WORKSHOP DATAMINING AND TAX
23 NOVEMBER 2017

PRIVACY CONSIDERATIONS ON DATA MINING AND PROFILING

FACULTEIT RECHTSGELEERDHEID

Dr. Sylvie De Raedt
Postdoctoral researcher

UNIVERSITEIT GENT

GENERAL OVERVIEW

- General principles on data protection -> applied on data mining and profiling in tax matters
  - Profiling =automated processing of personal data to evaluate certain personal aspects relating to a natural person (GDPR-def)
  - Example: potential fraud
- The impact of the Law of 3 August 2012

GENERAL PRINCIPLES ON DATA PROTECTION

- 70s: use of mainframes by public authorities, large amount of personal data can be stored and shared: public debate on the right to private life: is art. 8 ECHR sufficient for legal protection?

- No -> data protection regulation was established : set of rights for the data subject + obligations for the processor and controller of the data

- Legal instruments:
  - Council of Europe (Convention n° 108 (1980) on automatic processing of personal data),
  - EU (Directive 95/46 on the protection of personal data; Regulation 2016/679 (General Data Protection Regulation – GDPR)

GENERAL PRINCIPLES ON DATA PROTECTION SCOPE

- Every processing of personal data
- *Personal data* = data relating to an identified or identifiable **natural person**
  - Relating to: direct (e.g. income) or indirect (e.g. value of a house, if the owner of the house is identifiable; e.g. income of a legal person with an official name relating to a natural person (eg. shareholder)(ECJ 9 November 2010, SCHECKE)
  - ! Tax information on legal persons can contain personal data (e.g. tax return, information on directors, employees, ...)
  - ! -> Creating risk profiles of companies ***can*** involve personal data
  - Identifiable: encrypted data, used for tax data mining, are also personal data
  - ! a lot of processing is mixed -> the principles of data protection have to be respected (Opinion 4/2007 art. 29 WP)

GENERAL PRINCIPLES ON DATA PROTECTION SCOPE

- Every *processing* of personal data
  - Processing = collection, storage (in data warehouse) and every manipulation/treatment of personal data

- Conclusion: storage of (encrypted) personal data in a data warehouse, the mining of the data, the profiling = principles of data protection have to be respected

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- Which principles?

- *1. the processing has to be legitimate*

  - Limited reasons, e.g.consent
  - In the framework of taxation / data mining of profiling for tax purposes : this is mostly the case

  - processing is legitimate when:
  - - processing is necessary for compliance with a legal obligation or
  - - when necessary for public interest

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- Which principles?

- *1. the processing has to be legitimate*

  - Processing of certain categories of personal data is prohibited, unless specific conditions are fulfilled
    - (GDPR definitions)
    - Sensitive data and medical data (possibilities to remove the prohibition are irrelevant in tax matters):
      - Sensitive data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership + genetic data, biometric data for the purpose of uniquely identifying a natural person + data concerning a natural person's sex life or sexual orientation
      - Medical data (data concerning health)
    - Personal data relating to criminal convictions and offences (no prohibition for public authorities if processing is strictly necessary)

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- Which principles?

- *2. the condition of data quality has to be fulfilled:* personal data must be:
  - A.Collected only for specified, explicit and legitimate purposes (principle of purpose limitation)
    - Specified: in order to assess the principle of proportionality -> “taxation” is not specific enough
    - Explicit -> data subject has te be able to know ->
    - -> not easy to fulfil in data mining : processing of big data -> purposes not always known from the start
    - Incompatible reuse is forbidden (purposes of reuse are incompatible with the purposes of collection), unless allowed by an explicit law and insofar as strictly neccessary
    - What is incompatible reuse?: criterion of reasonable privacy expectation is important -> e.g. reuse of data of energy suppliers for tax profiling is incompatible reuse

    B. Adequate, relevant and not excessive for those purposes (principle of proportionality, or data minimisation)

    - is data mining of certain categories of personal data strictly necessaray for the specific purpose of the data mining / profiling?
    - -> not easy to fulfil in data mining -> as much as possible?

