SBM
STATE BAR OF MICHIGAN

Panel Discussion

# *Navigating International Privacy Rules: Today and Tomorrow*

**Deborah Gertsen**, Ford Motor Company
**Jill Phillips**, General Motors Company
**Robert Rothman**, Privacy Associates International LLC
**Mark Werling**, Chrysler Group LLC

# Purpose of Panel

- Explain some of the practical difficulties and approaches in complying with today's international privacy rules
- Discuss how those challenges may well be increased in the immediate future
- Use EU rules as the example because of their global influence

# Today: A Quick Refresher

# Legal Bases to Allow for Domestic Processing of Personal Information in EU

- Unambiguous consent.
- Performance of contract to which data subject is party.
- Compliance with legal obligation to which controller is subject.
- Protect vital interest of data subject.
- Performance of task carried out in public interest or exercise of official authority.
- Necessary for purposes of the legitimate interests pursued by controller or by the third party/ies, except where such interests are overridden by the interest for fundamental rights and freedoms on the data subject that require protection.

# Personal Information Processed in EU Must Comply with Certain Basic Principles

- The principles:
  - Notice
  - Choice
  - Security
  - Data Integrity
  - Access
  - Enforcement
  - Onward Transfer
- Much law surrounds the implementation of these concepts in each member state

# Available Legal Bases to Make the Personal Information Transferable Outside the EU

- Data subject consents
- The transfer is:
  - **To an entity in a country with "adequate" privacy laws (small number – does not include US)**
  - **Made pursuant to a standard clause contract drafted by the EU**
  - **Made pursuant to "binding corporate rules" approved by appropriate Data Protection Authorities**
  - **Made to the US to a Safe Harbor company (technically an adequacy determination)**
  - Made pursuant to ad hoc contracts approved by the appropriate Data Protection Authority
  - Necessary for performance of a contract with the data subject
  - Necessary on public interest grounds
  - Necessary to protect the vital interests of data subject
  - Made from a public register

How do these rules affect companies today and how do companies deal with them?

# Tomorrow: The Proposed Regulation

# Regulation vs. Directive

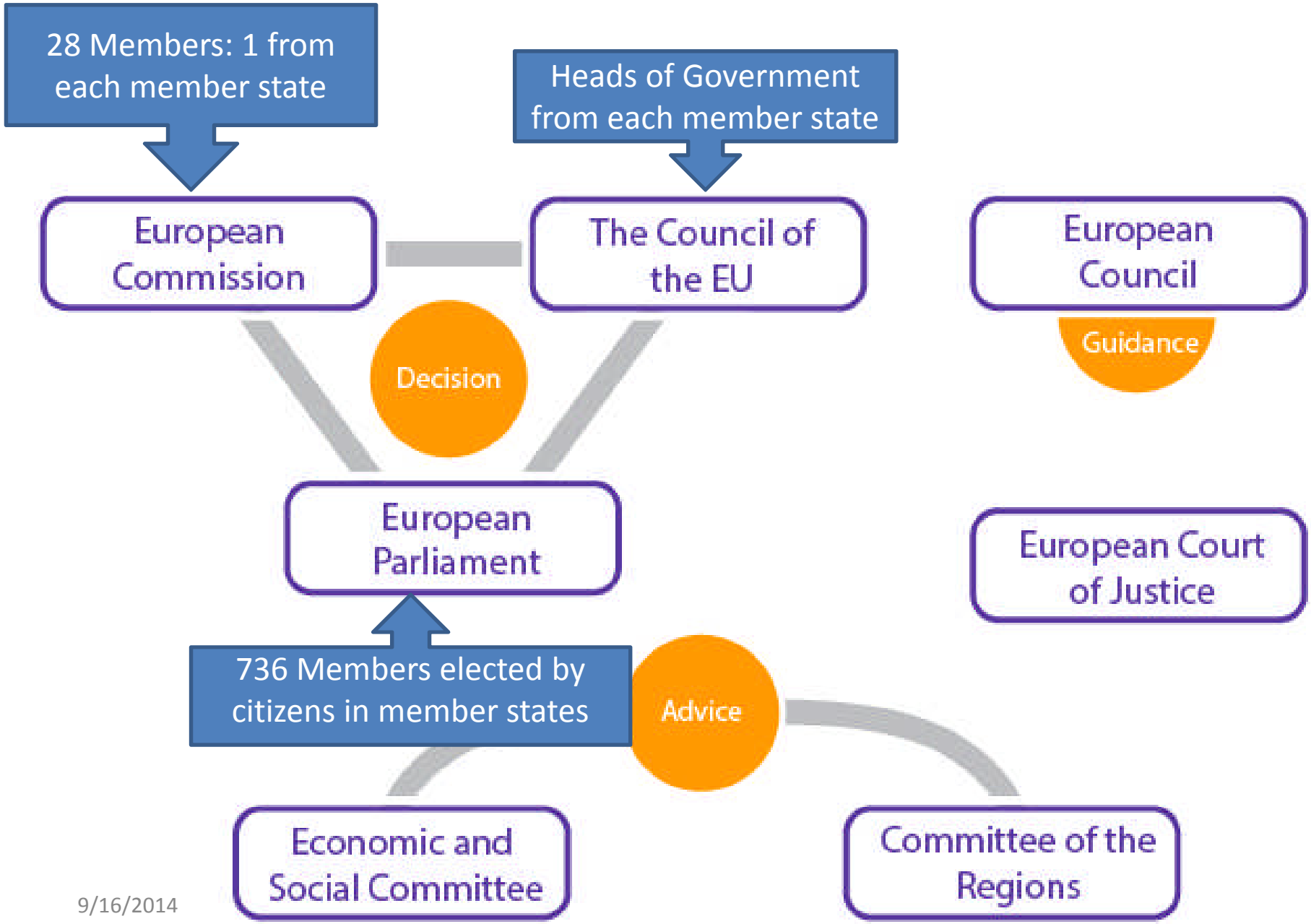
- Regulation intended to replace the current Data Protection Directive 95/46/EC

