DIGITAL MARKETING IN THE SPOTLIGHT: What is new, what are your obligations?

Ivana Bartoletti – Head of Privacy and Data Protection
Samuel Plantié – Principal Data Protection Consultant

Gemserv

Agenda

- **Introduction**
- **Cookies and other tracking technologies: dos and don’ts**
  - Tracking users online
  - Which technologies are we talking about?
  - Cookie banners consent
  - Cookie walls
  - Analytics
  - What does a compliant cookie banner look like?
- **Digital advertising: many third parties and joint obligations**
  - The advertising industry landscape
  - Consent in a chain of contracts
  - Are you joint controller with Facebook?
- **Questions and Answers**

Introduction

Introduction

- **Several recent cases, guidelines and official statements** confirm the shift of the **regulatory landscape** for online tracking and behavioural monitoring

- New **guidance on cookies and other tracking technologies** and authorities' action plan on digital advertising make **tracking online users more challenging** for delivering targeted ads, but also for analytics:
  - UK Information Commissioner Office (ICO) cookie guidance and report into AdTech and Real Time Bidding
  - French Commission Nationale de l'Informatique et des Libertés (CNIL) cookie guidance and action plan on online targeting
  - Irish Data Protection Commission (DPC) cookie guidance
  - German Conference of the Data Protection Authorities (DSK) cookie guidance

Introduction

- Large online advertising companies **are being scrutinised** but still fall behind the incentive to amend their business models:
  - Google fined €50 million in France in January 2019
  - Facebook fined $5 billion in the U.S. in July 2019
  - Investigations against Google and Quantcast in Ireland opened in May 2019

- **Smaller businesses are in scope** because of the advertising provider they select and the tracking technologies they choose to **implement on their websites**

Cookies and other tracking technologies: do's and dont's

Tracking users online

- It is widely communicated by European Data Protection Authorities that **GDPR standard consent is applicable** to **cookies and other online tracking technologies**

- **Legitimate business interest** is **not a lawful legal basis** for tracking and profiling users online, even for analytics (with some nuances)

- Consent must be **freely given**, **specific**, **informed**, **unambiguous**, by a statement or by a **clear affirmative action** (no opt-out)

Which technologies are we talking about?

- **Any technology** that stores or accesses information on the user's device is in scope, **not only cookies**
  - Pixel beacons
  - Tracking scripts
  - Tags
  - Software development kits in mobile applications
  - Unique identifiers (UIDs)
  - Local objects
  - Browser fingerprinting technologies

- A recent ECJ case (Planet49, C-673/17, 1st October 2019) ruled that **it did not matter if cookies were processing personal data or not**: accessing the user's device storage is in itself an invasion of their privacy sphere. **All cookies are in scope.**

Cookie banners consent

Consent must be **freely given, specific, informed, unambiguous, by a statement or by a clear affirmative action**, opt-out is simply not acceptable

A **bundled or global consent box is not considered as consent**

Emphasising the consent option over the decline option is deemed as **influencing users** towards consent

This is the **same if the option to decline consent is located in a second layer** with the option to agree in the first layer

Cookie walls

- For the French and German Data Protection Authorities, **a website cannot implement a cookie wall to restrict access to the website until users' consent** (i.e. forcing users to accept targeting cookies to access the website)

- However, the ICO said that **if an acceptable alternative to tracking is offered** to visitors to avoid tracking – such as a paid subscription – cookie walls could be considered lawful

- Further clarity and alignment from the European Data Protection Board is expected on this matter

