25]

"What personal data does the Autres Directions Foundation collect?
The Autres Directions Foundation collects and processes, ***only after express consent*** *of the person concerned, the following (personal) data:*
- *Personal (first name and age only)*
- *Participation details (e.g., time, location and visitors' ID)*
- *Special personal information (skin colour, heart rate, photo face)*
- *Health data (length, weight, BMI)".*[26]

AD relies on the legal ground 'consent' for the processing of personal data during the Mirror Room experience, as stated in their privacy policy. According to the DPD, consent is a legitimate ground to process personal data if it is specific, informed and freely given by the data subject.[27] However, the GDPR has enhanced the requirements for obtaining data subjects' consent, by additionally establishing the need for an 'unambiguous indication' of the individual's wish, provided through a 'statement or by a clear affirmative action'.[28]

The unambiguous indication of one's wish to give consent should be preceded by an explanation of the project in a clear, accessible and objective manner, at the time of the data collection. Additionally, it should clarify the aims and purposes of the project, as the agreement indication should ensure that no doubts have remained regarding the purposes of data processing. In case of multiple or further processing for scientific purposes, the data subject is allowed to give consent only to some of them.[29]

The second novelty concerning the consent is the positive indication of the consent by a clear affirmative action, avoiding the consent-collecting techniques, such as the

[25] *Ibid*.
[26] AD Privacy policy (Non-official translation).
[27] GDPR (n 2) art 4; art 11.
[28] *Ibid*.
[29] *Ibid*, Recital 33.

pre-ticketed opt-in boxes.[30] Recital 32 provides for both oral and written statements and outlines that implied consent, such as in case of silence, pre-ticked boxes or inactivity, should not constitute consent. Moreover, the affirmative indication of the data subject must encompass all the purposes for the processing, turning the transparency in the informational responsibility of the controller even more relevant.[31] It is important to stress that the requirements of informed, specific and freely given consent remain effective in the GDPR and will be covered by the principle analysis ('lawfulness') section.

Current Policy and Recommendations

Regarding the abovementioned novelties settled by the GDPR, the current privacy policy complies to the requirement of express consent of the data subject to process sensitive data, data sharing, encryption and minor's consent but remains unclear how the information is provided onsite and, consequently, whether the consent is sufficiently informed, freely given and unambiguous. Moreover, according to testimonials we had access to, the only occasion which there is an active affirmative (regarding lay people) of the data subject during the experiment is to allow or not the publication of the info profile at the 'we are website' (even though we understand that entering the mirror room is by itself a consent). For this reason, we would recommend a more detailed policy, which can be presented to the data subject in a clear, objective and accessible language.

For instance, we suggest the use of electronic means[32] (e.g. interactive displays outside the room, tablets), with a multi-language menu, consistent explanation about the extent of the consent and an outline of the most relevant parts of the privacy policy. We believe that a data subject interaction with the privacy policy provided through resources before entering the room could result in a clearer consent acknowledge.

[30] Paul de Hert and Vagelis Papakonstantinou, The New General Data Protection Regulation: Still A Sound System For The Protection Of Individuals? (1st edn, Elsevier 2016) <http://www.sciencedirect.com>
[31] GDPR (n 2) Recital 32.
[32] *Ibid.*

Finally, another issue to be considered regarding the legitimacy of the consent is the target public of the Mirror Room, as well as their legal capacity to give consent. Through its travelling installation, the experience is known to be constantly held during music festivals, where participants make use of alcohol and intoxicating substances. Our recommendation is that the Mirror Room Experience should avoid places where alcohol and drug consumption might be an obstacle to legitimate consent.

Principles

The EU General Data Protection Regulation (GDPR) is underpinned by a number of data protection principles related to the processing of personal data which drive compliance, as following:[33]

Lawfulness, fairness and transparency Rec.39; Art.5(1)(a)	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation Rec.50; Art.5(1)(b)	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimization Rec.39; Art.5(1)(c)	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy Rec.39; Art.5(1)(d)	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation Rec.39; Art.5(1)(e)	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality Rec.29, 71, 156; Art.5(1)(f), 24(1), 25(1)-(2), 28, 39, 32	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
Accountability Rec.85; Art.5(2)	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR[34]

[33] *Ibid*, art 5.
[34] *Ibid*, Recital 26.

Principle of Lawfulness

The principle of lawfulness mentions that "any processing of personal data should be lawful".[35] Particularly, Recital 40 and Article 6 of the GDPR proclaim explicitly that in order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject or other legitimate grounds for one or more specific purposes.

It is of the essence to examine the particularities of the consent as a legal ground used in the Privacy Policy. Initially, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.[36] Especially, in the case of sensitive data, such consent must be explicit,[37] and pertaining to one or more specified purposes of processing.

The data subject should be aware at least of the identity of the controller and the purposes of the processing of his personal data before gives the consent.[38] As stated before, the GDPR clarifies that, whenever the consent of the individual is mandatory for the processing of personal data,[39] it has to be "any freely given, specific, informed and unambiguous indication of his or her wishes. Precisely, the data subject, either by a statement or by a clear affirmative action (e.g. a person entering the Mirror Room), can agree to the processing of the personal data.[40]

Moreover, a declaration of consent pre-formulated by the controller should be presented in an intelligible and easily accessible form, using clear and plain language, without containing unfair terms.[41] In even more detail, if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.[42] Lastly, consent will not be presumed freely given when the data subject

[35] *Ibid,* art 5 (1); Recital 39.
[36] *Ibid*, art 7 (1); Recital 42.
[37] *Ibid*.
[38] *Ibid*, Recital 42.
[39] Lawrence Ryz and Lauren Grest, 'A New Era In Data Protection' Computer Fraud & Security (2016).
[40] Paul de Hert and Vagelis Papakonstantinou, (n 30).
[41] Council Directive 93/13/EEC on unfair terms in consumer contracts (1993) L95/29 .
[42] GDPR (n2) Recital 32.

has not a genuine or free choice or is unable to refuse or withdraw consent without detriment.[43]

"What personal date does AD collect?
AD collects and processes, after explicit consent of the ones involved, the following (personal) data:
- Personalia (First name and age)
- Participation details (i.e. time, location, visitorsID)
- Specific personal data (skin color, hartbeat, facial photograph)
- Health-related personal data (length, weight, BMI)
The specific personal data and health-related personal data will be collected and processed
through use of the following measuring devices and programming:
- Body weight scale (Weight in KG)
- Camera 3d image - Kinect (Length, posture and position)
- Camera's - optical sensors (FaceReader, FacePiRes, FaceSwap)
An info-profile is created based on the participant's (personal) data."

Pursuant to the privacy policy of the experiment, it is only briefly mentioned that they collect and process (sensitive) personal data, after explicit consent of the ones involved. Moreover, they clarify that in order to participate at the Mirror Room project, the data subject must be 16 years old (the minimum age) or has explicit consent from parent or lawful guardian.[44] Furthermore, at their privacy notice, it is mentioned only how the participants can contact the AD, without any specific detail for their identity. Therefore, as regards the principle of lawfulness, we consider that the AD's privacy policy is vague.

Notwithstanding, as we have mentioned before, it is good that it has systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity, if the participant is under 16 years old. Further, AD should keep in mind that consent should be verifiable.

[43] *Ibid,* Recital 42.
[44] AD Privacy policy (Non-official translation).

