Climategotchi: A report on GDPR compliance
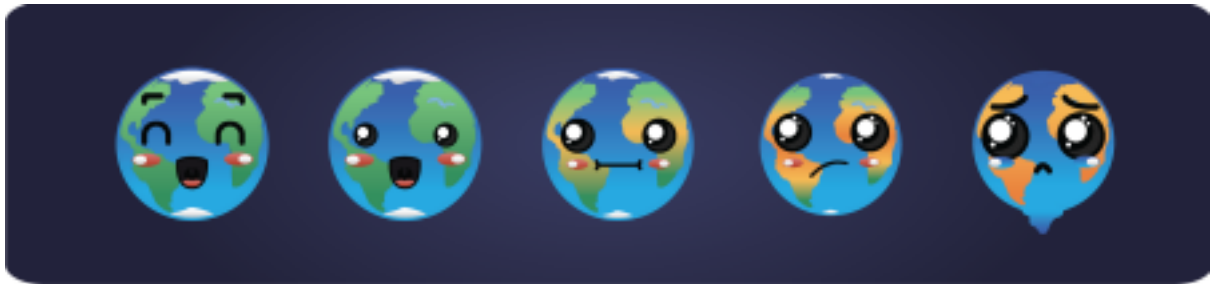
Cecilie Nyhus
Amanda Terhonen
Nadezda Kustova

Table of Content

Introduction

1. Presenting Climategotchi and the purpose of the report

Climategotchi is a prototype of a mobile application (also referred to as "the App" and "the Application") created as a part of the Bachelor's program in Media and Interaction Design at the Department of Information and Media Science at the University of Bergen. Climategotchi is designed to encourage its users to make climate-friendly choices in their everyday lives. The user takes care of a virtual globe which is affected by the user's completion of climate-friendly challenges generated by the App.

The purpose of this report is to address some of the privacy and data protection issues that arise from providing the App. These privacy issues will primarily be assessed from through the articles and recitals of the GDPR as well journalistic articles, guidelines of the EDPB and other sources. National laws and other regulations than the GDPR are excluded from the assessments made in this report.

The privacy issues arising from the App are approached by firstly identifying the issues and assessing them under the GDPR, and, where possible, providing solutions for the App to be GDPR-compliant. The report is written from a legal point of view and does not focus on how the technicalities of such solutions would work in practice. Rather, this report provides suggestions on developing the App in a privacy-friendly way to ensure compliance with the requirements laid down in the GDPR.

2. Structure of the report

This report is divided into four parts, each of which examines a main privacy topic relating to the App or the functionalities of the App. The topics that will be addressed are installing of the App and creation of the user account (part I), the challenge using the purchase activity of the user (part II), the challenge tracking the user's geo-location (part III), and privacy matters related to funding through in-app advertisement and the actual development of the App (part IV).

It is acknowledged that there are various privacy matters that this report does not cover. Due to the word limitation of the report, it has been chosen to focus on the above-mentioned topics as they present the most relevant and, in the authors' opinions, the most interesting privacy matters related to the App. These topics are considered interesting under GDPR due to the fact that all of the mentioned functionalities may heavily invade the users' privacy.

3. Method

The precondition for this report is that the App is a prototype, and that the actual processing of data has not yet begun. Due to the fact that the App is still a prototype, assumptions are made regarding what decisions the developer of the App would make when actually developing and providing it.

When assessing the above-mentioned topics, the purposes of the processing of personal data, the type of personal data being processed, and the legal basis for the processing are identified. To provide an overview, these essential findings are also presented in the table below (see table 1).

Key legal principles under article 5 of GDPR that are especially relevant for the chosen topics are presented throughout the report. It has been chosen that this report does not assess every legal principle, rather compliance with the most relevant principles to each functionality is assessed.

Purpose of processing	The type of personal data being processed	Legal basis for processing
Installing Climategotchi on the device	IP address	Art. 6(1)(b): Necessary for the performance of a contract
Creating an account for the user	Name Email Password	Art. 6(1)(b): Necessary for the performance of a contract
Purchase challenges	Purchase information	Art. 6(1)(a): Consent
"Bike to work" challenge:	Home and work addresses	Art. 6(1)(a): Consent

	Current geolocation	
In-app advertisement for receiving funding	The users' online activity and preferences on the App; cookie identifier code	Art. 6(1)(a): Consent
Further development of the Climategotchi App	The users' online activity on the App	Art. 6(1)(a): Consent

Table 1

4. Terminology

Before presenting the above-mentioned parts and topics, some time will be spent on briefly introducing a few key terms used further on in the report.

"*Personal data*" means *"any information relating to an identified or identifiable natural person" (data subject)"*, cf. art. 4(1) GDPR. In the case of Climategotchi, the user of the App is the data subject, as it is the user's data that is being processed.

In this report, the term *"data subject"* and "*the user"* are interchangeable notions.

A "*controller*" is *"the 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"*, cf. art. 4(7) GDPR. Thus, Climategotchi acts as a controller.

"Climategotchi" and "Controller" are referring, in this report, to the same actor and are interchangeable notions.

A "*processor*" is *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*, cf. art. 4(e) GDPR.

In this report it is assumed that Climategotchi will act as the processor.

Part I: Installing the Application and creating the user account (Nadezda Kustova)

First of all, the Climategotchi Application needs to be installed on the user's device. Then the user registers her-/himself to create an account. In the following it will be discussed what shall be done so that these processes comply with GDPR.

1. Installing of the Application

1.1. Purpose and personal data

The purpose is to get the Application installed on the user's phone, and the Controller needs to get a hold of the user's IP address and send the Application file to this IP address. IP is an "*online identifier*" cf. art. art. 4(1) GDPR and is therefore "*personal data*".

1.2. Legal basis

When the Application is being installed, the user and the controller have agreed on that the controller will provide the user with the Application. There is therefore a contract, in which the controller and the users are contractual parties. The controller needs the user's IP address in order to send the Application file. The IP address therefore is necessary for the performance of the contract.

This situation fulfils the conditions in article 6(1)b GDPR, that states that processing of personal data is lawful if it is "*necessary for the performance of a contract to which the data subject is party*". Therefore, the contract serves as the legal basis for processing of the user's IP address.

