GDPR – ISOGG Interim Guidance for DNA Project Administrators

As of 12 March 2018

GDPR - Context of ISOGG Guidance

- This guidance is prepared primarily for the benefit of administrators of DNA projects ("DNA project admins") which have members resident in EU countries.
- Some of the guidance will also be relevant to other DNA project admins, and to private genetic genealogists who manage other databases.
- The guidance is only a summary of the implications of GDPR – the text of the Regulation should be referred to if in doubt, or when action is required.
- The guidance is drafted by lay persons, for lay readers.
- The reliability and adequacy this guidance has not been assessed by a lawyer.
- The guidance may be updated from time to time in response to developments.
- It is prepared in slide format for the benefit of local ISOGG DNA Interest Groups etc.

GDPR 2017 – What is it?

- The General Data Protection Regulation 2017 is a regulation of the European Union (28 countries, including Ireland, Netherlands, Sweden and UK).
- Its primary objective is to protect EU residents against the misuse of their personal data.
- It enters into force on 25 May 2018.
- It does not require national enabling legislation (although there is an even more stringent bill now before the UK Parliament; the eventual Act will apply even after Brexit).
- Its 88 pages comprize 173 recitals (guidance) and 99 articles.
- In this presentation recitals are referenced *superscript* and articles subscript.
- Full text is at http://eur-lex.europa.eu/eli/reg/2016/679/oj

GDPR - Definitions and [possible interpretations]

- **"Personal data"**: any information relating to a "data subject" 4.1 [e.g. a project member]; GDPR doesn't apply to personal data of deceased persons. *27*
- **"Genetic data"**: personal data relating to genetic characteristics, including DNA analysis, *34* which give unique information about project member's health/physiology. 4.13
- **"Pseudonymisation"** [anonymising]: processing of personal data so it can't be attributed to a project member, provided it is "kept separately" [from contact information]. 4.5 *26*
- **"Consent"**: specific, informed, unambiguous, affirmative and revocable consent freely given [by a project member] to processing of their personal data. 4.11
- **"Processing"** includes storage and disclosure of personal data. 4.2
- Processing may be by "**controllers**" 4.7 [e.g. DNA testing companies]; or by "**processors**" 4.8 [e.g. contractors 28.3]; or by "**third parties**", including individuals [e.g. DNA project admins] who are authorized to process personal data under the direct authority of a controller. 4.10
- **"Supervisory authority"**: 4.21 includes national authorities such as Ireland's Data Protection Commission (DPC) and UK's Information Commissioner's Office (ICO).

GDPR - Scope

This issue is dependent on interpretation of definitions:

- GDPR applies to processing of personal data [of EU residents] by a "controller" [e.g. a DNA testing company], regardless of whether processing takes place in the EU or not, 3.1 and regardless of whether the "controller" is "established" in the EU or not. 3.2, 3.3.
- GDPR does not apply to processing personal data [of EU residents] by "a natural person in the course of a purely personal or household activity and thus with no connection to a commercial activity". 2.2c [18]

Note GDPR is silent on its applicability to processing personal data of EU residents by "natural persons", wherever resident, whose activities do have a connection with to a commercial activity [e.g. DNA project admins]. It is also unclear whether GDPR applies to unguarded DNA data [see below], especially if anonymized. However it would clearly be imprudent to rely on these ambiguities.

GDPR - Rights of DNA project members

Under GDPR, DNA project members resident in the EU have several statutory rights:

- Processing of personal data to be lawful, fair, transparent, accurate, relevant & limited;[5] *39, 60*
- "Right to withhold/withdraw consent" for processing personal data for specific purposes;[6, 7] *43*
- "Right to be informed" of personal data held, however it was obtained;[13, 14]
- "Right of access" to their personal data;[15] *59, 63*
- "Right to rectification" of errors or omissions;[16] *65*
- "Right to erasure/to be forgotten", especially if consent is withdrawn;[17] **65, 66**
- "Right to complain" at any time direct to their "supervisory authority";[12.4, 13.2d, 14.2e, 15.1f]
  Note This is additional to de-facto rights to complain to testing company/project admin.
- Technical rights to "restrict processing",[18] "data portability",[20] "object",[21] "automated decision-making" and "profiling".[22]

Most of these rights relate to testing companies, but some may relate to DNA project admins.