In particular, the GDPR imposes onerous requirements on consent[45], which the AD should include in its policy in order to be in full compliance with the Regulation. The AD also, as the controller, should keep records, so they can demonstrate that consent has been given by the relevant individual.[46] The AD should specify in its privacy policy the characteristics of a lawful consent, namely:

Main characteristics of consent
-Explicit -Plain language
-Affirmative action -Consent to all purposes of processing[47]
-No power imbalance: consent is not be legal if there is a clear imbalance of power between the individual and the controller[48]
-No power imbalance: consent is not be legal if there is a clear imbalance of power between the individual and the controller[49]
-Unbundled consent (when different processing activities are taking place)
-Withdrawable; establishment of process to manage requests to withdraw consent[50]
-Additional protection for children[51]; clear privacy policies if they are aimed at children
-Where consent has been given under the Data Protection Directive, it will continue to be valid under the Regulation if it meets the aforementioned conditions of the Regulation[52]. If not, AD may contact previous participants to obtain a fresh consent that is valid under the GDPR[53].

Principle of Fairness and Transparency

[45] Tanguy Van Overstraeten, *The General Data Protection Regulation A Survival Guide* (1st edn, 2017) <http://file:///C:/Users/user/Downloads/TMT_DATA_Protection_Survival_Guide_Singles.pdf> accessed 4 May 2017.
[46] *Ibid.*
[47] GDPR (n2) Recital 43.
[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*
[51] *Ibid*, Recital 58.
[52] *Ibid*, Recital 171.
[53] *Ibid* (n45)

Personal data shall be processed fairly and in a transparent manner in relation to the data subject.[54] Specifically, the principle of fair processing means transparency of processing, particularly vis-a-vis individual (a data subject).[55] Subsequently, under the transparency principle the controller is obliged to keep the data subjects informed about how their data are being used.[56]

Precisely, the principles of fair and transparent processing require that the data subject has to be informed of the existence of the processing operation and its purposes, the existence of profiling, about the identity and address of the controller[57] as well as any further necessary information.[58] In other words, the data subject should understand easily that personal data concerning him/her are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.[59]

It is also important to mention that "where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing".[60]

"AD processes personal data for the WE ARE DATA project. In this Privacy Statement AD will inform you about who we are, to what ends we store your data, how you will be able to enforce your privacy rights and other possibly relevant information. This PS is applicable to the WE ARE DATA - Mirror Room and the participants' profiles that subsequently follow. AD strives to take proper care of personal data and aspires to act within the confines of the law personal data protection and the law on telecommunication."

[54] *Ibid.*
[55] *Ibid,* (n23)
[56] *Ibid.*
[57] *Ibid.*
[58] GDPR (n2) Recital 60.
[59] *Ibid*, Recital 39.
[60] *Ibid*

As regards AD' s privacy policy, it is stated who AD-Mirror Room is/are, how it/they store data, how they are able to enforce privacy rights and other possibly relevant information.

Current Policy and Recommendations

In this respect, we consider the privacy policy is vague, without providing many details, so it is not easily understandable as it should be. For instance, in the privacy policy, the 'controller part' is not explained in detail and in Dutch language, as stated before. Thus, non-Dutch cannot understand easily who exactly is the controller behind that project (e.g professionals or companies), so people have to search in AD's website for more information, where an English translation is provided.

Even more, at the entrance door in the Mirror Room, it is written *"Please enter the Mirror Room and experience how it feels to 'become data'. Do you want to share your information or do we reveal too much? Enter at your own risk".* This is not definitely in compliance with the GDPR transparency principle since natural persons should be aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to such processing,[61] even though we realize it is a marketing strategy to attract visitors. Therefore, processing operations must not be performed in secret and should not have unforeseeable negative effects.

The GDPR requires more extensive information to be provided than the Data Protection Directive.[62] According with the transparency principle, AD should provide information notices, to ensure transparency of processing, addressed to the public or to the data subject, which has to be concise, easily accessible and easy to understand (e. in English language), with clear and plain language. The AD should communicate their privacy notice and they should upload it on their website, so stakeholders can be informed easily. Additionally, visualization – at least in Dutch

[61] *Ibid*, Recital 39.
[62] Karin Tien, The Data Protection Principles UnderThe General Data Protection Regulation' (*Taylorwessing.com*, 2017)<https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html> accessed 28 April 2017.

and English language- can be used when addressed to the public[63], through an accessible onsite digital mean (e.g., a tablet), so it may give a meaningful overview of the intended processing.[64]

Furthermore, since the Mirror Room is possible to attract children/young adults, they should include at their privacy policy clear and plain language for children, so they can easily understand the processing of their personal data.[65] Lastly, it is significant to underline that in order to enhance transparency and compliance with the GDPR, the establishment of certification mechanisms and data protection seals and marks shall be considered by the AD-Mirror Room in a dialogue with a respective authority, allowing data subjects to quickly assess the level of data protection of relevant products and services.[66]

The principle of purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[67] The purpose of processing data must be visibly defined before processing is started since processing for undefined purposes is not in compliance with EU data protection law.[68] In particular, the purpose of processing must be explicitly specified as well as made manifest by the controller.[69]

Moreover, the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.[70] Besides, there is a non-exhaustive list of factors –in the GDPR- when

[63] GDPR (n2) Recital 58.
[64] *Ibid*, Recital 60.
[65] *Ibid*, Recital 58.
[66] *Ibid*, Recital 100.
[67] *Ibid*, art 5.
[68] *(n23).*
[69] *Ibid.*
[70] GDPR (n2) Recital 50.

assessing whether the processing of data for a new purpose is incompatible with the purposes for which the data were initially collected.[71]

Additionally, during the aforementioned assessment, the controller should take into account "any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations".[72] Subsequently, further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original processing purposes.[73]

"To what end does AD process your personal data?
AD collects and processes personal data for the following goals:
- Making the Mirror Room available
- Build a participation database, as to aid the Mirror room
- To create a (participant)info-profile, based on the collected data
- To compare (personal) data and info-profiles of participants with other participants
- To improve the system at hand, the so-called Mirror Room."

According to the Privacy Policy, the AD processes personal data for several purposes:

-Making the Mirror Room available
-Build a participation database, as to aid the Mirror room
-Creation of a (participant)info-profile, based on the collected data
-Comparison of (personal) data and info-profiles of participants with other participants
-Improvement of the system at hand, the so-called Mirror Room

[71] *Ibid*, art 6 (4).
[72] *Ibid.*
[73] *Ibid*, art 5.

Current Policy and Recommendations

The aforementioned purposes are not specified and explicit, but vague. For instance, it is indicated that the collection of the personal data will be held for the operation of the Mirror Room; but what is the specific purpose of Mirror Room's operation? Stating that it aims to raise awareness over 'datalization' of people is not enough under the light of the GDPR as the latter is broad and not explained in much detail. Moreover, questions encompassing how much data are needed in order for the Mirror Room to be available, what is the reason for comparing the gathered data, or how you improve the Mirror Room by collecting all this sensitive data can also be raised.

For instance, in Israel, the creation of biometric database (including high-res facial photos and two index fingers) was planned for preventing the forging of ID cards and passports, prohibiting anyone from assuming a false identity by replacing the documents with a biometric one using data from the aforementioned database.[74] Another example is the Guardian, a new airport security platform which compares millions of images per second, helping to identify travelers in areas with high foot traffic and supplements the identification process for border control agents.[75] The aforementioned examples illustrate that the processing of sensitive data is important for safety reasons like protect citizens from a terrorist attack. With the operation of the Mirror Room, the participants understand how easily they can become data and how "technology can and will make (them) transparent", but is this a legitimate reason for collecting all this sensitive data and compare info-profiles of participants?

