Stop privacy panic:
The new EU rules explained for tax professionals

General Data Protection Regulation (GDPR)
EU Regulation 2016/679

April 19, 2018

EDWARD HENDRICKX
Partner
EJP 's–Hertogenbosch
+31 73 850 72 80
edwardhendrickx@ejp.nl
www.ejp.nl

ANDRE GROENEVELD
Manager Accountancy
EJP 's–Hertogenbosch
+31 73 850 72 80
andregroeneveld@ejp.nl
www.ejp.nl

"Everyone has the right to the protection of personal data concerning him or her."

- Charter of Fundamental Rights of the European Union

What is GDPR?

EU regulation (2016/679) which binds all EU member countries

Effective as of May 25, 2018

Protects

- Personal data
  of natural persons
  processed wholly or partly
  by automated means or by other means

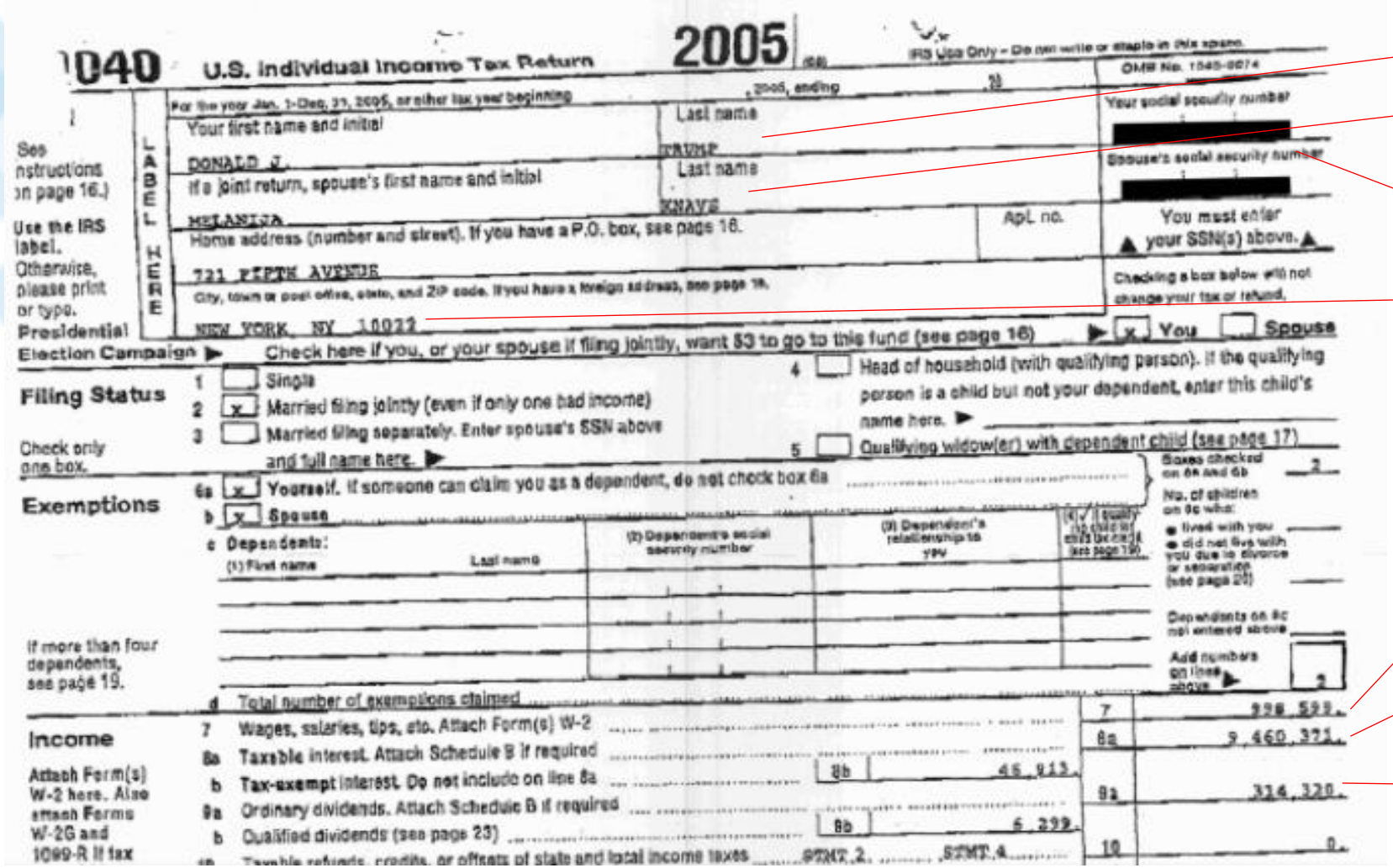
Do you process personal data?