1.3. Principles and the user's rights

Principles of transparency, data minimisation and purpose limitation cf. art. 5 are central. They shall be considered in light of the fact that in a contract the user cannot choose to not provide certain information, because it will reflect negatively on his/her access to the Application. Thus, it is important that the user is well informed about the purpose and is not asked to provide more data than what is necessary for the purpose.

The purpose of the contract has to be clear, not only from the controller's perspective, but also from the perspective of a reasonable data subject.[1] The use of clear and not complicated language is essential to make the purpose understandable for the user. That will also ensure transparency. As for the data minimisation, collection of excessive information can be avoided if the scope of the necessary data is objectively assessed by the controller prior to the processing[2].

The user shall also be informed that he/she as a contract party cannot freely terminate processing of her/his data, but has to terminate the contract first, because that in its turn will remove the legal basis for processing[3].

2. User Account

2.1. Purpose and personal data

After the app is installed, the user will have to create an account, so that the data generated by his/her activity in the app will be connected to the account. The account must be unique to avoid the user's data mixing up with the data from other users. In order to create a profile, the user will have to provide his/her name, surname, email, and create a password. With this type of data one can undoubtedly identify the data subject, and it shall considered as "*personal data*" cf. art. 4(1) GDPR.

2.2. Legal basis

Creating a user account is necessary for the core part of the Application's functionality – to keep the data in order. User's account is inseparable with the Application, and one cannot use the Application without creating an account. The fact that the user cannot choose whether he/she wants to create an account indicates that it is a part of a contract for the use of the Application. User's information for is therefore necessary for the performance of a contract cf. art. 6(1)b GDPR.

2.3. Principles

---

[1] A commentary, p. 331
[2] See EDPB guidelines 02/2019, p. 9
[3] A Commentary, p. 331

Principles of transparency, data minimisation and purpose limitation cf. art. 5 are also relevant for this purpose. The measures to comply with the principles are the same as for the purpose of downloading the app.

Part II: Purchase challenges (Cecilie Nyhus)

1. Presentation of the purpose of data processing: Providing the purchase challenge

One of the challenges provided by Climategotchi is based on the purchases made by the user. By choosing a challenge based on purchases, the user is encouraged to be more environmentally friendly by being challenged to, for example, not purchase meat for a week. (The challenge of not purchasing meat for a week will be used as an example throughout this part of the report.)

To run this challenge, Climategotchi must be able to identify the individual users of the App and collect information on whether the specific user has purchased meat for a limited period of time. This information will be processed to determine whether the challenge has been completed or not.

In order to comply with the GDPR, Climategotchi must, as the controller, first and foremost set out a purpose of the processing of personal data in accordance with the principle of purpose limitation.[4] The principle of purpose limitation is regarded as a cornerstone of data protection as it is a necessary precondition for many other fundamental requirements, such as the requirement of proportionality and legitimacy.[5] Compliance with this principle ensures that the data subject knows exactly for what purpose their data is being processed, that the purpose is not unlawful, and serves as a guarantee for the data subject that the collected data is being processed for this purpose only. Not having limited the purpose of data processing, will make superfluous all other privacy-related assessments. Describing a specified, explicit and legitimate purpose is therefore the first thing for a controller to address.

As mentioned above, the purpose of processing personal data is to determine if the user has purchased meat or not during the limited period of the challenge, in order to ensure that the challenge has been completed.

---

[4] Art. 5(1)(b) GDPR
[5] A Commentary, p. 315

2. The type of data processed

Knowing the purpose of the data activity, the next step for Climategotchi is to consider what kind of data is necessary in order to achieve the purpose.

If the chosen challenge is to not buy meat for a week, it is not sufficient for the Climategotchi to process information only regarding the stores in which the user has been shopping. Climategotchi also needs information on which specific products have been bought. This could for example be done by collecting receipts from the stores in which the users have been shopping and checking for purchases of meat.

At first sight, it may seem like purchase information falls under the category of "ordinary data", cf. art. 6 GDPR. However, an issue arises if Climategotchi collect detailed information on user-purchases. By collecting receipts, Climategotchi runs the risk of processing personal data on, for example, the health of the users. This would be the case if a user e.g., purchases medication related to a specific heart disease. Personal data concerning health is listed as one of the "special categories of data" in art. 9 GDPR. The issue of collecting special categories of data is that Climategotchi then needs not one but two legal bases for processing.

Climategotchi can approach this issue in one of two ways: Either the Climategotchi must find a legal basis for the processing of sensitive data in both art. 6 and 9 GDPR, or Climategotchi must find a way of retrieving the data needed but avoid processing special categories of data. The following paragraphs will further examine these two options.

2.1 Legal basis for processing special categories of data

Special categories of data are types of personal data that needs more protection because it is particularly sensitive[6]. Special categories of data, or sensitive data, is defined in art. 9(1) GDPR and includes *inter alia "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (...) data concerning health or data concerning a natural person's sex life or sexual orientation"*. Art. 9(2) GDPR provides that processing of sensitive data shall be prohibited unless one of the listed exceptions are met. In order to lawfully process sensitive data, the controller must have a legal basis both under art.

---

[6] A Commentary, p. 369

6 and art. 9 GDPR.[7] The list of exceptions under art. 9 GDPR is exhaustive, and the exceptions must be interpreted restrictively.[8]

For Climategotchi, the relevant legal basis to consider under art. 9 GDPR is the exception regarding explicit consent as provided in art. 9(2)(a) GDPR. For a controller to rely on this exception, the controller must obtain explicit consent from the user to process their sensitive data. Explicit consent has a higher threshold than the requirement of "consent" as a legal basis in art. 6(1)(a) GDPR, since explicit consent requires a higher degree of precision and definiteness as well as a precise description of the purpose of processing.[9]

Remembering that the purpose of collecting detailed information on the purchase history of the users is to check if any meat has been purchased, Climategotchi will not be able to present a purpose of the processing of e.g., health data. Needless to say, Climategotchi cannot, for that reason alone, rely on art. 9(2)(a) GDPR as a legal basis for the processing of special categories of data.

