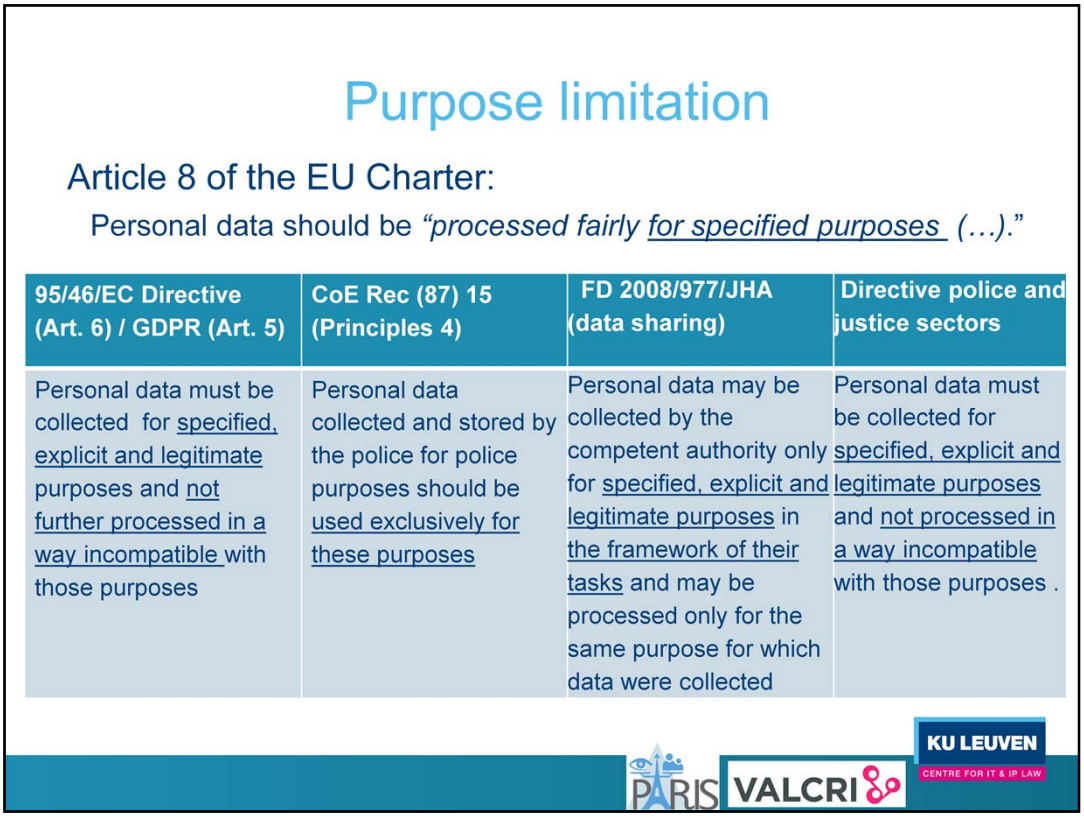
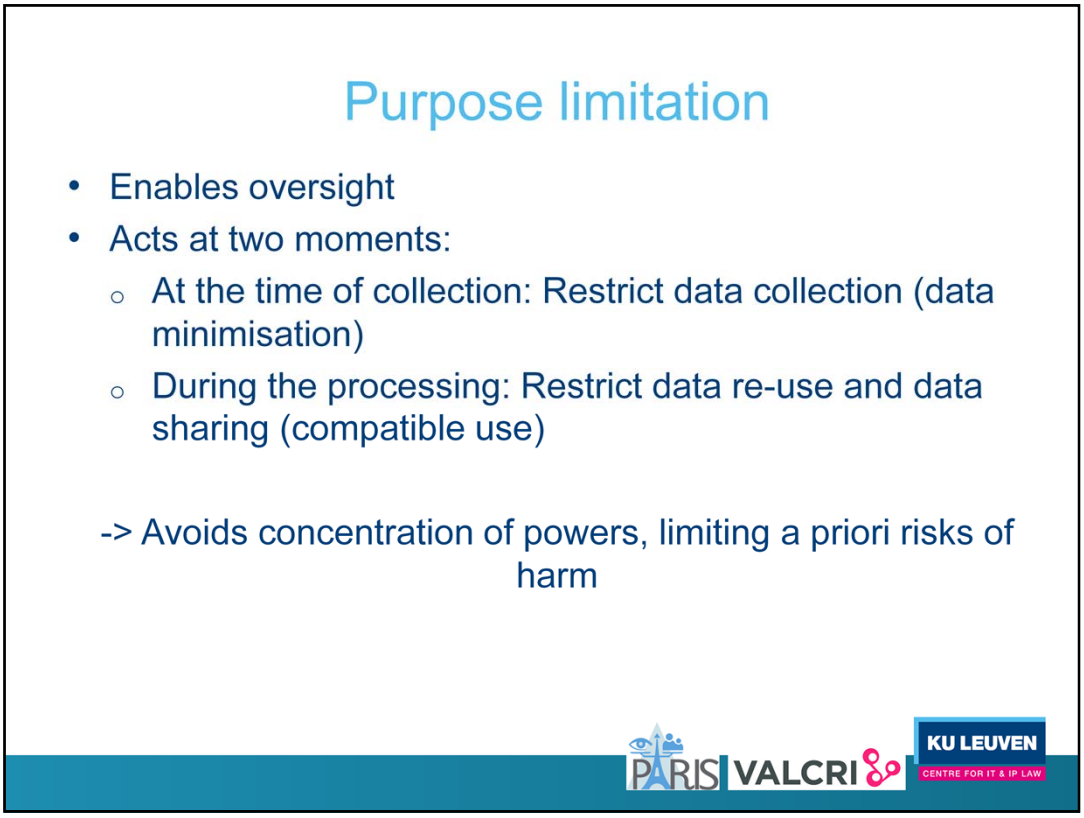
- Ensuring an efficient use of information by police authorities is at the center of the debate right now – and have been for some years already. Failures in information sharing or information availability are always pointed out after a tragedy such as terrorist attacks of 9/11, 2004, 2005, Januaray 2015, November 2015.
- This new societal demand is pushing police to adopt a new "intelligence-led policing" approach. Intelligence-led policing means that police is using methods from Intelligence to process the information available to them. Basically this means 3 things:
    - data should be merged,
    - data should proceesed to be transformed into intelligence
    - Data should flow, ie it be made available on request.
- This is challenging one cornerstone principle of data protection: purpose limitation. Purpose limitation is about: restricting data collection, fragmenting databses and reducing data sharing.

