Centre for Information Policy Leadership Working Session

Profiling, Automated Decision-Making and Cross-Border Data Transfers under the GDPR

Tuesday, 7 November 2017

Brussels

Centre for Information Policy Leadership
Hunton & Williams LLP

Welcome & Introduction

Bojana Bellamy

President

Centre for Information Policy Leadership

Centre for Information Policy Leadership
Hunton & Williams LLP

CIPL at a Glance

BRIDGING REGIONS
BRIDGING INDUSTRY & REGULATORS
BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

55+ Member Companies	We **INFORM** through publications and events	We **NETWORK** with global industry and government leaders
5+ Active Projects & Initiatives	We **SHAPE** privacy policy, law and practice	We **CREATE** and implement best practices

20+ Events annually

15+ Principals and Advisors

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, Brussels and London
- Founded in 2001 by leading companies and Hunton & Williams LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age

Twitter.com/the_cipl
https://www.linkedin.com/company/centre-for-information-policy-leadership
www.informationpolicycentre.com

2200 Pennsylvania Ave NW
Washington, DC 20037
Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium
30 St Mary Axe
London EC3A 8EP

CIPL GDPR Project Deliverables to Date

www.informationpolicycentre.com

5 Workshops and working sessions

- Amsterdam (Kick-off), Paris (DPO, Risk), Brussels (Certifications), Madrid (Transparency, Consent, Legitimate interest) , Dublin (Regulating for Results)

7 CIPL Papers Submitted to WP29

- DPO
- Risk and DPIA
- One Stop Shop and Lead DPA
- Certifications
- Transparency, Consent, Legitimate Interest
- ePrivacy Regulation
- Regulating for Results

4 CIPL Responses to WP29 Guidance

- DPO, Data Portability, Lead SA, DPIA

GDPR Readiness Survey Report 2016

CIPL Papers in Progress

- Profiling and Automated Decision-Making
- Security Breach Notification

Centre for Information Policy Leadership
Hunton & Williams LLP

Special Opening Remarks

Giovanni Buttarelli

European Data Protection Supervisor

Centre for Information Policy Leadership
Hunton & Williams LLP

Session I

Profiling and Automated Decision-Making under the GDPR: GDPR Provisions and the Guidance by the WP29, Risks and Benefits and Best Practices

Moderator:

- Bojana Bellamy, President, Centre for Information Policy Leadership

Panelists:

- Tobias Judin, Legal Adviser, Norwegian Data Protection Authority
- Guilda Rostama, Legal Counsel, Commission Nationale de l'Informatique et des Libertés (CNIL)
- Emily Sharpe, Privacy and Public Policy Manager, Facebook
- Neil Wilson-Perkin, Senior Manager, Data Privacy and Records Management, Lloyds Banking Group
- Kimon Zorbas, Vice President Government Relations & Privacy, Europe, Nielsen
- Stephen McCartney, EU Director of Privacy, Pearson Plc
- Peter Fleischer, Global Privacy Counsel, Google, Inc.
- Monika Tomczak-Gorlikowska, Senior Legal Counsel, Data Privacy, Shell

Profiling and Automated Decision-Making – A29WP Guidance

Tobias Judin | legal adviser

Centre for Information Policy Leadership Working Session
7 November 2017

Datatilsynet
The Norwegian Data Protection Authority

Risks and benefits

- Benefits
  - Market segmentation and relevance
  - Resources and efficiency
  - Reduces potential for human error

- Risks
  - Opaque
  - Inaccuracies
  - Access to remedy?
  - Stereotypes, social segregation and filter bubble
  - Discriminatory effects?

Profiling

- Profiling v. automated decision-making
- Implications and challenges
- Profiling and children

Automated decision-making

- decision
- based solely on automated processing
- legal effects concerning him or her or similarly significantly affects him or her

A right to object or a prohibition?

- Recital 71:

  *The data subject should have the right not to be subject to a decision (…) However, decision-making based on such processing, including profiling, **should be allowed** where (…)*

- GDPR system

  «Rights» chapter not just about rights

  Section 4: «Right to object **and** automated individual decision-making»

A right to object or a prohibition?

- What if it is a right to object?

1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

2. *Paragraph 1 shall not apply if the decision:*

   (a)is necessary for entering into, or performance of, a contract between the data subject and a data controller;

   (b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (c)is based on the data subject's explicit consent.

