Legal Basis/Bases

Legal basis

And some rule-of-thumb questions…

Necessary for contract: *"is there an agreement?"*

Necessary for legal obligation: *"what law requires it?"*

Necessary for vital interest: *"is life at risk?"*

Necessary for public interest: *"is this described in law?" (tax, health, …)*

Necessary for legitimate interest: *"would individual expect it?"*

Consent: *"is this truly optional for both of us?"*

Necessary for a contract

"Is there an agreement between us?"

"Necessary" = no less intrusive way to do it

Directly linked to delivery of contract/service (Article 29 WP)

So, do I need **that** information/process, or can I deliver with less?

» E.g. pseudonyms, attributes, …

» E.g. trusted third parties

For example: site-licensed on-line content

Necessary for a legal obligation

"Is there a law requiring it?"

Law should specify required processing

» Do what it says, and no more

For example: employee salaries => HMRC

Necessary for vital interests

"Is someone's life at risk?"

And, by Art.9(2), Special Category Data only if they are incapable of consenting

Other Art.9(2) provisions cover, e.g. occupational health

- Specific and often subject to additional conditions
- Basis may be "necessary for contract", "legitimate interests", etc.
- Must satisfy conditions for those, too

For example: 999 mobile phone location, life-threatening allergies, …

Necessary for public interests

"Is there a law permitting it?"

The least clear justification. Is it…

» Helping someone else with their legal obligation? (Art.29) or

» Legitimate interests for public authorities? (ICO, sometimes) or

» Where law **permits** you to exercise special powers? (cf. *Foster v British Gas*)

UK Data Protection Bill heading for the last of these

Same as Legitimate Interests, but no need to consider DS rights/freedoms!

» So (DS plea) use LegInt if appropriate till ICO tells you it's a "task"

For example: prevention/detection/investigation of crime (DPA s.29)

Necessary for legitimate interests

"Would the individual expect this?"

Three tests for data controller:

» Is purpose legitimate? and

» Is processing necessary to achieve purpose? **and**

» Are benefits overridden by rights & freedoms of individuals?

Individual can demand review of third test if his/her risks are different

For example: (Recital 49) protecting network & information security

Free Consent

"Is this truly optional for both of us?"

Designed to be narrow: "reduce over-use of consent"

- Individual informed of consequences of granting/refusing consent
- No (significant) detriment
  - E.g. not bundled with service, not in imbalanced relationship
- Expressed by positive action (no pre-ticked boxes)
- Revocable at any time, by same means as it was given

If this looks hard, consent is probably the wrong basis

Rule of (ANC's) thumb: does process let individual lie/walk away?

For example: (usually) choice of social media avatar