Webinar:
Profiling and Automated Decision Making under the GDPR

Thursday, 27 July 2017

Speakers

Moderator: Bojana Bellamy
President
Centre for Information Policy Leadership

Monika Tomczak-Gorlikowska
Senior Legal Counsel – Data Privacy
Shell International Ltd.

Neil Wilson-Perkin
Senior Manager – Data Privacy and Records Management
Lloyds Banking Group

Centre for Information Policy Leadership
Hunton & Williams LLP

Webinar Agenda

1. GDPR Project Status
2. Overview
3. Profiling ≠ Automated Decision Making
4. Profiling – Key Points
5. Examples of Profiling in Different Sectors
6. Profiling Under the GDPR
7. Right Not to be Subject to Solely Automated Decisions
8. Meaning of Legal Effect and Similarly Significant Effect
9. Nature of Art. 22(1)
10. Which Interpretation is Correct?
11. Profiling, ADM and the Role of Organisational Accountability

Centre for Information Policy Leadership
Hunton & Williams LLP

CIPL GDPR Project Objectives

Multistakeholder project started in March 2016, bringing together industry leaders, DPAs, Commission, EU Member States, ministries and experts

Consistent interpretation by all Member States and stakeholders

Consistent further implementation by Member States, EU Commission and DPAs/EDPB

Constructive, forward-thinking and future-proof interpretation enabling EU Digital Single Market and data-driven innovation, while protecting privacy

Best practices, opportunities and challenges in the implementation

Bridging stakeholders and building trust

Centre for Information Policy Leadership
Hunton & Williams LLP

5 Project Focus Topics

Data Privacy Programmatic Management

Core Principles and Concepts

Individual Rights

International Data Transfers

Relationship with EU DPAs and Smart Regulation

Centre for Information Policy Leadership
Hunton & Williams LLP

CIPL Project Deliverables to Date

5 Workshops and working sessions

- Amsterdam (Kick-off), Paris (DPO, Risk), Brussels (Certifications), Madrid (Transparency, Consent, Legitimate interest), Dublin (Smart Regulation)

5 CIPL Papers Submitted to WP29

- DPO
- Risk and DPIA
- One Stop Shop and Lead DPA
- Certifications
- Transparency, Consent, Legitimate Interest

ePrivacy Regulation Consultation Response

4 CIPL Responses to WP29 Guidance

- DPO, Data Portability, Lead SA, DPIA

GDPR Readiness Survey Report

3 CIPL Papers in Progress

- Smart Regulation
- ePrivacy Regulation
- Profiling and Automated Decision Making

Centre for Information Policy Leadership
Hunton & Williams LLP

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

Key Points about Profiling

Profiling is ubiquitous and at the heart of computing and data processing – evaluate, analyse or predict is what computers do today and will do more of tomorrow.

Likely to increase with 4th industrial revolution, machine learning/AI and increase in computing power.

Profiling also occurs in the public sector and focus should not be on the private sector exclusively.

Much profiling is a fundamental part of operations and is beneficial and positive. There should be no default negative connotation.

Profiling is often used as a decision making tool to support all kinds of internal and external decisions.

Aggregation of data for later evaluation (pre-profiling) should not be "profiling" under GDPR.

Centre for Information Policy Leadership
Hunton & Williams LLP

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 Diagnostic

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.

Centre for Information Policy Leadership
Hunton & Williams LLP

Profiling under 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**)

Centre for Information Policy Leadership
Hunton & Williams LLP

Automated Decision Making under the GDPR - Right Not to be Subject to Solely Automated Decisions

Individual Right – Art. 22(1) + Recital 71

- Individuals have **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) (a) (b) & (c)

- **Authorised by law (b)**
- **Necessary to perform contract (a)**
- **Based on explicit consent (c)**

Art. 22(3) Controller must provide: safeguards + right to obtain human intervention + ability to express view + to contest decision.

Children's data - Recital 71

- No solely ADM with respect to a child.

Special categories of data – Art. 22(4)

- Solely ADM on special categories of data in Art. 9(1) can be based only on explicit consent, or in substantial public interest (for public sector) + controller must provide safeguards.

ADM requires DPIA for high risk – Art 35(3)

- Risk assessment is a tool for determining whether an automated decision has a similarly significant effect.
- The goal should be to identify, via risk assessment, decisions that truly have an adverse impact on individuals after mitigations have been applied.

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.

Centre for Information Policy Leadership
Hunton & Williams LLP

Meaning of Legal Effect and Similarly Significant Effect

What is the meaning of legal effect?

(Depends on applicable law)

- **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?

(Effect must be contextual and must be similarly impactful as a legal effect)

- **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

Centre for Information Policy Leadership
Hunton & Williams LLP

Questionable additional Examples of "Similar Significant Effect"

Examples of possible cases of "similar significant effect" that have been proposed with which we disagree:

1. Location tracking for push notifications
2. Loyalty programs
3. Behavioral advertising – in a great majority of situations, this does not have a similarly significant effect on people, unless based on sensitive data or causing discrimination or harm
4. Monitoring of wellness, fitness, health data via wearable devices

These items should not be covered by "similar significant effect" – Why?

