Datatilsynet

MyHeritage Ltd.

Your reference	Our reference	Date
	20/02231-2	19.08.2021

Order to provide information - Complaint against MyHeritage Ltd - Unclear Privacy Policy

1. Introduction

The Norwegian Data Protection Authority have received a request from Forbrukerrådet (the Norwegian Consumer Council, hereinafter "the NCC") to investigate MyHeritage Ltd. ("MyHeritage"), on the basis of a memorandum provided by Bing Hodneland advokatselskap DA ("Bing Hodneland") from 14 January 2020.[1] The memorandum is based on the information provided through MyHeritage's Privacy Policy, and where applicable, MyHeritage's Terms of Service. The request to investigate MyHeritage pertains to alleged breaches of the General Data Protection Regulation ("GDPR").

According to the memorandum, MyHeritage's documentation does not comply with the information requirements that ensue from Article 5 GDPR, cf. Articles 12, 13 and 14.

In the course of the investigation by the Norwegian Data Protection Authority we have relied on MyHeritage's Privacy Policy[2] (last updated on 17 December 2020); Terms and Conditions[3] (last updated on 18 April 2020); DNA Informed Consent Agreement[4] (last updated 29 May 2020); MyHeritage Privacy Definitions[5], and the Cookie Policy[6].

2. Structure of the order to provide information

The competence of The Norwegian Data Protection Authority to investigate MyHeritage is outlined in chapter 3. A summary of the relevant requirements under GDPR follows below (chapter 4). Excerpts from MyHeritage's documentation, in conjunction with a headline of the relevant information requirement under the GDPR, follow the summary (chapter 5-7). Legal references to Articles in this order refers to GDPR, unless otherwise stated. MyHeritage use

[1] See "MEMORANDUM CONCERNING MYHERITAGE LTDS' TERMS OF USE, PRIVACY POLICY, ETC" (https://fil.forbrukerradet.no/wp-content/uploads/2020/03/20200324-ke-dnatest-memorandum-eng.pdf)
[2] https://www.myheritage.no/privacy-policy
[3] https://www.myheritage.no/terms-and-conditions
[4] https://www.myheritage.com/dna-informed-consent-agreement
[5] https://www.myheritage.no/FP/Company/popup-privacy-definitions.php?dispLang=EN
[6] https://www.myheritage.no/FP/cookie-policy.php

Postal address: P.O. Box 458 Sentrum N-0105 OSLO
Office address: Tollbugt 3
Phone: +47 22 39 69 00
Fax: +47 22 42 23 50
Ent.reg: 974 761 467
Home page: www.datatilsynet.no/en/

both fully capitalized headlines and non-capitalized headlines. These are referred to below as section and heading, respectively.

The information MyHeritage is required to provide is set out in chapter 8.

3. Procedural background

3.1. Ex officio investigation

The request to investigate MyHeritage was not lodged on behalf of a data subject pursuant to Article 77 GDPR. The Norwegian Data Protection Authority have reviewed the request and opened the case *ex officio*.

The *ex officio* investigation is pursuant to Article 57(1)(a), which provides the supervisory authority the task to monitor and enforce the Regulation, as well as Article 58(1)(a) which provides the supervisory authority the investigative powers to order the controller and processor to provide any information it requires for the performance of its tasks.

In order to clarify the issues further and for you to express your views on the matter, we order you to provide us with the information enlisted further below.

3.2. Territorial scope

Article 3(2) prescribes that the Regulation applies to the processing of personal data of data subjects in the European Union by a controller not established in the Union, where the processing activities relates to the offering of goods or services to data subjects in the Union. As the MyHeritage service is available to Norwegian data subjects in Norway, MyHeritage's processing of personal data from Norwegian citizens falls within the territorial scope of the GDPR.

3.3. Competence

According to the MyHeritage privacy policy, the company is headquartered in Israel. MyHeritage is the legal person that determines the purposes and means of the processing of personal data. As such, MyHeritage is the controller for the processing of personal data of EEA data subjects pursuant to Article 4(7).

