A GDPR Compliancy Report

on

Climategotchi

Øyvind Brurberg Haugland

Julie Ullerud Lind

JUS294-2-A

Privacy and Data protection - GDPR

SPRING 2021

Words: 8961

TABLE OF CONTENTS

1 Introduction

1.1 About Climategotchi and the Report

Climategotchi is a gamification app created by students from the Department of Information Science and Media Studies at UiB. It is inspired by the game Tamagotchi and provides the user with a personal avatar, shaped as a virtual globe, that encourages the user to undertake weekly climate-friendly challenges. The state of the virtual globe and the score of the user relies on the completion of these challenges. To make the user experience seamless, all the challenges entail digital monitoring of the user's behavior. The very nature of these activities triggers the right to protection of personal data as protected in Article 8 of the Charter of Fundamental Rights ("CFR"), and the right to respect for private life in Article 7 CFR and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom ("ECHR").

When Climategotchi enters the mobile application (app) ecosystem it will be subject to data protection laws that govern the rights to protection of personal data and privacy. The most relevant legal framework is the General Data Protection Regulation (EU) 2016/679 ("GDPR"). For the use of online identifiers, the Directive on privacy and electronic communications (2002/58/EC ("ePrivacy Directive")) has an important provision in Article 5(3).

The principles and obligations stipulated in these legal acts must be embedded into Climategotchi's design, functionality, and privacy policy. The aim of this report is to give guidance on how Climategotchi can develop and launch while being compliant with these data protection laws. The introduction will give a short overview of the relevant rules and how they apply. The introduction will also go through the processing activities the report will focus on and allocation of responsibilities of the different actors involved. The main section will focus on the following three issues. Firstly, how Climategotchi can ensure that their processing activities are lawful and with appropriate legal bases. Secondly, how Climategotchi can comply with the principles in Article 5 and address the data protection issues that may arise. Thirdly, how Climategotchi must comply with key accountability and risk obligations in Chapter IV-V GDPR.

1.2 Data Protection Laws

The GDPR is built on the previous Data Protection Directive (Directive 95/46/EC ("DPD"). The conceptual framework is retained and case-law of The Court of Justice of the European Union (CJEU) under both legal acts are relevant. In addition, opinions, guidelines, recommendations, and best practices from both the Article 29 Working Party and European Data Protection Broad ("EDPB") are relevant for the report. The Art.29 WP was the working party for the entry of the GDPR and the EDPB is an independent European body that ensures consistent application of the Regulation (Article 70(1)). Although these documents are not binding, they are important for the understanding of the GDPR.

The ePrivacy Directive is under review and the proposed Regulation on Privacy and Electronic Communications is now being negotiated in the European Parliament. The proposal contains new provisions relevant to apps.[1] However, this report will analyze Climategotchi under the current ePrivacy Directive.

1.3 Application of the GDPR and the ePrivacy Directive

The application of the GDPR is determined by its material and territorial scope. The material scope is laid down in Article 2, which states in paragraph one that the regulation applies to "processing of personal data wholly or partly by automated means". Thus, the question Climategotchi must ask is whether the app will process any personal data. The concepts of 'processing' and 'personal data' are defined in Article 4. Article 4(1) defines personal data as "any information relating to an identified or identifiable natural person ('data subject')", while Article 4(2) defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data". Because of these broad and technology-neutral definitions, almost every data activity an app provider takes part in are covered by the material scope. This is illustrated in recital 24 of the ePrivacy Directive, which states that "terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere". Subsequently, personal data is not only personal information about the user. It is also information about the user's device and behavior on the app. This may also reveal information about other data subjects, such as the phone number to a friend in the contact list. In other words, the very personal nature of mobile

[1] See Proposal for a Regulation on Privacy and Electronic Communications https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

device usage means that Climategotchi will process a large amount of personal data when it launches its app. These activities will be covered by GDPR's material scope (Article 2(1)). None of the exceptions to GDPR's material scope in Article 2(2) are triggered.

The territorial scope is defined in Article 3. Pursuant to paragraph one the Regulation applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union". As the controller of Climategotchi will be a Norwegian company established in Norway, their processing activities falls within the territorial scope. Furthermore, the Regulation will apply "regardless of whether the processing takes place in the Union or not" (Article 3(1)). This means that the Regulation will apply even if the user of Climategotchi leaves the EEA. The GDPR's would even apply if the company sets up outside the EEA, provided that Climategotchi's "processing activities are related to […] the offering of goods or services" to data subjects in the EEA (Article 3(2)(a)).

The ePrivacy Directive applies to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community" (Article 3). Since Climategotchi is an information society service, they are not subject to the directive. However, Article 5(3) constitute an exception to this and has a broader scope. This article will apply if Climategotchi use any type of tracking technology that entails "the storing of information, or the gaining of access to information already stored" on the mobile device (so called "online identifiers"). Pursuant to recital 30 in the GDPR such online identifiers constitute personal data, and thus, both the GDPR and the ePrivacy Directive applies to this activity.[2]

1.4 Identification of Climategotchi's Processing Activities

The GDPR is meant to be integrated to Climategotchi as a whole. Climategotchi's processing activities determines how this may be done, and how the principles, rights, and obligations in the GDPR applies to the app. Therefore, we find it beneficiary to focus on some selected processing activities.

[2] See to this effect Case C-673/17 (planet49). See also Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, page 11.