- Example of which are the promises of the intelligence-led paradigm: Minority report
- This is not science-fiction anymore: technology is being developped to visualise big datasets and ease police work.
- From a data protection viewpoint, this means that:
    - we need to allow the creation of mass databases
    - We should authorise a free flow of information between police authorities (ideally of the world) to stop criminals.
- In other words: No more restrictions on data collection and on data sharing. And this is extremely shocking from a data protection perspective. Why? Because of the the purpose limitation principle.



Police purposes are all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.

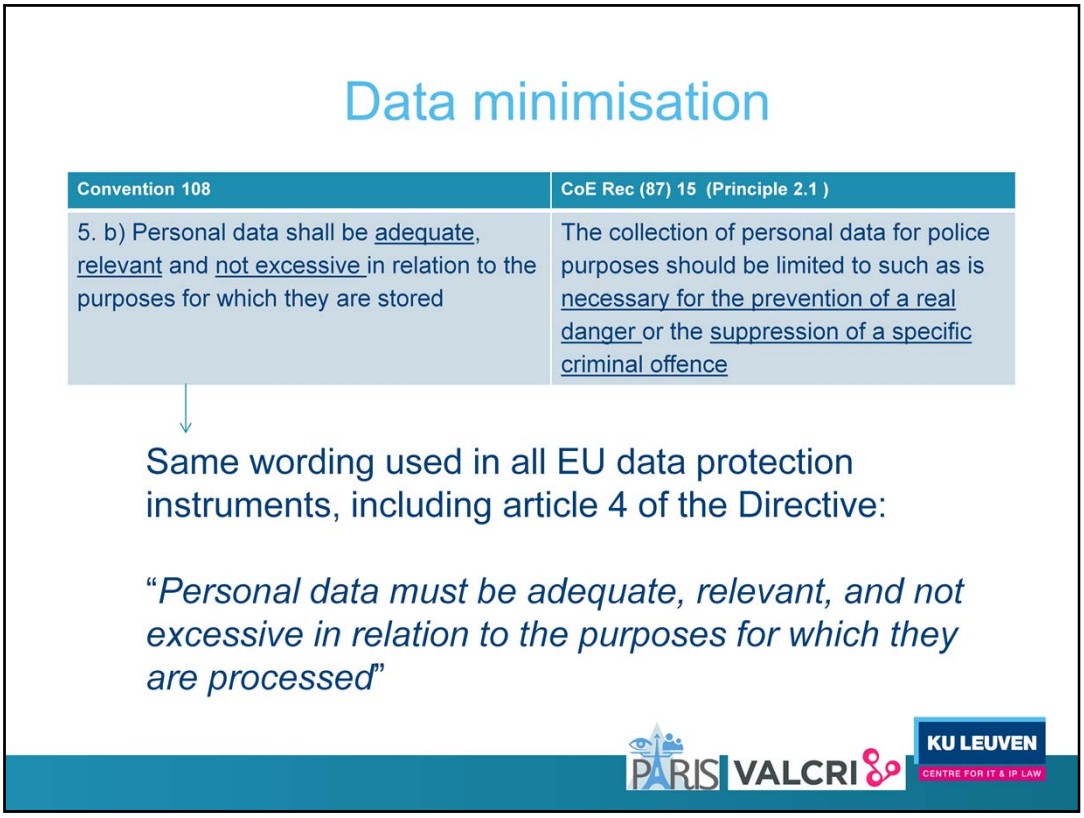


- The very role of purpose limitation is to prevent the creation of mass databases, the linkage of the information. Data protection legislations were drafted in