The concept of data protection law

Controlling informational risks through (not to) the right to data protection

BACKGROUND

Harm-based vs risk-based approaches of protection

In liberal legal systems, laws usually apply a reactive harm-based approach: if harm occurs, the responsible person must restore the original state.

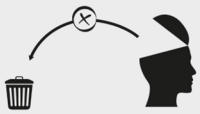
However, in certain situations, laws apply a proactive risk-based approach: they seek to prevent harm before it may occur.

GENERAL REASONS FOR A RISK-BASED APPROACH

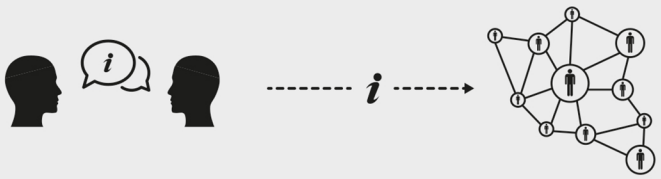
A risk-based approach may be preferable, for example, if harm cannot be restored (e.g. in the case of death)...

... or if it is difficult to determine, reactively, which single action has caused the harm (e.g. in the case of environmental pollution).

REASONS FOR RISK-BASED APPROACH REGARDING PERSONAL INFORMATION



The same idea applies to personal information: Once somebody knows something about another one, it is impossible to erase that information...



... and it is difficult to prove afterwards whether this information has been passed on and abused (e.g. by false friends, insurance companies, etc.).

INFORMATIONAL POWER ASYMMETRY AS THRESHOLD FOR LEGAL PROTECTION

The **ECHR** affirms protection only if personal information is *systematically and permanently* stored (not protection of information per se).

The **BVerfG*** sees the special risk in the *automated* processing (i.e. access data instantly and globally, create vast profiles and repurpose the data).

Against this background, how will the ECJ assess data processing risks?

* German Constitutional Court