The report will focus on the processing activities that is necessary for Climategotchi to function as a gamification app. This includes the processing activities that are needed for the most developed climate-challenges, namely 'biking to work instead of driving' and 'not buying meat at the grocery store'. This gives the following processing of personal data:

- Collecting, storing, and sharing name, photo, and score of completed challenges
- Collecting and analyzing age
- Collecting, storing, and using email
- Collecting and analyzing location data ("*geo tracking"*)
- Collecting and analyzing heart rate
- Collecting and storing workplace
- Collecting and analyzing purchase history from grocery stores through the user's Trumf-membership
- Collecting, storing, and sharing online identifiers, such as IDFA, API, pixels, and SDK

For the sake of simplicity, the listed processing of personal data will be referred to as Climategotchi's *processing activities.* The data subject of these personal data's will be referred to as Climategotchi's *users.*

1.5 The responsibility of Climategotchi's processing activities

1.5.1 Key Actors under the GDPR

A cornerstone of the GDPR is effective identification of relevant actors and allocation of responsibility and liability. This ensures effective protection and implementation of the rights and freedoms of data subjects (recital 29 GDPR). The key actors in this regard are the controller and the processor. The controller is the one who "alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4(7)), while the "processor" is the one who "processes personal data on behalf of the controller" (Article 4(8)). Thus, the main responsibility and liability lay on the controller. In accordance with the principle of accountability (Article 5(2)), the controller must comply with the principles in Article 5(1) and demonstrate such compliance. The controller must also ensure the data subjects rights in Chapter III, as well as complying with all the obligations set out in Chapters IV-V. The processor on the other hand has limited responsibility as it acts on instructions from the controller and in accordance with their data processing agreement (Articles 28(3) and 29).

Consequently, these actors allocate different responsibilities under the GDPR and are crucial to identify before examining the different data protection issues Climategotchi may encounter. However, as Climategotchi still is a prototype without any specific plans for development, this landscape is difficult to map. For the report, we will assume that the creators of Climategotchi are the ones who will set up a company, own the app and have the factual influence over it. If this influence involves determining and controlling the reason and objective behind the processing activities, they would be the "controller" (Article 4(4)). In the following sections Climategotchi will be referred to as both the app and the 'controller'.

Entering the mobile application ecosystem normally entails partnering up with several stakeholders and third-party services. Climategotchi must use an operating system, like Apple iOS or Google Android, and the app must be offered on an app store through a manufactured device. In addition, Climategotchi will have to use third-party services for developing the app and storing all the personal data. Other potential business partners may be analytics and advertising providers, or a social media platform for connecting Climategotchi to a social media account. All these services raise privacy issues concerning the responsibility of the data subject's personal data. In the following section this will shortly be addressed.

1.5.2 Use of Third-Party Services

Two pressing data protection issues arises when using a third-party service. Firstly, Climategotchi must examine if the third-party will take part in Climatgotchi's processing activities as a joint controller or as a processor. Secondly, Climategotchi must address if the service entails any personal data being transferred to countries outside the EEA ("third countries"). The latter will be shortly addressed in section 3.4.

The first issue is crucial to effectively allocate the GDPR's obligations and responsibilities between Climategotchi and their business partner. A joint controllership is established if Climategotchi determines the "purposes and means" of a processing activity "jointly" with one or more entities (Article 26(1)). Pursuant to case-law of the CJEU, a broad and theological approach should be taken to determine this. In the case of Fashion ID, a joint controllership was established between Facebook and a website operator for the website's use of Facebook's 'like' button for marketing purposes.[3] Even though Facebook did not share this

[3] Fashion ID, C-40/17, ECLI:EU:2018:1039

purpose, they both pursued economic interests and jointly decided the means of the processing.[4] It did not matter that the website itself did not access the personal data Facebook processed.[5] Pursuant to this understanding, joint controllership is likely to be established with many of the above-mentioned third-party services. Especially if Climategotchi uses analytics and advertising services, or a social platform for connecting Climategotchi to a social media account. If such joint controllership is established, Climategotchi and their partner would be obliged to "determine their respective responsibilities" in an arrangement (Article 26(1) and this must be made available to the data subject (Article 26(2)). The allocation of responsibility in this agreement must reflect the entities factual degree of presence and influence in the processing operation.[6]

A processor is involved if Climategotchi delegates a processing activity to a third-party and this party "process personal data" on Climategotchi's "behalf" (Article 4(8)). This will most likely apply to the use of cloud services. Here it would be under the responsibility of Climategotchi as a controller to ensure that the partnership is in line with the obligations set out in Article 28. This means that they need to set up a data processing agreement with the cloud-service (Articles 28(3). The processor on the other hand is obliged to act in line with the agreement and on the instructions of Climategotchi (Article 29). If the processor goes beyond this, they will be considered a controller in respect of that processing (Article 28(10)).

-

[4] Ibid, para 80-81
[5] Ibid para 82
[6] Ibid para 70

2 Legal Basis for Climategotchi's Processing Activities

2.1 The Principles of Lawfulness and Purpose Limitation

One of the key principles of the GDPR is the principle of lawfulness, which requires personal data to be "processed lawfully" (Article 5(1)(a)). As a controller, Climategotchi is responsible for compliance with this principle by ensuring that each processing activity listed in section 1.4 are compliant with relevant laws and have a legal basis prior to the processing. Such legal basis is exhaustively regulated in Article 6. If the processing involves special category of data, the processing is forbidden unless one of the exceptions in Article 9(2) applies. For this type of data Articles 6 and 9 are cumulative.[7]

In order to examine what legal basis is the most appropriate for the different processing activities, one must first look at the purpose behind the activities. In line with the principle in Article 5(1)(b), personal data shall be "collected for specified, explicit and legitimate purposes". However, the function of this purpose identification is not only to apply the proper legal basis. It also sets the boundaries for further processing since this is, as a rule, prohibited unless the purpose is compatible with the initial purpose (Articles 5(1)(b) and 6(4)). Furthermore, identifying the purpose is a pre-requisite for assessing the application of the other principles in Article 5 and choosing the appropriate data protection safeguards. The latter will be addressed in section 3 and 4.