Without diving deeper into the other listed exceptions in art. 9(2) GDPR, it can be concluded that none of these are relevant to examine as potential legal bases for the processing of special categories of data in this regard.

2.2 Only purchase information relevant for the purchase challenges will be processed

As concluded above, Climategotchi cannot rely on the exceptions listed in art. 9(2) GDPR to process special categories of data. This entails that Climategotchi cannot legally collect receipts from purchases made by the users and process data retrieved from them. It is then necessary to find another way of collecting the data necessary to run the purchase challenges.

To comply with the GDPR, Climategotchi must pay attention to the principle of data minimisation, cf. art. 5(1)(c) GDPR. The principle of data minimisation provides that personal data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*.[10] Thus, this principle requires Climategotchi to only retrieve purchase data relevant for the challenges, i.e., information on whether meat has been purchased or not.

---

[7] Recital 51, GDPR
[8] A Commentary, p. 375
[9] A Commentary, p. 377
[10] Art. 5(1)(c) GDPR

It is assumed that the providers of purchase data for Climategotchi are the stores in which the user makes their purchases. Instead of Climategotchi retrieving the complete receipts from the stores, the principle of data minimisation requires Climategotchi to only retrieve data on meat purchases. In order for this report to solely focus on privacy issues, the report will not further address the technical challenges of how Climategotchi will retrieve this information but merely assume that Climategotchi can be provided with specific purchase information from the stores in which the users have made purchases. In addition to this, it is assumed that the stores are already processing purchase data from their customers and that this information can be shipped to/provided for Climategotchi.

In conclusion, to obtain the necessary data in compliance with the GDPR, Climategotchi must obtain purchase data from the stores in which the users have been shopping, and, in addition, make sure that stores only provide data on purchases of meat.

3. Consent as a legal base for processing purchase information relevant for the purchase challenges

As it has been concluded what type of personal data is needed and how it should be obtained, the legal basis for processing of the personal data will now be examined.

In order for the processing of personal data to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate base laid down in art. 6(1) GDPR, including when processing is necessary for the controller to comply with legal obligations or is necessary for the performance of a contract to which the data subject is party.[11]

When deciding which legal basis is most appropriate, one must take into account the type of data processed as well as the purpose for which it is being processed.
Access to the purchase history of the users are needed to run the purchase challenge. However, the purchase challenge is not necessary for the performance of the contract which is the functioning of the App itself. For this reason, art. 6(1)(b) cannot be relied upon as a legal basis for providing the purchase challenge.

---

[11] Recital 40 GDPR

Another legal base to consider is art. 6(1)(a) concerning consent given by the user. Unlike art. 6(1)(b), consent as a legal base does not entail a necessity test, and so it may be relied upon where the controller wishes to process data that is not necessary for the core purpose of running Climategotchi on the user's device. This is the case where the controller offers a service which the user can choose to use or choose not to use, e.g. a purchase challenge. If the user consents to the processing, they confirm that Climategotchi can obtain and process the purchase data needed. If the user does not consent, Climategotchi cannot use the purchase data and the challenges which rely upon this data will not be available to the user. The user is provided with a free choice which is supported by the fact that the user can decide which of several presented challenges they wish to take on.

Consent is defined in the GDPR as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.[12] Four cumulative criteria are presented. To comply with the GDPR, the consent must be:

1. freely given,
2. specific,
3. informed, and
4. unambiguous

3.1 Freely given

For consent to be freely given, the data subject should have an actual free choice in deciding whether they wish to consent to the processing or not. This entails that the data subject should not feel compelled to consent or endure negative consequences if they do not consent.[13]

Furthermore, consent must not, as a main rule, be bundled, i.e., where consent is tethered to the controller's provision of services, and the processing of data is not necessary for the performance of the service.[14]

Lastly, the data subject should be able to withdraw their consent without detriment.[15]

---

[12] Art. 4(11) GDPR
[13] A Commentary, p. 182
[14] A Commentary, p. 352, cf. art. 7(4) GDPR
[15] Recital 42 GDPR

In light of the above, Climategotchi should be especially aware that there should be no pre-ticked boxes when asking for the user's consent to process their purchase information, and that the user shall not be put in a less desirable situation if choosing not to consent. A less desirable situation could be if the user by not consenting would be excluded from accessing other non-related challenges. Furthermore, it is important for Climategotchi to be aware that consent to process purchase data must not be tethered with consent to install the App on the mobile device or to process location data etc. since this would make the performance of other non-related services conditioned by the consent to this specific processing of data.

Upon giving consent, the user shall also be informed of their right to withdraw consent at any time. This criterion can be met by making a "pop-up"-notice upon consenting. Withdrawing consent shall be as easy as giving it.[16] In practice, Climategotchi can make an easily accessible option of withdrawing consent in, for example, the "option" or "setting" section of the App.

3.2 Specific

The second element needed for consent to be valid is that it must be specific. This entails that the processing of data must be linked to a specific data activity, that the parameters of the activity are clearly defined, and that the consent is specific to the purpose which must not be formulated in a general or vague manner.[17] Consent, however, can cover all processing activities carried out for the same purpose.[18] This means that if, for example, the collected data needs to be both organised and stored in order to fulfil the stated purpose, the consent will cover both organising and storage of the data.

This criterion provides that Climategotchi must clearly distinguish the various data activities to be performed as well as their parameters, e.g. it is necessary to distinguish between obtaining purchase information for the purpose of providing a specific challenge in the App and using the same information for marketing purposes. At the same time, Climategotchi must describe the purposes in some detail. In practice, obtaining the purchase data of the user can be described as Climategotchi processing the said data for the purpose of making available the purchase challenge and informing the user of the status of the challenge.

---

[16] Art. 7(3) GDPR
[17] A Commentary, p. 183
[18] Recital 32 GDPR

3.3 Informed

In order to meet the criteria of being informed, the data subject should have prior knowledge of the parameters of the data processing activity. The criterion is elaborated in recital 42 GDPR stating that the data subject should *"be aware at least of the identity of the controller and the purpose of the processing for which the personal data are intended"*.[19] There is thus a close link between the criteria of specificity and that of being informed as well as the principle of transparency.