the 70's in reaction to governments' plans to create mass databases about their citizens, be it to improve the efficiency of public administration (in France), for census purposes (in Germany). By memories of WWII and risks of totalitarism were still vivid. Data protection was conceived as a way to prevent abuse of power by public auhtorities.

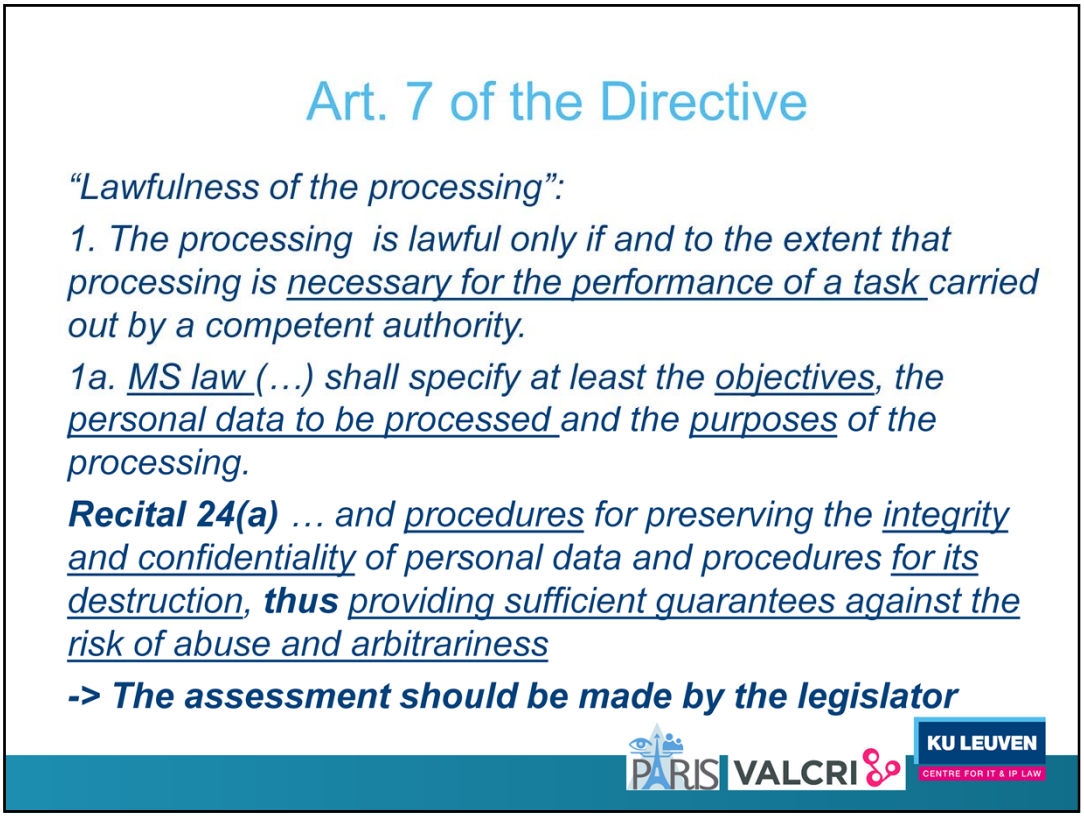
- It worked, ie it could be interpreted in that sense because the technological environment permitted it. Collection, storage were expensive, systems were not interconnected (not networked). Practices were adapted to this technological enviroment. For police, criminal intelligence files were not as evolved, organised crime was not yet an issue of international concern, police held mainly data about the people they suspected of having committed a criminal offence and the information remained separated from the criminal records.