2.2 The Purposes of Climategotchi's Processing Activities

Article 5(1)(b) requires personal data to be collected for "specified, explicit and legitimate purposes". Pursuant to the wording, the purpose must be sufficiently identified, clear and unambiguous, and pursue a lawful interest. The latter relates to "all provisions of applicable data protection law".[8] What these conditions requires in practice must be assessed on a case-by-case basis. However, the conditions should be seen in conjunction with the principle's objective, which is to ensure transparency and trust between the data subject and the controller (recital 39).

Consequently, Climategotchi must determine what they want to achieve with each processing activity, and then examine if this satisfies Article 5(1)(b). Examples of purposes that are too

[7] A Commentary, Oxford 2020, page 376 – 377
[8] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 20

vague and unambiguous are “improving users experience”, “marketing” or “IT-security”.[9] However, the level of preciseness depends on the context.

Tablet 1 illustrates how this may be done with the purposes behind the processing activities in section 1.4. Using a tablet like this would also be in line with Climategotchi’s obligation to keep a “record” of “the purposes of the processing” (Article 30(1)(b)).

Tablet 1

Purpose	**Processing Activity**
To create a user account on the app	Colleting and storing name, photo, and email
To verify the eligibility to create an account due to the age limit of 18	Collecting and analyzing age
Keep a record of completed challenges to set and maintain the right state of the virtual globe	Storing scores of completed challenges
To share scores of completed challenges with other users of Climategotchi in the app	Sharing name, score, and photo
Automatically verify that the user bikes to work and completes the “transportation”-challenge	Collecting and analyzing location data Collecting and storing address of workplace
Additional verification that the user biked and not drove to work by revealing the pulse of the user	Collecting and analyzing heart rate
Automatically verify that the user did not purchase meat and completes the “not buying meat”-challenge	Collecting and analyzing purchase history from grocery stores through Trumf-membership
Market and increase engagement in the app by sending updates about new challenges	Collecting, storing and, using email

[9] Ibid. page 52

Use an analytic provider to gain insight in the use, popularity, and usability of the app for improving and optimizing the functioning and design of the app	Collecting, storing, and sharing online identifiers, such as pixels, SDK and API
Use third-party marketing providers to find a target audience, tailor the marketing thereafter and create user engagement in the app	Collecting, storing, and sharing online identifiers, such as IDFA, API, pixels, and SDK

2.3 Legal Basis for Climategotchi's Processing Activities

There are only three legal bases in Article 6(1) the above-mentioned processing activities can rely on, namely consent (Article 6(1)(a), the necessity for the performance of a contract (Article 6(1)(b)), and legitimate interests (Article 6(1)(f)). For the use of online identifiers, Article 5(3) of the ePrivacy Directive states that this is "only allowed on condition that" that the user has given "consent".

Furthermore, Climategotchi must rely on an additional legal basis in Article 9(2) for the use of 'data concerning health'. Here, Climategotchi must first examine what processing of personal data constitute such data and then if any exceptions in Article 9(2) could apply. Health data is defined in Article 4(15) and covers any "personal data related to the physical or mental health of a natural person". Subsequently, Climategotchi's use of heart rate is covered since this data is inherently related to the "physical health" of the user (Article 4(15)). Given the nature of this processing activity, the only possible legal bases are explicit consent in Article 9(2)(a). Purchase history on the other hand is not inherently related to the user's health, but the compilation of the data could reveal food allergies, smoking and drinking habits or similar health issues. According to WP29's guidelines on health, such raw data must be given a closer assessment. One must examine «the character of the data» and the «intended use». Only when this data alone or in combination with other information can say something about the data subject's health, the data is covered by Articles 4(15) and 9(1).[10] Thus, the question is whether the analysis of the purchase history, considering its purpose, will say something about the user's health. In this case, the purpose is to verify that the user completed a challenge by not buying meat. Over time, this will only say something about the user's

[10] WP29 ANNEX - health data in apps and devices in in Directive 95/46/EC

meat-eating habits. The nature of this information has no strong link to the user's health. However, the decisive element here is that the purpose is not related to the health of the user, but the undertaking of a climate-challenge. This does not say anything about the user's health. Consequently, purchase history is not 'data concerning health' (Article 4(15)).

In tablet 2 we provide an overview of what legal bases the different processing activities could rely on. Then we will give a reasoning to the application of each legal bases, as well as how Climategotchi may tackle the different challenges that arise when relying on them.

Tablet 2

Processing activity	**Legal Bases**
Colleting and storing: • name • email • age • scores of completed challenges Collecting, analyzing, and storing: • location data • workplace • purchase history	Necessary for the contract and/or the precontractual relationship (Article 6(1)(b) GDPR)
Collecting and storing: • photo Sharing with other users of Climategotchi: • name • photo	Consent (Article 6(1)(a) GDPR)
Collecting and analyzing: • heart rate	Consent (Articles 6(1)(a) and 9(2)(a) GDPR)
Collecting, storing, and sharing with analytic providers and marketing providers: • Online identifiers	Consent (Article 6(1)(a) GDPR and Article 5(3) of the ePrivacy Directive).
Collecting and using: • email	Legitimate interests (Article 6(1)(f) GDPR)

2.3.1 Performance of a contract with the data subject (Article 6(1)(b) GDPR)

According to Article 6(1)(b) processing is lawful if it is "necessary for the performance of a contract to which the data subject is party" or "in order to take steps at the request of the data subject prior to entering into a contract". Under this legal basis one must first examine if there is a valid contract between the controller and the data subject. The relevant contract in this case would be the service Climategotchi provides to its users; the app itself. This service would be governed in the *terms and conditions.* For the precontractual option in the provision, downloading the app would be the "request of the data subject" (Article 6(1)(b)).