Based on this, we consider that you do not have any establishments in the EEA. Consequently, there is no 'main establishment' pursuant to Article 4(16), and the processing of personal data in question does not qualify as 'cross-border processing' pursuant to Article 4(23). Therefore, the cooperation mechanism set out in Article 56(1) and Chapter VII Section 1 of the GDPR does not apply. For this reason, the Norwegian Data Protection Authority are competent to perform our tasks under the GDPR in relation to the *ex officio* investigation in accordance with Article 55(1).

4. Legal background

4.1. The responsibility of the controller

The controller is responsible for, and must be able to demonstrate compliance with GDPR, as stated in Article 5(2).

The responsibility of the controller is also regulated in Article 24 and further specified in Article 25. Article 25 specifies in particular the obligation of the controller to implement data protection by design and by default, while Article 24 impose the obligation on the controller to implement technical and organisational measures to ensure that the processing is performed in accordance to the legal framework as set out in the GDPR.

4.2. Lawfulness of processing

According to Article 5(1)(a), personal data must be processed "lawfully, fairly and in a transparent manner in relation to the data subject".

Article 6(1) states that processing shall be lawful only if and to the extent that at least one of the requirements in (a) to (f) applies.

If the controller relies on consent under Article 6(1)(a), Article 4(11) stipulates that consent of the data subject means any *freely given, specific, informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Article 7 sets further conditions for a consent to be valid. In particular, when the consent is given in the context of a written declaration, the request for consent shall be presented in a manner that is clearly distinguished from other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject shall have the right to withdraw the given consent. Withdrawing consent shall be as easy as to give consent, and the right to withdraw consent should be clearly stated prior to giving consent. When assessing whether the consent is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 9 prohibits the processing of special categories of data, unless one of the conditions in Article 9(2) applies. If the processing of personal data falls under Article 9, the controller is required to obtain both a valid legal basis under Article 6 and meet one of the conditions in Article 9(2).

4.3. Transparency

The principle of transparency is one of the fundamental data protection principles.

Information to the data subject, as required under Articles 13 and 14, shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language pursuant to Article 12.

Article 13 sets forth the specific information the controller must provide when data is collected from the data subject. This includes, among others, the identity and contact details of the controller and the controller's representative, if applicable; the purposes of the

processing and the legal basis for the processing; the legitimate interests pursued when relying on Article 6(1)(f); whether the personal data will be transferred out of the EU/EEA, and more.

To ensure fair and transparent processing, the controller shall provide the data subject with the information set out in Article 13(2) at the time of collection. This includes, among others, the retention time of the personal data; the existence of rights such as access to, erasure of, and to object to the processing operation, as well as the right to data portability; the right to withdraw consent; the right to lodge a complaint with a supervisory authority, and more.

Article 14 lists the information the controller shall provide the data subject when the personal data is not obtained from the data subject. In addition to disclosing the same information as noted under Article 13, the controller shall also disclose the categories of personal data and from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

The specific information to be provided is recounted under point **6**.

5. Clarity and availability of the presented information under Article 12

According to the memorandum, MyHeritage does not provide the documentation in accordance with the requirements set out by Article 12.

The memorandum highlights the length of the documentation, complicated language, lack of clarity created by inadequate and non-binding translations, and the documentation's occasionally over-complex and random structure and presentation as an impediment to the data subjects' rights following Article 12.

The use of translated versions of the privacy policy and the terms of use is highlighted as an attempt to bring clarity to the use of the MyHeritage services. As indicated by the memorandum, such tools may in general ease the clarity of the documentation and provide the users with a better understanding of the terms they agree to, and provide better information concerning how MyHeritage make use of their personal data.