Under the GDPR, the purpose limitation is crucial, so the AD should specify further their purposes or link them with an additional -more significant- purpose (e.g.

[74]'Ilan Lior , 'All Israelis Will Have To Join Biometric Database From Next Year, Minister Says' (*haaretz.com*, 2017) <http://www.haaretz.com/israel-news/1.728256> accessed 26 April 2017.

[75]Jesse Davis, 'New Airport Security Face Recognition Platform Helps Safeguard Borders' (*Benzinga*, 2017). <https://www.benzinga.com/pressreleases/17/04/p9333392/facefirsts-new-airport-security-face-recognition-platform-helps-safegua> accessed 26 April 2017.

research purpose) than the operation of the Mirror room. It is also of the essence that the stated purpose reflects the practice of the AD.

Data minimization

Pursuant to the principle data minimization[76], personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed. Therefore, the controller should adopt internal policies and implement measures of minimizing the processing of personal data.[77] It is a general principle and should be present in all the stages of data collection.[78]

At AD's Privacy Policy, it is not mentioned any adopted measure to comply with the principle of data minimization.

Current Policy and Recommendations

Due to the fact that the AD's privacy policy is vague pertaining the purpose of processing, it is not clear if the data minimization is implemented properly. AD' s privacy notice should give the essence that they apply the principle of the data minimization, by processing personal data that are strictly limited to what is necessary for their relevant purpose.[79] Thus, AD should rethink to minimize the collection of personal identifiable information. For instance, AD should explain how exactly contributes to achieve their purposes either the collection of the photo or other sensitive personal data of the participants or their publication or saving health data for a maximum of 2 years. Further, AD may consider from the beginning of the data processing to anonymize/pseudonymize data or restrict uses of information to those that are acceptable from not only a personal, but also a societal point of view

[76]GDPR (n2) art 5 (1c).
[77]*Ibid*, Recital 78.
[78]Robert Thorburn, Sophie Stalla-Bourdillon and Eleonora Rosati, 'Iclic Data Mining And Data Sharing Workshop: The Present And Future Of Data Mining And Data Sharing In The EU', Computer Law & Security Review (2017).
[79]Christopher Kuner, '*European data protection law: corporate compliance and regulation',* ed. edn, Oxford University Press, Oxford [2007].

especially from the aspect that data processing may give a rise to concerns in connection with discrimination, lack of choice and democratic speech by putting individuals into predetermined categories.[80]

Principle of Accuracy

The accuracy principle stands for the maintenance of the personal data up to date where necessary and accurate, regarding the data processing purposes.[81] It is not a new requirement for data processing in relation to the Directive as the new provision only included the obligation to erase or rectify the data *without delay.*[82] The accuracy principle is one of the pillars of the 'Data Quality Principle' and it can be profoundly relevant when the data concerned in the process is related to health data and is potentially risky to the data subject (e.g. an allergy, blood type). In this sense, the quality of the data is directly related to its reliability. Therefore, the assessment of the purpose to which the data is being processed is directly linked to the relevance of its accuracy. Moreover, Recital 39 of GDPR provides for that 'every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted',[83] posing an inferred obligation to the data controller.

"It is your own responsibility to ensure correctness of your personal data, as well as to ensure that they are up to date*. SAD is, except in cases of premeditation or negligent behaviour, not liable for factual errors or activities arising from your incorrect or outdated information.*

Insight and correction

You can ask AD for an insight- or correction request*. You are advised to clearly indicate that you are requesting an insight- or correction request based on art. 35*

[80]Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics,* 11 Nw. J. Tech. &Intell. Prop. 239 (2013).
[81]GDPR (n2) art. 1; art 5 (d).
[82]*Ibid.*
[83]GDPR, Recital 39.

law on personal data protection. Keep in mind that it might be necessary to share a copy of your personal ID to check personal identity. The email can be found above".[84]

Regarding the compliance to the accuracy principle, AD adopts, analogically to regular contracts, a hold harmless clause, relieving its responsibility over all possible damage derived from incorrected or outdated information. It also provides individuals with an access channel to require the correction or updating of data, in compliance with the right to rectification, which have maintained similar provision under the Directive and the GDPR.[85] The privacy policy does not explicitly mention which safeguards are to be put in place in order to ensure the correctness of the personal data collected, shifting the 'burden' to the data subject.

Current policy and Recommendations

First and foremost, it is necessary to consider the purpose of the data processing to assess the need to a strict policy regarding the accuracy of the data collected. According to AD's policy, the personal data is collected to create a participation info-profile database and compare to other participants with the aim to make the experience available and improve its system.[86]In the website of the experiment (www.wearedata.nl), the purpose is presented as a tool to raise awareness regarding privacy and data protection in the era of big data and social networks.[87] Solely the purpose of creating consciousness on one's daily data generation does not require for a rigorous policy of data accuracy and, therefore, the current policy would be in compliance with the GDPR by offering a direct communication channel with the data subjects. The picture changes if the data collected will be furthered processed without being anonymized which, according to the policy, is not the case ('the data sent to our partners will only be transmitted after name and pictures have been removed').[88]

[84]AD Privacy policy (Non-official translation).
[85]GDPR (n2) art. 16.
[86]*Ibid*, art 16.
[87]Thomas Blom,TijlAkkermans, Hester Swaving (n1).
[88]AD Privacy policy (Non-official translation).

According to some experimental results accessed by our team, participants' personal data were said to be inaccurate in relation to age range and weight. Whether those data were provided or inferred, the interpretation can be performed as following: participants did not want to provide their real personal data or the algorithms and tools used to infer the individual's data is lacking correctness. In either way, our recommendation is that the false data provided by a participant and the wrong inferred data can be also used to leverage the discussion over algorithms' flaws and discrimination. Lastly, we would recommend an additional step to the experiment: the manual cross-checking of the accuracy of the data processed by the Mirror Room's machines. It would not just enhance quality and reliability of the data processed, but would also help in the sharpening of the algorithms and machine learning.

Storage Limitation Principle

This principle establishes that personal data should be maintained during the minimum period necessary to accomplish the purpose to which it was collected for, or for longer periods when safeguard measures are ensured.[89] In order to assure the compliance to the storage limitation principle, the controller should make periodical reviews over the data stored and the purpose it serves and erase it when assessed that the data is no longer necessary in the fulfillment of its purpose collection.[90] The principle does not bring innovation in relation to the Directive provision, but should be read in the light of the new 'right to be forgotten' or simply right to erasure. The provision grants individuals the right to have their personal data deleted when met the conditions are met, namely processing is no longer necessary, the data subject have withdrawn his/her consent or has objected the processing, amongst others.[91] It is important to highlight that the right to objection and erasure should not conflict

[89] GDPR (n2) art. 5 (e).
[90] *Ibid*, Recital 39.
[91] *Ibid*, art. 17.

with the controllers' legitimate grounds for processing such as freedom of expression, public interest, etc.[92]

> ***"Data conservation***
> *AD reserves the right to save and conserve the personal data as long as the project is running,* ***with a maximum of two years****. After these two years, anonymised info-profiles*
> *remain available for scientific purposes.*
> ***Resistance***
> *You can resist/complain about the use of your personal data for* ***commercial purposes****. When you claim (through any means of contact) that you do not want to be contacted anymore, we will save the required data in a file specifically for this purpose and your other personal data will no longer be used for these purposes."*

AD privacy policy provides for a maximum retention period of two years, without providing the data subject with a reasonable justification for keeping the data in the period. Recital 39 sets that personal data should be limited to a 'strict minimum' and, for this reason, we do not agree that there is a legal compliance regarding the retention clause. Furthermore, the policy solely recognizes the right to erasure in relation to the use of the data for commercial purpose, limiting the application and effectiveness of the data subject's right.

