14th International Conference on Genetic Genealogy, Houston, 23-24 March, 2019

GDPR
and the Project Administrator

by

James M Irvine

Member:

GOONS, ISOGG, OFHS, SGS

ISOGG GDPR Study Group

jamesmirvine@hotmail.co.uk

www.clanirwin-dna.org

Overview

- GDPR
- ISOGG *Interim Guidance for DNA Project Admins*
- use of secondary web sites
- other responses to GDPR
- other laws/codes relevant to Project Admins

What is GDPR?

- GDPR is the European Union's **General Data Protection Regulation** 679, 2016
- entered into force: 25 May 2018
- applies to: 28 European Union nations + EEA (Lichtenstein, Norway, Iceland)
- primary objective: to protect EU residents against the misuse of their personal data
- text has: 88 pages: see http://eur-lex.europa.eu/eli/reg/2016/679/oj
  173 Recitals (guidance) (referenced *superscript*)
  99 Articles (referenced subscript)

GDPR – Rights of individual DNA project members

Under GDPR, all DNA project members resident in the EU now have **seven statutory rights**:

- Processing of personal data must 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- "**Right to be forgotten**", especially if consent is withdrawn;[17] *[65, 66]*
- **"Right to complain direct to their "supervisory authority"** at any time;[12.4, 13.2d, 14.2e, 15.1f, 77]
  NB This is additional to de-facto rights to complain to testing company/project admin.

These rights involve more complex paperwork for members, admins and testing companies.

GDPR terminology

- **"Personal data"**: any information relating to a "data subject" 4.1 e.g. an EU-resident project member;
- **"Genetic data"**: personal data relating to genetic characteristics, including DNA analysis, *34* which give unique information about a project member's physiology or health 4.13
- **"Pseudonymisation"**: non-attributable processing of DNA data, e.g. DNA data identified by kit no. and kept separate (i.e. in different files) from name and contact data 4.5 *26*
- **"Processing"** includes the storage and disclosure of personal data; 4.2 may be by:
  "**controllers**" e.g. DNA testing companies 4.7, or
  "**processors**" e.g. contractors 4.8 28.3, or
  "**third parties"** e.g. DNA Project admins who, under the direct authority of a controller, are authorised to process personal data" 4.10 (FTDNA Group Administrator Terms section 4A)
- **"Consent"**: must be clear, specific, informed, unambiguous, affirmative, revocable and freely given by a project member, to processing of their personal data 4.11
- "**Supervisory authority":** agency in each EU member state responsible for implementing GDPR 4.21

Applicability of GDPR to DNA Project Admins

GDPR applies to the processing of

- personal data of EU residents by "a natural or legal person, public authority, agency or other body" *4*
- personal data of EU residents even **if processing takes place outside the EU**, 3.1 , and even **if the "controller"**, e.g. FTDNA, **is "established" outside the EU** 3.2, 3.3.
- personal data for **research for genealogical purposes** 89.1 *160*
- genetic data, **"in particular DNA"** by any organisation or individual, **without "consent"** 9.2a *34*

However **GDPR does not apply to** the processing of

- personal data by an individual "in the course of a **purely personal** or household **activity**, and thus **with no connection to a commercial activity**" 2.2c *18*
- data held by a not-for-profit body with consent of individuals 9.2d *142*
- personal data of **deceased persons** *27, 160*
- **pseudonymised** personal data for **historical research for genealogical purposes** *4.5, 5*.1b, 9.2j, 25.1 *26, 50, 160*

The interpretation of these terms may vary from project to project and from authority to authority, and may depend on how widely the processed data is disseminated.