However, MyHeritage claims that the translations are not binding on the company. A consequence of this is that the documentation may be less clear, as the end-user will have to double check for discrepancies in the translation and the official English version. To provide sufficient clarity, translations should be of a high quality to provide the end-users with a correct understanding of the terms they agree to and information on how their personal data is being used, so that the end-users can have confidence that they can trust the translation.

The memorandum brings attention to a lack of clarity, due in part to the Terms and Conditions, which includes matters governed by data protection legislation. An example of this is the inclusion of a description of processing activities and the specification of the legal basis. The Article 29 Working Party has explicitly advised against this practice:

> "The requirement that the provision of information to, and communication with, data subjects is done in a "concise and transparent" manner means that data controllers

> should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use."[7]

Similarly, the memorandum refers to the DNA Informed Consent Agreement. The DNA Informed Consent Agreement applies to the sharing of DNA-results with MyHeritage for research purposes.

The DNA Informed Consent Agreement states that participation in DNA-based research is contingent on users reading and accepting MyHeritage's Terms and Conditions. As there are no rules governing which document takes precedence over the other, it is unclear what a consent to the DNA Informed Agreement entails.

The unclear hierarchy between the documents is relevant in all cases where the user is required to navigate between documents with legal effects. According to the memorandum, the Terms and Conditions contains a number of general formulations that expand, restrict or supplement the content of the consent agreement.

The memorandum highlights, among others, that there are several shortcomings or errors in the translation. For example, it is mentioned that the privacy policy use the term "legitim interesse" instead of "berettiget interesse" to describe Article 6(1)(f), as well as "spesielle kategoriske data" as a translation of the term "special categories of personal data", instead of "særlige kategorier av personopplysninger" used in the official Norwegian translation of the GDPR.

Another example provided by the memorandum is the sixth paragraph under the section "**DNA Services**". The paragraph seems to provide MyHeritage with a right of use for the DNA-samples:

> "*By submitting DNA samples to us and/or DNA Results to the Website, you grant us a royalty-free, world-wide license to use your DNA samples, the DNA Results and the resulting DNA Reports, and, solely for purposes of the DNA Genealogy Services, any DNA samples and/or DNA Results you submit for any person from whom you obtained legal authorization as described in this Section and the resulting DNA Reports, to the minimum extent necessary to allow us to provide the Service to you. The license you grant to us is not perpetual, and it is revocable as you are able at any time to delete your DNA Results and DNA Reports permanently from the Website and to have us destroy your DNA samples."*

The right is seemingly limited to the extent necessary for MyHeritage to deliver the service to the end-user, although the reach of the right of use is difficult to ascertain from the provided paragraph. The first paragraph in the same section provides examples of what fall under the DNA Services, but is qualified with "*among others*", and a note that the use of the service is subject to the agreement of the Terms and Conditions and privacy policy.

[7] Guidelines on transparency under Regulation 2016/679, WP260 rev.01, para. 8.

The sixth paragraph also contains a general clause limiting MyHeritage's liability. In the clause, MyHeritage state that the data subject release MyHeritage from "*any and all claims, liens, demands, actions or suits in connection with the DNA testing, DNA samples, DNA Results and/or DNA Reports, including, without limitation* […] *invasion of privacy*". This clause seems to be in breach of Article 82, which provides data subjects with the right to compensation for damage suffered as a result of an infringement of GDPR.

6. Information obligations under Articles 13 and 14

This section will provide a summary of the obligations of the controller to inform and communicate with the data subject concerning the processing of their personal data, including a preliminary evaluation of MyHeritage's fulfilment of these requirements.

MyHeritage presents information to the data subject concerning the processing of their personal data in different ways spanning several documents, as mentioned in the introduction: The Terms and Conditions, Privacy Policy, Cookie Policy, DNA Informed Consent Agreement and MyHeritage Privacy Definitions. MyHeritage considers the Cookie Policy to be *"part of, and incorporated into,"* the Privacy Policy. The Privacy Policy *"should be read in conjunction with the Terms and Conditions"* according to MyHeritage. The DNA Informed Consent Agreement is presumably for the purpose of collecting consent to the processing of personal data, while the Privacy Definitions provides an overview of the available settings in the service, and their status as enabled by default or not.

