# How an Austrian took over Europe, again, kind of –
## History and outlook on the Data Protection Territory Dilemma

Netpoet (AKA Frank Stiegler / STIEGLER **LEGAL)**

Revision Online 2022

# Topics today

1. Problems and options of processing personal data outside the EU lawfully
2. Previous attempts to tackle the problem
3. How are controllers, processors and supervisory authorities dealing with the issue?
4. EU's current attempt to solve the problem
5. Conclusion

1

# Problems and options of processing personal data outside the EU lawfully

# Key hurdle: Art. 44 ff. GDPR

„Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

# GDPR: Scope of Application

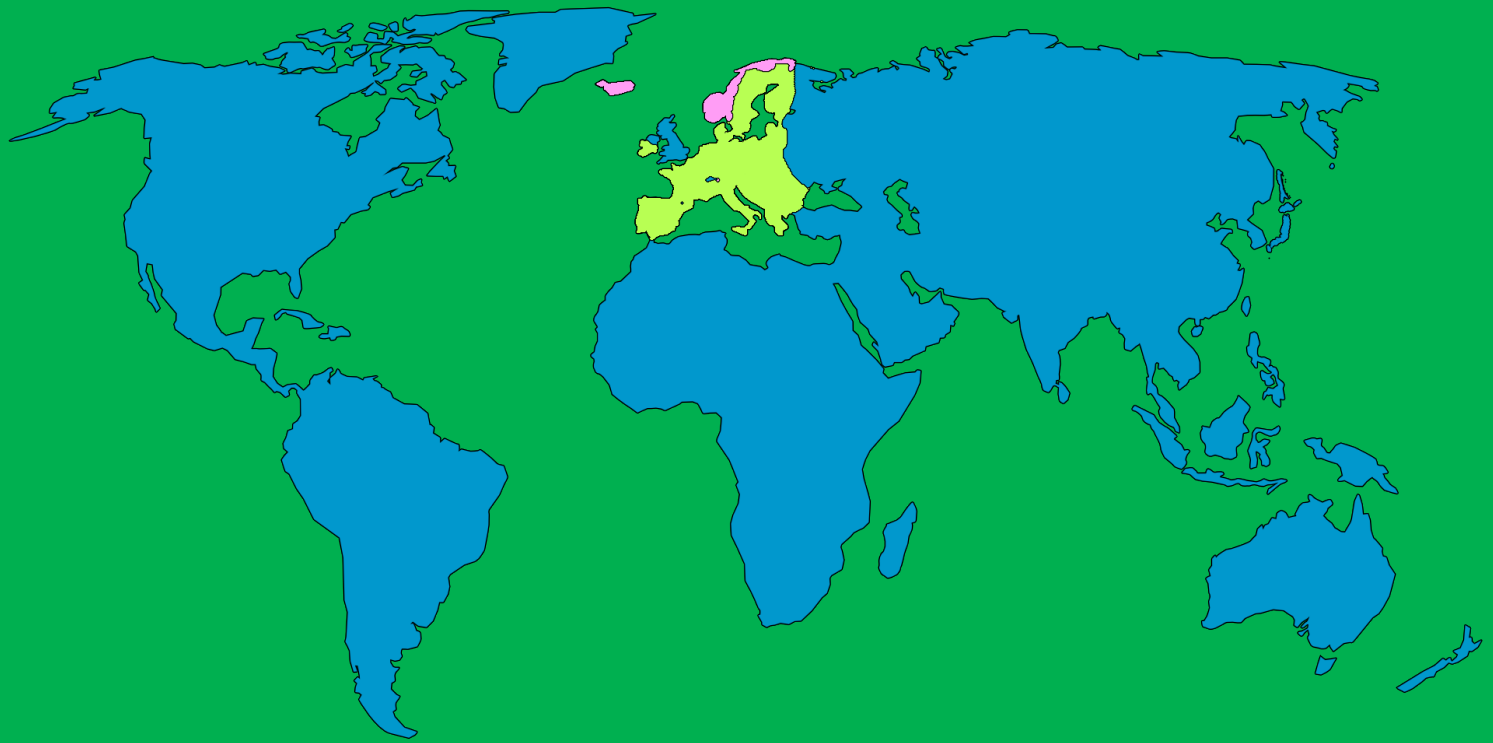
- GDPR is not applicable when natural persons process personal data (PD) in the course of purely personal or household activities.
- GDPR is applicable whenever PD on data subjects is processed who are in the Union, also when the controller or processor is not established in the Union (conditions apply, but mainly all commercial or surveillance purposes).