The next step under this legal basis is to examine if the respective processing activity is "necessary" for the performance of the contract. Pursuant to guidelines of the EDPB, the term "necessary" must be interpreted strictly and objective. Climategotchi cannot only base this on what is permitted according to their *terms and conditions*. As stated by the EDPB, the term has an independent meaning in EU law. It must reflect the objectives and principles of data protection law, in particular the fairness principle.[11] Thus, the question is whether Climategotchi could offer their app without processing the personal data. In addition, if the purpose behind the processing could be met with less intrusive means and if the processing corresponds with the users' reasonable expectations.[12] The starting point for the assessment is the purpose of the processing.

The processing of age is a necessary step for entering into the contract with the user, because Cliamtegotchi needs the age in order to verify if the user is eligible for the service. The same applies to the processing of name and email since it is necessary for setting up an account. This would also be necessary for the performance of the service because Climategotchi must ensure that the user gets the correct service (correct personal globe) when they log in. However, collecting the user's picture for the account would not be necessary as Climategotchi would be able to set up an account and provide the service without a profile picture.

Furthermore, storing scores of completed challenges is necessary for the performance of the service, since the core function of the app is to maintain a good status of the virtual globe by

[11] 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 , Page 8
[12] Ibid page 8 and 4.

completing different challenges. The same argument could be applied to the processing of location data, workplace, and purchase history (the data connected to the challenges). However, this requires an in-depth analysis where the out-come depends on how one look at the service Climategotchi provides.[13]

One possibility is to look at the challenges as two different elements in the same service. In this scenario, one could argue that the processing activities is not strictly necessary for the functioning of the app and should rely on consent (Article 6(1)(a)). This is because the app will maintain half of its functionality if the user only undertakes one challenge. And if the user is only interested in one of the challenges, processing connected to the other challenge would be contrary to the user's exceptions. However, the problem with this approach is that Climategotchi risks bundling consent by making parts of the service conditional upon consent (Article 7(4), see section 2.3.2.2). To illustrate, the user would have to consent to geo-tracking in order to take part in the transportation-challenge. This could easily be considered unfair (Article 5(1)(a)) and make the consent invalid because it would not be freely given (Article 4(15) and Article 7(4)).

To avoid the above-mentioned scenario, Climategotchi might take another approach and look at the two challenges as two separate services in the app. In this scenario Climategotchi must let the user decide which challenges they want to undertake and customize the app thereafter. If the user only selects one of the two challenges, Climategotchi will have to leave the other challenge out of the app and process only the data necessary for the selected service. In this way, Climategotchi ensures that the processing activity is strictly necessary for the function of the app and in accordance with the expectations of the user. However, in this scenario, it is very important clearly distinguish the processing of heart rate as this requires “explicit consent” (Article 9(2)(a)). Also, information about this should be provided (Article 13(2)(e)).

2.3.2 Consent as a Legal Basis

Article 6(1)(a) GDPR stipulates that the processing of personal data is lawful if the data subject has given “consent” to the processing. The notion of “consent” is clarified in Article 4(11) and additional obligations are set out in Articles 7 and 8. These conditions also applies

[13] Specifying how the service is offered is a prerequisite for examining the necessity-term. See 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, page 7

to the use of "consent" in both Article 5(3) of the ePrivacy Directive and Article 9(2)(a) GDPR.[14] However, Article 9(2)(a) sets an even higher threshold by requiring "explicit consent".

Consent must be given prior to the processing and its validity must be demonstrated by Climategotchi (Article 7(1)). Thus, the burden of proof lays on Climategotchi. In the following sections we will look at the different conditions Climategotchi must comply with when using consent as a legal basis. Article 8 will not be addressed since the age limit of the app is 18 years old, and thus not "offer[ed] directly" to a child under the age of 13 (Article 8(1) and personopplysningsloven § 5).

2.3.2.1 Specific Consent

The consent must be "specific" (Article 4(11)). The meaning of this becomes clear in Articles 6(1)(a) and Article 9(2)(a), which both states that consent must be given for "one or more specific" purposes. Pursuant to recital 32, this entail that the GDPR requires separate consent for each purpose. However, the EDPB has stated that "consent may cover different operations, as long as these operations serve the same purpose".[15] Once again, the importance of identifying the purpose of each processing activity first becomes clear. This decides how many consents Climategotchi needs to obtain.

2.3.2.2 Freely Given Consent

Article 4(11) further stipulates that the consent must be "freely given". This has several aspects Climategotchi must be aware of. Firstly, Climategotchi must ensure their users "real choice and control".[16] The most important element of this is the right to "withdraw" the "consent at any time" and "as easy" as it was "to give consent" (Article 7(3)). The withdraw must be without detriment (recital 42).