6.1. The identity and contact details of the controller

Under Articles 13 and 14, the controller shall provide the identity and the contact details of the controller, as well as the contact detail of the data protection officer or representative in the EEA if the controller has one.

MyHeritage's privacy policy provides the company name MyHeritage and the email address privacy@myheritage.com as a point of contact for various privacy-related issues. In addition, the privacy policy mentions the email dpo@myheritage.com at the very end of the document. The privacy policy does not refer to the email address dpo@myheritage.com elsewhere.

The privacy policy does not provide the contact details of a designated representative in the Union pursuant to Article 27.

Based on the information provided in the privacy policy, it does not appear that MyHeritage disclose sufficient information concerning the identity of the controller, such as business address, organisational number or similar supplementary company information.

It appears that MyHeritage does not provide any information relating to an appointed representative pursuant to Article 27. As an Israeli company located outside of the EEA, such information is required under Articles 13 and 14, pursuant to Article 27 cf. Article 3(2).

6.2. Purpose and legal basis for the intended processing of personal data

Under Articles 13 and 14, the controller shall provide the purpose for which the personal data are intended to be processed, as well as the legal basis for the processing.

Information concerning MyHeritage's processing of personal data spans several documents, as mentioned above – primarily the Privacy Policy, but also the Terms and Conditions, DNA Informed Consent Agreement, Cookie Policy and Privacy Definitions - making it difficult to gain an overview of the total scope of processing operations that are carried out.

MyHeritage lists five general purposes for the processing of personal information under the section "HOW DO WE USE YOUR PERSONAL INFORMATION" in the privacy policy. Information about the purposes for processing IP-addresses, click stream data and cookies are specified in a separate section called "COOKIES AND NON-PERSONAL INFORMATION".

More specific examples on how the personal data will be processed can occasionally be found elsewhere, for example in the Terms and Conditions, where MyHeritage state that it reserves the right to update the DNA Health Reports based on new information, data or scientific findings.

The legal grounds for processing personal data is, according to the privacy policy, "*in the majority of cases*" (1) that the data subject consent; (2) that the processing is necessary for the performance of a contract; (3) to comply with a relevant legal obligation that the controller is subject to, or (4) MyHeritage's legitimate commercial interests.

In addition, MyHeritage specifies that an explicit consent is required for processing special categories of data, which includes genetic data. The legal basis is in this case directly connected to a specific processing operation as it is stated that genetic data is processed "*as part of the DNA Services"*.

For the *"majority of cases"* as mentioned above, the legal basis is not connected to a specific processing operation. MyHeritage lists four of the six applicable legal bases found in Article 6 without connecting the legal bases to the specific processing operations. The two remaining legal bases found in Article 6(1)(d) and 6(1)(e) are presumably not suited for the processing operations of MyHeritage.

Information concerning the purpose and legal basis of the intended processing of personal data is presented in a disjointed manner, spanning multiple documents. This presentation hinders the data subject's ability to gain an overview over what personal data is being processed and for which purpose they are being processed.

6.3. <u>The legitimate interests pursued by the controller or by a third party</u>

Under Articles 13 and 14, the controller shall disclose the legitimate interests pursued by the data controller or by a third party if the processing is based on Article 6(1)(f).

The use of Article 6(1)(f) ("legitimate interests") is referred to throughout the document in different manners, such as *"legitimate commercial interests"*, *"legitimate business interests"* and *"legitimate interests"*.

It is not clear from the documentation which processing activity is carried out pursuant to Article 6(1)(f), or which legitimate interests the processing pursues.

It is not clear if the references to different terminology also reflects a difference in the assessment of MyHeritage's legitimate interests in relation to the different processing operations.