3.4 Unambiguous

The criterion of non-ambiguity entails that consent must be shown as *"a clear, affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement"*.[20] This provides that consent is not valid if it is obtained in the form of e.g., pre-ticked boxes or if the data subject is in doubt about whether they have consented or not.

To comply with this criterion, Climategotchi could present the processing activity and its purpose in line with the above-mentioned criteria, and hereafter letting the user actively decide whether to consent to the processing or not by for example providing an unticked box for the user to tick off if they wish to consent.

4. Principles of processing of personal data

Bearing in mind the above-mentioned criteria, the processing of the purchase data of the user will meet the requirements of consent according to the GDPR. However, the controller must also bear in mind the key principles of processing personal data as laid down in art. 5 GDPR. For the purpose of providing the purchase challenge, the principles of purpose limitation[21], data minimisation[22], and storage limitation[23] are particularly relevant for Climategotchi to address. The principle of purpose limitation and data minimisation has already been addressed in section 1 and 2 of this part of the report. The principle of storage limitation should also be briefly addressed. This principle prohibits the storage of data in a form which permits identification of the data subject beyond the time necessary to achieve the purposes of processing.[24] For

---

[19] Recital 42 GDPR
[20] Recital 32 GDPR
[21] Art. 5(1)(b) GDPR
[22] Art. 5(1)(c) GDPR
[23] Art. 5(1)(e) GDPR
[24] A Commentary, p. 318

Climategotchi, this entails that whenever a purchase challenge has been completed, or at least when the period of the challenge is over, Climategotchi is obliged to delete information on the user's purchases. In other words, storing of personal data on the purchases made by the user is only legitimate as long as the purchase challenge is active.

5. Information to be provided where the personal data has not been obtained from the data subject

For the purpose of this report, it is assumed that purchase data disclosing meat purchases made by the user will be provided to Climategotchi by the relevant stores. The personal data is thus not obtained directly from the data subject but indirectly from a third party. To comply with the GDPR, Climategotchi must therefore consult art. 14 GDPR which lists the information that must be provided for the data subject. The entire list of information as set out in art. 14 GDPR will not be examined in this report. Just two types of information that are particularly important for Climategotchi to pay attention to will be presented.

Firstly, Climategotchi must inform the user about the categories of personal data that are being obtained.[25] This is important to comply with the principle of transparency and fairness, as it, together with knowing the purpose, allows the user to understand that their purchase data is being obtained and that this is due to the functioning of the purchase challenge.

Secondly, Climategotchi must inform the user from where the purchase data is being obtained.[26] By informing the user that the purchase data is being obtained from specific stores, the user is allowed to potentially challenge the legality of the initial collection done by the stores, thereby ensuring the principle of fairness.[27]

---

[25] Art. 14(1)(d) GDPR
[26] Art. 14(2)(f) GDPR
[27] A Commentary, p. 444

Part III: "Bike to work" challenge (Nadezda Kustova)

1. The service

The point of the challenge is to register if the Application user is really biking to work when the challenge is activated. The user provides the work and home addresses. The user's current geolocation is going to be recorded in order to register the speed and the route of movement. These parameters are going to be analysed to determine if the user is indeed biking to work and therefore completes the challenge. If, for example, the analysis shows that the movement is characteristic for driving, the challenge won't be completed.

2. Purpose

To ensure the compliance with GDPR it is important that the purpose is specified prior to processing. Climategotchi is in the development phase. It means that the developers can precisely plan what type of data they will request for the challenge, choose the suitable legal basis, determine the period of storage, find suitable data protection safeguards, and work out potential security issues before they arise.

Art. 13 GDPR applies in the cases where the data is collected from the data subject and is therefore relevant for Climategotchi. It states that the user shall be informed about the "*purpose for the data processing*". Art. 5(1)(b) GDPR states in addition that the personal data shall be collected "*for specified, explicit and legitimate purposes*". It is meant to ensure that all stakeholders are able to understand the purpose, that the data subject is making informed choices, and to prevent illegal processing of personal data.

In the case of "bike to work challenge" the purpose for processing the data is to determine if the user is really biking to work and therefore completes the challenge. The purpose is detailed enough to be unambiguous for the reader, but at the same time not too detailed to be confusing. The language is clear and understandable. The purpose doesn't include activities that contradict national or the EU/EEA law, and therefore the purpose is lawful.

3. Data

3.1. Addresses and geolocation

For achieving the purpose, the following data are necessary: the user's work and home addresses and current geolocation. In art. 4(2) GDPR the "*location data*" is named as an identifier through which the user can be identified directly, indirectly or in particular reference to. The user can also be identified through the information about the user's place of work and home address. It is therefore "*personal data*" cf. art. 4 GDPR that will be processed.

3.2. Heart rate data

In addition, developers wanted to record the user's heart rate. That would be done to see if the heartbeat is in accordance with the one expected of a person who is biking. Question is if the heart rate data is necessary for achieving the purpose. As it is explained above, the addresses and geolocation are enough to ensure the control over the user's activity. Heart rate will be excessive, and the use of it will contradict with the data minimisation principal cf. art. 5(1)(c) GDPR.

Also, heart rate is a biometric data that belongs to the special category of data regulated in art. 9(1) GDPR. There are stricter rules for processing of this data, as e.g., a requirement of "*explicit consen*t" cf. art. 9(2)(a) GDPR. It will make it complicated to get the user's consent for processing of data that is not even necessary for achieving the purpose. It would therefore not be recommended to include processing of the heartbeat.

4. Legal basis

4.1. Choice of legal basis

An important factor in determining the legal basis here is the fact that the user chooses the challenge from several others, and thus stands free to engage and complete this particular challenge. As it is pointed out in part II point 3, freedom of choice to enter the challenge has a close connection with the user's freedom to decide whether his/her personal data will be processed. Such an empowerment of the data subject with control over personal data is characteristic for consent as legal basis cf. art. 6(1)(a) GDPR. (see part II, point 3)

Conditions in articles 6(1)(a), and 4(11) GDPR that define "*consent*" were explained in detail in part II point 3.4. Further on it will be presented how the articles apply in the Climategotchi case.

