# Face2Gene GDPR Compliance Declaration

## 1. What is Face2Gene?

Face2Gene is a suite of phenotyping applications that facilitates comprehensive and precise genetic evaluations. FDNA, Inc. ("**FDNA**") uses facial analysis, deep learning, and artificial intelligence to transform big data into actionable genomic insights to improve and accelerate diagnostics and therapeutics.

## 2. Background

With the rapid advance of healthcare technologies – such as mobile medical apps and cloud computing – and their increasing integration with social media, personal data[1] protection has become of paramount importance.

The European Union has adopted the EU General Data Protection Regulation 2016/679, known as the General Data Protection Regulation ("**GDPR**"). As a company with EU users, FDNA has taken certain actions and has adopted policies and procedures in order to implement the GDPR to enhance the data protection of the personal data of its EU users.

## 3. Steps implementing GDPR

FDNA has implemented the appropriate safeguards to meet GDPR requirements as part of a corporate commitment to protecting personal data through a strong security and privacy compliance management; for instance:

1. Creating a data mapping inventory mapping all our data flows, differentiating between personal data and non-personal data. We are constantly updating and maintaining this data mapping as a record of our processing activities.
2. Mapping and determining our lawful basis for processing of personal data.
3. Adapting FDNA's Privacy Policy and service Terms of Use in accordance with the GDPR principles, mainly transparency and introducing a privacy notice on our site. Our updated Privacy Policy may be found at: www.face2gene.com/privacy-policy. Our updated Terms of Use may be found at: www.face2gene.com/terms-of-use.
4. Putting in place or updating existing data protection policies, such as an updated Information Security Policy, Data Subject Access Request Policy, Incident Management Procedure, and Retention Policy.
5. Implementing an authentication system that ensures that a person is in fact who he or she claims to be before being allowed access to the application.
6. Creating a system for receiving, tracking, and implementing data subjects' rights requests. Users may request access to their personal data, the account deactivation, deletion of user account, deletion of personal data, etc. Please visit our Privacy Policy for more information.

[1] Personal data under GDPR means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

7. Updating the customer contact processes and implementing communication preference-setting systems.
8. Adjusting security measures to be adequate and appropriate under the GDPR principles to the types of personal data we process. For more information about our information security measures please visit: www.face2gene.com/security-privacy.
9. Putting in place appropriate internal procedures for breach notification; these are detailed in the company SOP (Standard operating procedure) for Incident Response.
10. Updating the backup processes to be aligned to our Retention Policy and GDPR data retention principles.
11. Updating our list of sub-processors and amended our terms of agreement with them to comply with GDPR.
12. Appointing a data protection officer (DPO), which is in charge, globally, to protect the personal data of our users and to align our relevant policies with the GDPR. Our DPO's contact details are as follows: dpo@fdna.com.
13. Designating a representative, who should act on behalf of FDNA and may be addressed by any EU supervisory authority. Our representative's contact details are as follows: [COMPLETE].
14. Conducting regular and periodical risk analysis for its products analyzing software and data security as well as the data protection impact assessment where required under GDPR.
15. Implementing appropriate internal procedures to ensure that the secure processing of personal data is further safeguarded by the general duty on employees, to ensure that data remain confidential.
16. Maintaining a record of processing activities under FDNA's responsibility that contains all of the information required by Art. 30 GDPR.
17. Using "Standard Contract Clauses" (SCC) approved by the EU Commission to ensure compliance with applicable EU data protection and privacy regulations for its EU users.

## 4. Data minimization

Pursuant to the data minimization principle provided for in Art.5.1.(c) GDPR, FDNA does not store health information that allows the identification of a patient, such as name, address, dates and identifying numbers, other than facial photographic images. These images may be uploaded if user has obtained an appropriate informed consent. Facial photographic images uploaded by users of Face2Gene are stored in an encrypted file volume on our servers in Ireland and are not accessible by other users of Face2Gene by default, unless explicitly and actively designated otherwise by the user. An automatic learning algorithm is applied anonymously on all facial photographic images stored in its Face2Gene file volume in order to train and improve the FDNA Technology.

## 5. Questions

If you have any questions about the way we handle your personal data, whether under GDPR or other laws applicable to you, please contact our DPO at dpo@fdna.com.

Last updated: January 1, 2023