Furthermore, Article 7(4) states that "freely given" means that the "performance of the contract" cannot be "conditional on consent" (unless the processing is caught by Article 6(1)(b)). As already mentioned, Climategotchi cannot bundle the consent by making the

[14] Article 5(3) must be applied in conjunction with the GDPR. See guidelines 05/2020 on consent under Regulation 2016/679, page 6. See also this effect Case C-673/17 (planet49) para 60-65
[15] Ibid. page 14
[16] Guidelines 05/2020 on consent under Regulation 2016/679, page 7. See also recital 42.

functionality of the service conditional on the consent when it isn't necessary. This would be the case if Climategotchi made the completion of the “transportation-challenge” conditional on the use of heart rate. In other words, Climategotchi cannot put inappropriate influence and pressure on the user or mix the consent with the *terms and conditions* of the service. Such consent is presumed not to be freely given (recital 43).

In addition, freely given consent requires that Climategotchi allows their users to choose which processing activities they want to consent to. As stated in recital 32, “when the processing has multiple purposes, consent should be given for all of them”. If the users are presented with an *all or nothing* option, the consent is not freely given.

2.3.2.3 Informed and Unambiguous Consent

The consent must be informed (Article 4(11)). Article 5(3) of the ePrivacy Directive goes even further and states that the “subscriber or user concerned” must be “provided with clear and comprehensive information”. These requirements are built on the principle of transparency (Article 5(1)(a)), and they are crucial for Climategotchi’s users to understand what they are agreeing to, as well as trusting Climategotchi with their personal data.[17] The information that is necessary to provide may be found in Articles 13 and 14.

Furthermore, the consent must be an “unambiguous indication of the data subject's wishes” provided “by a statement or by a clear affirmative action” that “signifies agreement to the processing” (Article 4(11)). In other words, it must be obvious that the user of Climategotchi consents to the processing activity.

How Climategotchi can ensure both sufficient information and unambiguous consent in the app is interconnected. The information must be provided “clearly distinguishable from” Climategotchi’s other matters, such as the *terms and conditions* of the service (Article 7(2) GDPR). We recommend providing this information in a *privacy policy* that is clearly presented next to a box where the data subject must tix “agree” for the different processing activities. A silenced and pre-ticked box cannot be used as it would be unfair and not an affirmative act.[18] To get a balance of sufficiently precise and understandable information, we

[17] Ibid. Page 15
[18] See also recital 32 and Planet49 with regard to online identifers.

recommend providing the information layered and granular. The purpose behind the processing should be given in the box, while the rest should be presented in the *privacy policy.*

2.3.2.4 Explicit Consent

The processing of heart rate is prohibited unless the user of Climategotchi gives "explicit consent" to it (Article 9(2)(a)). The term explicit "refers to the way consent is expressed by the data subject" and sets a high threshold compared to Article 6(1)(a)).[19] This data requires higher protection because "the context of their processing could create significant risks to the fundamental rights and freedoms" (recital 51). Climategotchi will ensure this if they use an electronic form with signature instead of a ticking box.[20]

2.3.3 Legitimate interests (Article 6(1)(f) GDPR).

According to Article 6(1)(f) GDPR the processing is lawful if it is "necessary for the purposes of the legitimate interests pursued" by Climategotchi. However, this provision calls for a balancing test, where the "interests or fundamental rights and freedoms" of Climatgotchi's users cannot override Climategotchi's interests.

If Climategotchi were to use this legal basis, they would have to perform and demonstrate the balancing test. Based on WP29's four sets of criteria, Climategotchi should follow this procedure:[21]

1) Does Climategotchi pursue a "legitimate interest"?
2) What impact does the processing activity have on Climategotchi's user?
3) Has Climategotchi applied any additional safeguards to prevent any undue impact on the data subjects?
4) Are Climategotchi's interests proportional when looking at the impact on Climategotchi's users?

This procedure will be illustrated with the use of email for sending updates on the app. Pursuant to recital 47 GDPR, "direct marketing purposes" could constitute a "legitimate

[19] Guidelines 05/2020 on consent under Regulation 2016/679, page 20
[20] Ibid. Page 21
[21] WP29, «Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC», 2014, page 33

interest". Thus, the question would be if the processing is proportionate when looking at how it impacts the user. In this assessment there are several relevant factors. First, Climategotchi should consider the user's "reasonable expectations […] based on their relationship with" Climategotchi (recital 47 GDPR). Here the user might not expect the way the email is used because it was given in the context of setting up an account. However, the amount of personal data is limited, and the nature of email is not very sensitive. Hence, the impact on the user is not very intrusive. On the contrary, updates about the app could have a positive effect on the user. Consequently, if Climategotchi provides an easy opt-out box in the mail and establish safeguards to make sure the email is not shared with others, they will pass the balancing test and be compliment with Article 6(1)(f).

3 Principles

3.1 The Data Protection Principles in Article 5

Article 5 of the GDPR is a collection of seven principles concerning lawful processing of personal data. The principles are at the very core of the GDPR, as they make up the guiding principles for compliant processing of data. Article 5 is formulated as guidelines that express the spirit in which GDPR is written and is therefore meant to help interpret the remainder of the regulatory regime found in the GDPR. However, the controller is responsible for compliance with the principles and must demonstrate such compliance (Article 5(2)). Infringements are subject to the highest fines under the GDPR (Articles 83(5)(a)).

The principles of lawfulness and purpose limitation was deliberated on in section 2 of the report. In this following section the report will focus on the remaining principles in Article 5. However, the principles of accountability (Article 5(2)), and integrity and confidentiality (Article 5(1)(f)), is closely related to the obligations of the controller in Chapter IV and should be dealt with in-depth in relation to this (section 4). Thus, this section will give an in-depth analysis of the following principles:

- Fairness
- Transparency
- Data minimization
- Accuracy
- Storage limitation

First, the report will shortly go through the principles and how they apply to Climategotchi as both an app and a controller. After, the potential compliance problems with the principles will be dealt with. Hereto, all the relevant principles will be examined together. This is because the principles are intertwined and the measures Climategotchi must implement to address the compliancy problems applies to more than just one principle.

