GDPR:
What you all need to know and what needs to be done

Welcome and Thank You!

- My name is Florian Vogler
- panagenda helps customers Analyze and Optimize Collaboration & Communication
- Our customers run over 10 million licenses of our solutions in more than 70 countries

Florian Vogler
CEO
panagenda

@panvof


Y M C A


GDPR

Agenda

- What is the GDPR?
- Data Controller and Data Processor
- Requirements for collecting/storing/processing
- Rights of data subjects
- From old to new / Obligation to inform
- More obligations
- Broader Topics
- SSOT vs. MSOT
- Data Breaches
- One slide on how panagenda can help
- Resources
- Q&A

What is (the) GDPR / EU-DSGVO

- **G**eneral **D**ata **P**rotection **R**egulation
  - **A**lgemene**V**erordening**G**egevensbescherming
  - **EU-D**aten**S**chutz**G**rund**V**er**O**rdnung

- Becomes effective on May 25, 2018
- Protects Citizens of the European Union and their personal data
  - Applies to any organization collecting/storing/processing personal data of EU citizens

- Personal Data = *any* data relating to a person
  - Email-Address, Name(s), IP-Address, Color of hair, …

- Sensitive Data
  - Genetic, Biometric, Sex Life, Health, Racial or Ethnic Origin, Political Opinions, Religious or Philosophical Beliefs, Trade Union Membership, …

Before we move on

- I am not a lawyer

- GDPR is complex
  - Depends on the type of data (personal vs. sensitive)
  - Depends on the type of organization (e.g., business vs. bank vs. insurance vs. gov.)
  - Other laws may extend or overrule GDPR
    - E.g., necessity to document (the history of) a transaction (purchase)
    - This may even be different from country to country
      - however, a EU country ~~cannot~~ must not weaken GDPR (except for the level of penalty)

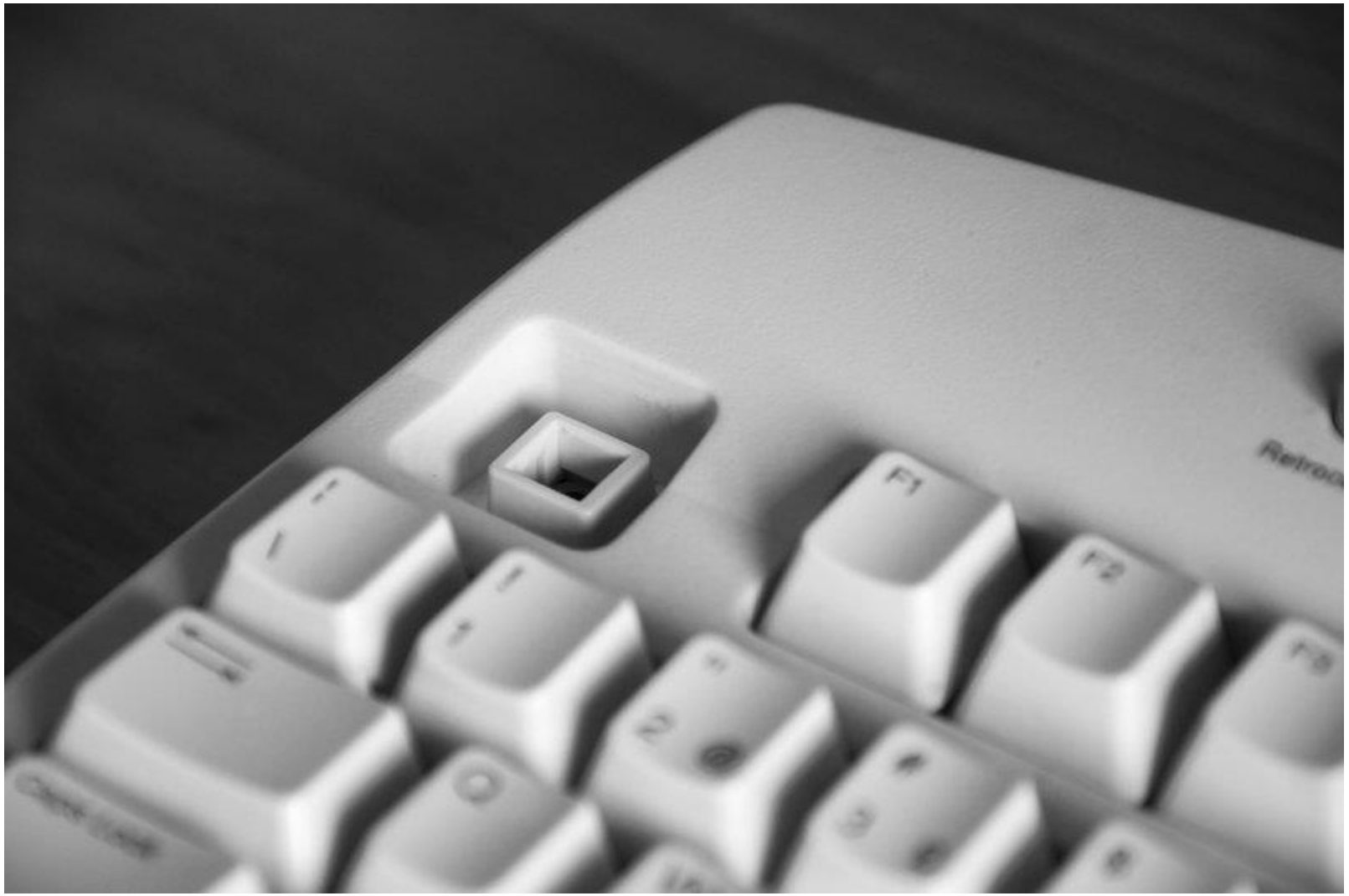
- GDPR is important – fines of *up to*
  - 10 million EUR or 2% of worldwide turnover (responsibilities)
  - 20 million EUR or 4% of worldwide turnover (personal data)