Possible categorisation of DNA project admins under GDPR

	Possible category:	Controller	Joint controller	Processor	Third party	GDPR doesn't apply
Definitions	GDPR article / (recital) critical wording	4(7) "determines the purposes & means of processing"	4(7), 26 transparent arrangement required to apportion responsibilities/obligations	4(8), 27, 28, 29 / (81), (95) "on behalf of controller" "governed by a contract" guarantees required	4(10) "**a natural person** or organisation **under the direct authority of a controller** (e.g. FTDNA) or processor, **who is authorised to process data**" (see also FTDNA Administrator Terms section 4A)	2.2(b) / (18) "a purely personal activity with no connection to a commercial activity" 5.1(b), 9.2(j), 89.1, (160) "pseudonymised data for historical research for genealogical purposes
Issues	Acceptability to superisory authorities and to FTDNA	(clearly the role of the relevant testing company)	FTDNA would be most unlikely to to consider either concept to be acceptable		interpretation by supervisory authorities is likely to remain unclear; likely to vary from project to project	
Responsibilities & obligations	Summary	too onerous for most conscientious admins to accept	admins would be in a weak position to negotiate acceptable terms in the "arrangement"	too onerous for most admins to accept	minimal	minimal
	Territorial scope	3	) all	3	-	-
	Processing lawful, fair, transparent	5.1	) controller	5.1	5.1	5.1
	accountability	5.2	) roles	-	-	-
	"legitimate interest" in lieu of consent	*6.1f*	) would	-	*6.1f*	-
	conditions for consent	7	) need	-	-	-
	Processing of special categories	9	) to	9	9	9
	Rights of data subjects	12-23	) be	23	-	-
	Obligations of controller & processor	24-31	26) apportioned	28, 29	29	29
	Security of processing	32	) between	32	-	-
	Reporting security breach	33, 34	) FTDNA	33	-	-
	Data protection impact assessment	35, 36	) and	-	-	-
	Data Protection officer	37-39	) project	37-39	-	-
	Liability to judicial remedy under GDPR	79	) admins	79	-	-
	Liability to compensation under GDPR	82	) in	82	-	-
	Liability to fines under GDPR	83	) detailed	83	-	-
	Liability to penalties	84	) arrangement	84	84, (148)	84, (148)

GDPR – Sanctions for infringements, e.g. if a supervisory authority upholds a complaint

- **Compensation**: "controllers" liable for damage suffered [82]
- **Fines**: " " to fines up to 4% of total worldwide annual turnover [83]
- **Penalties:** if a fine on an individual would be "a disproportionate burden", a **reprimand** or **corrective order** must be "effective, proportionate and dissuasive" [84, *148*]

Note

1. Supervisory authorities unlikely to be pro-active on genetic genealogy.
2. In UK the ICO is stressing the benefits of "soft" enforcement.
3. After 10 months I am unaware of any complaint against a project admin.
4. A formal complaint to a supervisory authority could still lead to a project admin being:
   - involved in extended exchanges with officials unfamiliar with genetic genealogy or FTDNA
   - required to meet ad hoc, even conflicting, sanctions by different supervisory authorities.
5. Some DNA project admins in US are apprehensive of civil actions.

Such developments would damage the traditional character of FTDNA's DNA projects.

Responses to GDPR by ISOGG

1. **For ISOGG itself**: to sanitise the ISOGG websites (ably implemented by Tom Hutchinson)

2. **For testing companies**: to encourage their adoption of practices relating to GDPR that
   - minimize risk of GDPR complaints, and
   - encourage potential complaints to be directed to the company rather than to project administrators or to national “supervisory authorities”.

3. **For individual project members**: to respect for their rights under GDPR.

4. **For Project Admins**: to develop, publish and promote a code of practice that
   - respects the spirit of GDPR but minimizes unnecessary workload, and
   - minimizes the risk of GDPR complaints being directed to “supervisory authorities”.

ISOGG's
Interim Guidance on GDPR for Project Admins

- prepared by an ISOGG Study Group
- published in March 2018 at www.isogg.org/wiki/General_Data_Protection_Regulation
- aimed primarily at DNA project admins with members resident in EU countries;
- based on a moderately precautionary interpretation of many grey areas; e.g.
  draws on the "third party" interpretation: "good practice" rather than "best practice"
- only a summary of the perceived implications of GDPR –
  if in doubt or if action is required, refer to the text of the Regulation;
- drafted for lay readers, by lay persons, not by lawyers;
- endorsed by FTDNA;
- has now been on-line for 12 months without significant criticism.

ISOGG *Interim Guidance for DNA Project Admins*

–

Overview of Action items

1. List of “Don’t”s to minimise complaints.
2. List of “Do”s to minimise complaints.
3. A pro-forma Project Privacy Statement.
4. Actions in event of a data request.
5. Actions in event of a data breach.
6. Actions in event of a complaint.

NB Appropriate actions will vary from project to project.

Additional actions are needed for DNA projects which

(a) have a secondary, public website,

(b) process data on living persons other than that supplied by testing company, or

(c) process “guarded data” (i.e. mtDNA Coding Region results, Factoid results, Population Finder results, BAM data).