Your own files
- Employees
- UBOs
- Business contacts; lawyers, accountants, notaries, GGI, etc.

Clients
- Name, contact details, birthday, copy of identification document, tax identification number etc.
- Personal income taxes
- UBO registrations (GDPR vs 4th Anti Money Laundering Directive, AMLD4 2015/849)
- Etc.

Others
- Employees of clients (wage taxes, etc.)
- Spouses / children of clients (estate planning, etc.)

Personal income taxes



1040 U.S. Individual Income Tax Return 2005

Your first name and initial: DONALD J.
Last name: TRUMP
If a joint return, spouse's first name and initial: MELANIJA
Last name: KNAVS
Home address (number and street): 721 FIFTH AVENUE
City, town or post office, state, and ZIP code: NEW YORK, NY 10022

Filing Status
2 [x] Married filing jointly (even if only one had income)

Exemptions
6a [x] Yourself
b [x] Spouse

Income
7 Wages, salaries, tips, etc. 998,599.
8a Taxable interest 9,460,371.
b Tax-exempt interest 46,913
9a Ordinary dividends 314,320.
b Qualified dividends 6,299
10 0.

Name
Spouse
Social security nr.
Address
Salary
Interest
Dividend
Etc. etc. etc.

https://www.nytimes.com/interactive/2017/03/14/us/politics/document-Donald-Trump-2005-Tax.html

Rights of natural persons

Right to review th ile
- Name: Donald Tru
- Birthday: June 14,

Right of correctio
- Name: Donald Tru
- Birthday: June 14, 1946

Right of restriction
- Name: Donald Trump
- Birthday: Ju

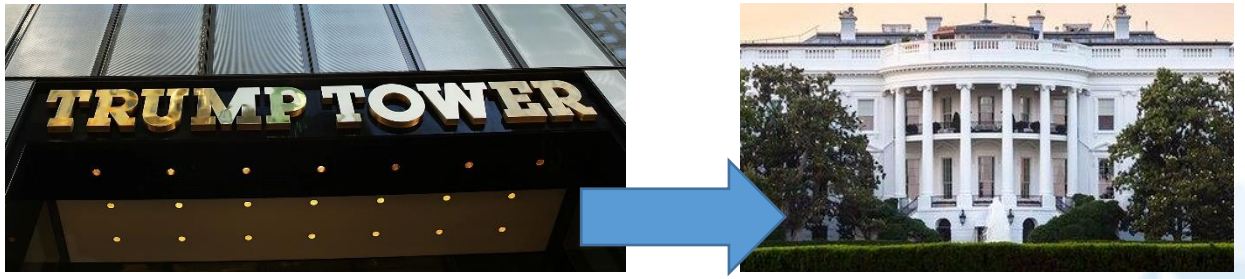
Right to be forgotten
- Name: deleted
- Birthday: deleted

Exception: files can be saved for local (tax)law compliance

Right of human review ("computer says no")

```
System output
- Today: April 19, 2018
- Name: Donald Trump
- Birthday: June 14, 1946
- Analysis: Donald Trump is 71 years old
```

Right to data portability



Obligations of companies

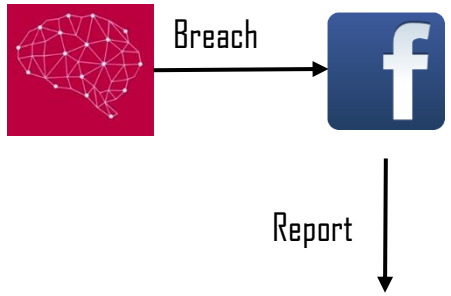
Clear permission required
Can we use also your e-mail address to send you a monthly news mail?