Current policy and Recommendations

The privacy policy clearly requires some adaption regarding the storage limitation principle. First, we suggest a revision of the data retention clause by changing the data detainment period or by detailing the legal justification and purpose to maintain the personal data for the period of two years. Second, the policy should be adapted to the new 'right to be forgotten' introduced by the GDPR by replacing the 'Resistance' clause to a broader one, in compliance with the article 17.

Integrity and Confidentiality Principles

[92] *Ibid*, art. 17 (3).

The Integrity and Confidentiality principle comprises the obligation that the controllers must ensure that security measures are in place to protect the personal data from intern and extern unlawful access, accidental loss, destruction or damage.[93] In the same way a store uses security measures to safeguard its physical inventory (security guards, alarms, restricted electronic access), a controller need to adopt security mechanism to avoid the loss or theft of the personal data administered by it.

"Confidentiality and security

*AD will take **suitable technical and organizational measures** to secure personal data from unauthorized access. The data in the online database **will be stored in an encrypted fashion**. The data in the installation itself (MR) will be encrypted as well. The installation itself will be closed off using a steel lock with Lock-box."*

The current privacy policy provides for security mechanisms to ensure the integrity and confidentiality of the personal data stores. The encryption technique is considered to be an efficient manner to ensure confidentiality by obstructing the content access from unauthorized third parties and it is largely used. In addition, the security measures taken to protect the mirror installation itself also cooperate to the compliance with the principle.

Current policy and Recommendations

Our recommendation to this principle regards the private parties (processor) AD contracts to take over part of the data processing, on behalf of contractual obligation. Unlike the Directive, the GDPR has brought a better balance regarding the responsibility over the burden to ensure technical measures which safeguard the personal data. According to article 32, 'the controller **and the processor** shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (bolded emphasis added)'.[94] In the same fashion is

[93] *Ibid*, art.5 (f).
[94] *Ibid*, art 32.

the right to compensation and liability.[95] Therefore, we recommend a processor contractual revision following the steps provided in "Personal scope" part of the report.

Principle of accountability

According to the new accountability principle[96]of GDPR, the controller shall be responsible for, and be able to demonstrate compliance with the data protection principles (the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality). This new EU legal-regulatory regime is strongly supported by stricter accountability of those who are responsible for personal data.[97]

Giovanni Buttarelli, the European Data Protection Supervisor[98] underlined that "the accountability principle helps in moving data protection from theory to practice".[99] This principle imposes an increased compliance burden and implies "a cultural change which endorses transparent data protection, privacy policies and user control, internal clarity and procedures for operationalizing privacy and high level demonstrable responsibility to external stakeholders and Data Protection Authorities".[100]

Additionally, the accountability measures comprise of strong technical and organizational measures in order to ensure and demonstrate compliance, namely appropriate data protection policies, data protection through privacy by design and by default, IT security risk management, data breach notifications, data protection

[95] *Ibid*, art 82: *'Any person who has suffered material and non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'.*

[96] *Ibid,* art. 5 (2).

[97] Gumzej, Nina. "Data protection for the digital age: comprehensive effects of the evolving law of accountability." *Tribuna Juridică* 4 (2012): 82-108.

[98] The European Data Protection Supervisor (EDPS)

[99] Giovanni Buttarelli, The accountability principle in the new GDPR (2017) <https://edps.europa.eu/sites/edp/files/publication/16-09-30_accountability_speech_en.pdf> accessed 28 April 2017.

[100] Sebastian le Cat, 'GDPR Top Ten: #2 Accountability Principle | Privacy | Deloitte' (*Deloitte Nederland*, 2017) <https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-2-accountability-principle.html> accessed 4 May 2017.

impact assessments (DPIA), prior consultations and Data Protection Officers, records of processing activities, code of conducts and self-certification.[101]

Pursuant to GDPR, it is significant to establish transparent internal data protection and privacy policies, as well as effective internal processes and tools to implement these policies.[102] As an illustration, the controllers' obligation to notify all personal data processing operations taking place in the EU to their competent local supervisory authorities[103] will be replaced by the principle of accountability with regard to the controller.[104] This means that controllers have to maintain an internal record of processing activities under their responsibility.[105]This record will contain controller' s name and contact details, purposes of the processing, description of the categories of data subjects and of the categories of personal data, retention periods, general description of the security measures employed, etc.[106]

Furthermore, guidance on the demonstration of compliance by the controller[107] could be provided by approved codes of conduct, approved certifications.[108] These codes of conduct may calibrate the obligations of controllers[109] and provide assistance to small companies while applying the Regulation.[110]

AD's Privacy Policy does refer to any measure adopted to be incompliance with the new principle of accountability. Besides, it is not compliant even with the Directive 1995, since it does not provide any reference to the previous obligation to notify all personal data processing operation taking place in the EU for the competent DPA's (Articles 18 and 19, Directive 1995)

Current Policy and Recommendations

[101] Giovanni Buttarelli (n99)
[102] *Ibid.*
[103] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995), art 18; art 19.
[104] Paul de Hert and VagelisPapakonstantinou, (n30)
[105] GDPR (n2) art 30.
[106] *Ibid*, art 30 (1).
[107] *Ibid*, art 24; art 40.
[108] *Ibid*, Recital 77.
[109] *Ibid*, Recital 98
[110] Paul de Hert and VagelisPapakonstantinou, (n30).

The AD, through its privacy notice, do not adhere properly the principles of the GDPR and do not demonstrate that is in compliance with these principles. For instance, in their privacy policy, it is not mentioned that AD keep either internal records of data processing or approved codes of conduct. Therefore, the AD should make sure that these principles are adhered to by setting the internal records structure correctly and comprehensively.[111] In addition, the AD has not developed a breach reposting mechanism, so they should create one. AD should maintain an internal breach register[112] and report personal data breaches to their supervisory authority and as well as to the data subject.[113]

In line with the aforementioned, in order to guarantee compliance with the GDPR, AD should update or create suitable policies that clarify how they process personal data. Moreover, they should think other compliance measures, like creating a clear compliance structure and allocating responsibility for compliance. Additional technical measures could be applied such as minimizing processing of personal data, pseudonymization, as well as providing participants with greater control and visibility and implementing suitable security measures.[114] AD should also inform and train their partners on how to apply these policies related to accountability principle.[115] Lastly, AD should communicate to external stakeholders and supervisory authorities the quality of the implementation of these measures.[116]

Furthermore, the Privacy Policy does not mention accountability of the processors. Hence, AD may include at their notice that each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller.[117]

In the context of accountability principle, AD should adopt appropriate measures to comply with the personal data breaches which constitute a new security breach communication law for all data controllers regardless of their sector.[118] Specifically, AD should ensure that it has adopted proper procedures to detect, report and