# Some examples of when this becomes relevant

- commercial Facebook/Instagram/whatever page
- Google Analytics, Maps, Fonts, AdWords
- AWS hosting +
- Salesforce
- Zendesk
- Jamf

…or even any EEA-based provider using a subcontractor outside the EEA

# „EU“ = EEA (European Economic Area)

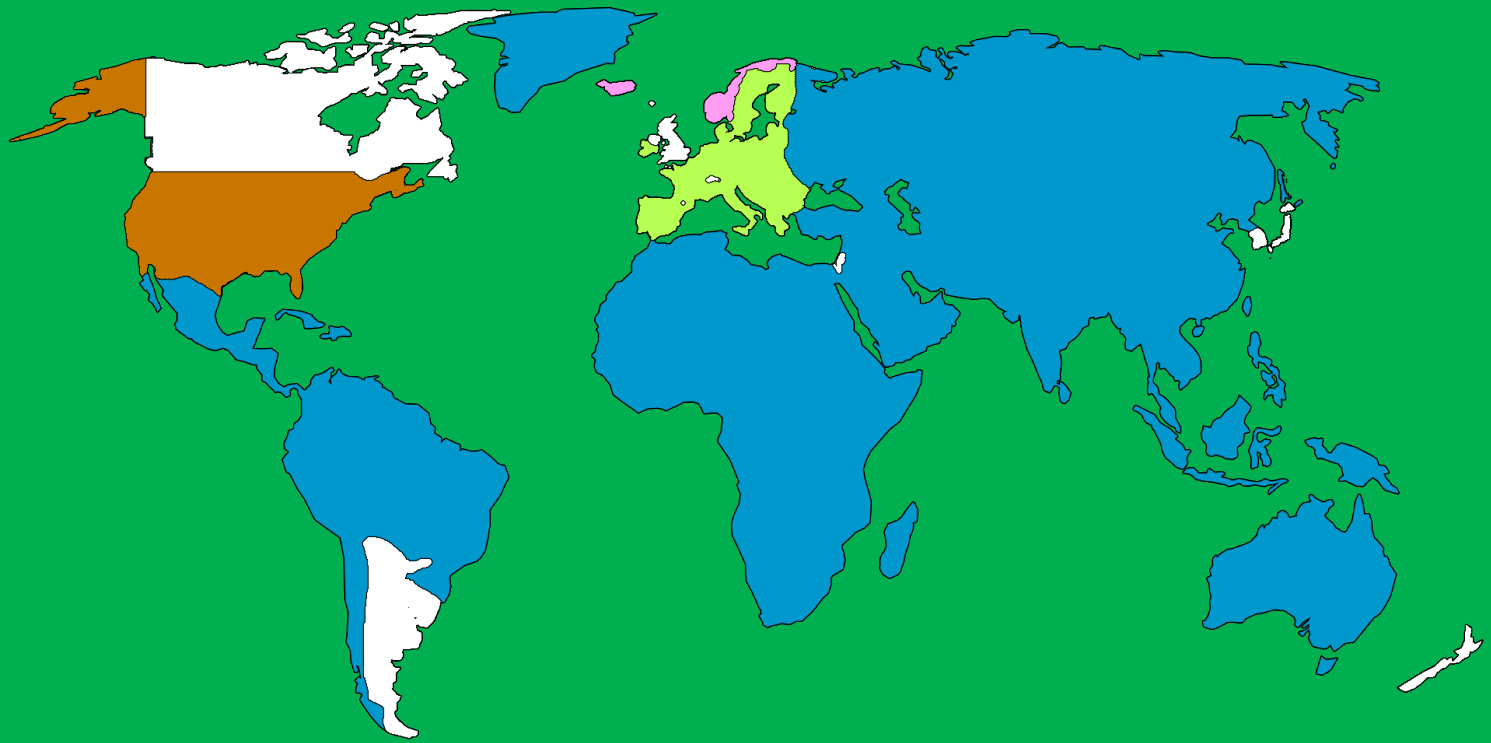


# We Are Not Alone (Adequate DP Levels, Art. 45)

## „Good“ countries (list here)

- Andorra
- Argentina
- Canada (commercial organisations)
- Faroe Islands
- Guernsey
- Israel
- Isle of Man
- Japan (2021)
- Jersey
- New Zealand
- Republic of Korea (2021)
- Switzerland
- UK (under GDPR and Law Enforcement Directive, 2021)
- Uruguay

# … and the US?!?



# US Laws that make an adequate DP Level unlikely

- Foreign Intelligence Surveillance Act of 1978 (FISA)
- US Patriot Act of 2001
- US Freedom Act of 2015
- Clarifying Lawful Overseas Use of Data Act of 2018 (CLOUD Act)

# Microsoft‘s futile attempts to withhold data

2013-2018, Microsoft lawsuit (ultimately) against the US Department of Justice.