Analytics

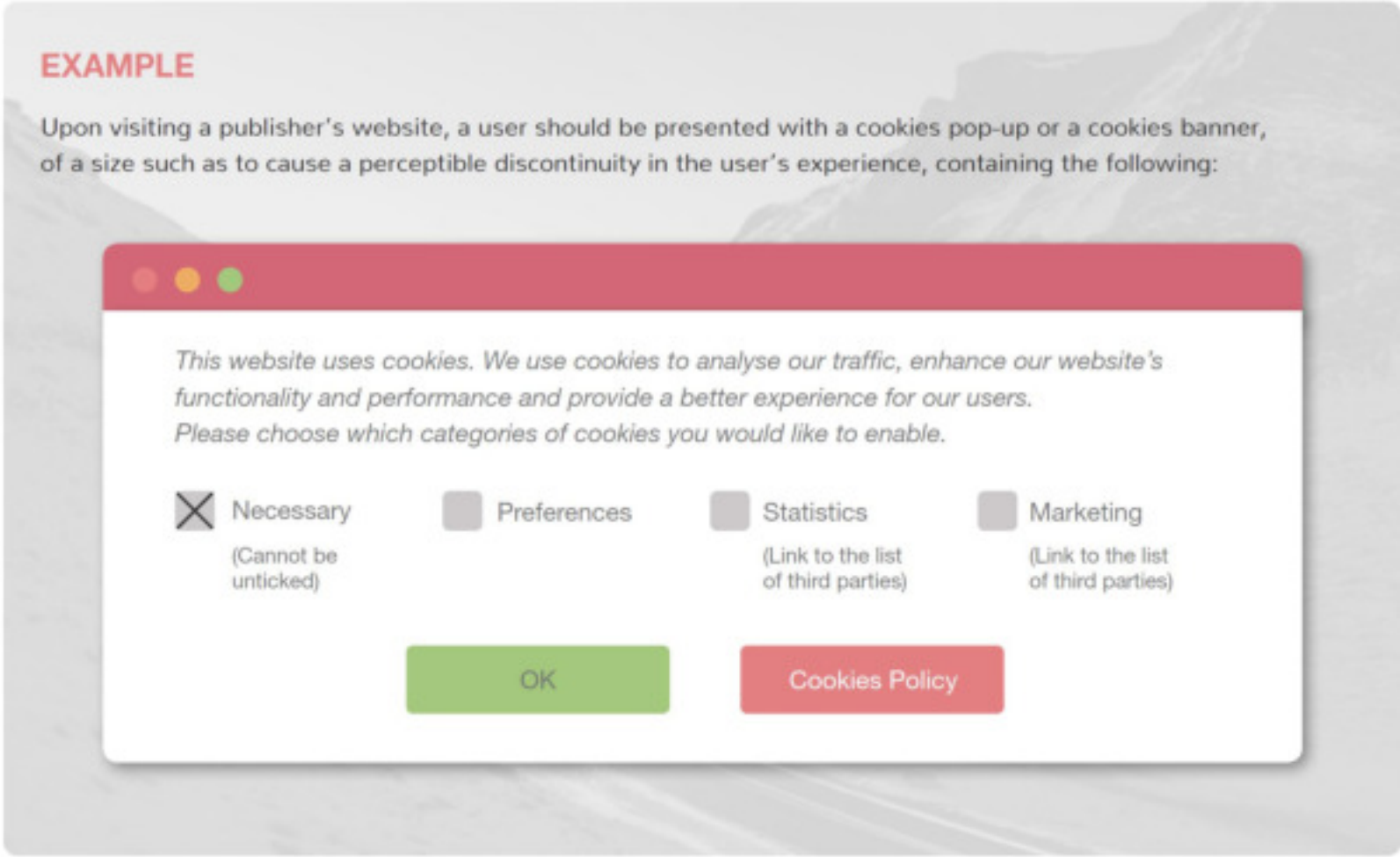
- Analytics cookies **cannot be considered as strictly necessary** and consent must be collected

- However, analytics cookies used on the basis of legitimate interest (opt-out) could be tolerated when **no data is transferred to third parties** to be matched with additional data sets (by using a first party module on the website)

- Third party analytics solutions such as the ones provided by **Google and Facebook are excluded**, since these services will **inevitably match the data collected with their own sources**

