Findings and recommendations – use of Microsoft products and services

Adeline Morris
Massimo Attoresi
Snezana Srdic
Zsofia Szilvassy
EDPS

47th DPO meeting, 8 May 2020

Overview

- The inter-institutional licence agreement
- Microsoft as controller
- The controller-processor agreement
- Data location, transfers, disclosure
- Technical measures
- Planning new services
- Q&A

The ILA (2018)

- Negotiated umbrella agreement:
  - Master Business Services Agreement
  - Enterprise Agreement
- Enrolments
- Standard documents, e.g.
  - Online Services Terms
  - Product Terms
  - Data Protection Addendum

The procurement process

- Commission = lead institution
  - manages the contract
  - assists other institutions with implementation
- Other institutions = controllers
  - accountable
  - ensure data protection by design and default

Microsoft as controller

- Unilateral amendment
- Limited data protection obligations
- Insufficient purpose limitation

Unilateral amendment

- Unlimited right to modify standard documents
- Standard documents may trump negotiated provisions
- Recommend: unambiguous order of precedence + changes by common agreement

Limited obligations

- Negotiated terms only cover data *provided* through use of the *online services*
- Microsoft decides how other categories of data protected
- Recommend: broaden scope to cover all personal data

Insufficient purpose limitation

Insufficient purpose limitation

- "*to provide the Product or Professional Services*" (MBSA)
- Data Protection Addendum
  - "*providing personalized user experiences*"
  - "*ongoing improvement*"
  - no "*advertising or similar commercial purposes*"
  - as controller for "*legitimate business operations*"
- Recommend: specific + exhaustive set of purposes

Consequences

- Dual legal regime: GDPR and Reg. 2018/1725
- Makes supervision and enforcement messier
- Brings in legitimate interests processing by the back door?
- Recommend: institutions be sole controllers

Controller-processor agreement

- Controllership rights
- Sub-contractors
- Audit rights
- Recommend: comprehensive controller-processor agreement

Sub-processors

- General authorisation is limited in scope
- No other authorisations?
- Insufficient information on sub-processors
- Don’t want to authorise? Stop using Microsoft software

Sub-processors

- Recommend:
  - prior authorisation for all sub-processors
  - full information
  - institutions give authorisation freely

Audit rights

- "*Security audits*" arranged by Microsoft
- Not data protection audits?
- Not audits "*conducted by the controller*"

Audit rights

- Recommend:
  - detailed, effective audit rights
  - full information
  - regular, risk-based audit programme

Data location

- *Some* data *provided* through use of *'core' online services* stored in EU
- Other data can be transferred outside EU/EEA
- Route taken by data in transit unknown

International transfers

- Limited instructions on what to transfer, when and for what purpose
- No detailed safeguards
- SCCs not compliant

Unauthorised disclosure

- Microsoft can disclose if considers has a legal obligation
- Protocol and Reg. 2018/1725 may not protect institutions

Consequences

- Difficult to check compliance if data outside EU/EEA
- Difficult to protect data in transit if don’t know route
- Difficult for data subjects to enforce rights if no safeguards
- Difficult to enforce EU law to prevent disclosure

Consequences

- Recommend:
  - location of data specified for each service
  - complete safeguards for transfers
  - strict controls + full info on disclosure
  - control over sub-processors
- Or: processing in EU/EEA as a rule
- Consider strategy for medium term

Technical measures

- Block unlawful flows
  - functional controls (e.g. diagnostics configuration)
  - network filters (as necessary)
- Test applied measures
  - indeed seek provider’s support, yet...
  - challenge provider’s assumptions and statements

Planning new services

- Cloud Computing GLs still valid
  - This guidance details them on the contractual part
- “Cloud option” methodology
  - High level assessment on whether “candidate” to the cloud. If so...
  - Identification of available solution or requirements for procurement.
  - Assessment of the specific DP risks in supporting the targeted processing

Questions?

EDPS

thank you!

@EU_EDPS

For more information:

www.edps.europa.eu

edps@edps.europa.eu