- Article 288 of the Treaty on the Functioning of the European Union:

*A **regulation** shall have general application. It shall be binding in its entirety and directly applicable in all Member States.*

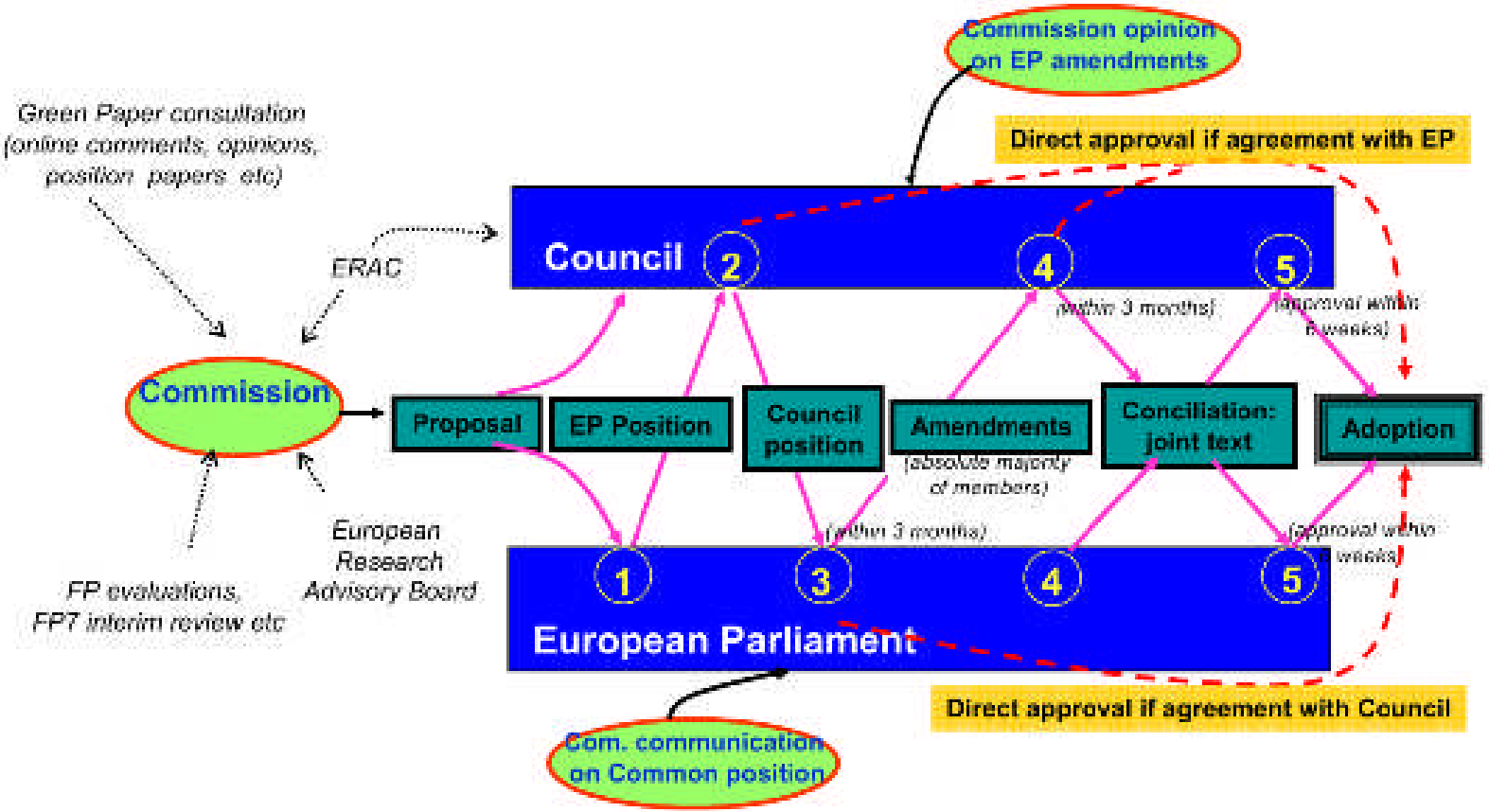
*A **directive** shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods"*

# Some EU Basics



# The "Ordinary legislative procedure"

(ex "*co-decision*")




From http://europarltv.europa.eu/en/player.aspx?pid=2943a9f1-0a1a-4f7c-9fe8-9f82009fa481

# Status

- Commission proposed draft Regulation in January 2012
- European Parliament assigned to Committee on Civil Liberties, Justice and Home Affairs (LIBE), Jan Philipp Albrecht, Rapporteur
- Pushed hard by Viviane Reding, former Justice Commissioner and now MEP
- LIBE Committee received thousands of suggested amendments from MEPs, consulted with various groups and interests
- In October, 2013 passed a “compromise version”
- Compromise version passed by entire European Parliament in March 2014
- Currently under consideration by European Council
- Significant political intrigue, fueled by recent European elections and NSA scandal, but general local consensus is “something” will pass

# Mrs. Reding & Mr. Albrecht

# SELECTED FEATURES OF THE PROPOSED REGULATION

# Extra-Territorial Application of Regulation

## Arts 3,25

- Purports to apply to the processing of the personal data of EU residents by a controller or processor outside the EU (e.g., where processing is actually conducted overseas or in the cloud) where the processing is related to:
  - Offering goods or services to the EU residents
  - The monitoring of behavior of the EU residents
- In this situation, the controller or processor has to designate a representative in the one of the EU states where the above activities take place (Art 25)
- The language of this provision strengthened in EP version after Snowden/NSA and subsequently strengthened further by the Council.

# Fines and Enforcement Arts 75-79

- Individuals have a right to lodge a complaint with a DPA
- Individuals have a right to seek judicial action against controllers or processors for damages sustained from unlawful processing (Arts 75,77)
- Organizations and associations have the right to lodge complaints and seek judicial remedies on behalf of injured individuals
- Fines of up to Euro 100 million or 5% of world turnover, whichever is higher

# Impact Assessments (Risk Analysis)

Article 32a (prev. 33)

- Controllers/processors to determine if "*specific risks" relating to rights and freedoms of data subjects are present. (*Art 32a(2) lists examples of specific risks)
- Processing data of over 5000 subjects in 12 mo. period, employee data, children's data, healthcare data, profiling, sensitive data
- Depending on what risks - foreign controllers must appoint representative in the EU, DPO must be appointed within the company, lifecycle data protection impact assessment must take place
- Company DPO must monitor process (Art. 37(1)(f)) and impact statements must be furnished to DPA (Art 34(6))
- Prior draft provision requiring the impact assessment be made public - removed

# Breach Reporting (Art 31, 32)

- Definition of “Personal Data Breach“(Art 4(9)) broader than most US definitions
  - Definition of “Personal Data” also changed (Art 4(2))
- **Processor** must notify the controller "*immediately after establishment of a personal data breach*" (Art 26 (2)(f), Art 31(2)
- **Controller** must notify DPA after the personal data breach has been established.
  - “Without undue delay” (presumed 72 hours)
  - Art 31(3) contains a list of information that must be in the notification, most of which the controller will be unlikely to know
  - Required regardless whether the data was encrypted
- **Controller** must notify data subjects without undue delay after notifying the DPA:
  - If breach *"likely to adversely affect the protection of personal data or privacy of the data subject“* or, under EP version, affect the data subject’s “*rights or the legitimate interests* **“**

# One Stop Shopping

- The Regulation will establish a ‘one-stop-shop’ for businesses: companies will deal with one single supervisory authority (DPA), not 28
- DPA will depend on the place of establishment, as designated by the company
- Challenges
  - If Techco has its main establishment in Ireland and a Greek citizen wants to complain about Techco, how does he do it?
  - Requires more enforcement harmonization than currently evident

# Consent (Art.7, 82)

- Prior draft provision requiring consent for commercial direct marketing removed
- Employee consent not valid unless freely given Art. 82(1)(b)
- Burden of proof to show valid consent is on the controller
- If consent is obtained in a document dealing with other matters it must be "distinguishable in appearance" from rest of provisions (Art.7(2))
- It must be made as easy to withdraw consent as it is to give consent
- The execution of a contract or provision of a service cannot be made conditional on the furnishing of a consent not necessary for the contract or service
- Processing of the personal data of a child under the age of 13 in connection with the offering of goods or services is lawful only with the consent of a parent or guardian

# Accountability Art 22

- Must be able to demonstrate compliance to DPA (Arts 22(1), 29)
- Mandatory requirement to adopt policies and procedures (Arts 11, 12)
- Need verification/audit mechanism to document compliance with Regulation (Art 22(3))
- Implement security measures appropriate to risks and data (Art 30)
- Need to be able to demonstrate compliance with privacy by design and by default requirements over the entire data lifecycle (Art 23)

# International Data Transfers Arts 40-45

- An adequacy determination can be made with respect to a territory within a country (California?) or a *"processing sector"* within a country (Art 41(1))
- Allows for transfers among members of groups which hold a "European Data Protection Seal," a seal granted by a DPA

# International Discovery Demands (43a)

- No judgment of a non-EU court or decision by a non-EU administrative agency requiring a controller or processor to disclose personal data is enforceable in the EU
- If such a judgment or request arises the DPA must be notified without delay and there can be no compliance without DPA approval
  - The DPA will decide if the disclosure is really necessary under exceptions for public interest and defense of legal claims
  - DPA will notify national authorities and the subject(s) of the data requests of the request

# Data Protection Officer (1) (Arts.35,36,37)

- Obligated to appoint a Data Protection Officer (DPO) if the controller or processor:
  - Has more than 250 employees or processes personal data of more than 5,000 data subjects in a 12 month period
  - Has certain core activities
    - Regularly monitors data subjects
    - Processes special categories of information, such as location data, children's personal data or certain employee data

# Data Protection Officer (2) (Arts.35,36,37)

- DPO must:
  - Be appointed based on privacy expertise and for a period of at least 4 years for an employee or 2 years for an external DPO
  - Not have other duties that conflict with DPO responsibilities
  - Report directly to executive management
  - Be involved in a timely manner in all issues of personal data protection
  - Be independent and not *"receive any instructions as regards the exercise of the function."*
  - Be provided with all means, including *"staff, premises, equipment"* to carry out his duties and maintain his professional knowledge
  - Not be dismissed unless he/she does not fulfill duties of DPO
- Tasks (Art 37) generally include internal advice and education, compliance monitoring, document maintenance, breach issues, impact assessments, interacting with DPAs, etc.

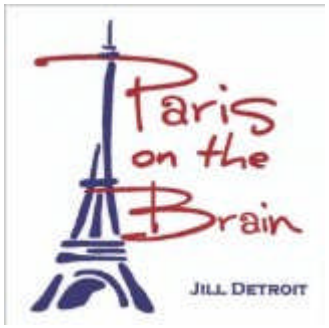
# Right to be Forgotten (Erasure) Art 17

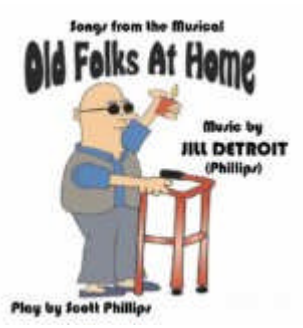
- Data subjects generally have right to obtain from controller erasure of data and abstention from further dissemination
- Suppression of data not good enough, except in limited circumstances (Art 17(4))
- A controller that has made data public must take all reasonable steps to have data that the individual requests them to erase also erased by third parties and to report actions of third parties in that regard to the data subject (Art 17 (2))