- The question is which role does the principle still play in today's framework?


Data Collection
PARIS
VALCRI
KU LEUVEN
CENTRE FOR IT & IP LAW



- "real danger" should be understood as not being restricted to a specific offence or offender. It includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed. It only excludes unsupported speculative possibilities. (Explanatory memorandum CoE Rec 87) -> broad approach.
- In practice, the assessment of which data are necessary to achieve the purpose of the processing are defined by the legislator, in the instrument regulating the processing.
    - This is true for all EU databases such as VIS, SIS, ect.
    - This is true for EUROPOL : as a way of example, Europol's traditional approach to Analysis Working File (AWF) was to limit the information included in the file and its processing to the specific purpose of the AWF as set up at the time of its creation. Opening orders also specify the conditions under which data may be shared. This way, each AWF forms a closed universe in which all data flows are strictly controlled.

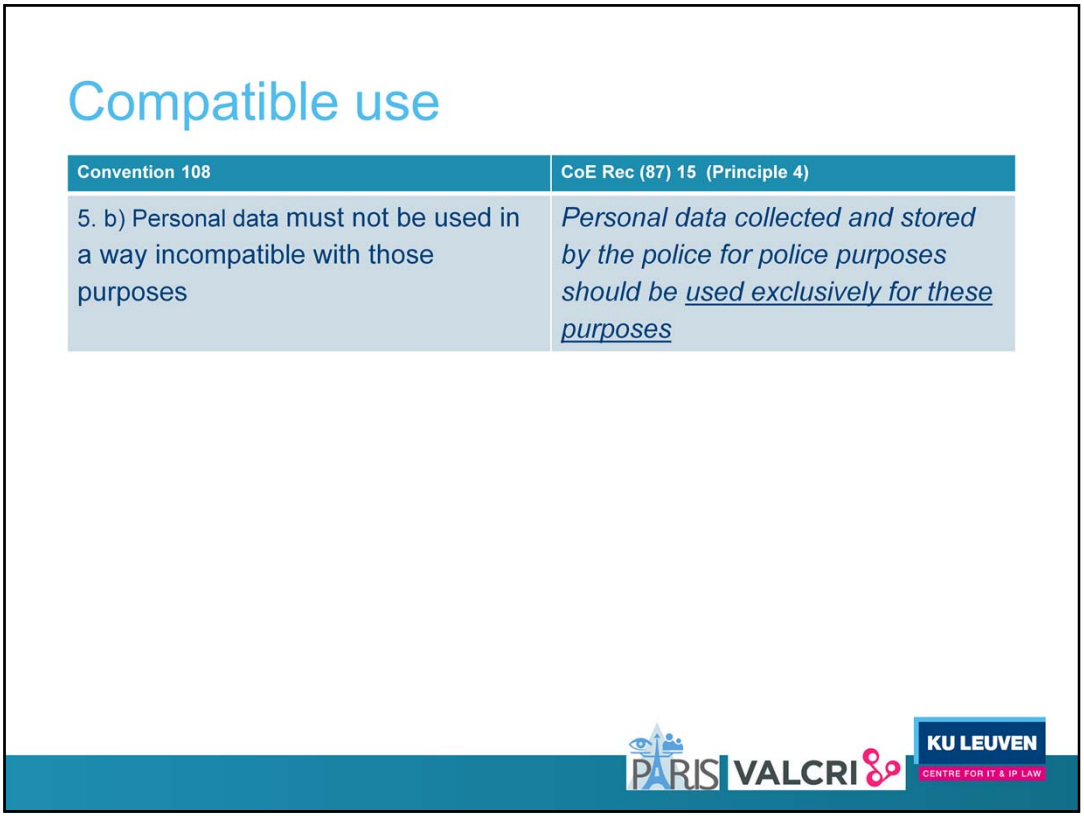


- This practice has been codified in the Directive.
- This is a strong safeguard – at least at first sight. It is only as strong as the purpose of the processing is defined narrowly and as the database cannot be linked to other information, or cannot be shared with other law enforcement authorities. If too rigid it will not stand.
- Let me explain what is happening with EU databases and at Europol.
    - EU databases: The purpose of the database is being broadened to allow more public authorities (law enforcement and EUROPOL) to access the content of the database. E.g. EURODAC