3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement **suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests, at least **the right to obtain human intervention** on the part of the controller, to express his or her point of view and to contest the decision.*

A right to object or a prohibition?

- What if it is a right to object?

1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

2. *Paragraph 1 shall not apply if the decision:*

   (a)is necessary for entering into, or performance of, a contract between the data subject and a data controller;

   (b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

   (c)is based on the data subject's explicit consent.

3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*

A right to object or a prohibition?

- (a), (c), third paragraph only makes sense if prohibition

1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

2. *Paragraph 1 shall not apply if the decision:*
   (a)is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   (b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
   (c)is based on the data subject's explicit consent.

3. *In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*

Automated decision-making

- Safeguards and accountability

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

tobias[at]datatilsynet.no
linkedin.com/in/tobiasjudin

Profiling and Automated Decision-Making under the GDPR: GDPR provisions and WP29 Guidance, Risks, Benefits and Best Practices

GDPR provisions on profiling and automated decision-making (ADM) and what is the difference

The WP29 draft guidance on profiling and ADM

Initial reactions of organisations to the WP29 draft guidance

Profiling and ADM – Deep dive into Specific Issues and Questions for Discussion

Centre for Information Policy Leadership
Hunton & Williams LLP

Profiling and ADM – Key Issues and Questions for Discussion

Profiling in the GDPR – Key Points and Examples

Automated Decision-Making in the GDPR – Art. 22

Meaning of Legal and Similarly Significant Effects

What is Human Intervention?

ADM and Children

Art. 22(1) – Direct Prohibition vs. Right to be Invoked

Profiling & ADM: Organisational Accountability and Best Practices

Profiling is NOT the same as Automated Decision Making (ADM)

Profiling (Art. 4(4)) → **All GDPR requirements apply**
Art. 21 (Right to object)

Automated processing (AP) that **evaluates**, **analyses,** or **predicts** personal aspects, e.g.:

- Work performance
- Economic situation
- Personal preferences
- Health
- Interests
- Reliability
- Behavior
- Location
- Movements

ADM (Art. 22) → **GDPR Protections + Art. 22 (ADM)**

Solely automated decision (based on AP, incl. profiling) + legal effect or similarly significant effect.

Art. 35(3)(a) ADM sometimes requires a DPIA.

Recital 71 ADM producing legal or similarly significant effects should not be made with respect to children. Does not prohibit **all** profiling regarding children.

Art. 70(1)(f) EDPB will issue more guidelines, recommendations and best practices for "further specifying the criteria and conditions for decisions based on profiling" under the exceptions in Art. 22(2).

Centre for Information Policy Leadership
Hunton & Williams LLP

Profiling in the GDPR

No general prohibition against profiling

All GDPR requirements and safeguards apply to profiling

- E.g. appropriate legal basis for processing; purpose specification; transparency/notices; data quality; DPIA for high risk; data security; rights of individuals (access, correction, objection, erasure); data transfers.

Specific right to object (**Art. 21(1)**) where processing (including profiling) is based on:

- Public Interest **Art. 6(1)(e)**
- Legitimate Interest **Art. 6(1)(f)**

Absolute right to object to processing for direct marketing (**Art. 21(2)**)

- Should be brought to attention of data subject clear and separate from any other info (**Recital 70**)

Examples of Profiling in Different Sectors

1. Banking and Finance

- **Profiling is widely used in banking and finance. Often linked to regulatory requirements stemming from national, EU and international laws, regulations, and regulators' guidance , e.g.:**

  - **Prevention, detection and monitoring of financial crime**
  - **Debt management**
  - **Credit and risk assessment**
  - **Responsible lending to protect customers and markets**
  - **Fraud prevention**
  - **Anti-money laundering**
  - **Know your customer**
  - **Financing of terrorism**
  - **Tax evasion**
  - **Bribery and corruption**
  - **Cyber-crime**

  - **Profiling is also used for credit scoring and approval and customer segmentation.**

2. Health Services, Prevention, Diagnostic, Care and Medical Research

- **Profiling is widely used in this area, resulting in a wide range of real benefits.**
- **e.g. analytics to understand a syndrome and prevent recurrence, or understanding links between particular symptoms and drugs/medicines.**