The Article 29 Working Party recommends the controller to provide information on the legitimate interests balancing test that is needed to process the personal data according to Article 6(1)(f).[8] If the privacy policy does not provide such information, the Article 29 Working Party stress that the information provided to the data subject should make it clear that the information can be obtained upon request. The Article 29 Working Party highlights that such information is essential for effective transparency cf. Article 12.

This information is not found in the privacy policy, and information about contacting the controller concerning the balancing test could not be located in the privacy policy, except for the email set up for general inquiries – privacy@myheritage.com.

6.4. The recipients or categories of recipients of the personal data

Under Articles 13 and 14, the controller shall disclose information about any recipients or categories of recipients of the personal data.

The definition of "recipients" can be found in Article 4(9) and is defined as "*a natural or legal person (...) to which the personal data are disclosed, whether a third party or not*". The Article 29 Working Party stress that the controller must provide information on the recipients that is most meaningful for data subjects, in light of the principle of fairness. The Article 29 Working Party highlights that this will generally be the named recipients, although grouping the recipients by categories may also be adequate in certain situations.[9]

The privacy policy states that personal and genetic information is processed and stored in the company's data centres in the United States. The third point in the list under the section "WILL MYHERITAGE DISCLOSE ANY OF YOUR PERSONAL INFORMATION TO THIRD PARTIES?" provides information about named recipients of third-party platforms and DNA test shipping companies.

Under the second point in the same section, MyHeritage state that they will disclose the personal information of data subjects "[…] *(b) if required to protect our rights, privacy or reputation, or the property of other users* […]"

The memorandum brings attention to the lack of specification concerning the recipients of the personal data, with the exception of one named third-party ("PWNHealth LLC").

[8] Guidelines on transparency under Regulation 2016/679, WP260 rev.01, see the annex to the guidelines, p. 36
[9] Guidelines on transparency under Regulation 2016/679, WP260 rev.01, see the annex to the guidelines, p. 37

However, the privacy policy of MyHeritage has been updated after the analysis contained in the memorandum to specify the names of main service providers.

It is unclear under which circumstances MyHeritage will disclose a user's information to "*protect our rights, privacy or reputation, or the property of other users"*, as well as the legal basis for such a disclosure.

6.5. Relevant information on the transfer of personal data out of the EU/EEA

Under Articles 13 and 14, the controller shall disclose relevant information on the transfer of personal data out of the EU/EEA. The relevant GDPR article permitting the transfer and the corresponding mechanism should be specificed. Information about the appropriate or suitable safeguards and the means by which to obtain a copy of them should also be provided.

The privacy policy state that the personal data will be processed and stored in the company's data centres in the United States.

The relevant contractual warranties and/or the grounds for transferring the personal data pursuant to Chapter V of the GDPR is not disclosed in MyHeritage's privacy policy. As further elaborated below under 6.8., MyHeritage seems to rely on consent as a mechanism to transfer personal data to data centers located in the United States.

The service permits the transfer of genetic and other health information to all countries where MyHeritage's services are available, as the users may share the information between themselves.

Information concerning the privacy implications of potential transfer of genetic and health information to all countries where MyHeritage's services are available is not explicitly addressed.

It follows from MyHeritage's privacy policy that data subjects can send a written request by email to receive details of the basis on which the personal information is transferred outside of the European Economic Area.

MyHeritage does not disclose which legal basis the transfer of personal data is based on, relying instead on data subjects sending a written request rather than disclosing the information publicly in the privacy policy. In addition, no information concerning the appropriate or suitable safeguards could be located in the privacy policy, apparently in breach of the information requirement under Articles 13 and 14.

6.6. The period of time personal data will be stored

Under Articles 13 and 14, the controller shall provide information about the period of time the personal data will be stored, or the criteria used to determine this period if it is not possible to determine the exact period of time.