Centre for Information Policy Leadership
Hunton & Williams LLP

Legal Effect and Similarly Significant Effect – Key Questions

- Can there be a list of clear-cut cases of decisions with "legal or similarly significant effect"?
  - If so, it would appear to eliminate risk assessment from a broad swath of processing activities, at least with respect to a determination of whether human intervention in decision-making is required.
- Can certain decisions be excluded from such lists as a matter of principle?
- Can behavioral or targeted advertising ever meet the "legal or similarly significant effect" threshold?
- How will cases in the middle or grey zone be decided? Should industry propose or ask for standards and guidance?
  - The UK ICO says the similar effect must be "**more than trivial**". But shouldn't the bar be higher than that to be similar in significance?
  - ICO also says decisions must be "**negative**". This makes sense and should be supported – One might interpret a favourable decision with respect to some people to be an implicit negative decision about others (e.g. special offers, invitations, etc.) But **Art. 22** should not be interpreted to cover such indirect impacts.

Centre for Information Policy Leadership
Hunton & Williams LLP

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.	**Right to be invoked**: Solely ADM permitted unless individual affirmatively invokes right.

Centre for Information Policy Leadership
Hunton & Williams LLP

Interpretation 1: Direct Prohibition

Art. 22(1) Solely ADM **prohibited unless exception** applies

↓

Art. 22(2)(a)(b)(c) exceptions:

(a) Contract (b) Law (c) Consent (Explicit)

Organisations can never make solely AD producing such effects where processing based on Art. 6(1)
(d) Vital Interest
(e) Public Interest / Official Authority – unless Art. 22(2)(b)
(f) Legitimate Interest

↓

Art. 22(3) Controller must provide safeguards + right to human intervention + ability for individual to express view + and contest automated decisions made to **perform a contract** Art. 22(2)(a) or based on **explicit consent** Art. 22(2)(c)

Interpretation 1 appears to significantly limit the ability to engage in automated decision making without human intervention/review.

Centre for Information Policy Leadership
Hunton & Williams LLP

Support for Interpretation 1

Interpretation 1 is supported by:

A **Law Makers Intent**: Law makers intended strong protections against impactful decisions based solely on automated processing in certain contexts.

B **Legislative History:** Implementation of Art. 15 of the Directive and national law predating the directive support a general prohibition on ADM.

- Art. 15 DPD implemented as a prohibition by Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden and Ireland.
- Art. 10 French data protection law 1978 also indicates a prohibition.

C **ECJ Human Rights Approach**: This interpretation may be more in line with the fundamental human rights approach of the European Court of Justice.

D **Provision Language**: Rights to be affirmatively invoked under the GDPR phrased in positive terms. (i.e. The right to do something – obtain / receive / object) See **Art. 15, 16, 17, 18, 20, 21**.

But **Art. 22(1)** is phrased in negative terms (i.e. The right NOT to be subject). Arguable this indicates no affirmative action is required by data subject.

Centre for Information Policy Leadership
Hunton & Williams LLP

Interpretation 2: Right to be Invoked

Art. 22(1) ADM **permitted** unless individual invokes right

If invoked, both prospectively and retrospectively, data subject can no longer be subject to ADM under any processing ground except those listed in the exceptions under **Art. 22(2)**.

↓

Under **Art. 22(2)(a)(b)(c)** it's not possible or relevant to prospectively invoke the right.

i.e. automated decision is made to perform a contract; because it is authorised by law; or after subject has provided explicit consent.

↓

However, if unhappy with the outcome of an automated decision made to perform contract or based on consent, **Art. 22(3)** provides individual with ability to retrospectively seek human intervention, express point of view and contest decision.

No review available if decision is authorised by law. **Art. 22(2)(b)**

Centre for Information Policy Leadership
Hunton & Williams LLP

Support for Interpretation 2

Interpretation 2 is supported by:

A **Individuals Must Invoke Other GDPR Rights**: Other rights under the GDPR have to be invoked - *Data subject "shall have the right to… do something…"* If **Art. 22(1)** is a right, then it must also be invoked.

B **Legislative Intent**: If the legislator intended the right to be a prohibition they would have explicitly stated this. (*"Controller shall not…."*)

C **Implementation of Art. 15 DPD**: UK and Norway implemented Art. 15 of the Directive as a right to be invoked.

D **Modern Data Processing**: Interpretation 2 is more in line with modern data processing realities.

E **Other GDPR Protection**: There are other protective measures under the GDPR such as notice requirements (**Art. 13(2)(f)**, **Art. 14(2)(g)** and right to access **Art. 15(2)(h)**), with the purpose of alerting the individual of the right in **Art. 22**.

Centre for Information Policy Leadership
Hunton & Williams LLP

Which Interpretation is Correct?

1. Are there other plausible, textual and non-textual arguments for Interpretations 1 and 2?

2. Which interpretation is the Court of Justice of the European Union (CJEU) more likely to follow?

3. If **Art. 22** is a direct prohibition, what are some examples of automated decisions (based on legitimate interest, vital interest and public interest processing) that would no longer be possible?

4. How can the impact of interpretation 1 be limited (assuming it is correct)?
   a) Narrow the scope of covered ADM – narrowly define "similarly significant effect".
   b) Focus on organisational accountability, to avoid risks and harms for individuals.

Centre for Information Policy Leadership
Hunton & Williams LLP

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.

Q&A Discussion

If you would like to ask a question, please hit *7 (star 7) to unmute your phone.

Please hit *6 (star 6) to mute your phone again.

Bojana Bellamy
President
Centre for Information Policy Leadership

Contacts

Bojana Bellamy
President
Centre for Information Policy Leadership
Bbellamy@hunton.com

Markus Heyder
Vice President & Senior Policy Advisor
Centre for Information Policy Leadership
Mheyder@hunton.com

Hielke Hijmans
Senior Policy Advisor
Centre for Information Policy Leadership
Hhijmans@hunton.com

Sam Grogan
Global Policy Privacy Analyst
Centre for Information Policy Leadership
SGrogan@hunton.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

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

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

FOLLOW US ON TWITTER
@THE_CIPL