3. Cyber-Security, Network and Information protection, Incident Prevention and Diagnostics

Centre for Information Policy Leadership
Hunton & Williams LLP

Examples continued…

4. **Insurance**
   - Whole industry based on profiling and risk assessment, both pre-contract and during coverage.
5. **Human Resources**
   - e.g. Analytics for purposes of employee retention; people development and promotion, compliance with company policies and codes of conduct / business ethics; screening for purpose of compliance with export control and economic sanctions law.
   - Recruitment.
6. **Improvement of Products and Services and Operational Efficiencies**
   - e.g. Energy and utility companies use profiling to predict energy consumption, demand and supply, usage peaks etc.
   - All organisations use profiling to improve effectiveness of website architecture.
7. **Marketing, Advertising and Personalised Services**
   - e.g. Recommendations based on profiles, previous and peer purchases.
   - Retail, hotel and travel services loyalty programs.
   - Customer segmentation.
8. **Public sector**
   - e.g. Tax authorities, policing.

Automated Decision-Making in the GDPR

ADM under GDPR

- Art 22 (1) - **right not to be subject to decision** based **solely on automated processing**, including profiling, which produces **legal effects,** or **similarly significantly affects** them.
- Exceptions Art. 22(2): Necessity of contract, authorized by law, explicit consent

Meaning of Legal Effect and Similarly Significant Effect

What is Human Intervention? Art. 22(3)

- What is involved? Manual decision from scratch? Review ADM decision? Review ADM process?
- WP29 – must be carried out by someone with authority & competence to change decision.

ADM and Children - Recital 71

- No Solely ADM with Respect to Child – WP29 says not absolute prohibition.

Notice and Individual Access – Art. 13(2)(f); 14(2)(g); 15(1)(h)

- Individual has a right to be informed about the existence of ADM and a right of access.
- Individual has a right to obtain meaningful information about the logic involved, as well as the significance and consequences of such processing

Meaning of Legal Effect and Similarly Significant Effect

What is the meaning of legal effect?

WP29 – Legal Effect means processing activity that has an impact on someone's legal rights or affects a person's legal status or their rights under a contract.

- **Examples**
  - Affecting legal status of individuals
  - Affecting accrued legal entitlement of a person
  - Affecting legal right
  - Public rights - liberty, citizenship
  - Affecting contractual rights – banking, insurance, employment, online credit application
  - Private right of ownership
  - Human rights under ECHR (perhaps?)

What is the meaning of similar significant effect?

WP29 – The threshold for significance must be similar, whether or not the decision has a legal effect. The effects of processing must be more than trivial and must be sufficiently great or important to be worthy of attention.

- **Examples**
  - Eligibility and access to essential services – health, education
  - Visa/entry to a country, residence, citizenship
  - School/university admission
  - Educational test scoring
  - Decision to categorise in a tax bracket for tax deductions
  - Decision to promote or pay bonus
  - Access to energy services and determination of tariffs
  - Any decisions that have adverse/negative impact on individuals
  - Decisions having direct and substantial effect - much more than trivial
  - Decisions that create long term harm and high risks for individuals

The Nature of Art. 22(1)

Article 22(1) = direct prohibition or right to be invoked ?

Interpretation 1	Interpretation 2
Direct prohibition: Solely ADM prohibited unless exception – contract/law/explicit consent. (WP29 View)	**Right to be invoked**: Solely ADM permitted unless individual affirmatively invokes right.

KEY QUESTION – Under a direct prohibition approach, which automated decisions would no longer be possible? (i.e. ADM based on legitimate interest)?

Profiling, ADM and the Role Organisational Accountability

1. CIPL believes that the focus should be on the spirit of the law and achieving organizational accountability with respect to profiling and ADM.

2. What can organisations do (more of and better) to ensure protection for individuals, but still be able to carry out profiling and ADM?

    - Transparency
    - Policies and procedures (including for advertising + behavioral targeting)
    - Impact assessments / Risk assessments / DPIA
    - DPO's role and involvement
    - What does meaningful human intervention mean and how to achieve it?
    - Fair processing (avoiding processing of sensitive data; accountable algorithms)
    - Implementing other safeguards
    - Tools and icons
    - Oversight and audits
    - Demonstrate and evidence compliance with these accountability measures.