GDPR – Obligations

Obligations on "controllers", e.g. testing companies:

- Details are outside the scope of this presentation, but the obligations are onerous;[24] they include record keeping,[30] appointing a "data protection officer",[37] submitting a "code of conduct" for approval by their "supervisory authority",[40] and, if "established" outside the EU, appointing a "representative" in the EU.[4.17, 27] *80*
- Response of Ancestry.com: see www.ancestry.co.uk/cs/legal/privacystatement
- Responses of FTDNA, ISOGG: substantive responses now in hand.

Obligations on "third parties", e.g. DNA project admins:

Surprisingly GDPR is silent on specific obligations on "third parties". But this doesn't prevent a project member complaining direct to a "supervisory authority" about the conduct of their project admin. Clearly DNA project admins should:

- Respect rights of project members.
- Respect conditions of consent given by project members to the testing company.

GDPR – Sanctions for infringements

- **Compensation**: "controllers" are liable for damage suffered.[82]
- **Fines**: "controllers" are liable to fines up to 4% of total worldwide annual turnover.[83]
- **Penalties:** to be "effective, proportionate and dissuasive", e.g. a "Reprimand" where a fine would be "a disproportionate burden on a natural person".[84,] *148*

Note An undesirable contingency is the possibility of even minor or unjustified complaints to "supervisory authorities" that lead to:

- DNA project admins becoming involved in protracted correspondence with officials who are unfamiliar with genetic genealogy and with FTDNA's DNA projects, and/or
- DNA project admins being required to meet ad hoc and even conflicting requirements by different "supervisory authorities", e.g. to submit to an audit, cease processing data.[58.1b, .2f]

Such developments could damage the transnational character of FTDNA's DNA projects.

GDPR – ISOGG Strategy

1. To promote respect for the rights of DNA project members under GDPR.
2. To promote practices by DNA project admins that will minimize risk of GDPR complaints being directed to national “supervisory authorities”.
3. To support DNA testing companies’ adoption of transparent best practices with respect to GDPR that will minimize risk of GDPR complaints, and encourage potential complaints to be directed to them rather than to DNA project admins or to national “supervisory authorities”.

To develop these strategies an ISOGG Study Group is supporting FTDNA’s responses to GDPR in a variety of ways, and has prepared this presentation to assist individual DNA project admins.

GDPR - Action items for DNA Project Admins - Overview

1. List of “Do”s to minimize complaints.

   Example of DNA Project Privacy Statement

2. List of “Don’t”s to minimize complaints.
3. Actions in event of a data request.
4. Actions in event of a data breach.
5. Actions in event of a complaint.

Note Appropriate actions will vary from project to project.

The following recommended actions address DNA projects which have a secondary website but which do not process guarded data (e.g. mtDNA Coding Region results, Factoid results, Population Finder results, BAM data).

Some actions are not relevant to projects without secondary websites.

Additional actions will be appropriate for projects which process guarded data.

GDPR - Action items for Project DNA Admins - 1
"DO"s to minimize risk of complaints

- DO advise members of the personal data you hold, e.g. apart from data they may have volunteered to you by e-mail, the only data you hold is that which appears on the personal data pages of the relevant testing company/ies.
- DO remind members why you hold their personal data – e.g. to meet project goals.
- DO ensure your project's published goals are up-to-date and prioritize data privacy.
- DO use password protection for any databases you hold.
- DO advise members that they should contact their testing company direct to access/update/query/complain about personal data and consent, unless their concerns are only relevant to project administration.
- DO respond to members' queries without undue delay.
- DO encourage members to address any complaints to testing company or project admin.
- DO publish a privacy statement tailored to meet your project's needs – see Example.

GDPR - Example of DNA Project Privacy Statement

that could be posted at https://www.familytreedna.com/groups/xxxxx-dna/about/background

xxxxxxx DNA Project Privacy Statement

As Administrator and Co-administrators of the xxxxxxxx Project we give priority to protecting your privacy and to the confidentiality of your personal data. In particular we will not publish your name, e-mail address or other contact details, or share this information with any other project member or other person or organisation without your specific written approval.