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- Which principles?
- *2. the condition of data quality has to be fulfilled*: personal data must be:
  - C. Processed fairly and in a transparent way (the transparency-principle)

- -> also data mining
- -> 2 important transparency rights :
- 1.general right to information (13 and 14 GDPR)(on purposes, on recipients, …)
  - Art. 13.2.f. GDPR: when personal data is collected from the data subject: informed on the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
  - Practice: tax return is accompanied by a vague privacy statement
- 2. general right to access (15 GDPR): access to involved logic

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- Which principles?

- *2. the condition of data quality has to be fulfilled*: personal data must be:
  - D. other principles of data quality that require (mostly) technical measures: principle of accuracy, principle of storage limitation, appropriate security measures
    - -> in framework of data mining and profiling (GDPR considerations):
    - - appropriate mathematical or statistical procedures for the profiling,
    - - ensure that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised,
    - - prevent discriminatory effects on natural persons

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- 3. *automated individual decisions which include evaluating personal aspects relating to a data subject are forbidden* (art. 15 Directive 95/46, art. 22 GDPR)
  - "personal aspects": e.g. person is a potential fraud (not: the conditions for taxation are fulfilled)
  - "decision" = legal effects or significantly affects the person, e.g. decision for a tax audit
  - "automated" = solely automated processing, without significant human intervention (not: the automated processing has been a an aid)
  - -> ! data mining that leads to profiling is – as such - not forbidden
  - -> profiling followed by an individual decision is forbidden

GENERAL PRINCIPLES ON DATA PROTECTION PRINCIPLES

- 3. *automated individual decisions which include evaluating personal aspects relating to a data subject are forbidden* (art. 15 Directive 95/46, art. 22 GDPR)

- Exception:
  - 1) there is a legal basis (GDPR refers to profiling for fraud and tax evasion monitoring)
  - 2) which lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests
    - Belgian Data Protection Law: possibility to express his or her point of view
    - GDPR: considerations: inform the data subject, the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision

- Even then: basis principles of data protection have to be fulfilled.... See previous remarks -> moving towards the principles of non-discrimination to assess data mining and profiling?

LAW OF 3 AUGUST 2012

- (1) Is there a legal basis in Belgium for automated individual decisions on personal aspects of the tax payer (audit because of risk to be a fraud)?

- Article 5 § 1 of Law of 3 August 2012:
  - (free translation) “the Ministery of Finance can combine the personal data gathered in the framework of its legal assigment in order to establish a datawarehouse which – on the one hand - allows to perform targeted audits on the basis of risk indications and – on the other hand – to perform analysis on relational data”

- = legal basis for data mining, at the most a legal basis for profiling (see preparatory documentation of the Law), not a clear legal basis for automated decision-making

LAW OF 3 AUGUST 2012

- Conclusion:

- Automated decision making is still prohibited,
- substantial human intervention has to be present -> no transparency
- In practice: selection of audits is made by central tax autorities on the basis of risk profiles -> mandatory for local tax authorities

LAW OF 3 AUGUST 2012

- (2) are there suitable measures to safeguard the data subject's rights ?

- Article 5 § 2 Law 3 August 2012: The Sectoral Committee on the federal government (within Privacy Commission) has to authorize the addition of every category of data to the datawarehouse
- ***can*** be a safeguard of the data subject's rights:
  - Purpose limitation: e.g. control on incompatible reuse
  - Proportionality: is data mining of certain categories of personal data strictly necessaray for the specific purpose of the data mining / profiling?
  - Transparency: authorizations are public

LAW OF 3 AUGUST 2012

- (2) are there suitable measures to safeguard the data subject's rights ?

- Practice: authorization 08/2015:
  - unclear definition of categories of personal data (transparency…)
  - no remarks on principle of purpose limitation (but no problem with reasonable privacy expectations? (belcotax, tax returns, …))

LAW OF 3 AUGUST 2012

- (2) are there suitable measures to safeguard the data subject's rights ?

- Others?

- the right to obtain human intervention?
- The right to express his or her point of view?
- The right to obtain an explanation of the decision reached after such assessment (and to challenge the decision)?

CONCLUSIONS

- Tax data mining and profiling = (mostly) processing of personal data
- Data mining on sensitive and medical data is principally forbidden
- Reuse of incompatible information is principally forbidden
- automated individual decisions which include evaluating personal aspects relating to a data subject are forbidden, unless legal basis + safeguards
- There is no clear legal basis to allow automated decision making
- Insufficient measures to safeguard the data subject’s rights