    - EUROPOL: At Europol, they initially had 23 disconnected Analysis Work Files. But the silo-based approach is hindering the efficiency of its analytical work as information stored into one database might be useful to improve the quality of the criminal analysis produced with regard to another database. This functional separation give analysts a "fragmented picture" of the crime, preventing them from connecting some dots and thus making the right links. A few years ago, they changed the approach and merged their 23 disconnected AWF into 2 AWF: one on "serious and organised crime" and the other on "counterterrorim". Analysts are given access to all the information contained in the AWF but they are required to focus their analysis on a specific and predefined purpose. They are thus given access to a broader range of data. The limitation is put on the use they can make of these data.
- In addition: is the definition of the raw data to be inserted into the database

sufficient? What about “non personal data” used to make very detailed profiles of individuals (eg traffic data?) or of the inferences made? If we regulate the data to be processed, the data protection framework should really get interested in these information.

To conclude on data minimisation, even if the Directive takes an interesting step by codyfing this practice, I am not sure the extent to which it is be effective in practice. This safeguard is important to organise further control of abuse of power but it is not sufficient by itself. It should be complemented by other measures.


Use limitation
PARIS
VALCRI
KU LEUVEN
CENTRE FOR IT & IP LAW



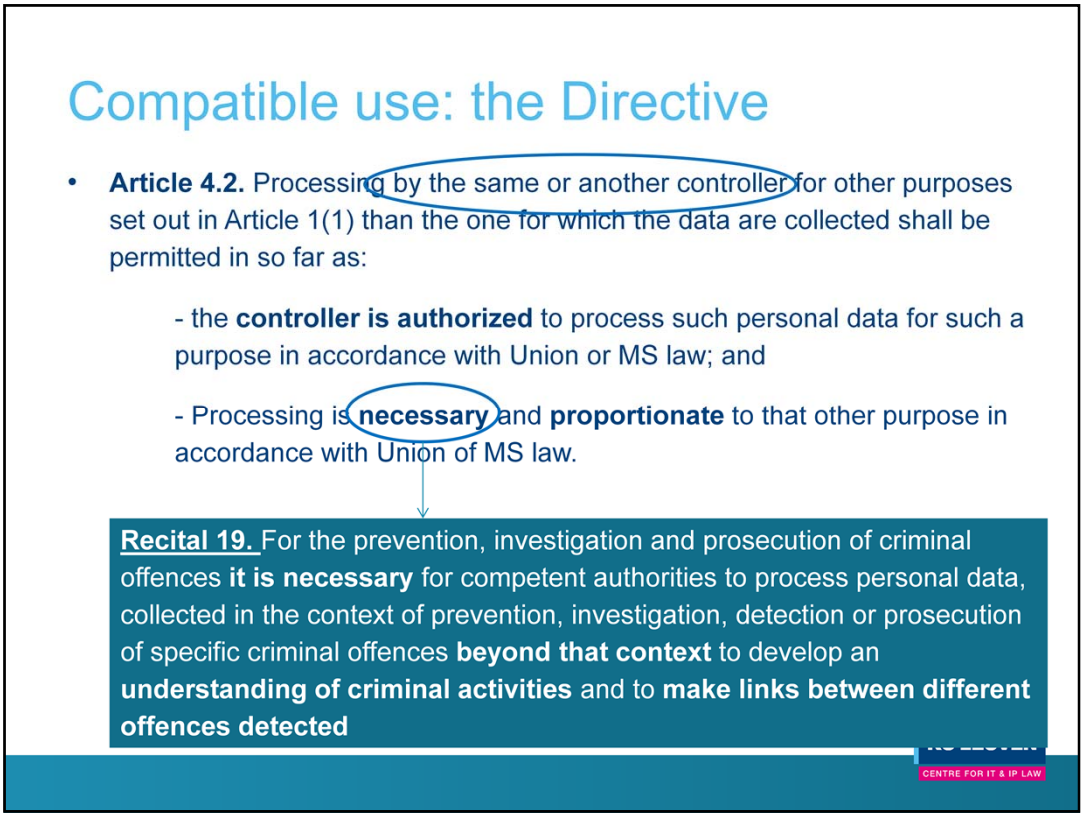
The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.