Four of the most prominent topics – out of *MANY MORE*!

or a room full of elephants

- You must rigorously monitor, track and protect personal data
  - Elephants: Email and “local” Downloads
- Data Collection with clear GDPR Info and Double Opt-In
  - Elephant: none, except for “Think Imprint” / cease-and-desist orders
- The right to be forgotten
  - Elephants: Backups, Internal vs. External
- You may only store what’s really needed and must maintain it
  - Elephants: Collected too much before? Got lots of existing data? Delete you must.

There is no escape



GDPR affects you IF … (examples)

- You collect *any personal data* from European citizens
  - That includes European citizens working for companies in the European Union
- You have a website, that European citizens (can) visit
- You sell whatever to European citizens, independent of whether you have a presence in the EU
- The European Union:

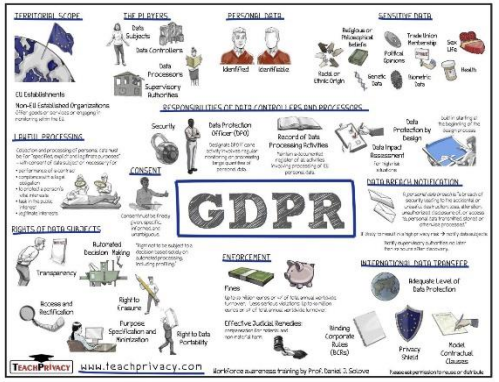
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
The Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United Kingdom

GDPR affects you ...

- Independent of whether you are a one wo/man shop or huge enterprise
- The only difference of a one wo/man shop is that everything is shared in one brain :)
  - Don‘t forget external sharing!

GDPR

- Does not apply to exclusively personal or familial activity
- Requires one or multiple Data Protection Officers (DPO)
  - Whilst an SME may not necessarily be required to have a DPO, you still have the majority of obligations → you should have one.
- Requires one or multiple people to be responsible for personal data
  - These are to be communicated to „data subjects“ (citizens of the EU)
- One more thing: sorry for all the text
  (legal text is hard to further condense or illustrate)



Data Controller and Data Processor

- Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

- Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

- In many cases Data Controller and Processor are in the same org.
- Cloud: IBM, Microsoft, Salesforce, MailChimp, Hootsuite, Facebook, LinkedIn, etc. etc. etc.
  - Data Controller = (Employees in) Your Organisation
  - Data Processor = Cloud Provider (provided the data is properly encrypted)

  The Data Processor **must** be GDPR compliant, too! (e.g., EU Privacy Shield)

Collecting/Storing/Processing of Personal Data

- Must be for „specified, explicit and legitimate purposes“

- Requires consent of data subject **or** a necessity for
  - performance of a contract
  - compliance with a legal obligation
  - protecting a person‘s vital interests
  - a task in the public interest
  - legitimate interests

- Must be minimized to only the necessary extent
- Must be correct; if incorrect must be deleted or corrected
  - Incorrect means: not legitimate>delete, not necessary>delete, or wrong>correct/del.

