Workshop on documentation under "New 45": Case studies for threshold assessment

For each of the three scenarios below, please go through the draft form for a threshold assessment and see which criteria you think they meet. There is no need to justify your assessment on the form in these case studies (while in a real threshold assessment, the controller would need to do so in some cases).

A. Data loss prevention

EUI's HR and IT departments want keep a closer eye on its staff's internet and e-mail use. EUI handles lots of sensitive information and there have been a number of leaks affecting EUI's interests recently.

The product they currently favour supports breaking SSL-encrypted connections (to detect exfiltration of internal documents). It can be set up to exclude certain domains from this (online banking and similar). The vendor would do parts of the technical management of the system remotely from a service centre in a third country.

The system also allows monitoring turnaround times for exchanges with the outside world, and some middle managers would be interested in using this for evaluation purposes.

B. Staff evaluation

EUI's HR department is reviewing the staff appraisal process. The new process streamlines the previous version and sticks closely to the Staff Regulations.

The appraisal guide for line managers mentions that they may take metrics from the case management system into account (number of cases closed, deadlines missed and similar). The guide also points out that pure numbers are not always a good indicator of performance (e.g. colleagues who closed fewer, but more complex cases than the average or deadlines missed due to circumstances beyond their control).

C. High-tech CCTV

EUI wants to upgrade its CCTV system following a reassessment of its security needs.

Apart from standard CCTV covering entry points and similar, this will also include an automated number plate recognition system at the entrance to the car park and a system to automatically track persons in open areas on EUI premises (courtyard used as break area, not publicly accessible, only activated outside of working hours). Another aspect is that following a remodeling of EUI premises, there is now a publicly accessible plaza on EUI premises, just in front of EUI's main entrance, which locals often cross or spend time in (some of the railings have become favorite spots of local skaters). For this plaza, EUI's security team wants to install a similar tracking system with "loitering detection", meaning that it will automatically focus on persons remaining in place "abnormally long" and put the footage on the CCTV operator's main screen.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

I Header			
Name of processing operation	[name]		
Controller contact point	[name and contact details]		
Record of processing operations	[record reference]		
DPO consultation	[date of feedback]		
Approval	[name and date]		
II Criteria for high risks			
Criterion: do your processing operations present any of the characteristics mentioned below?	*Applicable? Yes [if so, describe how] / No [if borderline: why not?]*		
	A	*B*	*C*
1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting. *Examples: a bank screening transactions under applicable law to detect possibly fraudulent transactions*			
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects *Example: automated staff appraisal ("you're in the lowest 10% of the team for the number of cases dealt with, so you'll receive a 'unsatisfactory' mark, no discussion")* *Counterexample: a news site showing articles in an order based on past visits of the user.*			
3. Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of internet use. *Examples: covert CCTV* *Counterexample: overt CCTV of garage entry not covering public space*			
4. Sensitive data: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive. *Examples: pre-recruitment medical exams and criminal records checks, any use of 1:n biometric identification // Counterexample: photos are not sensitive as such*			

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

5. Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage. *Examples: European databases on disease surveillance* *Counterexample: internal phone directory*			
6. Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *Example: covertly merging access control logs, computer logs and flexitime declarations to detect absenteeism // Counterexample: transferral of personal file following a change of institution.*			
7. Data concerning vulnerable data subjects: situations where there is an imbalance of power in the relationship between the position of the data subject and the controller. *Examples: children, asylum seekers // Counterexample: EUI staff are not a priori considered as vulnerable vis-à-vis their employer concerning standard procedures laid down by the Staff Regulations.*			
8. Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage, especially where personal and social consequences of the deployment of a new technology may be unknown. *Examples: machine learning, connected cars // Counterexample: 1:1 fingerprint access control*			
9. Data transfer to recipients outside the EU/EEA *Examples: outsourcing to companies outside the EU/EEA; structured cooperation with an international organisation leading to the exchange of personal data.*			
10. Preventing data subjects from exercising a right or using a service or a contract. *Examples: exclusion databases, credit screening // Counterexample: establishment of rights on entry into service (this is only about leaving persons "worse off" compared to the status quo ante).*			
III Conclusion			
Number of "Yes" ticked above			
Assessment: if you have two or more "yes" in the list above, you should carry out a DPIA. If you consider that in the specific case at hand, risks are not "high" even though you have two or more "yes", explain and justify why you think the processing is in fact not "high risk".			