Use of Microsoft Products and Services: Findings and Recommendation

47th DPO Day Online Edition

Adeline Morris  Massimo Attoresi  Snezana Srdic  Zsofia Szilvassy

8th May 2020
Table of contents

1. Inter-Institutional Licence Agreement
2. Microsoft as Controller
3. Controller-Processor Agreement
4. Data Location, Transfer, Disclosure
5. Technical Measures
Inter-Institutional Licence Agreement
Inter-Institutional Licence Agreement (2018)

- Negotiated umbrella agreement
  - Master Business Services Agreement
  - Enterprise Agreement

- Enrolments

- Standard documents, e.g.
  - Online Services Terms
  - Product Terms
  - Data Protection Addendum
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
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
• 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 ii

GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
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
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

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’

Recommend:

• detailed, effective audit rights
• full information
• regular, risk-based audit programme
Data Location, Transfer, Disclosure
• 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

Recommend:

• location of data specified for each service
• complete safeguards for transfers
• strict controls + full info on disclosure
• control over sub-processors
Technical Measures
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
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 and Answers