Subject: extraterritoriality of law enforcement seeking electronic data on a non-US citizen on e-mail data stored outside the US (Ireland).

Several levels of jurisdiction, all the way up to the US Supreme Court, which had planned to decide in mid-2018.

The Trump administration passed the CLOUD Act on 6 Feb 2018.

The court rendered the case moot in April 2018.

# US Laws that make an adequate DP Level unlikely

- Foreign Intelligence Surveillance Act of 1978 (FISA)
- US Patriot Act of 2001
- US Freedom Act of 2015
- Clarifying Lawful Overseas Use of Data Act of 2018 (CLOUD Act)

There are probably more.

And remember, this covers just the US.

# So the problem basically is,

- A GDPR data subject has rights.
- (Third-country) authorities demand data on data subject from any company under its jurisdiction.
- Company cannot lawfully deny access.
- Data subject has no way of enforcing its rights, not even for access.

# Our current options (art. 45 ff. GDPR)

- ~~Adequacy decision (EU Commission) (45)~~
- Appropriate safeguards (46)
- Binding corporate rules (47)
- Transfers not authorized by EU law (48)
- „Specific situations“ (e.g. consent, 49)

# Appropriate safeguards (46)

## Art: 46 no. 1:

„only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

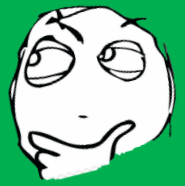
## „Official" (approved) safeguards necessary

## EU Standard Contractual Clauses (SCCs)

- Decision of 15 June 2001 („old SCCs")
- Decision of 4 June 2021 („new SCCs")

# Our current options (art. 45 ff. GDPR)

- ~~Adequacy decision (EU Commission) (45)~~
- Appropriate safeguards (46)



- Binding corporate rules (47)
- Transfers not authorized by EU law (48)
- „Specific situations“ (e.g. consent, 49)

# Binding Corporate Rules (BCR, 47)

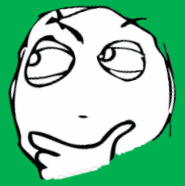
Art. 47 no. 1:

> „The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they: […]"

There are none.

# Our current options (art. 45 ff. GDPR)

- ~~Adequacy decision (EU Commission) (45)~~
- Appropriate safeguards (46)



- ~~Binding corporate rules (47)~~
- Transfers not authorized by EU law (48)
- „Specific situations“ (e.g. consent, 49)

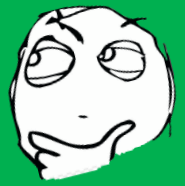
# Transfers not authorized by EU law (48)

„Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.“

Nope.

# Our current options (art. 45 ff. GDPR)

- ~~Adequacy decision (EU Commission) (45)~~
- Appropriate safeguards (46)



- ~~Binding corporate rules (47)~~
- ~~Transfers not authorized by EU law (48)~~
- „Specific situations“ (e.g. consent, 49)

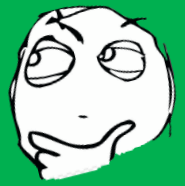
# Specific Situations (49)


Art. 49 no. 1 lists these options:

- ~~explicit consent after having been informed of possible risks of the transfers due to the absence of adequacy decision and appropriate safeguards;~~
- ~~necessary to fulfill a contract with, or in the interest of, the data subject;~~
- ~~necessary for reasons of public interest;~~
- ~~necessary to exercise or defence of legal claims;~~
- ~~necessary to protect vital claims;~~

# Our current options (art. 45 ff. GDPR)

- ~~Adequacy decision (EU Commission) (45)~~
- Appropriate safeguards (46)



- ~~Binding corporate rules (47)~~
- ~~Transfers not authorized by EU law (48)~~
- ~~„Specific situations“ (e.g. consent, 49)~~

2

# Previous attempts to tackle the problem

# International Safe Harbor Privacy Principles (2000-2015)

- Developed between 1998 and 2000, EU Commission adequacy decision in July 2000.
- CJEU rendered it invalid in Oct 2015 because,

„legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life".