Centre for Information Policy Leadership
Hunton & Williams LLP

Session II

Cross-Border Data Transfer Mechanisms under the GDPR

Moderator:

- Christopher Docksey, Director-General, European Data Protection Supervisor, honoris-causa

Panelists:

- Bruno Gencarelli, Head of Unit, European Commission (TBD)
- Nicola Coogan, Assistant Commissioner, Irish Data Protection Commission
- Corinna Schulze, Director, EU Government Relations, Global Corporate Affairs, SAP
- Caroline Louveaux, Assistant General Counsel, Privacy and Data Protection, MasterCard
- Gary Davis, Global Director of Privacy & Law Enforcement Requests, Apple, Inc.

Cross-Border Data Transfer Mechanisms under the GDPR

Adequacy & Privacy Shield

How to maximise the usefulness of the BCR?

What are the possible roles of codes of conduct and certifications as accountability and cross-border transfer frameworks?

Is there scope for improving the application of Standard Contractual Clauses?

Why is global interoperability between transfer mechanisms important and what are the existing opportunities to advance such interoperability?

Centre for Information Policy Leadership
Hunton & Williams LLP

Adequacy & Privacy Shield

- Industry Perspectives on Adequacy
- Status of Previously Found Adequate Countries
- Prospects for Additional Adequacy Findings (e.g. Japan)
- Privacy Shield Issues

Maximizing the Usefulness of BCR

- **Still perceived as a gold plate approach, suitable for large organisation with large resources, a dedicated DPO and large teams.**

- **BCR need to be made scalable to facilitate wider use:**
  - ***Streamline Approvals***: BCR approval process should be further streamlined and improved to facilitate faster processing times.
  - ***Recognised Certification***: BCR should be leveraged and "upgraded" to GDPR certification under Articles 42 and 43 of the GDPR.
  - ***Fast Track Re-Approval***: Companies that update their BCR to be in compliance with the GDPR should not be required to go through another comprehensive review and re-approval process, but should have a special "fast track" process
  - ***Transfers Outside Corporate Group***: Data transfers to a BCR approved company and also between BCR approved companies should be allowed based on BCR compliance by the company or companies and without any additional transfer mechanism (e.g. model clauses or derogations)

Centre for Information Policy Leadership
Hunton & Williams LLP

Certifications and Codes of Conduct

Developing GDPR certifications for purposes of data transfers should be a strategic priority for the Commission and/or EDPB.

Must be sufficient incentives and benefits for organisations to consider GDPR certifications and codes of conduct, in addition to the many certifications that they already pursue (e.g. ISO, or CBPR, or other national privacy seals/marks).

Certification process must be scalable and affordable, for all sizes and types of organisations.

Certifications and codes of conduct for data transfers must be developed at EU level and must work in all EU member states.

Regarding certifications, the ultimate goal should be to facilitate the interoperability of GDPR certifications with other transfer mechanisms such as the APEC CBPR and other relevant certifications (ISO standards, Japan Privacy Mark, etc.).

Code of conduct should also be developed with an eye on their potential role under the GDPR as a transfer mechanism. Ways in which such codes might be leveraged to obtain approval or certification under other transfer mechanisms or vice versa must be considered from the start.

The development of codes should include as much consistency as possible between codes covering the same industries and business practices.

Improving the Applications of Standard Contractual Clauses

- ***Bringing SCC in Line with GDPR***: Given the substantial administrative work involved, companies should be able to rely on their existing SCC with a reasonable time frame for updating them to the new SCC once they are available

- ***No Processor-to-Processor SCC***: It is imperative that workable and commercially viable solutions are created to enable lawful transfers between EU-processors and non-EU processors and sub-processors.
    - CIPL believes this should not necessarily be created by the Commission and/or the WP29/EDPB, but instead that relevant industry should lead the creation of model terms and clauses to cover processor-to-processor data transfers.

- ***Legal Uncertainty***: SCC currently being challenged in the Court of Justice of the EU. What are potential impacts on business processes, business partner relationships and digital and data strategy?

Centre for Information Policy Leadership
Hunton & Williams LLP

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton & Williams Privacy and Information Security Law Blog
www.huntonprivacyblog.com

FOLLOW US ON LINKEDIN
linkedin.com/company/centre-for-information-policy-leadership

FOLLOW US ON TWITTER
@THE_CIPL