[111] Sebastian le Cat, (100).
[112] GDPR (n2) Recital 85.
[113] *Ibid*, Recital 86.
[114] Tanguy Van Overstraeten (n45)
[115] Giovanni Buttarelli (n99)
[116] *Ibid.*
[117] GDPR (n2) art 30 (2b).
[118] Ruth Boardman, Bird &Bird, guide to the General Data Protection Regulation (2017).

investigate a personal data breach.[119]This could involve assessing the types of data AD holds and documenting which ones would fall within the notification requirement in case of a breach.[120] Moreover, AD's data processors should report personal data breaches to AD.[121] Lastly, AD should report personal data breaches to its supervisory authority and in some cases, to affected data subjects.[122]Data controllers should also maintain an internal breach register.[123]

The EDPS advices that "the new rules are not inforce quite yet - but it is already clear what lies ahead in terms of future obligations. Getting ready now is ideal timing - as part of risk management, don't leave it until the last minute".[124] Thus, as a last recommendation, AD should preventively actas regards to data protection since decisions have to be taken *ex ante* processing.[125]

DPIA and Privacy by design (PbD)

Legal ground for Data Privacy Impact Assessment (DPIA)

The GDPR in Section 3, Chapter IV mandates the requirements and the procedure of Data Protection Impact Assessment (hereinafter, DPIA). The DPIA should, in particular, apply to "large-scale processing operations which aim to process a considerable amount of personal data and may affect a large number of data subjects and which are likely to result in a high risk".[126] For instance, such kind of processing operations can be those which, especially, "involve using new technologies[127], or are of a new kind and where no data protection impact

[119] ICO, Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now, (2017) https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf accessed 28 April 2017.
[120] *Ibid.*
[121] Ruth Boardman (n118)
[122] GDPR (n2)Recital 85; art 33.
[123] *Ibid*, art 33(5).
[124] Giovanni Buttarelli (n99)
[125] *Ibid*
[126] GDPR (n2) Recital 91
[127] English Oxford Living Dictionaries: New technology is the technology that radically alters the way something is produced or performed, especially by labour – saving automation or computerization.

assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing".[128]

Additionally, considering that the nature, the scope, context and purposes of the processing is likely to result in high risk to the rights and freedoms of natural persons, the controller shall, prior to processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The GDPR refers to some examples related to high risk processing in Article 35 (2). Such high risk might result from specific types of processing as well as the extent and frequency of processing.[129] Specifically, processing may be in a high risk, if it prevents data subjects from exercising a right or using a service or a contract, or because it is carried out systematically on a large scale.[130] For instance, high risk processing may take plane in monitoring activities, systematic evaluations or processing special categories of data.[131]

The assessment can be performed more than once, since controllers must ensure that a DPIA has been run on any *"high risk"* processing activity before it is commenced[132]; in other words it must be done whenever similar processing operations present similar high risk.[133] In that case, the controller shall seek the advice of the data protection officer when carrying out the data impact assessment.[134]

Firstly, it is necessary to clarify that carrying a DPIA is not mandatory for every processing operation, since it is a risk-based method. Risks should be identified and evaluated as long as it is executed on the basis of likelihood of risk occurrence and the expected impact of the consequences.[135] It is only mandatory when the processing is ''likely to result in a high risk to the rights and freedoms of natural

[128] GDPR (n2) Recital 89
[129] I*bid* Recital 94
[130] Van Overstraeten, *The General Data Protection Regulation A Survival Guide* 2017)

[131] Ruth Boardman, Bird &Bird, guide to the General Data Protection Regulation (2017).
[132] *Ibid*
[133] GDPR (n2)art 35 (1).
[134] *Ibid,* art 35 (2).
[135] Lucas Zolejnik, 'Data Protection Impact Assessment. First Guidelines' (*Security, Privacy & Tech Inquiries*, 2017) <https://blog.lukaszolejnik.com/data-protection-impact-assessment-first-guidelines/> accessed 3 May 2017.

persons''. In cases where it is not clear whether DPIA is required, the WP 29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law.[136]

The GDPR provides in its article 35(3) the cases in which a DPIA is required, in particular when a processing ''*is likely to result in high risks''.* However, it is not an exhaustive list. Consequently, DPIA will be required in case of (but not only):

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to Article 9 (1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale;[137]

(d) the competent supervisory authority considers that the processing is likely

to result in a high risk to the rights and the freedom of the data subjects.[138]

***"Autres Directions Foundation collect**:*
-Personal data (i.e. first name and age)
-Details regarding participation (i.e. time, location, visitors Identity Card)
-Specific Personal Data (i.e. skin color, heartbeat, facial photograph)
-Health related personal data (i.e. length, weight, BMI)
To what ends does AD process your personal data?
-Making the Mirror Room available
-Build a participation database, as to aid Mirror Room
-Create a (participant) info – profile, based on collected data
-To compare (personal) data and info- profiles of participants with other participants
-To improve the system in hand, the so-called Mirror Room."[139]

[136]Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ''likely to result in a high risk'' for the purposes of Regulation 2016/679.
[137]GDPR (n2) art 35(3).
[138]*Ibid*, Recital 91.
[139]AD Privacy Policy (Non – Official Translation).

As long as it concerns the collection and processing of the aforementioned data for Mirror Room purposes, AD should be in compliance with GDPR provisions with respect to personal data protection. Every processing of personal data constitutes an interference with the data subject's rights and freedoms and thus it must be justified. In this case, providing that AD collects and processes sensitive personal data in a large scale (potentially, at least) legal issues can occur. Besides, the nature of the data processed by the mirror room experience is likely to result in a high risk for its participants. Therefore, AD should incorporate in its standard business process the DPIA.

Another important issue is that DPIA must provide a proportionality analysis.[140] This analysis establishes whether the data used and processed are indispensable to fulfill the intended objective of the controller (connection with purpose limitation principle). In case that there is an alternative to achieve the intended task, it is necessary to explain why the chosen one is followed. Consequently, AD should explain in a more detailed manner the procedure that it is going to follow for processing the data and the necessity of this procedure in accordance to the purpose and the result envisioned to achieve.

The risks inner to the Mirror Room experience are evident since the beginning of the project and, therefore, will fall under the new requirements of the GDPR as of 2018. In that sense, a DPIA will have to be performed in order to ensure compliance while processing the project's data. Thus, AD should start to consider how the company should approach it. In other words, it is advisable that AD implements a formal DPIA alongside the project development process.

In addition, considering the likelihood of the project's data processing would result in a high risk to its participant, the GDPR provides for a new mechanism to protect data subjects called prior consultation.[141] Derived from its terminology, prior consultation comprises an advice from the supervisory authority preceding the process of the data. The rationale behind it is that the processing could result in high

[140] Lucas Zolejnik (n 128)
[141] GDPR (n2) art 36.

risk for individual's rights and freedom in the absence of measures taken by the controller to mitigate it.