The requirement to provide the data subject with information about the period of time the personal data will be stored is connected to the principle of data minimisation under Article

5(1)(c) and storage limitation under Article 5(1)(e). The Article 29 Working Party has stated that it is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing.[10]

MyHeritage state in the privacy policy that personal data will be continuously processed as long as the data subject is a user of the services. MyHeritage also provide information that personal data is retained after the data subject end the use of the service.

MyHeritage does not inform the user of the categories of data processed while the data subject is a user of the service. It is also unclear what personal data is necessary or relevant to process after the use of the services ends. Information on the legal basis of the further processing operation, and which criteria further storage time is based on, is not provided.

6.7. Disclosure of the right to request access to and rectification or erasure of personal data, etc.

Under Articles 13 and 14, the controller is required to disclose the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject, or to object to processing as well as the right to data portability.

MyHeritage provide a section called "DATA SUBJECT RIGHTS". This section covers data subjects in the European Union/European Economic Area, in addition to a wide range of other jurisdictions. The list summarize the rights the data subject "may" have. A statement that these rights "may be subject to certain exemptions" qualifies the list.

There are other references in the privacy policy to the option to review, amend and delete certain personal information, and change certain privacy settings in the service. There are also statements regarding DNA-information, where it is stated that data subjects have a right to have such information deleted.

As mentioned above, it is seemingly not possible for the data subject to get an overview over what personal data is processed and under which legal basis. Accordingly, it is not possible for the data subject to know which data is processed under Article 6(1)(f) for which the data subject can object to the processing of. Similarly, it is not obvious from the privacy policy which personal data falls under the right to data portability. In addition, the recounted rights are qualified in a way which makes it unclear for the data subject which rights applies.

6.8. Withdrawing consent

Under Articles 13 and 14, the controller shall provide information about the existence of the right to withdraw consent at any time. The right to withdraw consent follows from Article 7(3), which provides that consent shall be as easy to withdraw as to give.

Consent is mentioned throughout MyHeritage's documentation, as well as the right to revoke the given consent. Examples of this can be found under the section "LEGAL GROUNDS

[10] Guidelines on transparency under Regulation 2016/679, WP260 rev.01, see the annex to the guidelines, p. 38

FOR THE PROCESSING OF PERSONAL INFORMATION". The third paragraph under the section "DNA Services" in the Terms and Conditions provides MyHeritage permission to perform a wide range of processing operations on DNA samples by virtue of the data subject submitting the samples to MyHeritage.

In addition, the privacy policy state that the data subject consent to personal data being transferred to data centers located in the United States by providing MyHeritage with personal information.

Furthermore, the data subjects are advised to delete their account or contact privacy@myheritage.com to have the account deleted if they do not consent to the privacy policy. The relationship between the privacy policy as fulfilling the obligations under Articles 12, 13 and 14, and MyHeritage's requirement that the data subject consent to the privacy policy is unclear.

The right to withdraw consent is mentioned throughout the privacy policy. Similar to the point made under 6.7., it is unclear what personal data is processed on the basis of consent as a legal basis. As such, it is not clear from the privacy policy how the controller secures the data subject's right to be informed about withdrawing consent when the legal bases are not connected to the specific processing operation.

6.9. The right to lodge a complaint with a supervisory authority

Under Articles 13 and 14, the controller shall provide information about the data subject's right to lodge a complaint with a supervisory authority.

No information about the data subject's right to lodge a complaint with the supervisory authority could be located in the privacy policy.

6.10. Information about whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract

Under Articles 13 and 14, the controller shall provide information whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

As noted in the memorandum, MyHeritage provide a number of references to statutory and contractual requirements to provide personal data. The memorandum did not conclude on this point as it fell outside its mandate.

It is not clear whether or to what extent the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract. In particular, it is uncertain after reading the privacy policy whether MyHeritage relies upon users' acceptance of the Terms and Conditions for the processing of personal information.