# Attempts so far to overcome art. 44 ff. GDPR

- ~~Safe Harbor (Privacy Principles)~~
- Privacy Shield

# (EU-US) Privacy Shield (2016-2020)

- Developed in a hurry to replace Safe Harbor.
- EU Commission adequacy decision (4176/2016) in July 2016.
- All major providers submitted themselves to it.
- Controversy between the EDPB and the EU Commission on whether the problems addressed by invalidating Safe Harborg were solved in the Privacy Shield principles.

# And then Schrems happened. Again.

CJEU‘s „Schrems II“ ruling (C-311/18) in June 2020 did mainly two things:

1. It invalidated the Privacy Shield.
2. It clarified the lawful use of SCCs.

# CJEU in Schrems II on Privacy Shield

- Does not provide adequate safeguards to ensure an adequate DP level.
- Lack of limitation of powers conferred upon US authorities,
  and of actionable rights for EU subjects against US authorities.
- Ombudsman mechanism not binding (AKA „useless“).

(This is funny because that is essentially
why Safe Harbor wasn’t OK either.)

# CJEU in Schrems II on SCCs in a Nutshell

- The current SCCs (nowadays, „the old ones“) are, in theory viable.
- But it takes „appropriate measures“ to ensure an adequate DP level. Mere copy-and-paste is very likely enough.

  → Remember the hurdles Safe Harbor and Privacy Shield didn‘t overcome.

The problem:
Everyone did copy-and-paste at the time.

# Old SCCs

# By Sep 2021, „everyone“ had adapted to new SCCs.

- Modular structure, taking into account responsibilities (controller/processor).
- Supplementary (technical and/or organisational) measures (TOMs) are still necessary.

# Attempts so far to overcome art. 44 ff. GDPR

- ~~Safe Harbor (Privacy Principles)~~
- ~~Privacy Shield~~
- SCCs
  - ~~2001 (old)~~
  - 2021 (new)

3

# How are the involved parties dealing with the issue?

# Let‘s remember our options

~~Adequacy decision~~
(Art. 45)

None today, but maybe
in TEH FUTARE!

Appropriate safeguards
(Art. 46)

→ SCCs

- ~~2001 (old)~~
- 2021 (new)

So today, the new SCCs are really the only vessel companies have to guide cross-border data processing.

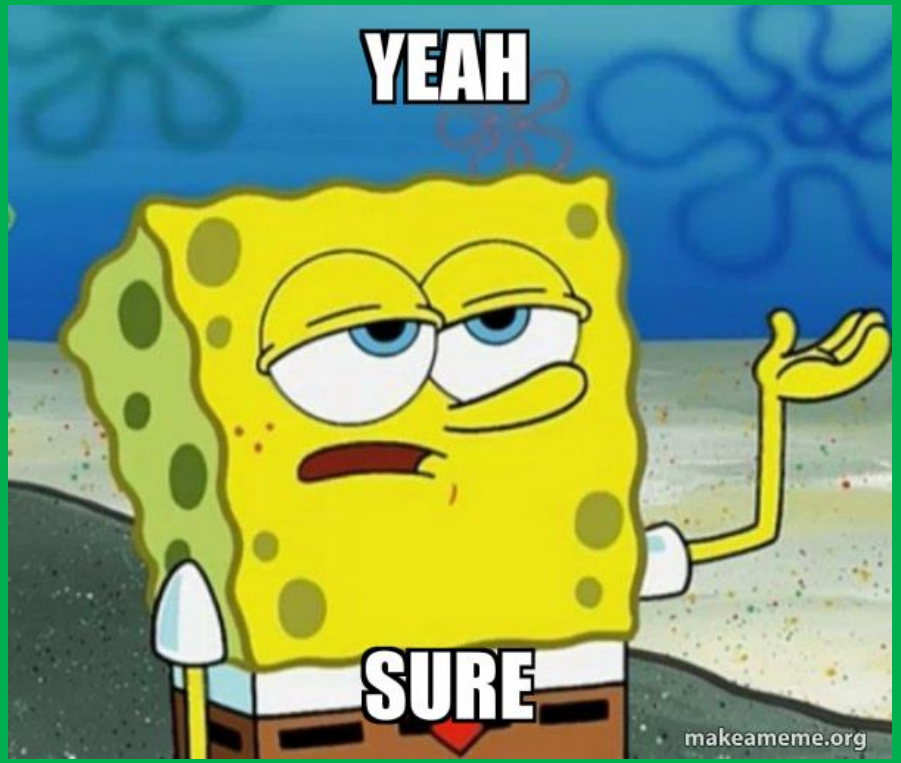
# What the EDPB says these TOMs can be

- Encryption (so that the processor cannot access them)
- Pseudonymisation (so that the processor cannot identify data subjects)
- Transmission to a "protected" person (e.g. a doctor who is "immune" to authorities' data access demands.
- Separation of duties (and data access) onto several providers in a way so that neither can access personal data on its own.

