

Does the GDPR Really Have Teeth? That Is, Will It Make a Difference?

Richard Hill

ISOC-CH

Workshop on GDPR

ISOC Portugal

25 May 2018

Outline of presentation

- Key differences to Directive
- Consent
- What if Microsoft Ireland case had been subject to GDPR?

Key Differences to Directive

- Extra-territorial effect
- Fines for non-compliance
- Data portability
- Right to be forgotten
- Most big data controllers seem to be OK with the GDPR, so no big change?

Processing allowed if consent Directive

- 7(a): “the data subject has unambiguously given his consent”
- 6.1(b): must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”

Processing allowed if consent Regulation

<http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>

- 6.1(a) : processing of data is lawful if “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=62305 1

And ...

- 5(a): data must be “obtained and processed fairly and lawfully”
- 5(b): data must be “stored for specified and legitimate purposes and not used in a way incompatible with those purposes”

So ...

- Was the consent sufficiently “specific”?
- Was data obtained “fairly”?
 - Does this open grounds to enquire if a data controller is abusing a dominant position to impose unfair terms and conditions on consumers who have no real choice?

When is consent freely given?

- Whereas (42): “Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment”
- Whereas (43): “Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance”

European Data Protection Supervisor:

https://edps.europa.eu/press-publications/press-news/blog/accept-and-continue-billions-are-clocking-digital-sweat-factories_en

What about previously collected data?

- GDPR Whereas (171): “Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation”

Microsoft vs. United States

[https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp._\(2018\)](https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp._(2018))

- US law enforcement seeks data held in Ireland re a drug dealer
 - Now moot because of CLOUD act
 - CLOUD act envisages transfers without judicial supervision and without treaty-level agreements
- <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>
- How would it be handled under GDPR?

Art. 48

- foreign transfers “may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty,”
- but “without prejudice to other grounds for transfer”

http://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

Public interest exception

- 49(1)(d): “necessary for important reasons of public interest”
- 49 (4) public interest must be one “recognised in Union law or in the law of the Member State to which the controller is subject”

Fighting crime

- “In general, Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest”

Interest of controller

- 49 (1): transfer “necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject”
- “The legitimate interest could, again, be the interest of the controller in not being subject to legal action in a non-EU state”

But ...

- Such transfers are permissible “only if the transfer is not repetitive,”
- only if it “concerns only a limited number of data subjects,” and
- only if “the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data”

So the correct legal answer is

- “It depends”
- Who could test the decision in court?
 - foreign drug dealer?
 - EU data protection authority?
 - EU citizen?
 - Would the data subject even know about the transfer?