GDPR – Action items for DNA Project Admins – 1

"DON'T"s to minimise risk of complaints

- DON'T release 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 consent (NB: e-mail addresses may be released to "Matches").
- DON'T keep contact details and DNA test result data on the same computer file.
- DON'T make public any personal data without specific consent of relevant member.
- DON'T reproduce FTDNA Matches pages without redacting first names.
- DON'T ignore member's queries, or delay replies 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.

GDPR – Action items for DNA Project Admins – 2

"DO"s to minimise risk of complaints

- DO advise members what personal data you hold – e.g. the only data you hold is that which appears on the personal pages of the relevant testing company/ies, plus any data they may have volunteered to you direct.
- DO advise members why you hold their personal data – e.g. "to achieve 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 remind members to address any complaints to testing company or project admin.
- DO **publish a privacy statement tailored to meet your project's activities**.

Example of a DNA Project Privacy Statement

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

xxxxxxxx DNA Project Privacy Statement

We the undersigned give you, as a member of this Project, priority to protecting your privacy and the confidentiality of your personal data.

What personal data about you do we hold or have access to? The only personal data about you that we hold or have access to is data that has been made available to us by DNA testing companies with your consent (to the access level you have chosen), and additional data that you may have given us direct by e-mail or by post. All personal data held in our files is password protected. Your contact information is stored in a separate file from your DNA test data. Your DNA test data is pseudonymized by use of your test kit number in lieu of your name. You may request an updated version of your personal data at any time.

What use do we make of your personal data? The only use we make of this data is that relevant to achieving the Goals of our Project as stated in our public website at [www.xxxxxxx]. 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 (apart from your "Matches") or organization without your specific consent unless we are legally obliged to do so. Nor will we share or publish your DNA test results except in pseudonymized form.

[Only applicable to Projects with secondary website:] We update our Project website every [xxx] months. We do not use cookies to collect personal data of visitors to this website.

For how long do we hold your personal data? We hold this data for as long as you remain a member of our Project. If you wish to withdraw from our Project you should advise us and FTDNA. You may make such a request at any time, and we will remove your data from our project files as quickly as practicable. 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 European Union's General Data Protection Regulation 2016 and with the most recent editions of FTDNA's Terms (www.familytreedna.com/legal), of the Genetic Genealogy Standards (www.geneticgenealogystandards.com/), and of ISOGG's guidance (www.isogg.org/wiki/ISOGG_Project_Administrator_Guidance).

We endeavour to respond promptly to any queries, errors, or concerns you may bring to our attention about our handling of your personal data associated with this Project. However you should be aware that some of your concerns may be better forwarded direct to the relevant DNA testing company.

[date] [name] Project Administrator [e-mail address] [name[s]] Co-administrator[s] [e-mail address[es]

GDPR – Action items for DNA Project Admins – 4, 5, 6

Actions by project admin in event of:	**complaint**	**data request**	**data breach**
Recommended in ISOGG Guidance if deemed a "**third party**":	*acknowledge* *rectify*	*acknowledge* *respond*	*acknowledge* *rectify*
	consider advising testing company		
Additional requirement of GDPR if deemed a "**controller**":	-	*respond* *within 1 month*	*report to* *supervisory authority* *within 72 hours**

*: reporting not required if breach is unlikely to result in a risk to the rights and freedoms of individuals.

The processing of a complaint by a project member to a GDPR Supervisory Authority about the conduct of a project administrator

- Various circumstances may arise:

Project member resident in:		EU country A	USA
Project admin. resident in:	EU country A:	) Supervisory	) GDPR
"	EU country B:	) Authority	) not directly
"	USA:	) in country A	) applicable