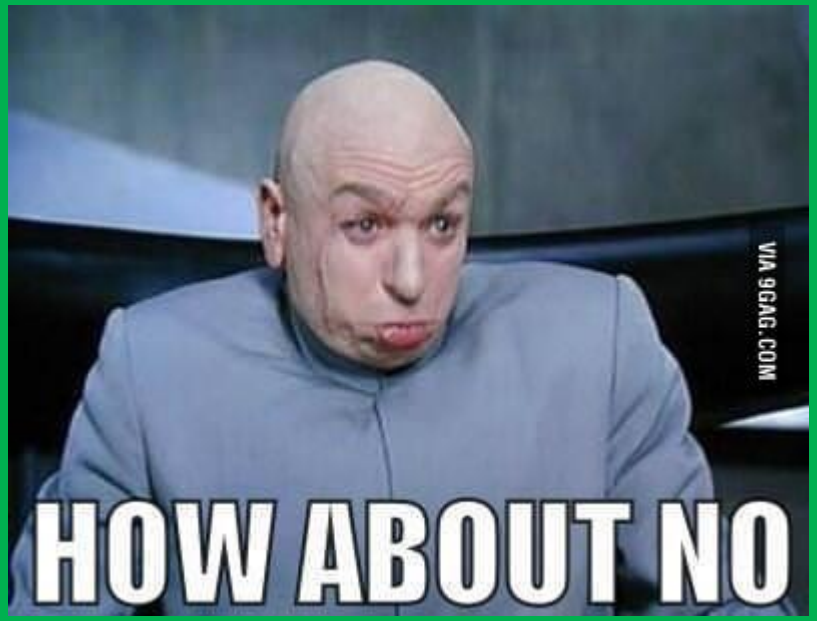
# Examples of TOMs I have stumbled across

- Duty of information in case an authority requests access to data;
- Sunset clause on „no requests received“ status;
- Regular information on the number, kind and outcomes of data requests, naming the requesting authority (if allowed);
- Going to court in the data subjects‘ name;
- Use of hardware security modules;

# Are all these things acts of good will?



# Do they solve the problem?



# How are the authorities dealing with this issue?

- Common denominator: „Let‘s not fine the controllers and processors who are trying their best to prevent harm from data subjects.“
- Wait for further notice until they need to act.
- Audits and fines not solely on the basis of cross-border transfer.
  Hey, a DP breach hardly comes alone…

¯_(ツ)_/¯

4

# EU’s current attempt to solve the problem

# Let‘s remember our options

## Adequacy decision (Art. 45)

What about we make a new safe harbor / privacy shield / data protection haven / data privacy bay / privacy compliance something?!?