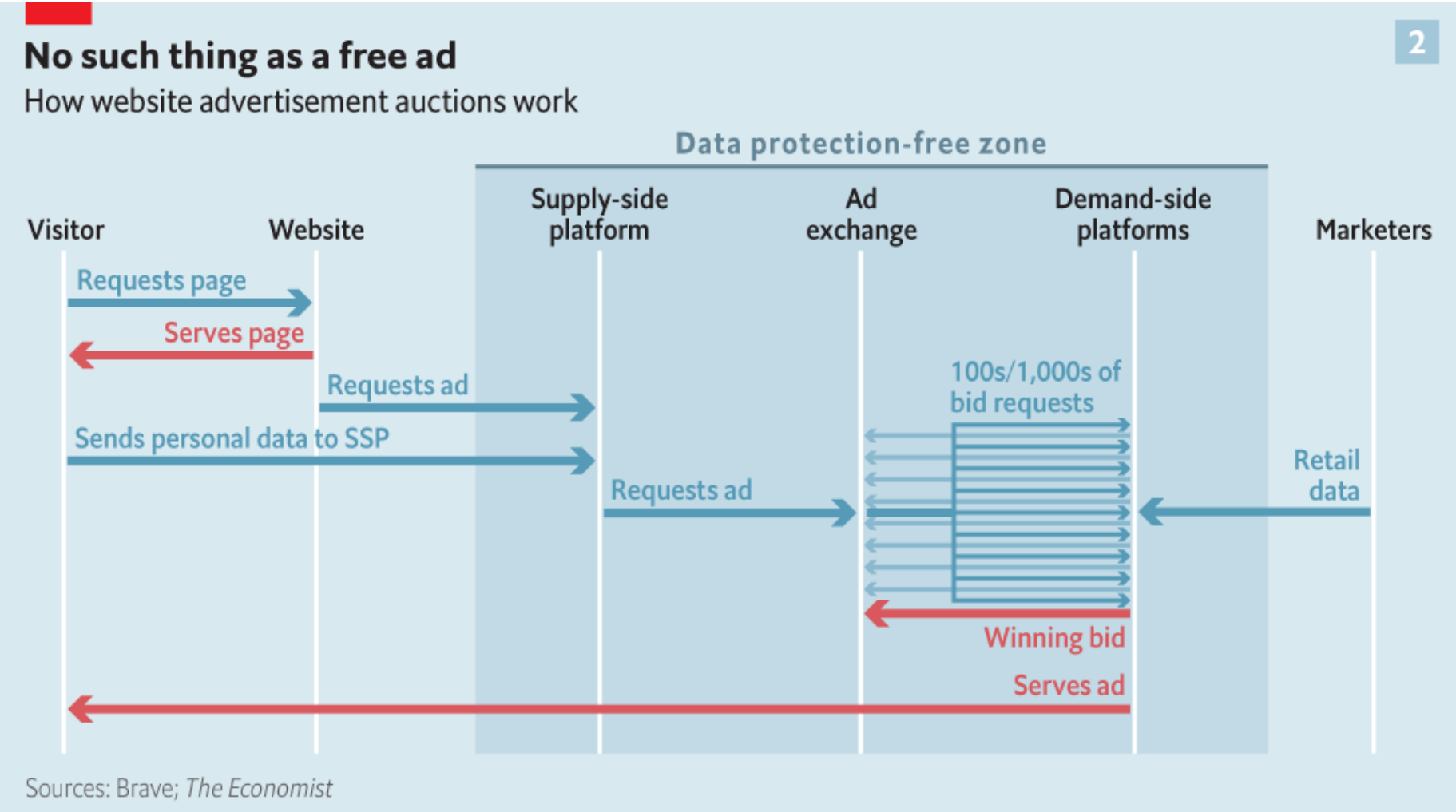
What does a compliant cookie banner look like?

- **No pre-ticked boxes** except for strictly necessary
- **Separated purposes**
- Link to the **cookies policy**
- List of **third parties**



Digital advertising: many third parties and joint obligations

The advertising industry landscape



The advertising industry landscape

- There is an **abundance of actors** involved in the digital advertising industry and most of them are **unknown to website publishers and visitors**

- Data collected through cookies and other tracking technologies **is massively leaked** through a **significant number of third parties** and **matched with their own data sets**, with little knowledge or even control from website publishers

- In an interview with the Financial Times on 29th August 2019, Simon McDougall, ICO, said the authority had been '***unsatisfied***' by the answers offered by the AdTech industry. '*What we're seeing is a **blind reliance on contracts** and no real attempt to assess whether the counterparty you're using is likely to have controls in place around security, retention.*'

Consent in a chain of contracts

In an enforcement notice taken in October 2018 against AdBroker named Vectaury, the CNIL ruled that **relying on contractual provisions** is not enough to **demonstrate** that consent has been properly collected by a website editor

Advertising providers can still be **challenged** to prove they have compliant and proper consent from website editors

Website editors must be able to **demonstrate** to their **advertising providers** that they have collected and recorded proper consent **from their visitors**

A **compliant cookie banner** and **proper consent recording** is going to be more and more required by advertising providers

Are you joint controller with Facebook?

- **Legitimate interest** cannot be used to upload your customers' emails to **Facebook Custom Audiences**: you must collect their **GDPR compliant consent** (Bavarian Data Protection Supervisory Authority, confirmed by Munich Higher Administrative Court on 26 September 2018). Facebook could ask you to **demonstrate** you have collected such consent.

- A Facebook **page administrator** is **joint-controller** with Facebook because both determine the purposes and means of processing (ECJ C-210/16, 5 June 2018)

- Website publishers are considered joint controllers with Facebook when the decide to use **Facebook modules on their website**, for instance a Like button (ECJ C-40/17, 29 July 2019)

- Data collected from websites cannot be assigned to Facebook users without their **consent**, which must be collected **both on the website and on Facebook** (German Federal Cartel Office 6 February 2019 and Italian Competition Authority 29 November 2018)

THANK YOU FOR LISTENING

Any Questions or Feedback

Ivana Bartoletti – Head of Privacy and Data Protection
Samuel Plantié – Principal Data Protection Consultant

Please feel free to contact:
dataprotection@gemserv.com

Gemserv

INVESTORS IN PEOPLE™ We invest in people Gold

ISO/IEC 27001 Information Security Management

ISO 14001

ISO 9001

CYBER ESSENTIALS PLUS