Accordingly, when planning to introduce a DPIA in their projects, AD should take into consideration the following steps:

- Identifying the need for DPIA;
- Describing information flows;
- Identifying privacy and related risks;
- Identifying and evaluating privacy solutions;
- Signing the DPIA outcomes back into the project plan.[142]

Privacy by Design

The concept of Privacy by Design (hereinafter, PbD) is a vision for creating data processing environments in a way that respects privacy and data protection in the design of products and processes from the start.[143]

The controller shall implement mechanisms to ensure that, by default, only the personal data that are essential for each specific purpose is processed. Furthermore, the data should not be collected or retained beyond the minimum necessary for those purposes. Those mechanisms shall ensure that by default personal data are not made accessible automatically, apart from the controller's activity.[144]

Privacy by design is an approach to projects that promotes privacy and data protection from the beginning.[145] Privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their

[142]Conducting Privacy Impact Assessments Code Of Practice (1st edn, 2017) <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf> accessed 4 May 2017.
[143]Pagona Tsormpatzoudi, *Privacy By Design: From Research And Policy To Practice – The Challenge Of Multi-Disciplinarity* (1st edn, 2017) <https://people.cs.kuleuven.be/~bettina.berendt/Papers/tsormpatzoudi_berendt_coudert_APF2015_with_bib_metadata.pdf> accessed 4 May 2017.
[144]GDPR (n2) art 25 (2).
[145] 'Privacy by Design' (*Ico.org.uk*, 2017) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 3 May 2017.

deployment, use and ultimate disposal.[146] This tool incorporates many advantages, as it is the essential tool in minimizing privacy risks and building trust. First of all, it helps to identify at an early stage potential problems which may occur in the future so as to when a company is asked to address them to be simpler and less costly.

Moreover, it increases awareness of privacy and data protection across the company. GDPR under Article 25 mandates ''that with respect to the state of the art and the cost of implementation, the controller shall, both at the time of determination of the means for processing and at the time of processing itself, implement appropriate technical and organizational measures and procedures in such way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject''. [147]

Recommendations

AD must take into consideration the protection of the data processed in its project, beginning with its installations. Since the machine is already established, we would recommend having privacy by design as a guidance for future infrastructure developments.

Precisely, the AD should operate Mirror Room based on that notion: "privacy should be taken into account throughout the entire engineering process from the earliest design stages to the operation of the productive system". [148] For instance, pseudonymised information constitutes a form of personal data, but it may be used by AD as a technique which may satisfy requirements to implement PbD.[149] Furthermore, since privacy has to be continuously protected throughout the life-

[146]Patrizio Campisi, *Security and Privacy In Biometrics* (Springer 2013).
[147]GDPR (n2) art 25.
[148] ENISA, Privacy and Data Protection by Design – from policy to engineering, (2014) < https://www.enisa.europa.eu/topics/data-protection/privacy-by-design> assessed 05.05.2017
[149] Ruth Boardman, Bird &Bird, guide to the General Data Protection Regulation (2017).

cycle of the Mirror Room[150], AD should consider an IT support staff. This IT staff should be accountable for the security of personal information.[151]

Thus, it should be consistent with recognized standards, which assure the confidentiality and integrity of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.[152] For instance, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published the "Privacy framework" (ISO/IEC 29100)[153] as an international standard[154]. Particularly, the AD' s IT department should focus on privacy-enhancing technologies[155] as well as on the eight privacy design strategies.[156]

Privacy Design Strategies

1. "Minimize"	**The amount of personal data that is processed27 should be restricted to the minimal amount possible. (e.g anonymization and use pseudonyms')**
2. "Hide"	**Any personal data, and their interrelationships, should be hidden from plain view. (e.g the use of encryption of data when stored, or when in transit)**
3."Separate"	**Personal data should be processed in a distributed fashion, in separate compartments whenever possible.**
4. "Aggregate"	**Personal data should be processed at the**

[150] Dr. Ann Cavoukian, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, (2017) <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 5 May 2017.
[151] *Ibid.*
[152] *Ibid.*
[153] ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, International Organization for Standardization (ISO) JTC 1/SC 27.
[154] ENISA (n148).
[155] "*Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system*".
European Commission, A Digital Agenda for Europe, COM (2010)245, (2010), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT> accessed on 05.05.2017.
[156] ENISA (n148)

	highest level of aggregation and with the least possible detail in which it is (still) useful. (e.g k-anonymity[157])
5."Inform"	**Data subjects should be adequately informed whenever personal data is processed (e.g Platform for Privacy Preferences or Data breach notifications)**
6. "Control"	**Data subjects should be provided agency over the processing of their personal data (e.g end-to-end encryption support control)**
7. "Enforce"	**A privacy policy compatible with legal requirements should be in place and should be enforced (related with the accountability principle)**
8. "Demonstrate"	**A data controller to be able to demonstrate compliance with the privacy policy and any applicable legal requirements. (e.g privacy management systems, and the use of logging and auditing).**

Hence, we recommend that AD use training programs for their partners and adopt relevant policies and procedures for implementing PbD techniques.[158] To comply with the GDPR, it is advisable that AD puts in practice its aim - privacy - in its internal structure and design. AD should think PbD as "a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices".[159]

Profiling

Currently applicable data protection framework in EU represented by Data Protection Directive does not provide the definition of profiling. The emphasis is

[157] Latanya Sweeney. k-anonymity: A model for protecting privacy. (International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems2002), 10(5):557–570.

[158] Ruth Boardman, Bird &Bird, guide to the General Data Protection Regulation (2017).

[159] Sylvia Kingsmill, Dr. Ann Cavoukian, Privacy by Design Setting a new standard for privacy certification (Deloitte)<https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF> accessed 4 May 2017.

rather put on right of data subjects against automated decisions.[160] The GDPR constitutes profiling as a sub-category of automated processing.

Profiling is defined in Art 4 (4) of GDPR as "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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." The notion encompassed three requirements that shall be met. The (i) process must be automated, (ii) personal data are at stake and (iii) used for assessment or prediction of certain personal aspects related to a natural person. Furthermore, legislation provides a non-exhaustive example of what shall be subject of the analysis of personal data. The newly created European Data Protection Board may draft further guidelines of how the definition should be interpreted.[161]

Current Policy

First issue to be addressed is whether the personal data are at stake when it comes to the conduct connected to the Mirror Room. This outcome depends on traceability aspects that were subject of the analysis in the previous part of the report. Second requirement is that it must be a form of automated processing of personal data. The Mirror Room collects the data through measuring devices (e.g. Kinect or optical sensors) and, based on the collection; it makes a decision in connection with participant´s reactions to specific modeled situations. The latter shall amount to automated processing of personal data.

Final prerequisite is that the personal data are used for analysis or prediction of specific personal aspects relating to data subjects. The profiling occurs when

[160] Directive 95/46/EC (n103) art 15.
[161] GDPR (n2) Recital 71.

automated decision process is guided by the profile.[162] For assessment of this aspect the special emphasis should be put on the released leaflet (or publicly available profile) that each data subject receives after visit of the Mirror room. The profile shows the outcome of the analysis of emotions and facial reactions. The result is a set of data offering a view on situations that subjects are afraid of, prejudices, perceptions and preferred appearances. However, this part relates only to the creation of the profile, but further application of the profile is absent. The third requirement is thus not met.

Recommendations

As it has been pointed out in the previous part, the profile is created from the collected data. Yet it does not seem that the profile itself is further used to make automated decisions. On the other hand, the data bears a great value and indeed, might be used for profiling purposes in the future. In case of forthcoming processing of personal data includes profiling, several obligations and rights are triggered by provisions of GDPR. We emphasize the following recommendations.

1. <u>What data are processed</u>

Firstly, it is of the essence to qualify personal data at stake from the reason that when it comes to sensitive data specified in Article 9 (1)[163] the controller must have (i) explicit consent of the data subject or pursue substantial public interest and (ii) safeguards rights and freedoms and legitimate interests of the data subjects.[164] It is questionable if raising awareness about data protection through Mirror Room would satisfy the test for substantial public interest considering potential alternatives. From

[162] Dmitri Kamarinou, Christopher Millard and Jatinder Singh, 'Machine learning with personal data: Profiling, Decisions and the EU General data protection Regulation' <http://www.mlandthelaw.org/papers/kamarinou.pdf > accessed 24 April 2017.