Rights of data subjects

- Data processing only after consent is given according to Article 6
  - Consent must be freely given, specific, **informed** and unambiguous
- Right of Information (Transparency)
- Right of Rectification
- Right of Erasure („Right to be forgotten“)
- Right of Restriction
- Right of Data Portability („Transport data somewhere else“) – think Cloud
- Right of Objection
- Right not to be subject to (exclusively) automated decision making

From old to new

- „Thank you for registering for our newsletter“
  (or text in contract, for example)

vs.

- What the GDPR now requires you to communicate
  in concise, transparent, intelligible and easily accessible form,
  using clear and plain language

Obligation to inform upon collection of personal data

- Name and contact details of responsible person/entity
- If applicable, contact details of Data Protection Officer
- Purpose of data processing and legal basis
  - Legal basis according to Article 6; e.g. Newsletter = Article 6-1(a) = the data subject has agreed to the processing of specific personal data
  - Should the legal reason be 6 -1(f), the legitimate interests pursued by the controller or by a third party
- The recipients or categories of recipients of the personal data, if any
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation (…)
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- the right to lodge a complaint with a supervisory authority

Obligation to inform upon collection of personal data

- Name and contact details of responsible person/entity
  - That‘s „YOU“ / your company/entity
- If applicable, contact details of Data Protection Officer
  - I‘d recommend you name some**one**
- Purpose of data processing and legal basis
  - Legal basis according to Article 6; e.g. Newsletter = Article 6-1(a) = the data subject has agreed to the processing of specific personal data
  - Should the legal reason be 6 -1(f), the legitimate interests pursued by the controller or by a third party
  - Example: „The purpose is to provide awesome service and the legal basis is Article 6-1a of GDPR“ – it‘s really that simple – obviously make it read a little better pls
- The recipients or categories of recipients of the personal data, if any
  - Who all will get this data (in most cases only which departments, sometimes also companies)
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation (…)
  - Any country and vendor outside of the EU, e.g. Hootsuite, Mailchimp, Smartcloud, MS Cloud, this or that or whatever – MUST be countries registered under eg EU privacy shield (US) or similar
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
  - Could be indefinite, until after the conf, for a year, 30 years, whatever – if indefinite I would add “or until you may want to be forgotten if so applicable” (again word better pls)
- the right to lodge a complaint with a supervisory authority
  - Just state as is

Obligation to inform upon collection of personal data

- The existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is (…)based on freely given consent(…), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Obligation to inform upon collection of personal data

- The existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
  - State as is just nicer to read
- Where the processing is (…)based on freely given consent(…), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
  - State as is just nicer to read (matches previous page)
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
  - For a newsletter: no. For buying a booth or making an order: definitely.
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
  - Careful: whilst in most cases not applicable, make sure you don‘t miss this one if you‘re doing *any* automated decision making based on data being entered.
    Whilst this is primarily targeted at „don‘t fire people because of data entered“ or „don‘t cease a contract based on history with a customer“, it is too vague to take too lightly imo. A simple „press 1 for support“ could be interpreted as automated decision making, as silly as it sounds. Worse, if „pressing 1“ ends in your data, it could be assumed „used for profiling“. Again, I may be stretching this – just fill this in, if applicable, to the best of your knowledge.