3.1.1 Principle of Transparency and Fairness

The principle of transparency and fairness can be found in Article 5(1)(a). This article states that personal data shall be “processed lawfully, fairly and in a transparent manner in relation to the data subject”.

Fairness in GDPR is fundamentally linked with lawfulness and transparency. A processing activity can be unfair, even though the lawful basis is covered. In short, complying with the "fairness"-principle means that Climategotchi as a controller, cannot obtain or process the data "through unfair means, by deception or without the data subject's knowledge".[22] This applies to the whole life cycle of the processing of personal data. Thus, Climategotchi need to assess whether the obtaining and processing of personal data is fair and reasonably expected to the user, and without causing detriment in an unjustified fashion. In this regard, Climategotchi must pay duly attention to how they retrieve the data from Trumf. This is a potential compliancy problem that will be addressed in section 3.2.2

Transparency is on the other hand centred around being clear and honest with the data subject about every aspect of the processing activities. Central elements of this principle may be found in Chapter III that governs the rights of the data subject, as well as Article 34 that obliges the controller to communicate data breaches to the data subjects. To comply with the latter, Climategotchi must implement safety routines to catch breaches themselves, and by functionality in which the data subject can report issues from within the app. Regarding Chapter III, the report will in the following shortly point out what type of information Climategotchi must give its users pursuant to Article 13 and 14.

Here it should be noted that these articles essentially govern the same information, but the difference is how the personal data is obtained from the data subject. Article 14 governs the information Climategotchi must provide when the user has given the information in the app, while Article 14 governs the information Climategotchi must provide when they obtain the information from Trumf. The first paragraph in both articles sets out minimum information that must be given, while the second paragraph gives some leeway by stating that the information must be given when it is necessary for "fair and transparent processing" (Articles 13(2) and 14(2)). To comply with the transparency-principle, all the information must be given in way that is "easily accessible and easy to understand, and where clear and plain language are used" (recital 39. See also Article 12(1)). This is essential to foster trust, and to make sure that the user is not "taken by surprise at a later point about the ways in which their personal data has been used".[23]

[22] A Commentary, page 314
[23] Article 29 Working Party, "Guidelines on transparency under Regulation 2016/679", page 7

According to the first paragraphs in both Articles 13 and 14, the following listed information must be provided to the user in the *privacy policy*.

- Climategotchi's contact information (the company); where they are located and how to contact them (letters a)
- Contact details to the Norwegian Data Protection Officer (letters b)
- Information about the purposes of the processing and the legal basis, as described in tablet 1 in section 2.2 and tablet 2 in section 2.3 (letters c)
- Regarding the use of the data subjects' email for marketing purposes, Climategotchi must explain the balancing test in short, in particular that they rely on their interest in marketing new services and update their users (letter d)
- If they will use third-party services that transfer data to third countries (see section 4.3), they need to provide information about this, to which country, what transfer tool they rely on (Article 45,46 or 49), as well as reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (letter f).

Furthermore, Climategotchi must be aware of the second paragraphs in both Articles, which lists information that must be provided if it is "necessary to ensure fair and transparent processing". This will be addressed in section 3.2.2.

3.1.2 The Principle of Data Minimization

The principle of data minimization can be found in Article 5(c), where it is stated that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')." The principle is specified in recital 39, which states that "[p]ersonal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means". This must be examined on a case-by-case basis. Essentially it falls under the responsibility of Climategotchie to examine what data, and how much data, is needed to fulfil the intended purposes described in tablet 1. This principle plays a big role in the processing connected to the data needed for the climate-challenges. This will be addressed in sections 3.2.1 and 3.2.2

3.1.3 The Principles of Accuracy and Storage Limitations

These principles may be found in Article 5(d) and (e), where letter d states that personal data shall be “accurate and, where necessary, kept up to date”, and letter e states that 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”.

To comply with principle of accuracy, the most important step Climategotchi must do is to embed into the design and functionality of the app the opportunity for the users to edit or remove their contact information. To comply with the principle of storage limitation, the most important step Climategotchi must do is to implement routines and measures to ensure that the retention period of each personal data is no longer than “necessary” by either deleting the data or anonymize it.

The principle of storage limitation requires Climategotchi to examine what the proper retention period of each data Climategotchi stores is. Here Climategotchi should follow the best practices in the field, but also implement routines that ensures that the personal data is always anonymized or erased when there is no longer a reason to keep personal data. The following two scenarios should be given duly attention:

- The storing of name, photo and email address is no longer “necessary” if the user no longer wants the service and thus do not wish to keep their account. Thus, it should be delated. The age should be deleted as soon as Climategitchi has verified the eligibility to create an account due to the age limit of 18.
- The personal data collected for completing the two challenges should be deleted when the app has verified the completion of a challenge and obtaining a score. Only the score which the user achieved must be stored for a longer period. This is also connected to the principle of data minimization and will be deliberated on in section 3.2.1 and 3.2.2.

3.2 Identifying Compliancy Issues with the Processing Activities

At first glance Article 5 seems like a list of separate principles. But the fact is that all the principles are intertwined with each other. For example, the intent of the principle of accuracy is to make sure no inaccurate data is stored in. This also combines with the principle of minimization; you shall not store more data than you absolutely need to fulfil the purpose.