4.2. Freely given

Condition of freely given consent shows that the data subject shall enjoy a high degree of autonomy when choosing whether or not to give consent.[28] This condition is met in Climategotchi's case, as the user is in no way weaker positioned than the controller, and therefore can take the decision independently, not being afraid of the negative consequences in case of not consenting.

Processing of geolocation data is neither a condition for downloading the Application and performance of the Application itself. The Application does not need geolocation data unless the challenge is activated, and the conditions in art. 7 nr.4 GDPR (see part II, 3.1) are met. That means that the way the Application is planned enables the user to give the consent freely.

4.3. Specific

Specificity condition implies that the user has to get clear information about the parameters of the activity which the user is asked to consent to.[29] Specificity criterion is supplied by articles 5(1)(b) and 6(1)(a) GDPR, both requiring to point out the purpose specifically. For the "Bike to work" challenge it means that the user has to be specifically aware of what the geolocation data will be used to determine if he/she really bikes to work when the challenge is active, and that parameters such as speed and route are taken into the analysis of the activity. Specificity of consent is interconnected with the requirement about the consent being informed.

4.4 Informed

The requirement of an informed consent has to do a lot with communicating the parameters of planned data activity to the user.[30] For Climategotchi it means that the controller has to ensure that the user is provided with the knowledge of how the geolocation is going to be used to decide if the challenge is completed, inter alia, how the speed and the route of the user's

---

[28] A Commentary, p. 182
[29] A Commentary, p. 182
[30] A Commentary, p. 182

movement are affecting the analysis of the activity[31]. Use of clear and understandable language is crucial at this point.

4.5 Unambiguous

This criterion shall be considered in light of Recital 32 GDPR. Based on that, the Climategotchi user shall provide consent "*by a clear affirmative act establishing an (...) unambiguous indication*" of his/her agreement. Again, following the recital, the user can do it by ticking a box, but it is very important that the boxes are not pre-ticked[32]. The same solution as for the purchase challenge can be used - let the user to tick the boxes after presenting the information about the purpose and the way of processing of data (see part II point 3.4).

4.6 Right to withdraw the consent

Eventually the user has to be informed about "*the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal of*" cf. articles 13 (2)(c) and 7 nr. 3 GDPR. It is important to ensure that it is as easy to withdraw the consent as to provide it cf. recital 42.

5. Principles

In compliance assessment all the principles in art. 5 GDPR have to be considered. Since all cases are unique, compliance with some principles may be more problematic than the others. Further on the principles that are most problematic in case of "bike to work" challenge will be pointed out, and the measures for compliance will be presented.

5.1 Purpose limitation

Art. 5 (1)(b) expresses the principle of purpose limitation, stating that the personal data shall "*not [be] further processed in a manner that is incompatible with those purposes*". For the challenge it is important that the user's addresses and location data are not further processed for the purposes that are incompatible with the purpose of determining if the user is biking or not.

5.1.1 "Walk to work" challenge

---

[31] A Commentary, p. 182
[32] C-673/17, Planet49, point 65

As the app develops it is possible that similar challenges about user's commuting will be introduced, like for example a "walk to work" challenge. The same data as in the "bike to work" challenge will be used: home and work addresses, and current geolocation. The purpose will differ slightly, focusing on walking instead of biking.

When it is considered to use personal data for a new purpose, the controller has to undertake an assessment if further processing is compatible with the initial purpose cf. art. 6(4) GDPR. If purposes are not compatible, there has to be a legal basis for the new purpose. For Climategotchi the question is if the purpose of determining if the user is walking, is compatible with the purpose of determining if the user is biking.

5.1.2 Compatibility assessment

Art. 6(4) GDPR states that the controller in compatibility assessment shall take into account the aspects that are named in the article. Aspects under letters a), b) and c) are the most relevant for Climategotchi.

Firstly, it has to be considered if there is "*any link between the purposes*"[33]. There is no direct link between the purposes, but it can be seen in the light of the fact that the purposes emerge from the closely related challenges and have almost the same algorithm as a source. Secondly, "*the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controlle*r". Both purposes emerge from very similar challenges focusing on the way of commuting, and the relationship between the user and the controller is the same. Finally, it is the "*nature of the personal data*"[34] needed for both purposes is exactly the same, and it is not a sensitive type of data. These are clear arguments pro compatibility.

Other aspects in art. 6 (4) d) - e) are not that relevant for the case of Climategotchi as, there won't be any other consequences of the further processing than there already are, and the safeguards are expected to be the same as for the purposes connected to the "bike to work challenge".

---

[33] art. 6(4)(a) GDPR
[34] art. 6(4)(c) GDPR

All in all, the purposes are compatible. That means that the address data and geolocation data can be processed for the purpose of "walk to work" challenge based on the consent given for the "bike to work" challenge.

5.2. Data minimisation

Principle of data minimisation is important for the "Bike to work" challenge, as it includes recording of geolocation of the user. Art. 5 (1)(c) states that in order to comply with the data minimisation principle, personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

The principle that the data shall be limited to what is necessary in relation to the purpose means that the technical solutions should organize the data processing the way that filters out excessive information that is not necessary to achieve the purpose. When it comes to this requirement the Climategotchi might face problems. The app developers are planning to have location tracking active during the whole challenge. There was no information about the length of the challenges, so it is assumed that the challenges will have duration between 3 and 10 days. Further evaluation will be built on an assumption the user chooses to complete a 7-day "bike to work" challenge.

Question is if it is necessary to track the user's location for all the days to determine if the challenge is completed. Recording of geolocation is necessary to see if the user indeed is traveling to work by bicycle and completes the challenge. Therefore, the recording of geolocation shall happen only when the user is supposed to travel from home to the working place. Recording of user's geolocation for the rest of the day will be excessive and in contradiction with the principle of data minimisation. I will in the following come with a suggestion on how the amount of data can be minimised without disadvantages for the challenge.