6.11. The existence of automated decision-making (profiling) and relevant information

Under Articles 13 and 14, the controller shall provide information on the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Following the privacy policy of MyHeritage, DNA Matching and Smart Matching presumably rely on some form of automatic decision-making and/or profiling. It is not clear from the privacy policy what the legal basis for the processing is, or if MyHeritage deem the processing to fall under Article 22.

Information concerning the functionality of the services are described in the privacy policy, but according to the memorandum the privacy policy lack information concerning the underlying logic of the processing.

6.12. External sources for the collection of personal data about the data subject

Under Article 14, the controller shall disclose the categories of data and from which source the personal data originate from if the personal data is obtained from someone other than the data subject.

The requirement must be read in light of the fairness and transparency principle. This entails that the descriptions of the categories must be precise enough to allow the data subject to understand the data processing.

Closely linked to ensuring the fairness of processing is the requirement to disclose the sources which the personal data originate from. The purpose of this requirement is to allow the data subject to review and potentially challenge the legality of the initial collection.

In the privacy policy it is mentioned that MyHeritage collects information from others than the data subject, for example in public and historical records. The privacy policy does not provide specific information enabling data subjects to assess where the information is collected from.

It is not clear if the information provided to the data subjects is more specific within the service itself in the case where information has been collected from external sources.

7. Collecting explicit consent for the processing of special categories of data

It is clear that a large amount of the processing undergone by MyHeritage pertains to special categories of personal data as covered by Article 9.

The prohibition to process special categories of personal data does not apply if one of the conditions in Article 9(2) is met, for example explicit consent to the processing pursuant to Article 9(2)(a).

MyHeritage's privacy policy indicate that MyHeritage rely on consent for at least some of the processing of special categories of data. One example highlighted in the memorandum is the

DNA Matching service, which facilitate the matching of DNA results between users. According to MyHeritage's privacy policy, the DNA Matching service is enabled by default.

Using default "opt-out" settings for processing operations relying on consent as a legal basis is not likely to be considered a freely given, specific, informed and unambiguous indication of the data subject's wishes pursuant to Article 4(11).

8. Order to provide information

Pursuant to the Norwegian Personal Data Act Section 23 and Article 58(1)(a) GDPR, we have the authority to order the controller to provide any information we require for the performance of our tasks.

On this basis, we require the following information:

Readability

1. How does MyHeritage ensure compliance with the requirements set out in Article 12 GDPR, especially in light of the arguments set out in point 5 and the memorandum?
2. In light of the previous question, please explain how the rights of a data subject relying on the translated documents are secured.
3. Please detail which documents, excluding the privacy policy, that include content with subject matter that fall under GDPR. Please provide your reasoning for incorporating the content into a document other than the privacy policy.
4. Please explain the interplay and hierarchy between the documents relating to data privacy.
5. Please explain how your answer to the previous question is relayed to the data subjects.
6. Please explain why the rights of EEA data subjects are bundled alongside other jurisdictions.
7. Please explain how EU/EEA data subjects receive sufficient information concerning their rights when the sections is qualified with "may", and that the rights "may be subject to certain exemptions".
8. Please explain how data subjects are informed of the collection of personal data from external sources, and how these procedures comply with the requirements set out in Article 14 GDPR.
9. Please explain why MyHeritage provides two different email addresses as a point of contact for data subjects.