☑ Yes ☐ No

Internal documentation
Internal audit trail, e.g.:
- Who is responsible
- What is the purpose of processing
- What kind of data is processed
- Protective measures
- How long do you keep the data

Privacy officer / data impact assessment
>250 employees and/or special data (racial/ethnic origin, political opinion, religion, biometrical/genetic data, medical data, sexual orientation)
Assessment of envisaged processing, purpose, necessity, risks and safeguards

Report of breaches

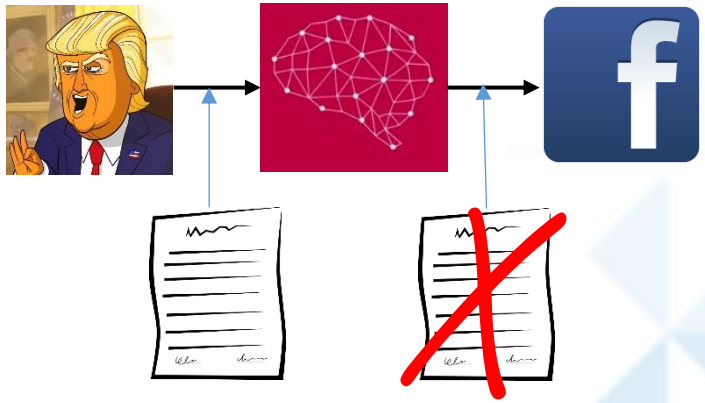


National privacy authorities.
(In main establishment country or in country of representative if outside EU. "Shopping" possible)

Privacy by default

We will **call** you back
Name: ✓
Phone: ✓
E-mail: ✗
Topic: ✓

Contracts with external processors to warrant privacy in line with GDPR



Tax advisors are often external processors

Privacy by design

Biggest company obligation

Have your systems and internal processes designed for privacy

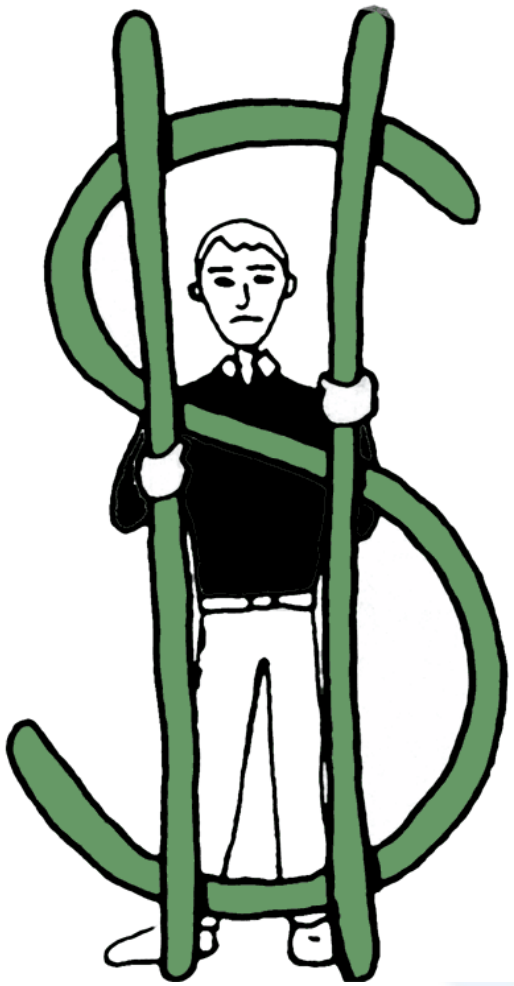
Examples:

- Digital security
- Access on need-to-know basis only
- Don't need, don't ask
- Use anonymized information when possible
- Delete data when no longer needed

Fines

Can be up to the higher of:

- 4% of the world wide annual turnover;
- € 20.000.000,-.



Case 1

EU-client wants to work in the USA for a year. He asks you for advice. You find a tax law firm in the USA from the GGI network and, although you haven't had contact before, you ask if they can assist you.

They are happy to help and ask if they can have a copy of your clients personal income tax return and some other information.

You ask your client if you can give this information to them. He e-mails you and gives permission.

What did you do wrong?

- Permission granted by e-mail is not sufficient.
- You do not know if the USA firm complies to the EU GDPR.

Solution 1

- You do not know if the USA firm complies to the EU GDPR.

Firms and companies outside of the EU must comply to GDPR when processing personal data of EU residents. You may only use a third party processor of personal data if you can guarantee the personal data will be processed according to GDPR. Sign a processors contract and be extra careful when dealing with companies outside the EU.