Hence by deleting, or altering, outdated data that is no longer accurate, you take a step towards complying with both principles at the same time. The same can be said for the principle of storage limitation. The controller must erase or anonymize data that is no longer needed, both reduces risk, amount of data stored, and improves accuracy of the personal data. Thereby the principles of data minimization, accuracy, security all benefit from compliance with the storage limitation principle.

Due to the intertwined nature of the principles the coming review will address all of the principles together in relation to each potential compliancy issue. To identify the different compliancy problems Climategotchi might face, there is a need to look back at the different processing activities shown in section 1.4 of the report. Here, the biggest difficulties arise when dealing with the processing activities related to the two climate-challenges, namely 'commuting by bicycle' and 'not buying meat'. Thus, the focus will be on the issues regarding processing of location data, heart rate and purchase history. These processing activities requires access to potentially large amounts of data, that is in varying degree sensitive. Especially heart rate stands out due to the sensitive nature of the data.

3.2.1 Challenge 1: Commuting by Bicycle

First, we need to assess what the purpose and functionality of the personal data is in relation to this challenge. Here the purpose and functionality of the processing revolve around the user completing the challenge by bicycling instead of taking the car to work. As the app intends to rely on automatic instead of manual input, the need for location data and heart rate-monitoring arises. The very nature of these processing activities in relation to its purpose creates potential compliancy problem with the principle of data minimization, storage limitation and security (integrity and confidentiality). On top of this there is a need for careful consideration regarding transparency in relation to all the potential compliancy issues. This will be examined in the following sections.

Regarding both the principles of data minimization and storage limitation, the first step Climategotchi must do is to examine what personal data is "necessary" to collect, and for how long it is "necessary" to store it, in order to verify the completion of the challenge (Articles 5(1)(c) and (e)).

Due to lack of technical insight, some assumptions must be made. For example, assuming when collecting GPS data from a phone or smart watch, that it is technically possible for

Climategotchi to be scripted in a fashion whereas only the travel speed is collected. Therefore, collecting an entire GPS track with location of start/stop and timestamps that can be used to identify personal information like workplace and home address is unnecessary to fulfil the purpose. By limiting Climategotchi to such a focused collection of GPS data, compliance with data minimization is ensured, as it is the bare minimum needed to fulfil the purpose behind the processing activity. Due to the lack of personalized data suitable for identification, compliance with the principles of storage limitation(anonymization) and security of the data subject will also greatly benefit from such a measure.

There is also a need to limit when and for how long Climategotchi is collecting information about the data subjects speed of travel. A normal feature to find in most apps using GPS is the possibility to choose between, a) whenever the app decides it is useful to fulfil the intended purpose, b) only when the app is in use and open on the device, or c) never. Thus, these options will be deliberated on. In this instance, permanent monitoring in option A does not fulfil any additional purpose over option B, as it simply gives Climategotchi greater means of collecting data it should not possess according to its purpose. Therefore, option B seems like the most fitting option to ensure that the purpose behind the collection is met, while retaining compliance with the principles mentioned in letter b, c, e and f.

Furthermore, Climategotchi intends on using heart rate-monitoring from smart watches as an additional form of verification. Just like with GPS data, there are a few options regarding obtaining this data. Option a) is to track and log the data subjects' heart rate. Option b) would be to use a simple script that confirms whether the subject is physically active or at a resting heart rate, and thereby automatically verify or deny completion of the challenge. Here the purpose will be fulfilled with option b, and since this requires less data and entails processing in a more secure way, this option should be selected due to the data minimization, storage limitation and confidentiality.

By choosing option b regarding both GPS data and heart rate, Climategotchi, bypasses any issues regarding the expanse of what they can collect from the data subject. This is helpful regarding the principle of fairness and transparency. These actions, and limitations, that Climategotchi should put on themselves to avoid the possibility of any form of illicit collection of personal data should also be relayed to the data subject. Clear, concise and honest information about Climategotchi' purpose(s) and actions taken to fulfil those purposes

are vital for the data subject to know both before, and after, entering a contract with Climategotchi. The latter will thus ensure compliance with the principles of fairness and transparency (Article 5(1)(a)).

3.2.2 Challenge 2: Not Buying Meat

Similarly to the first challenge, we first need to assess what personal data Climategotchi needs in relation to this challenge in light of the purpose. Worth noting is that also this challenge relies on automatic gathering and processing of personal data, but this time from a third party, namely Trumf. By cooperating with Trumf, Climategotchi will monitor whether a data subject buys any meat. Hence Climategotchi will need access to the data subjects purchase history in order to fulfill the purpose; completing the challenge.

As with the first challenge, only a small portion of the data actually Trumf processes needs to be relayed to Climategotchi. This poses a potential compliancy issue regarding the principle of data minimization, namely that Climategotchi shall only collect “adequate” amounts of data that is “relevant” and limited to what is “necessary” to fulfil the purpose (Article 5(1)(c)). The most obvious solution would probably be for Climategotchi to gain access to every grocery store receipt that Trumf collects and stores for their shared data subject during the challenge. No matter how simple, such a solution would be a clear violation of the principle of data minimization. A possible solution to this issue is found by using a simple API to access only the necessary data and running a script to decide if meat/animal products have been bought by the data subject. By doing this Climategotchi will restrict itself to only receive the bare minimum of data needed to assess whether the challenge is complete, whilst there is little to no need for any storage of personal data. The only data Climategotchi will possess in such a situation is a simple, automatically created, “yes/no” answer regarding completion of the challenge.