Compatible use: FD 2008/977/JHA

- 3.2. Further processing for another purpose shall be permitted in so far as:

- **It is not incompatible** with the purposes for which the data were collected
- The **competent authorities are authorized** to process such data for such other purpose in accordance with the applicable legal provisions; and
- Processing **is necessary and proportionate** to that other purpose

- Art 11. List of legitimate purposes:
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted
- Other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- The prevention of an immediate and serious threat to public security; or
- Any other purpose only with the prior consent of the transmitting MS or with the consent of the data subject, given in accordance with national law.



- Article 1 (1): Purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

- Recital 19 explicitly authorises big data analytics. It says it is necessary. So we can only hold to the second criteria: the one of proportionality. In that regard, it would have been helpful to include some of the criteria to take into account to do the porportionality assessment, as was done under the Regulation (Art. 6.3a) that's a pity that the criteria included into the Regulation to make the assessment of compatible use are not included or adapted for the Directive.
- What is also interesting is that this provision will apply to any data sharing with third parties. While the CoE Rec. distinguished between sharing with other police bodies, with other public authorities, international bodies and private parties, the Directive opts for setting the general principle and then to make qualifications.

To conclude about compatible use: Limitations will come from the law regulating the recipient's scope of competence (weak) and the test of proportionnality. The question is thus:

- which crietria will used to make this test
- how the data controller will be made accountable about the balancing.
- Is it through the verification of DPIA (but only for data processing with risks) ?

- On a systematic basis?
- Upon request of the supervisory authority?


Sharing with third parties
PARIS
VALCRI
KU LEUVEN
CENTRE FOR IT & IP LAW

Within the police sector

CoE Rec (87) 15 (Principles 2.1 & 4)	Directive police and justice sectors
5.1. Within the police sector: • Legitimate interest for data sharing • Scope of competence of recipient	• Further use is not incompatible with original purpose of collection • Scope of competences of recipient • Necessary and proportionate to that other purpose