Legal bases for processing personal data and related assessments

1. Please demonstrate how MyHeritage collects the *freely given, specific* and *informed* consent of its users in relation to both the processing under Article 6 GDPR, and Article 9 GDPR.
2. Please explain the function of the "opt-out" mechanism as described under headline **7.**, and the relation to the relevant legal basis, e.g. a valid consent.
3. Please explain how MyHeritage ensure that the right to withdraw consent is as easy as to give pursuant to Article 7(3) GDPR, when the privacy policy, for the most part, does not connect the legal bases to specific processing operations.
4. Please explain the processing activites taking place in the DNA Matching and Smart Match services, and the legal basis for them.
5. Please provide MyHeritage's assessment on whether or not the DNA Matching and Smart Matching services is an automated processing pursuant to Article 22.
6. Please explain the legal basis for disclosing information to *"protect our rights, privacy or reputation, or the property of other users"* and what the relevant criteria for such a disclosure is.
7. If MyHeritage rely on the legal basis "necessary for the performance of the contract", please explain what the basis for the contract is, what processing operations the legal basis covers, and how the service cannot be provided without the specific processing taking place.
8. The data subject is advised to delete their account or to contact MyHeritage to have their account deleted if they do not consent to the privacy policy. The role of a privacy policy is usually to provide information to the data subject about the processing of their personal data pursuant to Article 12-14. Please explain how MyHeritage views the function of a consent to the privacy policy, and if appropriate, how it relates to Article 6(1)(a) cf. Article 7.
9. Please explain the function of the data subject's consent to the processing of personal data as set out in MyHeritage's Terms and Conditions.
10. Please explain the reasoning for categorizing IP-addresses, click stream data and cookies in the Cookie Policy as non-personal information, and how and why MyHeritage deem the Cookie policy to be "*part of, and incorporated into*" the privacy policy if the Cookie Policy does not concern personal data.
11. Please attach the assessment carried out with regards to legitimate interests pursuant to Article 6(1)(f), including the purpose of differentiating between *"legitimate commercial interests"*, *"legitimate business interests"* and *"legitimate interests"*.
12. Please attach the record of processing activities pursuant to Article 30 GDPR to your reply.
13. Please attach the Data Protection Impact Assessment pursuant to Article 35 GDPR to your reply. If MyHeritage has not carried out a Data Protection Impact Assessment, please explain the reasoning behind this decision.

Transfers of personal data to third countries

14. If MyHeritage have a representative based in the EEA, in accordance with Article 27, please attach the mandate of the representative, including the date of the appointment.
15. Please explain the legal basis for transferring personal data outside of the EEA, and how this complies with MyHeritage's legal obligations under GDPR. In particular, we ask that you explain the use of the derogations in Article 49 if applicable. Please attach relevant assessments with regards to transfers of personal data pursuant to Chapter V of the GDPR.
16. Please explain why you require the data subject to send a written request to receive details of the basis on which the personal information is transferred outside of the EEA.

You may also provide any other comments you may have in response to the request to investigate.

We kindly ask that you reply to us by **24 September 2021.**

The powers of the supervisory authority
As a supervisory authority, we have investigative and corrective powers pursuant to Article 58. We have, *inter alia*, the power to issue warnings and reprimands to a controller, to impose limitations including a ban on processing and to impose an administrative fine pursuant to Article 83.

The right to not incriminate oneself
In line with the Norwegian Public Administration Act Section 48, we inform you that you may have a right to not answer questions or disclose documents or objects when the answer or such disclosure may subject you to an administrative sanction.

The right to appeal
You may lodge an appeal against the order to provide information in accordance with the Norwegian Public Administration Act Section 14. Note that the right to appeal only applies if you consider that you are not under an obligation or lawfully entitled to provide the information. An appeal must be lodged **within three days** of having received this letter. If we uphold our order, we will send the appeal case to Personvernnemnda, our appeal body.

Your access to case documents
You have a right to acquaint yourself with the documents in the case pursuant to the Norwegian Public Administration Act Section 18, unless Sections 18 to 19 provide otherwise.

Public access
We also want to inform you that as a main rule, all case documents are subject to public access in accordance with the Norwegian Act of Freedom of Information Section 3. If you

claim there is legal basis to partly or entirely exempt your response from the right of public access, please specify which parts and express your arguments on the matter.

If you have any questions, feel free to contact Kristian Bygnes (+47) 22 39 69 63

Kind regards

Jørgen Skorstad
Director, law

Kristian Bygnes
Legal adviser

Berit Bye Rinnan
Legal adviser

This letter has electronic approval and is therefore not signed