Furthermore, and as already mentioned, obtaining purchase information from a third-party poses a risk to the principle of fairness. Thus, Climategotchi must pay duly account to how they obtain this information, and that this is in line with the users' reasonable exceptions and without detriment in an unjustified fashion. One way of addressing this is providing sufficient information to the user about how Climategotchi accessed the purchase history. In addition to the information described in section 3.1.2, the information should include “which source the personal data originate” and “the period for which the personal data will be stored” (Article

14(2)(a)(f)). This would be necessary to “ensure fair and transparent processing” because it is information the user needs in order to know if they want to undertake the challenge (Article 14(1)).

In conclusion, Climategotchi will need to develop an algorithm that only obtains the bare minimum of what they need – whilst informing the data subject how they will act to fulfil the purpose; in this instance by retrieving limited information about purchase history from Trumf to assess whether the challenge is completed. The data subject shall be informed in which way this process works, and thereby gain knowledge about how anonymized and minimized the process and amount of data really is. By doing this Climategotchi is ensuring compliance with principles of data minimization, storage limitation, accuracy and last but not least, fairness and transparency.

4 Climategotchi's Responsibilities under Chapter IV-V GDPR

4.1 Accountability and Risk Obligations in Chapter IV GDPR

4.2 Transfers of Personal Data to Third Countries according to Chapter V GDPR

As mentioned in section 1.5.2 of the report, a pressing data protection issue with the use of third-part services is the possibility of data being transferred to countries outside the EEA ("third countries"). If Climategotchi uses third-party services that entail personal data being transferred to third countries, they must ensure that this is done in a manner that is compliant with the GDPR. The report will not focus on this in-depth but will shortly highlight what Climategotchi must consider if the data is transferred to third countries.

In accordance with the principle of accountability, the first step Climategotchi must take is to know and get an overview of their data transfers to third countries. Third countries in this regard are countries outside the EEA. The term "transfer of personal data" is not defined in the GDPR, but the CJEU has taken a teleological approach when deliberating on it. Both personal data transferred to another country and personal data accessed from another country are covered.[24] To illustrate, cloud services offered by a company from a third country will be covered even if the company stores the data in the EEA. Thus, all the different third-party services mentioned in section 1.5.1 could entail transfer of personal data to third countries and consequently be subject to the conditions in Chapter V (Article 44 GDPR).

If personal data will be transferred to third countries, Climategotchi must ensure that this is compliant with the relevant provisions in the GDPR prior to transfer. In particular, Climategotchi must rely on one of the transfer tools Chapter V GDPR lists and envisages. The aim of these is to "ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" when transferring the data (Article 44). The first tool is adequacy decisions pursuant to Article 45, where the European Commission gives out decisions that all or parts of a country has adequate level of protection and thus not need specific authorization. Here it should be noted that the CJEU recently ruled that the adequacy decision for the United States of America, *the EU-US Privacy Shield*, is invalid.[25] Thus, transfer to the United States must rely on either the second or third transfer tool. The second

[24] See to this effect, Case C-362/14 (Schrems I)
[25] The Judgment of C-311/18 (Schrems II)

tool may be found in Article 46. This article allows transfer when an adequacy decision has not been issued, if the controller provides "appropriate safeguards" and on the "condition that enforceable data subject rights and effective legal remedies for data subjects are available" (Article 46(1)). The third tool the controller may rely on are derogations from the restrictions set out in Article 49.

For the different types of third-party services mentioned in section 1.5.1, Climategotchi will most likely have to rely on "appropriate safeguards" in Article 46 as the majority of these services are offered by US companies or companies with mother companies in the US. However, relying on one of the listed appropriate safeguards in article 46(2) is not enough. The controller must ensure that the level of protection is effective in practice.[26] This means that the controller must assess if there is "anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards", and accordingly adopt supplementary measures. [27] [28] This has proven to be a resource-intensive and difficult task, leaving the controller with a big risk of being subject to liability and penalty in line with Article 83(5). Thus, we recommend Climategotchi to avoid such international transfer and rely on third party services that either keep the data in the EEA or transfer personal data to countries/areas that are covered by an adequacy decision.

[26] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, page 12
[27] ibid. See also this effect in Judgment in Schrems II, Case C-311/18
[28] ibid page 15

5 List of Legal Sources

5.1 Legal Acts

General Data Protection Regulation 2016: 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 Directive95/46/EC(‘GDPR’)

Privacy and Electronic Communications Directive 2002: 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 (‘ePrivacy Directive’)

5.2 Case-Law of The Court of Justice of the European Union (CJEU)

Judgment in Planet49, C-673/17, ECLI:EU:C:2019:801

Judgment in Fashion ID, C-40/17, ECLI:EU:C:2019:629

Judgment in Schrems I, Case C-362/14, ECLI:EU:C:2015:650

Judgment in Schrems II, Case C-311/18, ECLI:EU:C:2020:559

5.3 European Data Protection Board (‘EDPB’) Documents

EDPB 2019, “Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities”, Adopted on 12 March 2019

EDPB 2019, “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”, Adopted October 2019

EDPB 2019, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, Adopted on 20 October 2020

EDPB 2020, “Guidelines 05/2020 on consent under Regulation 2016/679”, Adopted on 4 May 2020

EDPB 2020, “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, Adopted on 10 November 2020

5.4 Art 29 (WP29) Working Party Documents

WP29 2013, ‘Opinion 3/2013 on Purpose Limitation’ (WP 203, 2 April 2013)

WP29 2014, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’ (WP 217, 9 April 2014)

WP29 ANNEX - “health data in apps and devices in in Directive 95/46/EC”, 5 February 2015

WP29 2016 “Guidelines on transparency under Regulation 2016/679”, 11 april 2018

5.5 European Union Agency for Network and Information Security Documents

Enisa, “Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR”, November 2017

5.6 Literature

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