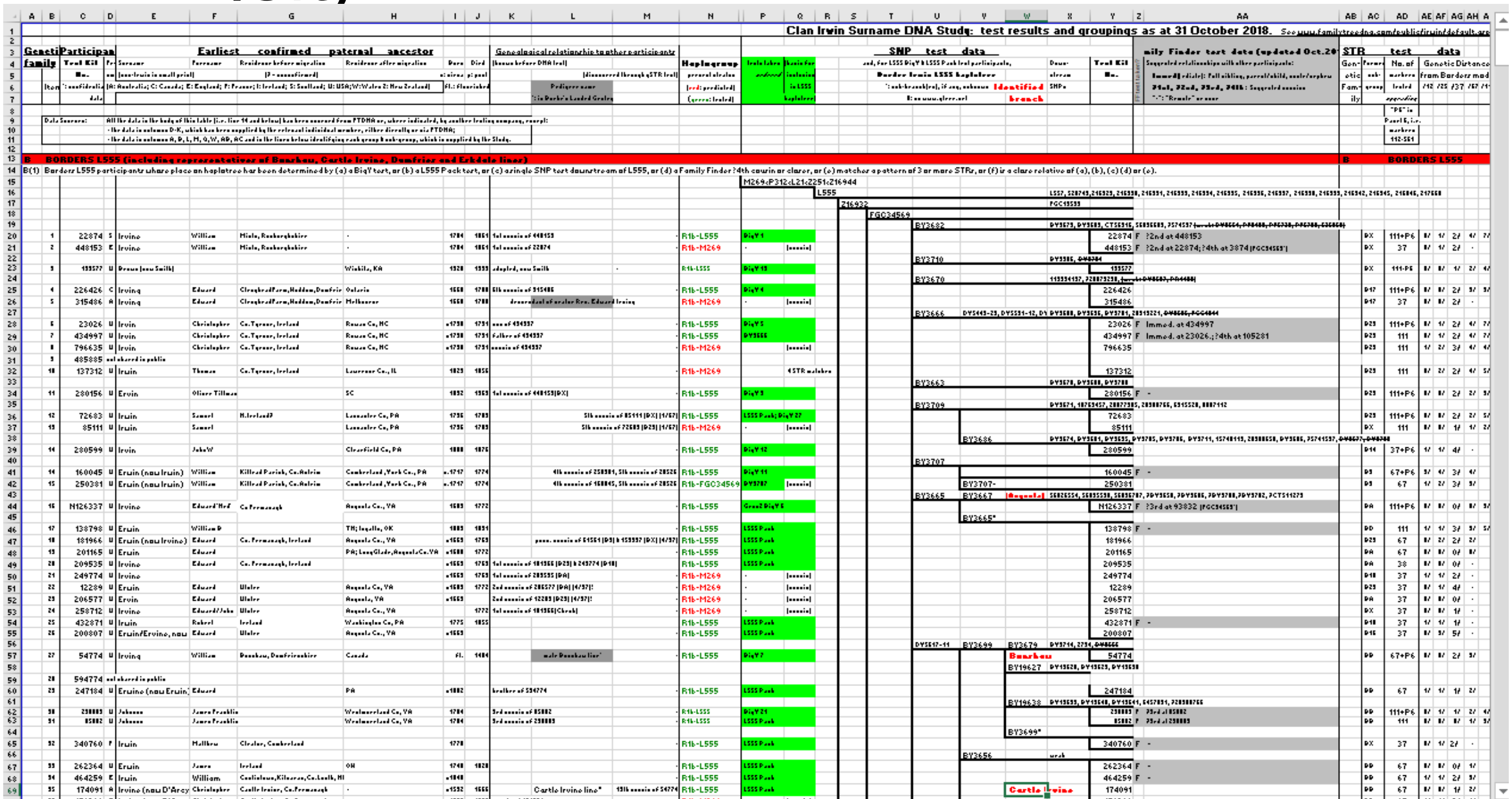
i.e. it is the place of residence of the complaining member that matters, not the place of residence of the project administrator.

Note If the complaint is against FTDNA (as opposed to a project admin), the complaint may be referred to the supervisory authority of the country of FTDNA's legal representative in Europe.