The suggestion is to give the App user an opportunity to choose the time frame for the location monitoring - to inform when he/she will normally commute to work. The location recording will happen within this time window. Since the work address is provided, the App can register if the user has arrived to work based on the user's location. When the user has arrived, the App can ask the user to confirm he/she has arrived. If the user confirms, the recording can stop

already then. This solution will minimize the data to the necessary minimum and ensure compliance with the principle.

5.3 Storage limitation

Art. 5(1)(e) states that the 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*". Recital 39 gives guidelines that the period for which the personal data are stored shall be limited "*to strict minimum*". In order to comply with the principle Climategotchi shall erase the address and location data, when it is no longer necessary for the purpose of determining if the user has biked from home to work.[35]

"Bike to work" challenge lasts for several days, it makes it problematic to decide when exactly the data shall be deleted. The expiration time will differ for the address information, and for the information collected after one ride to work. The data collected after one ride shall be deleted the moment it is registered that the user has indeed biked to work on that day. The purpose is achieved, and there is no need for further storage of this data. The address information on the contrary can be stored for the whole length of the challenge, as it will be used every day further on. The address information shall be deleted after the challenge is completed, as it is no longer needed.

To ensure transparency the controller shall provide the user with the information about "*the period for which the personal data will be stored*" Art. 13 (2) a). The user has to be informed about the storage limits before he/she gives the consent.

---

[35] Recital 39 GDPR

Part IV: Funding through in-app advertisement & developing the App (Amanda Terhonen)

1. In-app advertisement by third-party ad networks

When the App is actually developed from the prototype, funding will become a necessity. Climategotchi might consider securing funding by monetizing the App through in-app advertising. There are multiple funding options Climategotchi could choose from, however, in-app advertising model has become the most common way for free mobile applications to create revenue[36]. Therefore, this report assumes that in-app advertisement would be the funding option Climategotchi would choose to proceed with when dealing with the question of funding. Thus, this part focuses on identifying privacy matters that are important to take into consideration within this funding model.

In-app advertisement through third-party ad networks means, in practice, that targeted advertisements channelled from third-party ad network(s) will be displayed to the users on the App (i.e., Climategotchi sells ad space from the App for the purpose of displaying targeted advertisements). For this, Climategotchi will receive payments from the ad network. This app-monetization model means that personal data of the users would be disclosed to third parties (ad networks) for the purpose of targeting the users with advertisements. Information of the users' activity would be collected and processed for this purpose. Therefore, there are many privacy matters related to this funding model and risks for the users' fundamental rights (right to privacy).

2. Data collected with device identification technologies form personal data

In the in-app advertisement model, a third-party ad network serves as a broker between the publisher (e.g., Climategotchi) and advertisers[37]. The ad network collects data by placing cookies which are the primary tool that advertisers use to track users' online activity[38] or other

---

[36] Spaceø Technologies, 2021
[37] iapp 2021
[38] GDPR.eu 2021

similar device identification technologies[39] (collectively hereinafter "cookies") on a user's device for the purpose of displaying specific advertisements.

Cookies are small text files that are placed on the user's device which give insight on the user's activity and preferences. It may be noted that there are different types of cookies, though, this report focuses on so-called "marketing cookies" which collect data about the users' activity. The definition of personal data in GDPR is very broad and data will formulate to be personal data even if the data subject can be indirectly identified[40]. Cookies contain a unique identifier code and therefore data collected by using cookies, if it is enough to identify the data subject, is considered as personal data under GDPR. Generally, cookies, and especially marketing cookies, consist of personal data.

In case C 673/17 ("Planet 49" case) handled by the Court of Justice of the European Union ("CJEU"), CJEU confirmed that if data collected with cookies combined with other data of the data subject it may result to form personal data[41]. If a natural person can be associated with cookie identifiers combined with other unique information received by the servers, it may be used to create profiles of the data subject to identify them[42]. In targeted advertisement, cookies collect data on a user's activity to form a profile of the user so that advertisers are able to display more specific ads to the user. Therefore, if Climategotchi sells ad space from the App and discloses personal data of the users by allowing these ad networks to place third-party marketing cookies on the users' devices for the purpose of collecting and processing personal data, it is a form of processing personal data and falls into the scope of GDPR[43].

3. Obligations under GDPR remain in a joint controllership

A third-party ad network can either be a processor or a controller depending on the activities it performs when processing personal data. If the ad network processes personal data on behalf of the controller (i.e., Climategotchi) it would be deemed as a processor[44]. However, if an ad network determines its own purposes for the processing, it would be deemed as a controller[45]. If Climategotchi and the ad network jointly determine the purposes of processing, they would

---

[39] *For example, Software Development Kits which are commonly referred to as" SDKs"*
[40] Art. 4(1) GDPR
[41] C-673/17 point 45
[42] Recital 30 GDPR
[43] Art. 4(2) GDPR
[44] Art. 4(8) GDPR
[45] Art. 4(7) GDPR

be deemed as joint controllers, and they would have to agree on their respective responsibilities for compliance of the obligations under GDPR[46].

In this case it is most likely that Climategotchi and an ad network act as joint controllers. However, this does not affect the responsibilities Climategotchi has under GDPR and the users may exercise his or her right in respect of and against each of the controllers[47]. In the light of this, it is important that Climategotchi enters into cooperation with a reliable ad network which ensures an adequate level of data protection and complies with GDPR. This report focuses solely on the role Climategotchi has as a controller.

4. In-app advertisement constitutes a new purpose for processing personal data

Processing data by allowing third-party ad networks to track the users' activity on the App for the purpose of targeting users with specific ads, constitutes a new purpose of processing personal data. The principle of purpose limitation requires that personal data of the users are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes[48]. Therefore, for Climategotchi to comply with this obligation, it has to specify the explicit purpose for which the personal data is collected in the aim of securing funding through in-app advertisement by disclosing personal data of the users. The purpose of processing the users' personal data in this case is in-app advertisement by allowing third-party ad networks to place cookies on the devices of users to track the users' activity to then target the same users with specific advertisements.