Permission granted by e-mail is sufficient. However a signature can be preferable in case of complaints by the client.

Case 2

From: someone@somewhere.com
To: taxlawyer@xyz-taxfirm.com
Subject: RE: personal income tax question

Today I received your e-mail on personal taxes. However, I think it was meant for someone else. I shall delete it and consider it not send.

- Reportable breach of security. Personal information was received by someone unauthorized, even though it was by mistake of the sender.
- No reportable breach of security. Regardless of responsibility to client, this is no GDPR security breach as no systems have been illegally accessed.

Solution 2

- Reportable breach of security. Personal information was received by someone unauthorized, even though it was by mistake of the sender.

A breach of security can take place if data is accidentally unauthorized disclosed or transmitted. This breach must be reported to the privacy authorities and to the client within 72 hours after it has been discovered.

This makes e-mail a very insecure way to distribute files and advice. Even sending a CC to a third party (i.e. a notary who will prepare a deed you have advised about) can be risky if not all proper permissions have been given.

Case 3

A former client of you sends you a letter. Based on the GDPR he invokes the "right to be forgotten" and requests you to erase all your information about him from your files.

However, based on local tax legislation, as a tax lawyer you have to keep all your files accessible for at least 7 years.

What do you do?

- Delete all files as required by GDPR
- Keep the files as required by tax law

Solution 3

- Keep the files as required by tax law

Several rights of natural persons are being restricted by other legislation. The "right to be forgotten" for example will not extend to files that must be kept according to EU or Member State legislation.

Should you, for example, need to keep files based on USA law, then that is not a valid ground to keep the files.

All files that are not/no longer subject to be kept by (tax)law should be deleted instantly and this should be checked periodically for 7 years.

Case 4

- Your extremely rich client, from who you have GDRP-proof permission to process data, has no wife and no children.
- During a visit at your office he tells you that he is terminally ill and has a life expectancy of a few months. You do not make record of this information.
- He does not trust his only brother to responsibly spend his money. He asks you for advise to name his 12-year-old niece as only heir to his money, with it being safely guarded and low taxed until she turns 18. You give him advise.
- He gives you all the personal information of his niece and of the office of his lawyer who has accepted to act as a safe guard to the money. He asks you to work with a notary to formalize your advise.
- You do business with the notary and lawyer more often, you know they are GDPR-compliant and have contracts.

This is GDPR-compliant

There is a GDPR-problem

Solution 4 (1)

This is GDPR-compliant (most likely)

- *Your extremely rich client, from who you have GDRP-proof permission to process data, has no wife and no children.*
  You have a GDRP-proof contract. The fact that he has no wife or children is personal data, but (if this has been recorded) is covered by the contract.

- *During a visit at your office he tells you that he is terminally ill and has a life expectancy of a few months. You do not make record of this information.*
  Medical information is special personal data for which extra rules apply. However, as this information is not recorde.

- *He does not trust his only brother to responsibly spend his money. He asks you for advise to name his 12-year-old niece as only heir to his money, with it being safely guarded and low taxed until she turns 18. You give him advise.*
  As you do not have any information of the niece yet. As such there are no GDPR implications here yet.

Solution 4 (2)

- *He gives you all the personal information of his niece and of the office of his lawyer who has accepted to act as a safe guard to the money. He asks you to work with a notary to formalize your advise.*
  - At this point you will start processing personal data of the niece (if only informing the notary).
  - She has not given permission. Also: parents (not uncle's) permission required because she is younger than 13-16 (depending on member state). However, other justification to process data is possible.
  - The "protect her vital interest" exception does not apply in tax & legal (urgent medical situations only).
  - The "legitimate interests" of a third party (the uncle) can be applied here. He needs his niece's data processed to finalize his last will. However, care should be taken that the niece's fundamental rights and freedoms are not damaged. Because she is a child, this should be considered extra carefully.
  - However, exception can be a "grey area": This is GDPR-compliant (most likely)

- *You do business with the notary and lawyer more often, you know they are GDPR-compliant and have contracts.*
  You need to know this and have these contracts.