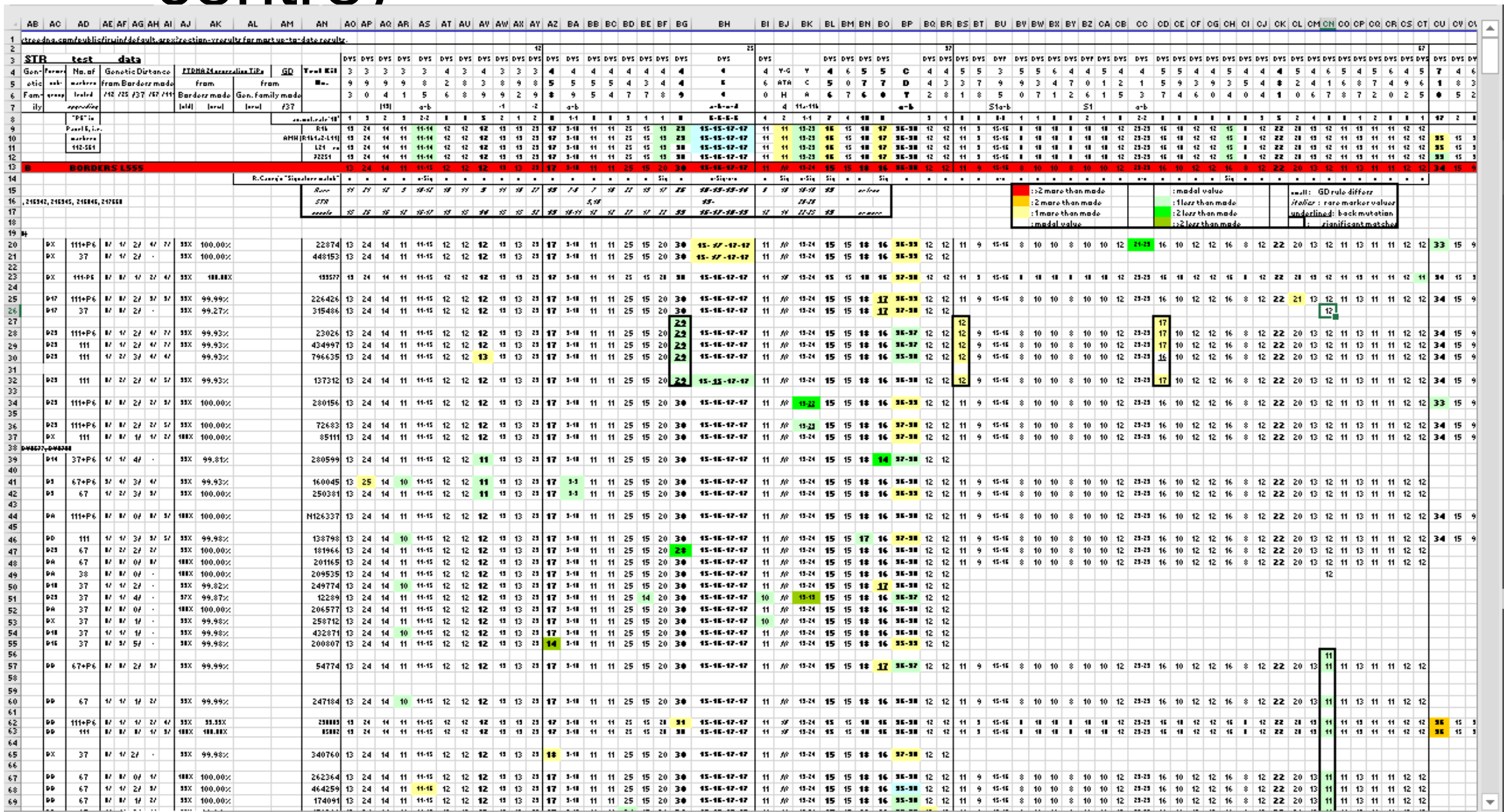
Use of "Secondary" DNA Project websites

- Cautions: - keep test data and members' e-mail addresses in different files
  - only show members who **"Opt in to sharing"** in public version
  - clarify cookie policy, e.g. "Admins do not make use of cookies"
  - use "cut & paste" from FTDNA public pages to avoid transcription errors
- Disadvantages: - labour intensive
  - needs regular updating
- Advantages: - spreadsheets very flexible, no need for Excel skills
  - ability to add more data e.g. modal GDs, 112->500 STR markers, SNP data, genealogical & FF relationships, non-FTDNA data
  - ability to use own fonts, colorizing, and sequencing of entries
  - gives better insight into project to admin, members & prospective members
  - helps stimulate project growth

Irwin Project website (top left)



Irwin Project website (top centre)



Irwin Project website (middle centre)

Additional protection of project member privacy

Possible **additional pro-active protection measures** include:

by individual project members:

- not using “Share in public” option
- using “Minimum access to project admins” option
- not using kit no. as password
- using false name, initials only etc.
- sheltering behind e-mail address of project admin
- not using GEDCOM or GEDmatch

by project admins:

- not sharing e-mail addresses, even with “Matches”
- not publishing any test results on public website

Responses to GDPR by national authorities

- Germany: - BDSG, more complex and stringent than GDPR, entered into force in 2017;
  - implementation is by the Federal Ministry of Internal Affairs;
  - additional legislation by individual states is anticipated.
- Ireland: - Data Protection Act (DPA) 2018 entered into force 25 May 2018;
  - implementation is by the Data Protection Commission ("DPC").
- UK: - Data Protection Act (DPA) 2018 entered into force 25 May 2018;
  - DPA will still apply after Brexit;
  - DPA is > twice as long as GDPR (tho' no more stringent for genetic genealogy);
  - implementation is by the Information Commissioner's Office ("ICO");
  - ICO website (www.ico.org.uk) stresses a "carrot and stick" approach and encourages proactive responses to GDPR.
- USA: - legislation along lines of GDPR enacted in California (CCPA), Colorado & Hawaii;
  - federal legislation is under consideration.