5. Transparency is important when disclosing personal data to third parties

Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject[49]. If Climategotchi discloses the users' personal data by allowing third-party ad networks to track the user's activity, it is important to be transparent that the users are aware of the tracking, its purposes, and who is receiving personal data of the users and to what purpose. Transparency is emphasized because it can be said that a user would not primarily assume that his or her activity will be tracked for marketing purposes and personal data disclosed to third parties when downloading the Climategotchi App.

---

[46] Art. 26(1) GDPR
[47] Art. 26(3) GDPR.
[48] Art. 5(1)(b) GDPR
[49] Art. 5(1)(a) GDPR

There can be multiple third-party ad networks that receive data, and these data flows may seem to be extremely complex in the eyes of the users when there are various third parties receiving personal data. This significantly increases the risks of the processing of personal data not being transparent enough and that the users are not aware enough of how their personal data is processed. It is important that the data subject is provided with information about how his or her data is processed, to what purposes and by whom. Climategotchi has to ensure that the users receive information on cookies and processing carried out by the ad networks so that the users are not taken by surprise at a later point about the ways in which their personal data have been used[50].

Among other obligations under GDPR, Climategotchi is obliged to provide information to the users when the data is collected from the data subject[51]. GDPR requires that, inter alia, the users are provided with information on the purposes of the processing as well as the legal basis for the processing[52]. Related to the principle of transparency, this information must be easily accessible for the users as well as easy to understand and presented in clear and plain language[53]. GDPR does not require any specific form of how this information is presented to the users, however, the most common way is to include a privacy policy in the App. Climategotchi should provide all this information on the privacy policy, which has to be at any time easily accessible for the users on the App.

When providing information for the users, attention should be given especially in the fact that the use of cookies includes a lot of technicalities which have to be communicated in an understandable way to the users who might not have any previous knowledge of how such technologies work. In addition, it is important to give information about all the third parties that will receive personal data of the users and specify to what purposes the data is processed as well as the respective roles of these third parties, especially when the ad network(s) and Climategotchi act as joint controllers.

---

[50] WP29 Guidelines on transparency, p. 7 point 10
[51] Art. 12(1) GDPR
[52] Art. 13(1)(c) GDPR
[53] Recital 3 GDPR

6. The users' consent must be obtained for advertising purposes

Under the principle of lawfulness personal data has to be processed lawfully in relation to the users[54]. Thus, every processing activity must have some legal basis. Climategotchi may only disclose personal data of the users for advertising purposes if it can base this processing activity with a legal basis under GDPR[55]. The lawfulness of processing personal data may be, inter alia, based on the data subject's consent, necessity for performance of a contract, legitimate interest of the controller, or if the controller is obliged by law to such processing[56].

Advertisement by third parties is not an essential function of the App and is not what the user is requesting by downloading the App and, therefore, consent is the appropriate legal basis for this kind of processing activity[57]. Processing personal data is lawful, if the user has "*given consent to the processing of his or her personal data for one or more specific purposes*"[58]. Thus, Climategotchi is obliged to request consent of the users for this type of processing, and the consent must be obtained prior to any processing activities carried out related to advertising purposes (i.e., before Climategotchi allows any third-party cookies).

Cookies are regulated by Directive 2002/58/EC ("e-privacy directive") which includes a provision that is relevant when complying with GDPR. The e-privacy directive requires that the users' consent is obtained in accordance with GDPR[59]. In the Plane 49 case CJEU stated that the concept of consent referred to in the e-privacy directive has to be read in conjunction with GDPR[60]. The users' consent must therefore meet the requirements for a valid consent under GDPR. As explained in Part II chapter 3. of this report, GDPR sets many requirements for a consent to be considered as valid[61].

Climategotchi's request for a valid consent has to be presented in a manner which is "*clearly distinguishable from the other matters*" (e.g., the general terms and conditions of the App) in an intelligible and easily accessible form by using clear and plain language[62]. The request for

---

[54] Art. 5(1)(a) GDPR
[55] Art 6(1) GDPR
[56] Art 6(1)(a-c)(f) GDPR
[57] EDPB guidelines on consent, p. 6 point 6
[58] Art. 6(1)(a) GDPR
[59] Art. 5(3) e-privacy directive
[60] C-673/17 points 63,65,66,71
[61] Art. 4(11) GDPR
[62] Art. 7(2) GDPR

consent should not be bundled with the acceptance of other terms and conditions of the App[63]. Climategotchi has to ensure that it is clear for the users to what their consent is requested for and that the users have an option to provide or not to provide his or her consent. For the requirement to be "distinguishable", Climategotchi may obtain the consent with a separate declaration and a tick-box function which is not pre-ticked and thus requires the user to actively give his or her consent.

The Planet49 -case confirmed that a pre-ticked checkbox is not considered to create a valid consent[64]. There might be some difficulties from the limited space that a mobile phone screen offers for displaying all this information. For Climategotchi to overcome this difficulty, the information and request for consent may be presented in a layered way[65]. Because the request for consent happens in the App by electronic means, the request has to be clear, concise and not unnecessarily disruptive to the use of the App[66]. Climategotchi must be able to prove that a user has consented to processing of his or her personal data[67] which it is obliged to do as well under the principle of accountability[68].

7." Cookie walls" are prohibited – the user's consent must be freely given

The Norwegian supervisory authority ("Datatilsynet") has given a preliminary conclusion concerning a case where a mobile application ("Grindr") shared personal data of its users with third parties for marketing purposes. Datatilsynet's preliminary conclusion was that consent was the appropriate legal basis for the app to disclose personal data of users but that the consents' Grindr had obtained were not valid. The users were said to be "*forced to accept the privacy policy in its entirety to use the app, and they were not asked specifically if they wanted to consent to the sharing of their data with third parties*"[69]. In the light of this, Climategotchi has to ensure that the users are not forced to consent to such processing and disclosure of their personal data by prohibiting the use of the entire App if such consent is not given. Therefore, the consent should be requested separately when a user is agreeing to, for example, the terms and conditions of the App or to the privacy policy.