How panagenda chose to publish GDPR information

- https://www.panagenda.com/imprint/#gdpr

Obligations of Data Collectors

- Obligation to inform all recipients, with which personal data was shared, of corrected or deleted personal data
- Obligation to inform data subject of such recipients, if so requested (by data subject)
- Obligation to inform authorities in case of a data breach within 72 hours

- Ensure Security of Personal Data
- Data Protection by Design and by Default
- Maintain records of processing activities (~ not < 250 employees)
- In case of high risk:
  Data Protection Impact Assessment and Prior Consultation
- Codes of Conduct and Monitoring of such

Further relevant topics regarding GDPR

- Timely information of authorities in case of a data leak/breach/hack
- Organizations must prove that they did „everything“ possible/feasible to prevent leak/breach/hack and what they did to do so

- Security
- Documentation/Knowledge/Control
  (where is what, accessible by whom, accessed by whom, …;
  especially: *where all is personal data*)
- Awareness/Culture/Countermeasures (SSOT vs. MSOT)
- Transparency (towards data subjects)

SSOT vs. MSOT and distributed storage

- Single Source of Truth vs. Multiple Sources of Truth
  - SSOT: There‘s exactly ONE place where customer/personal data is stored
  - MSOT: Well, customer/personal data is stored in many places …
  - SSOT > MSOT: Any distributed customer/personal data is synched with SSOT

- The big elephant of distributed storage
  - Screenshots, Attachments, Exports, Printing, …
  - Email Forwarding, Copying, …
  - Storing Files in many different places
    - Connections, SharePoint, Email, Network Drives, Local PCs, …

What‘s a (possible) data breach anyway?

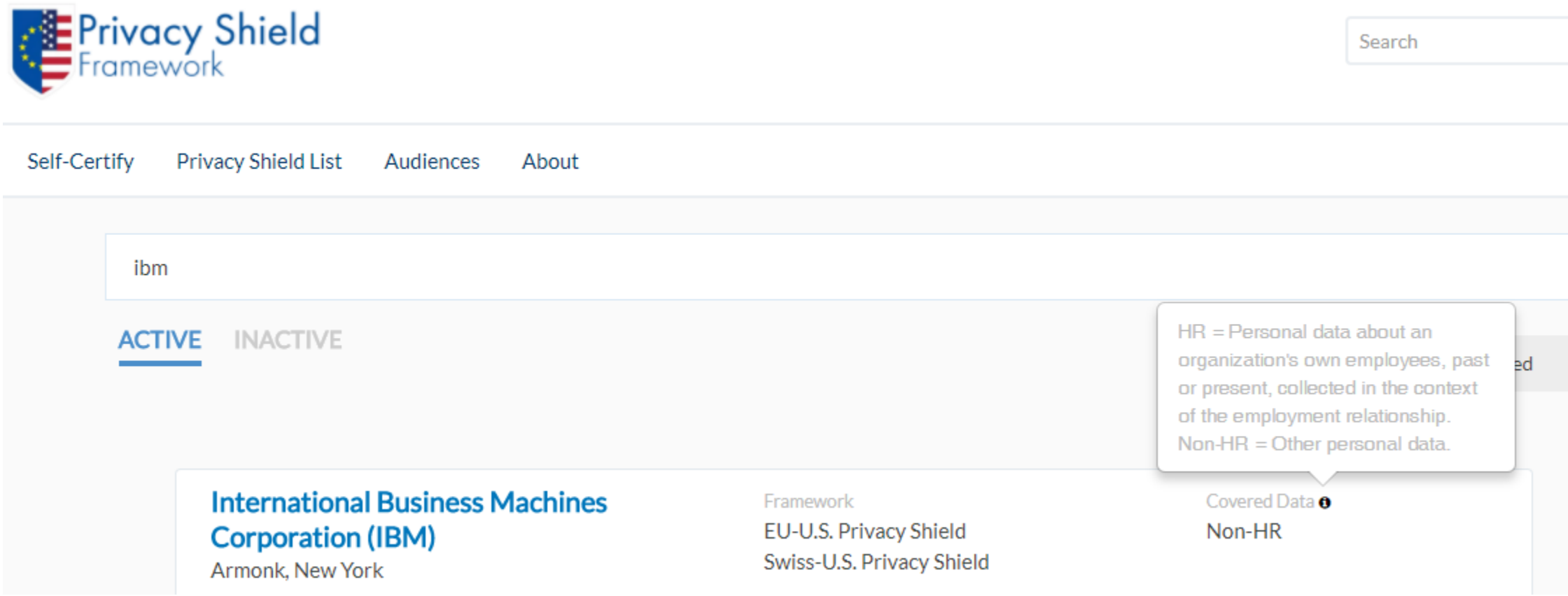
- Sharing of information
- Insufficient protection of information
- Transport of information without sufficient protection
- Loss of USB stick without sufficient protection
- Loss of Laptop without sufficient protection
- Loss of printed material
- Wrong access / misuse of access
- Hack/Attack
- …