Responses to GDPR by wider DNA community

GDPR has had some pretty devastating effects on the genetic genealogy community with the loss of the WorldFamilies.net website (and all the Surname Projects hosted there), the closure of genetic databases (Ysearch, mitoSearch), and the barring by companies such as Full Genomes Corporation and scientific journals (e.g. SurnameDNA journal) of EU residents from accessing their products. (Gleeson, 2018)

Response by Ancestry.com: Privacy Policy launched 14 Dec. 2017, updated 30 May 2018
see www.ancestry.co.uk/cs/legal/privacystatement

Response by FTDNA: Privacy Policy launched 23 May 2018, updated Sept., March 2019
see https://www.familytreedna.com/legal

Response by My Heritage: Privacy Policy launched 24 May 2018, updated 11 Oct.

Response by DNAGEDCOM: Privacy Policy updated 23 May 2018

Response by GEDmatch: Privacy Policy updated 20 May 2018

Other laws / codes

currently relevant to Project Admins

Genetic Genealogy Standards

- A 3-page Code of Practice published in January 2015 by a committee of 12 US experts to provide ethical and usage standards for the genealogical community to follow when purchasing, recommending, sharing, or writing about the results of DNA testing for ancestry.

  See http://www.geneticgenealogystandards.com/

- The Standards are now invoked by the ISOGG Interim Guidance on GDPR, and were incorporated in FTDNA's Privacy Statement.

UNCTAD Data Protection Regulations, 2016

(for governments and companies)

1. Organizations must be **open** about their personal data practices.
2. Collection of personal data must be limited, lawful & fair, usually with **consent**.
3. The purpose of collection must be **specified** at the time of collection.
4. Use or disclosure must be **limited** to specific purposes.
5. Personal data must be subject to appropriate **security** safeguards.
6. Personal data **quality**: must be relevant, accurate and up-to-date.
7. Data subjects must have rights to **access** and **correct** their personal data.
8. Data controllers must be **accountable** for compliance with these principles.

Future of Privacy Forum (FPF)

- FPF is a not-for-profit think-tank and advocacy group based in Washington DC.
- Membership: academics, consumer advocates and corporations including 23andMe, Ancestry, Amazon, Apple, Facebook, FTDNA, Google & Microsoft.
- FPF focuses on issues data privacy issues; it seeks to explore the challenges posed by technological innovation and develop privacy protections, ethical norms and workable business practices.
- FPF published *Best Practices for Consumer Genetic Testing Services* in July 2018; excellent 19-page document interpreting GDPR and US Federal law; https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf

FPF's *Best Practices for Consumer Genetic Testing Services* (2018)

Two examples:

- **Prohibited Sharing:** *Genetic Data, by definition linked to an identifiable person, should not be disclosed or made accessible to third parties, in particular, employers, insurance companies, educational institutions, or government agencies, except as required by law or with the separate express consent of the person concerned.* (III b)

- **Deletion** ("the right to be forgotten"):

  For Consumers who have agreed to an informed consent for research, companies may not be able to delete or remove their Genetic Data from … published results and findings.

  *If deletion is requested … Companies should remove **or restrict access** to Genetic Data when deletion is not possible due to legal or technological requirements or other limitations.* (IV d)

ISOGG *Interim Guidance on GDPR* – Future developments

Near future:

- Await forthcoming UK ICO newsletter on "DNA & pseudonymisation"
- Publish updated Guidance
- Seek FTDNA approval of updated Guidance.

Ongoing:

- Monitor supervisory authorities developments concerning GDPR
- Keep ISOGG Guidance updated as example of good practice, e.g. when/if CCPA/US Federal equivalent becomes law.

Summary

- GDPR has increased workload and damaged the genetic genealogy community.
- GDPR seems unlikely to be the devil that some have feared.
- ISOGG's *Interim Guidance* is standing up well.
- All project admins should publish a Privacy Statement.
- US Federal legislation likely.