The only personal data we hold is that relevant to meeting the published goals of our Project, and which has been made available to us by DNA testing companies, in the same format as they make it available to you, or which you have given us direct by e-mail or by post.

We hold this data indefinitely or until you request its deletion, and publish anonymized data at least [once a year] on our Project website (www.xxxxxxxxxx) where you may see its current status. You may also request a more updated version direct from the Project Administrator.

We will be pleased to correct any errors in your personal data that you bring to our attention.

At your request at any time we will promptly remove your data from our project files. However we cannot retrieve data that has previously been posted in the public domain.

In our administration of this project we endeavour to comply with the most recent guidance issued by ISOGG (https://isogg.org/wiki/ISOGG_Project_Administrator_Guidelines) and by FTDNA (www.familytreedna.com/learn/project-administration/gap-guidelines-ftdna-projects/), and with the Genetic Genealogy Standards (www.geneticgenealogystandards.com/).

We endeavor to respond promptly to any queries or complaints you may make about our handling of your personal data for this Project. However you should be aware that some of your concerns may be better forwarded direct to the relevant DNA testing company.

[names and e-mail addresses of project admins and co-admins]

GDPR - Action items for DNA Project Admins - 2 "DON'T"s to minimize risk of complaints

- DON'T release the name, e-mail address or other contact details of any project member, or any guarded DNA test results, to other project members or to anyone else without specific written permission.
- DON'T keep contact details and DNA test result data on same file.
- DON'T reproduce FTDNA Matches pages without redacting first names.
- DON'T delay replying to queries by project members by more than a month.
- DON'T retain data on members who have asked to be removed from your project.
- DON'T regard your GDPR precautions as a "one-off": they will need regular review.

Note "Hobbyists" resident in UK are not obliged to register with UK ICO, but it remains prudent for DNA project admins resident in UK to comply with the principles of GDPR.

GDPR - Action items for DNA Project Admins - 3 actions if a data request is received

- Responses should be concise, transparent, intelligible and easily accessible, using clear and plain language. 12.1
- Responses may be in writing, by electronic means, or, if requested, orally. 12.1
- GDPR requires “controllers” to respond to requests “without undue delay”, and within one month of receipt of request. 12.3

Note GDPR is silent on how quickly a “third party” should respond to requests for personal data, but good practice suggests at least that required of controllers.

DNA project admins should seek advice from the relevant testing company if in doubt, or if there is a translation problem.

GDPR - Action items for DNA Project Admins - 4 actions if a data breach occurs

- "Personal data breach" includes accidental loss or unauthorized disclosure of, or access to, personal data that has been stored or transmitted. 4.12
- If a "controller" becomes aware of a "personal data breach", GDPR requires the breach to be reported to the "supervisory authority" without undue delay, preferably within 72 hours of becoming aware of it. 33, *85*
- Reporting is not required if "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

Note GDPR is silent on action if a "third party" commits a data breach, but good practice suggests a DNA project admin should consider reporting the breach to the relevant testing company.

GDPR - Action items for DNA Project Admins - 5 actions if a complaint is received

- Acknowledge all complaints promptly.
- Act to remedy complaint.
- Cease publicising the relevant data until the complaint is resolved.

Note GDPR is primarily concerned about enabling EU residents to complain direct to a "statutory authority", and only makes passing reference to the handling of complaints by a "controller". 47.2h, i

GDPR is silent on action if a "third party" receives a complaint, but good practice suggests a DNA project admin should consider reporting the complaint to the relevant testing company.

GDPR Guidance – Future developments

- While the underlying intent of GDPR is clear, many of its detailed requirements are unclear in the context of genetic genealogy, of what is required of testing companies not resident within the EU, and of the thousands of private volunteers who administer DNA Projects whose membership includes tens of thousands of individuals around the world.

- It is thus likely that this guidance will require updating when FTDNA has clarified its responses to GDPR. This in turn will help clarify the responsibilities of DNA Project Administrators, including those resident in the UK under of the forthcoming UK Data Protection Act 2018.