How panagenda can help beyond Expertise & Services

- Domino Acess Rights
  - Who has/had what kind of access to what when
- Domino Usage
  - Who accessed what when and how
- Connections
  - Where to find all about whom
  - Who works with whom
  - Who shares information with externals
- Email Flow
  - Who communicates with whom
- Email Content
  - Attachments, Encryption, Automation, …
- Notes Clients
  - Management of local Replicas, Desktop Icons, Bookmarks, …
- Domino & Sametime
  - Changing and Deleting of Names / Content
- File Forensics
  - Metadata Inventory
  - Content Analytics

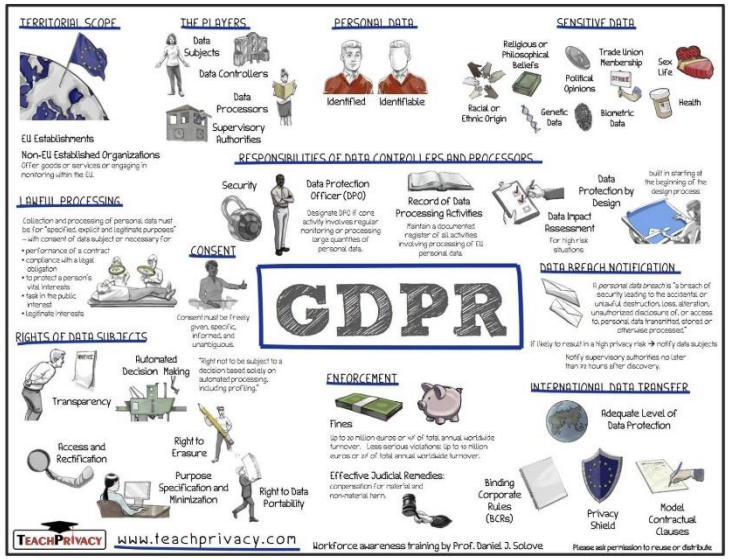
Resources

- https://www.privacyshield.gov/participant_search#



Resources (ctd)

- https://gdpr-info.eu/
- https://www.teachprivacy.com/gdpr-compliance-resources-training-get/
- https://www.eugdpr.org/



Resources (ctd)

- http://bit.ly/cnxGDPR
  - GDPR and IBM Connections
- http://bit.ly/docsGDPR
  - GDPR and IBM Docs
- http://www.ytria.com/WebSite.nsf/WebPageRequest/GDPR-considerationsen
  - GDPR considerations for your IBM Domino environment
- https://www.panagenda.com/portfolio-posts/eu-regulation-affecting-companies-worldwide-gdpr/?lang=de
  - Webinar recording of most of today's slides

Questions?

Florian Vogler
CEO
panagenda

@panvof

Headquarters, Austria:
panagenda GmbH (Ltd.)
Schreyvogelgasse 3/10
AT 1010 Vienna

Phone: +43 1 89 012 89
Fax: +43 1 89 012 89-15
E-Mail: info@panagenda.com

Germany:
panagenda GmbH (Ltd.)
Lahnstrasse 17
DE 64646 Heppenheim

Phone: +49 6252 67 939-00
Fax: +49 6252 67 939-16
E-Mail: info@panagenda.com

USA:
panagenda Inc.
60 State Street, Suite 700
MA 02109 Boston

Phone: +1 617 855 5961
Fax: +1 617 488 2292
E-Mail: info@panagenda.com

Germany:
panagenda Consulting GmbH (Ltd.)
Donnersbergstrasse 1
DE 64646 Heppenheim

Phone: +49 6252 67 939-86
Fax: +49 6252 67 939-16
E-Mail: info@panagenda.com

The Netherlands:
Trust Factory B.V.
11th Floor,
Koningin Julianaplein 10
NL 2595 AA The Hague

Phone: +31 70 80 801 96
E-Mail: info@trust-factory.com