---

[63] EDPB guidelines on consent p. 10 point 26
[64] C-673/17 point 65; Resital 32 GDPR
[65] A Commentary, p.350
[66] Recital 32 GDPR
[67] Art.7(1) GDPR
[68] Art. 5(2) GDPR
[69] Grindr -case 2021

The user must have an opportunity to make a genuine choice for accepting or declining the use of cookies. So-called "cookie walls" have been deemed to be unlawful because consent is not deemed to be freely given in this situation and therefore not valid. The users must always have true control over their data and should not be "tricked" into consenting to something a user is not truly aware of. Cookie walls prohibit a data subject to continue using a mobile application without allowing the cookies[70]. The request for a user's consent should not prevent the user from using the App.

It is important for Climategotchi to take in consideration, that the users will always have the right to withdraw a given consent[71]. This makes consent as a legal basis "problematic" in the eyes of the controller as processing is only lawful when there is a valid and active consent of the data subject which may at any time be withdrawn which means that there will no longer be a legal basis for the processing for that specific purpose after the withdrawal. However, withdrawal of a consent does not affect the processing activities that were based on and carried out prior to the withdrawal[72]. Climategotchi is obligated to inform the user of the existence of the right to withdraw his or her consent[73] which may be informed in the privacy policy of the App.

8. Privacy by design and default must be implemented in the development of the App

The users are granted other rights as well under GDPR in addition to the right to withdraw a consent. A user has, for example, the right to access his or her personal data stored by the controller[74] and the controller has to provide a copy of the user's personal data[75]. These rights have to be taken in consideration when actually developing the software for the App. The users may exercise their rights at any time and Climategotchi has to be able to fulfil the requests. Thus, the App should be developed in a way that makes it possible.

Climategotchi has to implement technical and organisational measures which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights

---

[70] EDPB guidelines on consent p.12 point 39
[71] Art. 7(3) GDPR
[72] Art. 7(3) GDPR
[73] Art. 13(2)(c) GDPR
[74] Art. (1) GDPR
[75] Art. 15(3) GDPR

of data subjects[76] which is referred to as "data protection by design". Therefore, the requirements for data protection should be reflected in the design decisions of the App[77]. It makes it easier for Climategotchi to comply with the obligations if these privacy matters are taken into account in the App's development process. For example, data should be encrypted when it is possible[78].

The App includes different functions that, in many ways, invades the users' privacy. For example, tracking a user's geo-location or receiving data about the user's purchase history. Even though atomisation of these functions might make it more convenient for the user to use the App, the default settings of these functions should be on set to protect the users' privacy in the most effective way. This means that the automated tracking should be set off by default which is referred to as "data protection by default"[79].

When installing the App, the default configuration should be set to "*maximum privacy as a default*"[80]. In the App, there are different toggles for different setting, for example, sharing geo-location data. All these toggles should be on default set to not share data automatically and leave it for the user to actively choose to have these functionalities on. The user should have the option deciding whether or not he or she is willing to that type of tracking. The scores of a user should not be "*shared to an indefinite number of natural persons without the user's intervention*"[81]. Therefore, the feature which allows a user to share his or her scores to other users should happen upon the user's active choice.

9. Further development of the App constitutes a new purpose for processing

Mobile apps are developed and improved throughout their lifecycle. Climategotchi might also wish to develop the App based on data about usage of the App. Further development based on usage data would require storing usage data of the users. Improvement and further development of the App constitutes again a new purpose for processing personal data. Thus, this triggers the same kind of privacy issues as third-party marketing cookies. Collecting usage data may happen by using a data analytics tool and Climategotchi has to inform the users the same as

---

[76] Art. 25 (1) GDPR
[77] Datatilsynes, Software development, 5. Design
[78] Art. 32(1)(a) GDPR
[79] Article 25(2) GDPR
[80] Datatilsynes, Software development, 5. Design
[81] Art. 25(2) GDPR

with the cookies.[82] Data analytics tools as well track the user and therefore the same scope of obtaining the users consent applies as well to this purpose.

When processing data for further development of the App, it is important to recognise which data are necessary and which are not. All kinds of data shall not be processed in the aim of further development. Under the principle of data minimisation personal data has to be limited to what is necessary in relation to the purposes for which they are processed[83]. Therefore, Climategotchi has to assess what kind of data is necessary for this purpose and only data limited to what is necessary for further developing the App may be stored for this purpose. Under the principle of storage limitation personal data personal data shall not be stored longer than is necessary in a form where the users can be identified[84]. Therefore, the purpose of further development of the App does not allow Climategotchi to store personal data in perpetuity, and if it is irrelevant to identify the users for the development of the App, the personal data stored should be anonymised so that the data subject cannot be identified.

---

[82] Art. 13(1)(c) GDPR
[83] Art. 5(1)(c) GDPR
[84] Art. 5(1)(e) GDPR

List of sources and abbreviations

Regulations and Directives

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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
  - (GDPR)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
  - (e-Privacy Directive)

Literature

- Docksey, Christopher; Bygrave, Lee A.; Kuner, Christopher; Drechsler, Laura, "The EU General Data Protection Regulation (GDPR) : a commentary", Oxford 2020
  - (A Commentary)

Case law

- C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband v. Planet49 GmbH
  - (C-673/17)

Guidelines

- Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, 29.11.2017 (11.04.2018).
  - (WP29 Guidelines on transparency)
- EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679,* Version 1.1*, 04.05.2020.*
  - (EDPB guidelines on consent)
- EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 08.10.2019

○ (EDPB guidelines on the processing of personal data)

Journal articles

● Datatilsynet, *Intention to issue 10 million fine to Grindr*, 10.05.2021, https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/
    ○ (Grindr-case 2021)
● Datatilsynet, *Software development with Data Protection by Design and by Default*, 28.11.2017, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true
    ○ (Datatilsynes, Software development)
● GDPR.eu, *Cookies, the GDPR, and the ePrivacy Directive*, 19.05.2021, https://gdpr.eu/cookies/
    ○ (GDPR.eu 2021)
● iapp, *Ad Network*, 19.05.2021, https://iapp.org/resources/article/ad-network/
    ○ (iapp 2021)
● Spaceø Technologies, *How Do Free Apps Make Money in 2021? – 11 Proven Strategies*, 01.01.2021, https://www.spaceotechnologies.com/how-do-free-apps-make-money/
    ○ (Spaceø Technologies, 2021)