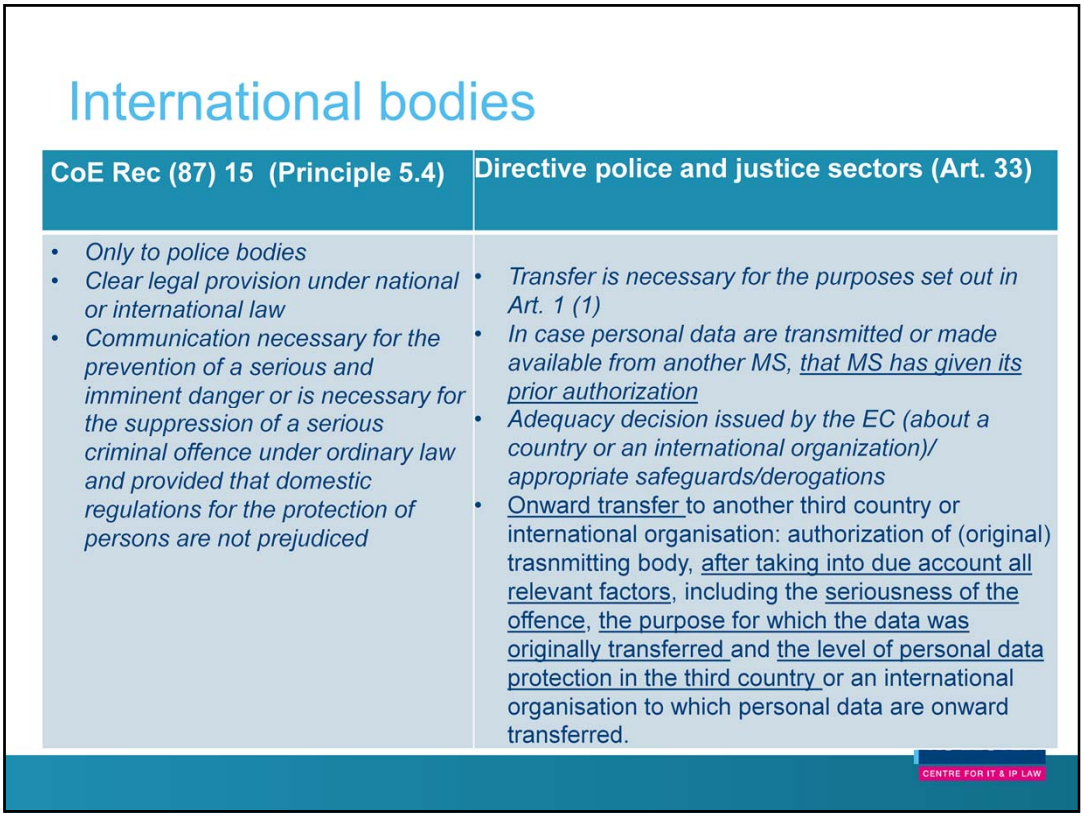
With other public bodies

CoE Rec (87) 15 (Principles 5.2)	Directive police and justice sectors

• Legal/DPA authorisation
• Indispensable to fulfill tasks of the recipient
  • AND not incompatible with original processing
  • AND legal obligations of transmitting party not contrary
• In the interest of the DS/ the DS has consented (or clear presumption)
• Necessary to prevent a serious and imminent danger
	• Further use is not incompatible with original purpose of collection
	• Scope of competences of recipient
	• Necessary and proportionate to that other purpose
	
	Art. 3 (8) - Public authorities which may receive data in the framework of a particular inquiry in accordance with national law shall not be regarded as recipients (ref. to applicable specific data protection rules).