## Appropriate safeguards (Art. 46)

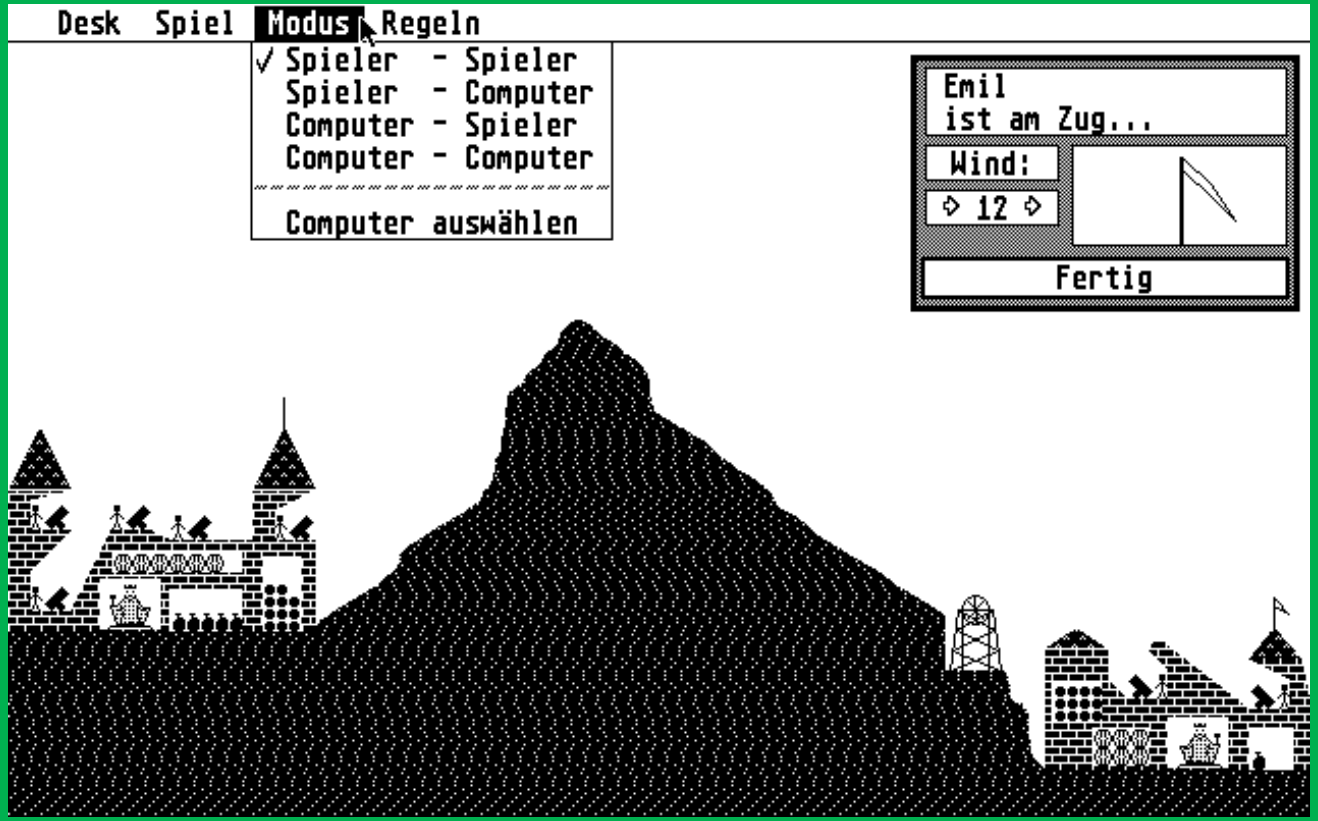
new SCCs

# The White House (25 March 2022) (source)

“The United States and the European Commission have committed to a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the Eur[illegible]n when it struck down in 2020 the Commission’s a[illegible]n underlying the EU-U.S. Privacy Shield framework.”


So far, there is no actual draft that could be analyzed.

# We need to get beyond MINE MINE MINE




#teamDatenschutz

# Max Schrems be like


## More precisely (on noyb.eu):

- No text to examine, no ways announced to overcome the CJEU hurdles of Schrems II (or Schrems I, really).
- Allegedly the US surveillance laws aren't changing, but those pose a critical threat to CJEU principles.
- "If [TADPF] is not in line with EU law, we or another group will likely challenge it. In the end, the Court of Justice will decide a third time."

5

# Conclusion

# The current status in conclusion

- So far, no EU Commission-approved set of principles has held up with the US because of the lack of effective data subject rights .
- No inter-partes agreement can solve the main third-country data processing problem, being national laws depriving data subjects of their GDPR rights (access, erasure, etc.).
- Effective measures render most services void in practice,
  ineffective measures are more or less useless.
- Currently, „good“ companies adopt to each new standard and find themselves uncertain what to do every few years.

# To make all this even more bizarre, ask this:

Would, e.g., Germany be a country with adequate DP levels if it were a non-EEA country without an adequacy decision?

To assess the “adequate level of DP”, let’s check Art. 45 no. 2 lit. (a):

[Important is] „the rule of law, respect for human rights and fundamental freedoms, […] as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects […];“

# Access to your data from your secret service?!?

These activies don‘t fall under the GDPR (Art. 2), and it‘s unlikely that there are adequate substitution rights.

→ Adequate levels of DP would be questionable even within EU member states.

## The solution?

As long as the US and the EU impose their respective laws onto each other, there cannot be a sustainable way to process GDPR-protected data in the US (or in any other „third country“, really).

# The solution?

Option 1: the US get rid of their laws that grant access to data worldwide without GDPR-sufficient data subject rights.

# The solution?

Option 2: the EU Commission lowers the GDPR standards on cross-border data processing.

# So far, EU Commission be like

# Thanks for watching!

www.stiegler.legal www.innara.net