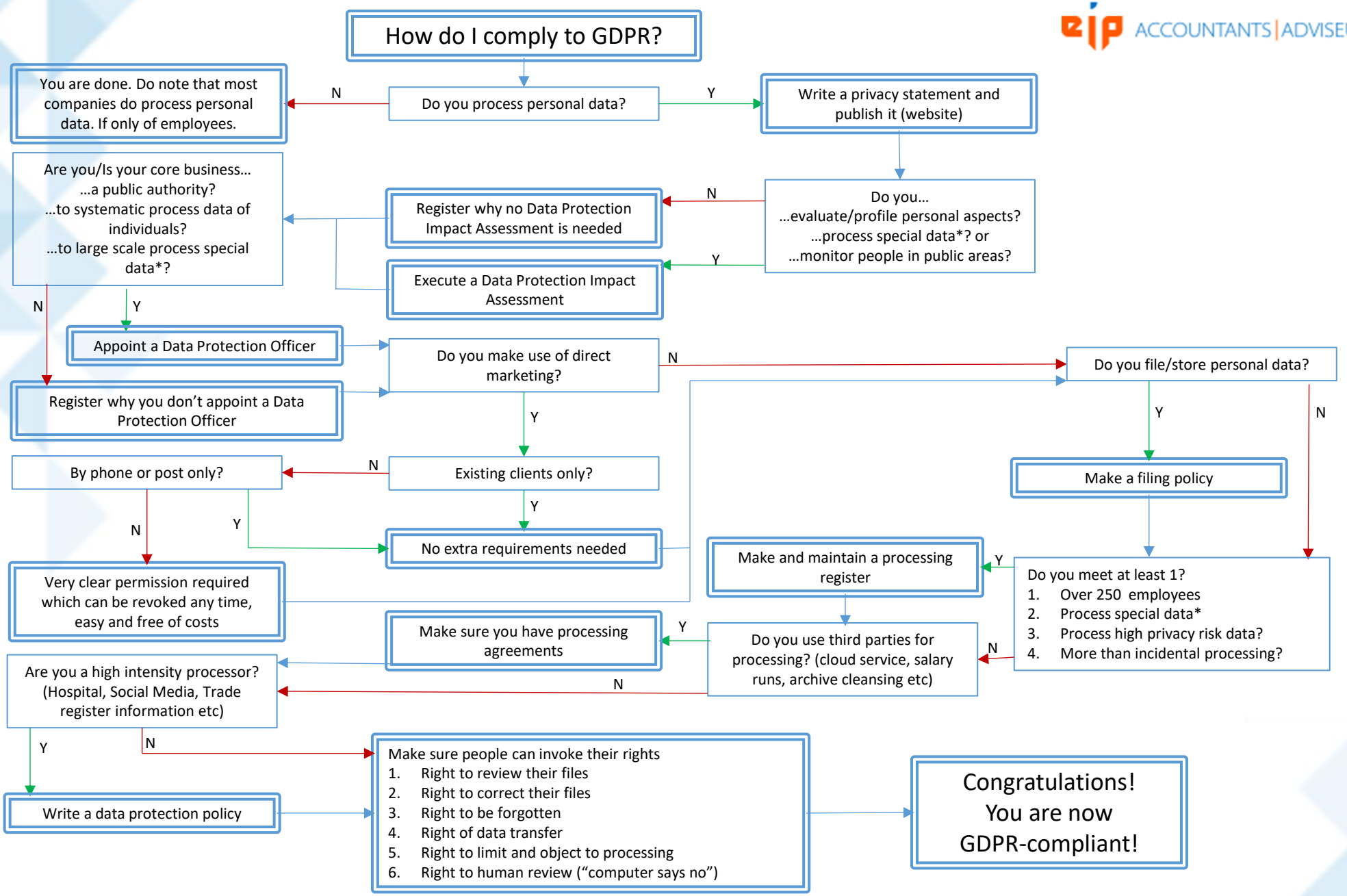
GDPR conclusions

- GDPR has a wi cope, you have more personal data than you think.
- Huge practica lications.
- Taxes are not ulated special personal data, but personal taxation does cover a lot of personal data.
- Make sure you rk with GDPR-compliant companies, which includes our fellow GGI-members with nd outside of the EU.

- 36 days left u May 25th
- So its time to stop start privacy panic.

Thank you!

How do I comply to GDPR?



*special data: race, ethnics, religion, sexual orientation, medical, genetic, biometric, political orientation, trade union membership