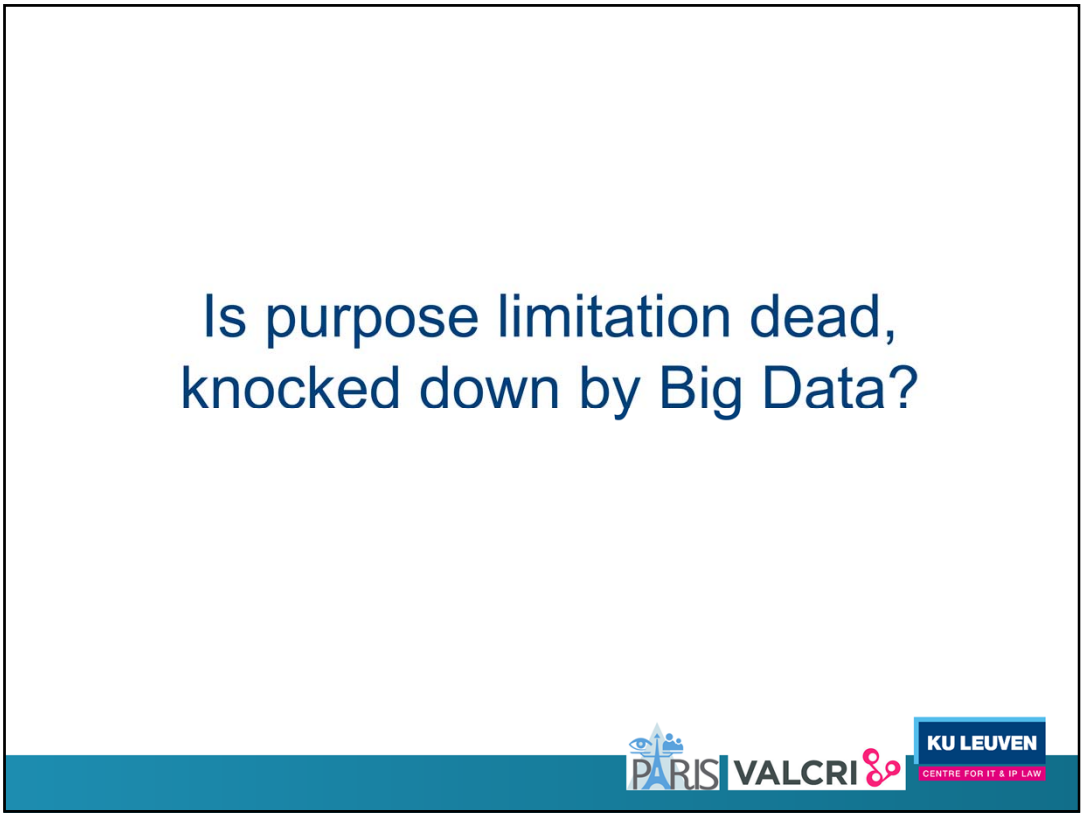
To private parties

CoE Rec (87) 15 (Principles 5.4)	Directive police and justice sectors
• Legal/ DPA authorisation • In the interest of the DS/ the DS has consented (or clear presumption) • Necessary to prevent a serious and imminent danger	• Further use is not incompatible with original purpose of collection • Scope of competences of recipient • Necessary and proportionate to that other purpose ***Recital 24(b)**: The Directive applies to the transfer except if purpose does not fall under the scope of the Directive*



- **To conclude about data sharing: Challenge here is about ensuring that the data transferred are processed according to the standards of the transmitting body. (the Directive is of minimum harmonisation).**
    - **One provision only : article 7a.** Member States shall provide that where Union or Member State law applicable to the transmitting competent authority provides specific conditions for the processing of personal data, the transmitting competent authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them. But how to enforce this provision? (PbD?) Nothing anymore about the request of the transfer.


Conclusion
PARIS
VALCRI
KU LEUVEN
CENTRE FOR IT & IP LAW



- Purpose limitation as we have implemented it so far seems linked to a specific technological environment and difficult to implement as such in our current technological environment.
- The wording of the Directive is broad enough to accomodate the use of big data and the implementation of ILP.
- We should thus reinvent how we implement the purpose specification principle. We should think of adequate counte weights to processing practices under big data. For that we need several complementary mechanisms.
- The Directive already contains some safeguards:
    - Requirement for the legislator to include into the law regulating police data processing activities to make the first proportionality assessment
    - Still we have seen an increased reliance on necessity and proportionality to further limit the processing activities. It is important to know who will make the assessment and who will check if this assessment is done correctly:
        - New provisions requiring the appointment of a DPO. But DPOs are internal to the organisation so they cannot be expected to veil for data subjects' rights
        - The role of supervisory authorities will thus be key. Hopefully DPAs will be entrusted with this role. This would enable to ensure consistency in the interpretation of the rules of both the GDPR and the Directive
    - Controls are facilitated by the provisions on logging.
- Data sharing is extensively allowed. Mechanisms of control should be implemented to ensure that once the data are shared they are processed according to the

provisions of the Directive or of national laws.

- The Directive foresees that the transmitting body can inform of specific processing conditions attached to the data. Within the EU we can expect that either the DPO of the recipient or the supervisory authority could check whether the data are processed according to these conditions. The obligation to log any operation on the data facilitates this control.
- But what happens when data are shared outside the EU? Which mechanisms are available? This is an important question that should be included into the agreeements or the adequacy decisions adopted by the EC.

fanny.coudert@law.kuleuven.be
KU Leuven Centre for IT & IP Law - iMinds
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip