



After the Cambridge Analytica Scandal and Calls for Stricter Privacy Rules What Will the Data Protection Regulatory Landscape Look Like

Ventsislav, Karadjov
Chairman
BULGARIAN COMMISSION FOR PERSONAL DATA PROTECTION

Deputy Chair
EUROPEAN DATA PROTECTION BOARD



European Data Protection Board (EDPB)

The EDPB is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

The EDPB is composed of representatives of the national data protection authorities and the European Data Protection Supervisor. The EDPB is established by the General Data Protection Regulation (GDPR), and is based in Brussels. The European Commission has the right to participate in the activities and meetings of the Board without voting right.

Bulgarian Commission for Personal Data Protection

The Commission for Personal Data Protection (CPDP) is the national supervisory authority of the Republic of Bulgaria responsible for the protection of personal data both in the public and private sectors.

Being the only data protection authority in the country, the CPDP has a wide range of investigative, corrective and advisory powers and performs a number of different tasks, such as investigations, corrective measures, awareness-raising and information campaigns, international cooperation, training, etc.

Cambridge Analytica Case

British political consulting company that combining data mining, data brokerage, and data analysis with strategic communication during the electoral processes;

Offices in London, New York City, and Washington, DC;

Performed data analysis services:

- In 2015: Ted Cruz's presidential campaign;
- In 2016: Donald Trump's presidential campaign as well as Leave.EU in UK

Subject of criminal investigations in US and UK

Cambridge Analytica Case

Scope:

Collected data of 87 million data subjects since 2014 according to Facebook;

At least 1 million Facebook users in the UK;

Influence voter opinion on behalf of politicians;

Following a risk review, the formal broader investigation launched in May 2017 began as one into the use of data analytics for political purposes.

UK Information Commissioner Elizabeth Denham:

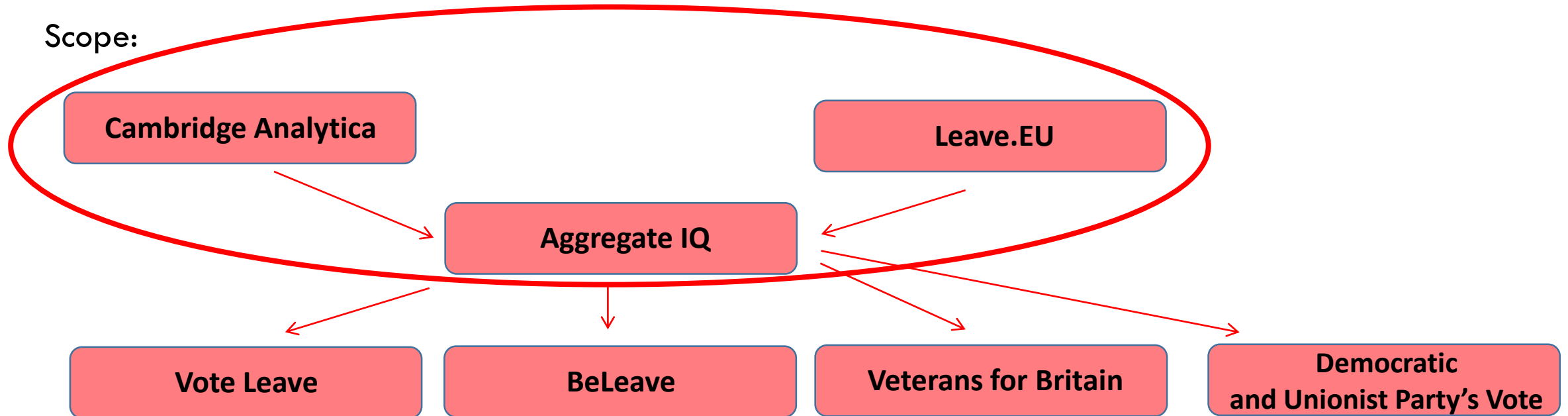
“We are at a crossroads. Trust and confidence in the integrity of our democratic processes risk being disrupted because the average voter has little idea of what is going on behind the scenes.

“New technologies that use data analytics to micro-target people give campaign groups the ability to connect with individual voters. But this cannot be at the expense of transparency, fairness and compliance with the law.”

“Fines and prosecutions punish the bad actors, but my real goal is to effect change and restore trust and confidence in our democratic system.”

Cambridge Analytica Case

Scope:



UK ICO vs. EDPB

ICO powers	EDPB powers
Information Notices to request provision of information from organisations in a structured way (with changes to legislation these can now be issued to individuals as well as data controllers);	Promoting common training programmes as well as exchange of knowledge and documentation and facilitating personnel exchanges between the supervisory authorities;
Enforcement Notices to require specific action to be taken by a data controller to comply with the Data Protection legislation;	Issuing guidelines, recommendations and best practices;
A Demand for Access to allow the Commissioner to attend at premises to carry out investigations and examine material relevant to her investigation (backed by a warrant to do the same if access is unreasonably refused);	Encouraging the drawing-up of codes of conduct and carry out the accreditation of certification bodies and its periodic review;
Monetary Penalty Notices to fine data controllers for breaches of the data protection legislation;	

UK ICO decision

Early 2017 - number of media reports claimed that Cambridge Analytica (CA) worked for the Leave.EU campaign during the EU referendum;

March 2017 – the ICO announced that it would begin a review of evidence as to the potential risks related the use of data analytics in the political process;

May 2017 – ICO launches a formal investigation;

February 2018 - focus on Facebook and CA were heightened by evidence provided to the ICO;
by the end of October 2018 – current phase of investigative work will be concluded;

Social dimensions of data breaches

- Public trust in the social media;
- Public pressure on DPAs for higher financial sanctions;

Economic and financial dimensions for Facebook

- Fallen stock prices;
- ICO fined Facebook £500,000 (\$663,000) over the data scandal (the maximum allowed).
- The Italian banking company UniCredit stopped advertising and marketing on Facebook



Source: NASDAQ

The road ahead...

- National Data Protection Authorities responsibility in the light of 4% of global turnover fine;
- National DPA needs substantial resources for doing their job
- Balance between privacy protection and civil and political rights
- Closer cooperation between national DPAs
- EU adequacy decisions

Thank you for your attention!

Ventsislav Karadjov

Chairman of the CPDP

Deputy Chair of EDPB

vkaradjov@cpdp.bg