[163] "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. "

[164] GDPR (n2) art 22(4).

this reason, the sensitive data shall be processed with explicit consent providing sufficient safeguards.

In case of non-sensitive data the controller may rely on three legitimate grounds for processing.[165] Taking into account the nature of the Mirror Room, the controller can process the data based on the performance of a contract or the explicit consent of a data subject.

2. Fostering Transparency

Apart from the general obligations reflecting the principle of transparency, Article 13 (2) (f) states that controllers "shall, at the time when personal data are obtained, provide the data subject with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." The current Privacy Policy informs data subjects about purposes and types of data that are collected. Although the Policy states what data are processed and how are they processed, the envisaged consequence and significance are presented very briefly ("info-profile is created"). To follow the principle of transparency with regard to specific requirements for profiling, it shall also state what outcome should be expected in connection with the content of the profile (assessment of prejudices, fears etc). It is also of the essence that this information is provided before or at the time collection of personal data.

3. Data Protection Impact Assessment

A controller of personal data shall be required to conduct data protection impact assessment in case of "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."[166] Considering

[165] *Ibid,* art 22 (2).
[166] *Ibid*, art 35 (3a).

data protection impact assessment, it is of the essence to determine whether profiling produces legal or similarly significant effects towards a natural person. More detailed evaluation of the process is presented in precedent part of the report.

Further Research

In the age of Big Data it is of the essence to examine further use of personal data collected for specific purpose. One of the most debated exploitation is for research. Currently, applicable data protection framework provides a possibility for further scientific research and states that such a purpose is generally compatible with processing of personal data provided that member states secure appropriate safeguards.[167] The similar rule is provisioned with regard to GDPR in Art 6 (4) and explanation provided by Recital 50 where is held that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations."[168]

However, the GDPR refrained from delegation of provision of appropriate safeguards by member states. On the other hand, in Article 89, it is stated that processing for research purposes shall be subjected to appropriate safeguards ensuring "that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization", e.g. by pseudonymisation.

"Sharing of data with third parties:

Your personal data will not be hired or sold to third parties, or in any other way or shape shared or transferred to third parties, with the exception of AD's partners - and ***only for scientific purposes. The data send to our partners will only be transmitted after name and picture(s) have been removed****."*

Recommendations

[167] Directive 95/46/EC (n103), art 6 (b).
[168] GDPR (n2) art 5 (1b).

Analysis of use of personal data through Mirror Room for scientific purposes poses several questions. Firstly, it shall be established what kind of research is available in connection with further processing. GDPR states in Recital 159 that a notion of research shall be interpreted in a broad manner "including for example technological development and demonstration, fundamental research, applied research and privately funded research." Until further guidance is provided by respective authorities it shall be presumed that Big Data analysis may fall within the term of scientific research.

Secondly, according to the Privacy Policy, anonymized info-profiles remain available for scientific purposes after the retention period. It is suggested that such measure is appropriate although anonymized data are not subject to GDPR and therefore anonymous information does not pose any obligations to the controller.[169] However, the data must be anonymized efficiently. In case that scientific research requires data which are not anonymized, it shall be undergone by pseudonymization techniques, as it is suggested by the legislation.

The latter is explicitly mentioned in the Privacy Policy declaring that "your personal data will not be hired or sold to third parties, or in any other way or shape shared or transferred to third parties, with the exception of AD's partners - and only for scientific purposes. The data sent to our partners will only be transmitted after name and picture(s) have been removed." It is of the essence to address if removal of a name and picture is sufficient. We would also suggest that profile number and time of visit of Mirror Room shall be also erased, as the pertinent data may be strong indicators of identifiability when combined with others. The principle of data minimization should be taken into account when talking about personal data for scientific purposes.

Conclusion and Follow-up

[169] *Ibid*, Recital 26.

In general, the AD's privacy policy was considered satisfactory and the team supports and encourages the initiative to raise awareness over the daily massive 'datalization'. However, as technology develops in a fast pace, so does the individuals concerns over their privacy. In this sense, having an up-to-date privacy policy is of paramount relevance for companies and NGO's to continue to achieve their aims in the data processing environment. Therefore, we consider an indispensable key to success to be in compliance with the GDPR before it enters into force in 2018. Besides the abovementioned recommendations, we would like to highlight some follow-up measures to ensure the project continuity:

-Record keeping in writing: contracts with processors, personnel (DPOs, employees), records of all activities and incidents (data breaches) are necessary measures to comply with the new accountability requirement;

-Re-negotiation: businesses are changing all the time and so does your contractors, suppliers, etc.

-Re-evaluation: Organizational modalities can change, new infrastructures can be made available, new standards for security measure can be set and new purposes can be laid out. The privacy policy should be adjusted in accordance to each substantial modification.

Annex

PRIVACY STATEMENT (non-official translation)

AD processes personal data for the WE ARE DATA project. In this Privacy Statement AD will inform you about who we are, to what ends we store your data, how you will be able to enforce your privacy rights and other possibly relevant information. This PS is applicable to the WE ARE DATA - Mirror Room and the participants' profiles that subsequently follow. AD strives to take proper care of personal data and aspires to act within the confines of the law personal data protection and the law on telecommunication.

Responsibility

AD is the responsible party (law of personal data protection).
To what end does AD process your personal data?
AD collects and processes personal data for the following goals:
- Making the Mirror Room available
- Build a participation database, as to aid the Mirror room
- To create a (participant)info-profile, based on the collected data
- To compare (personal) data and info-profiles of participants with other participants
- To improve the system at hand, the so-called Mirror Room

What personal date does AD collect?

AD collects and processes, after explicit consent of the ones involved, the following (personal) data:
- Personal (First name and age)
- Participation details (i.e. time, location, visitor's ID)
- Specific personal data (skin color, heartbeat, facial photograph)
- Health-related personal data (length, weight, BMI)

The specific personal data and health-related personal data will be collected and processed through use of the following measuring devices and programming:
- Body weight scale (Weight in KG)
- Camera 3d image - Kinect (Length, posture and position)
- Camera's - optical sensors (FaceReader, FacePiRes, FaceSwap)
An info-profile is created based on the participant's (personal) data.

Data Conservation

AD reserves the right to save and conserve the personal data as long as the project is running, with a maximum of two years. After these two years, anonymized info-profiles remain available for scientific purposes.

Minors

To enter the MR, the participant must have the minimum age of 16 or have explicit consent from parent or lawful guardian.
How does AD guarantee confidentiality in regards to personal data?
Confidentiality and security
AD will take suitable technical and organizational measures to secure personal data from unauthorized access. The data in the online database will be stored in an encrypted fashion. The data in the installation itself (MR) will be encrypted as well. The installation itself will be closed off using a steel lock with Lock-box.

Sharing of data with third parties

Your personal data will not be hired or sold to third parties, or in any other way or shape shared or transferred to third parties, apart from AD's partners - and only for scientific purposes. The data send to our partners will only be transmitted after name and picture(s) have been removed.

AD will share personal data when she is forced to do so based on a lawful duty, for example in case of a police inquiry. AD will also share personal data, after explicit consent from the participant, with third parties outside of the installation by showing this personal data and subsequent conclusion on computer screens.