# European Court of Justice in Google Case

- Decision of May 13, 2014
- Google's information indexing activities fall within the definition of "processing" under the Data Protection Directive and Google is a "controller" of the data
- Google is subject to the Spanish law even though the indexing is carried out in the U.S. because they have an advertising subsidiary located in Spain
- Google must comply with requests from data subjects to remove links to true and lawfully published information in search results because they are liable to constitute a significant interference with the data subject's fundamental right to privacy.
  - It is the linking of the different pieces of information that may be unlawful even though the original publication of each piece of information was lawful and is still available.
- A fair balance should be found on a case by case basis between the legitimate interests of internet users who may be interested in having access to information and the privacy rights of the data subject.
- The individual case is remanded to the Spanish courts for decision.

# THE TREAT

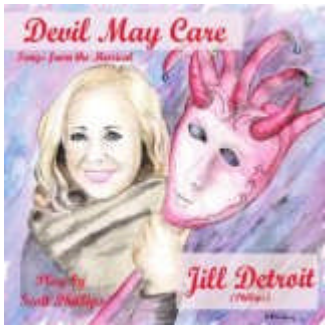



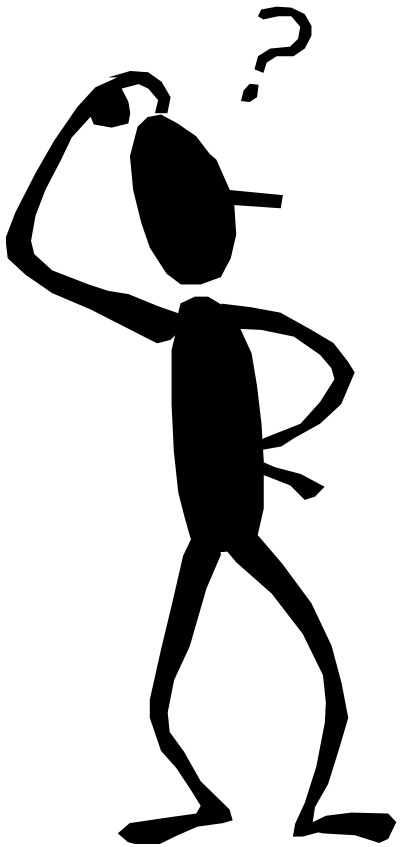



# Jill Detroit




# Q&A



# Backup

# Right of Access Art 15

- Data subjects have right to obtain confirmation of whether a controller is processing their personal information
- If personal data is being processed, controller must provide all the info in Art 15(1), including:
  - Purpose of the processing
  - Categories of data
  - All recipients (or categories of recipients)
  - The period for which the info will be stored
  - Source of data information
  - Requests for data from public authories

# Profiling Art 20

- ‘Profiling' is defined to mean “any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyze or predict in particular that natural person’s performance at work, economic situation, location, health, personal preferences, reliability or behavior”
- Natural persons can object to profiling and must be informed so in a highly visible manner (Art 20 (1))
- Exceptions:
  - Consent (Art 20(2)(c))
  - Performance of a contract (Art 20(2)(a))
  - Allowed by law (Art 20(2)(b))
- Where the results of profiling have legal consequences, there must be significant human involvement in the assessment and an explanation of the decision by a human must be provided when requested

# Processor Obligations Art. 26

- Data processors' legal responsibilities have increased. They now have legal responsibility, regardless of contract (still required), to directly:
  - Maintain documentation of processing operations (Art 28(1))
  - Provide appropriate security (Art 26(2)(c) , Art 30)
  - Notify controllers of breaches (Art 26 (2)(f), Art 31(2)
  - Appoint a DPO (Art 35(1))
  - Obtain controller's consent to conditions for retaining sub-processor (Art 26(2)(d)
- A processor becomes a joint controller if it processes data beyond controller's written instructions (Arts 26(4), 26(3))
- Processors and controllers have joint and several liability to data subjects in private lawsuits for breach of Regulation, unless one can carry burden of proof that it was not responsible (Art. 77)

# Privacy by Default/Design Art 23

- When determining how data will be processed, and during the processing, the controller must implement appropriate technical and organizational measures to assure compliance with the Regulation.
- The controller must ensure that by default only the minimum amount of personal data required for the relevant purpose is collected and it is retained only for the minimum time necessary