23andMe, Inc
February 1, 2016

23andMe takes the protection of your personal data very seriously. That is why we comply with the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework.

What is the U.S.-EU Safe Harbor Framework?

The U.S.-EU Safe Harbor Framework, established in 2000 by the U.S. Department of Commerce in consultation with the European Commission, sets forth a process for transferring EU/EEA residents' personal data to the U.S. Pursuant to this Framework, companies agree to adhere to the seven Safe Harbor Privacy Principles with respect to the personal information they receive. 23andMe has certified that it adheres to the Safe Harbor Framework.

What is the current status of the U.S.-EU Safe Harbor Framework?

On October 6, 2015, the European Court of Justice ruled that the then existing Safe Harbor Framework does not provide a valid legal basis for the transfer of personal data of EU/EEA residents to the United States. Since then the US and European authorities have been actively negotiating a replacement for Safe Harbor, but an agreement has not been reached. Despite this ruling, the U.S. Department of Commerce has advised that it continues to administer the Safe Harbor program until further notice.

What is 23andMe doing in response to the decision by the European Court of Justice to invalidate the U.S.-EU Safe Harbor Framework?

While negotiations continue, we want you to know nothing has changed - we continue to protect the personal data we collect.

- We will continue to comply in full with our Privacy Policy.
- We continue to adhere to the Safe Harbor principles. To view our Safe Harbor certification, click here. If you have concerns about our compliance with the Safe Harbor program, you should contact us.
- We continue to have in place technical and organisational measures that protect the personal data we process against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, that are appropriate to the particular type of data we collect.
- We continue to have in place procedures so that any third party we authorize to have access to the personal data, including processors, respect and maintain the confidentiality and security of the personal data. We minimize as much as possible the personal data to which we allow access. Any contractor of ours is obliged to process the personal data only on our instructions.
- We comply with the Data Processing Principles set out in Annex A (see below) to the European Commission approved Standard Contractual Clauses for data controller to data controller transfers outside the European Economic Area.
- We have no reason to believe there are local laws that would prevent us complying with the commitments set out in this statement and our Privacy Policy. If inquiries or requests are received from any enforcement agencies relating to personal data of our customers, they are always referred directly to our Privacy Officer. To date, we have not released any such information to enforcement authorities.

- We will co-operate in good faith and assist national or local data protection regulators in the countries where we have customers in dealing with any queries they have about our data protection practices.

- Our website, 23andMe.com, and our mobile application, have received TRUSTe's Privacy Seal, signifying that our privacy statement and practices have been reviewed for compliance with their program. You can view this by clicking on the TRUSTe seal.

  If you have any questions about this Statement, please email 23andMe's Privacy Administrator at privacy@23andme.com, or send a letter to:

  Privacy Administrator
  23andMe, Inc
  899 West Evelyn Avenue
  Mountain View
  CA 94041

ANNEX A to the Standard Contractual Clauses for Data Controller to Data Controller Transfers approved by the European Commission

DATA PROCESSING PRINCIPLES

1 Purpose limitation: personal data may be processed and subsequently used or further communicated only for purposes described in the data controller's privacy policy or subsequently authorised by the data subject.

2 Data quality and proportionality: personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3 Transparency: data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4 Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5 Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer and the data subject may always challenge a refusal before the authority.

6 Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data.

7 Data used for marketing purposes: Where data is processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8 Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based

solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject; and

ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to those parties; or

(b) where otherwise provided by the law of the data exporter.