Furthermore, participants can give explicit consent to have their info-profile published on www.wearedata.nl. Lastly, it is possible for participants to share their info-profile on social media, such as Facebook.

Processors

AD might hire private contractors to have them take over part of the process, on behalf of a contractual obligation. AD will ensure confidential and careful conduct with the personal data
through contractual clauses, in so called 'processors contracts'.
Outside of the cases mentioned above, AD will only share personal data to third parties when this is conforming to the law of personal data protection.

How can you contact AD?

Contact
AD is, for matters related to the 'WeAreData - Mirror Room', available at wad@autresdirections.nl.
It is your own responsibility to ensure correctness of your personal data, as well as to ensure that they are up to date. AD is, except in cases of premeditation or negligent behavior, not liable for factual errors or activities arising from your incorrect or outdated information.

Insight and correction

You can ask AD for an insight- or correction request. You are advised to clearly indicate that you are requesting an insight- or correction request based on art. 35 law on personal data protection. Keep in mind that it might be necessary to share a copy of your personal ID to check personal identity. The email can be found above.

Resistance

You are allowed to resist/complain about the use of your personal data for commercial purposes. When you let us know (through any means of contact) that you do not want to be contacted anymore, we will save the required data in a file specifically for this purpose and your other personal data will no longer be used for these purposes.

What was the last time this Privacy statement was changed?

AD holds the right to change the clauses in this privacy statement. You are personally responsible to stay up to date in regards to the latest version of this privacy statement. We advise you to regularly check whether amendments have been made.

Last time changed: 12-05-2016

Bibliography

Primary Sources

Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Council Directive 93/13/EEC on unfair terms in consumer contracts (1993) L95/29

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)

The Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', Analysis of the definition of Personal Data according to the Data Protection Directive [2007]WP 136

The Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"'[2010] WP169

Secondary Sources

Handbook On European Data Protection Law (1st edn, Publ Office of the European Union [ua] (2014)

Buttarelli, 'The accountability principle in the new GDPR Speech at the European Court of Justice' (2017)

Campisi, *Security and Privacy In Biometrics* , Springer (2013)

De Hert and Papakonstantinou, The New General Data Protection Regulation: Still A Sound System For The Protection Of Individuals? Elsevier (2016)

Gumzej, Nina. "Data protection for the digital age: comprehensive effects of the evolving law of accountability." *Tribuna Juridică* 4 (2012)

Kamarinou, Millard and Singh, 'Machine learning with personal data: Profiling, Decisions and the EU General data protection Regulation' (2017)

Kuner, '*European data protection law: corporate compliance and regulation',* ed. edn, Oxford University Press, Oxford (2007)

Ryz and Grest, 'A New Era In Data Protection' Computer Fraud & Security (2016)

Thorburn, Stalla-Bourdillon and Rosati, 'Iclic Data Mining And Data Sharing Workshop: The Present And Future Of Data Mining And Data Sharing In The EU', Computer Law & Security Review (2017)

Tsormpatzoudi, *Privacy By Design: From Research And Policy To Practice – The Challenge Of Multi-Disciplinarity* (2017)

Wang and Luo, Detecting Visually Observable Disease Symptoms from Faces, Springer Online, 2016

Latanya Sweeney. k-anonymity: A model for protecting privacy. (International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002).

Websites and blogs

Blom, Akkermans, Swaving, 'The Mirror Room, Who do we see… when you look in the mirror?' (We Are Data,2015) <http://wearedata.nl/en/mirror-room/>accessed 4 May 2017

Conducting Privacy Impact Assessments Code Of Practice (1st edn, 2017) <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf> accessed 4 May 2017

Dautlich, Information should not be regarded as Personal Data if it is too burdensome to confirm its status, (Out-law.com, 2012)<http://www.out-law.com/en/articles/2012/june/information-should-not-be-regarded-as-personal-data-if-it-is-too-burdensome-to-confirm-its-status-council-of-ministers-says/>accessed 4 May 2017

Davis, 'New Airport Security Face Recognition Platform Helps Safeguard Borders' (*Benzinga*, 2017). <https://www.benzinga.com/pressreleases/17/04/p9333392/facefirsts-new-airport-security-face-recognition-platform-helps-safegua> accessed 26 April 2017

ICO, Preparing for the General Data Protection Regulation (GDPR) 12 steps to take no (Ico.org, 2017) https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf accessed 1 May 2017

Johnson , What your heart rate is telling you, Harvard Health Publications, Harvard Medical School, 2015, <http://www.health.harvard.edu/heart-health/what-your-heart-rate-is-telling-you>, accessed 4 May 2017

Kalapesi, Rethinking Personal Data: Strengthening Trust, World Economic Forum, (Weforum.org, 2012), <http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf> accessed 4 May 2017

Kamarinou, Millard and Jatinder Singh, 'Machine learning with personal data: Profiling, Decisions and the EU General data protection Regulation',<http://www.mlandthelaw.org/papers/kamarinou.pdf > accessed 24 April 2017.

Leenes, Accountability and transparency in Big Data land, DSC/t Blog, (Tilburguniversity.edu, 2016), <https://www.tilburguniversity.edu/research/institutes-and-research-groups/data-science-center/blogs/data-sience-blog-ronald-leenes/> accessed 4 May 2017

'Privacy by Design' (*Ico.org.uk*, 2017) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 3 May 2017

Sebastian le Cat, 'GDPR Top Ten: #2 Accountability Principle | Privacy | Deloitte' (*Deloitte Nederland*, 2017) https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-2-accountability-principle.html accessed 4 May 2017.

Lior , 'All Israelis Will Have To Join Biometric Database From Next Year, Minister Says' (*haaretz.com*, 2017) <http://www.haaretz.com/israel-news/1.728256> accessed 26 April 2017

Thorburn, Sophie Stalla-Bourdillon and Eleonora Rosati, 'Iclic Data Mining And Data Sharing Workshop: The Present And Future Of Data Mining And Data Sharing In The EU', Computer Law & Security Review (2017).

Tien, The Data Protection Principles UnderThe General Data Protection Regulation' (*Taylorwessing.com*, 2017)https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html accessed 28 April 2017

Pagona Tsormpatzoudi, *Privacy By Design: From Research And Policy To Practice – The Challenge Of Multi-Disciplinarity* <https://people.cs.kuleuven.be/~bettina.berendt/Papers/tsormpatzoudi_berendt_coudert_APF2015_with_bib_metadata.pdf> accessed 4 May 2017

Van Overstraeten, *The General Data Protection Regulation A Survival Guide* (1st edn, 2017) http://file:///C:/Users/user/Downloads/TMT_DATA_Protection_Survival_Guide_Singles.pdf accessed 4 May 2017

Zolejnik, 'Data Protection Impact Assessment. First Guidelines' (*Security, Privacy & Tech Inquiries*, 2017) <https://blog.lukaszolejnik.com/data-protection-impact-assessment-first-guidelines/> accessed 3 May 2017

Sylvia Kingsmill, Dr. Ann Cavoukian, Privacy by Design Setting a new standard for privacy certification (Deloitte)<https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF> accessed 4 May 2017.

'Privacy By Design' (*Ico.org.uk*, 2017) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/> accessed 4 May 2017.

ENISA, Privacy and Data Protection by Design – from policy to engineering, (2014) < https://www.enisa.europa.eu/topics/data-protection/privacy-by-design> assessed 05.05.2017.

Dr. Ann Cavoukian, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, (2017) <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> accessed 5 May 2017.