ePrivacy Regulation

THE NEXT ITERATION OF THE EU COOKIE LAW

- **ePrivacy Regulation: Substance**
  - Article 8 on the use of terminal equipment (“the cookie provision”)
  - Article 9 on consent
  - Article 10 on browser settings
- **ePrivacy Regulation: Process**
  - Legislative procedure (official)
  - Legislative procedure (informal, actual)
  - Political situation in Parliament
  - Political considerations for ePrivacy Regulation

ePrivacy Regulation

SUBSTANCE

- "The use of **processing and storage capabilities** of terminal equipment and **the collection of information** from […] terminal equipment […] shall be prohibited, except on the following grounds:"
  - (old) it is *necessary* for the sole purpose of transmitting a communication over the Internet.
  - (old) it is *necessary* for providing an internet service requested by the user.
  - (old) the user has given their *consent* (in accordance with the GDPR).
  - (new) it is *necessary for web audience measuring,* provided its first party.
  - (new) (recitals) configuration checking and the mere logging of the fact that the user's device is unable to receive content [which may include ads] does not constitute access to a device or processing capabilities.

- "The use of **processing and storage capabilities** of terminal equipment and **the collection of information** from […] terminal equipment […]"
  - The general prohibition applies to any user interaction over internet, be it the use of **cookies** (reading/writing), the use of **device identifiers** (IDFA, AAID), the use of **device fingerprinting**.
  - The prohibition applies to personal and non-personal information stored on a device, such as images, recipes, directory information (address books).

cookies device fingerprints device IDs images directory

- Any third-party tracking or profiling is considered de facto privacy invasive, characterized as both unwanted and misunderstood by users.
- "Spyware, web bugs, *hidden* identifiers, **tracking cookies** and other similar ***unwanted*** **tracking tools** can enter end-users' terminal equipment without their knowledge [...] **trace the[ir] activities** [...] and *may seriously intrude upon the privacy of these end-users*." (Rec. 20)
- "Techniques that surreptitiously monitor the actions of end-users, for example by **tracking their activities online** [...] *pose a serious threat to the privacy of end-users*." (Rec. 20)

- Exception: (old) it is *necessary* for the sole purpose of transmitting a communication over the Internet.
  - Basic client/server communication necessary to load a website does not require consent.

- Exception: (old) it is *necessary* for providing an internet service requested by the user.
  - Session cookies, e.g. to keep track of a user's input when filling in online forms or providing shopping cart functionality, do not require consent.

- Exception: (old) the user has given their *consent* (new: in accordance with the GDPR).
  - **Freely given** (including a test whether consent is a condition for access), **specific**, **informed** and unambiguous indication of wishes by which he or she by a **clear affirmative action**, signifies agreement.
  - Businesses must be able to demonstrate that consent has been granted.
  - Consent must be easily revocable at any time.
  - Unclear that consent can be obtained by a first party on behalf of a third party, although Commission stated to IAB Europe that this would be the case, but clarification needed.
  - The skeptical view of online tracking and targeted advertising suggests that regulators may demand high levels of notice and consent, especially when it applies to third parties, as the law presupposes the technologies used for such purposes are extremely privacy invasive.

- Exception: (new) it is *necessary for web audience measuring,* provided its done by a first party.
  - First party analytics, and *probably* third parties acting on behalf of a first party as a processor do not require consent.
  - If first party analytics data is used for any other purposes, e.g. cross-domain analytics, used for ad-targeting, etc. the exemption no longer applies.

- Exception: (new) (recitals) configuration checking and the mere logging of the fact that the user's device is unable to receive content [which may include ads] does not constitute access to a device or processing capabilities.
  - Ad block detection does not fall in scope of Article 8(1).

- Use of technologies that collect data about users' devices as they search for Wi-Fi, Bluetooth, or other signals is prohibited. Except:
  - When used for the sole purpose of establishing a connection with a device.
  - Provision of "a clear and prominent notice informing of […] the collection, its purpose, the person responsible" and measures the user can take to stop the collection – and use for advertising.
  - Additional requirements under the GDPR are met.

- Impact of Article 8 on digital advertising:
  - Online tracking and ad-targeting will require prior affirmative consent.
  - Alternative legal grounds for processing under the GDPR, e.g. pursuing legitimate interest that is not overridden by user interests (opt-out), will no longer be available.
  - Offline tracking requires provision of an opt-out, including for use of that data for advertising.
- Breach of Article 8 can be fined with penalties as high as 10,000,000 EUR or 2% of global annual turnover (whatever is higher).

- Consent means consent under the GDPR, including all adjacent obligations and limitations. (previously covered)
- “Where technically possible and feasible, consent may be expressed by using the appropriate technical settings of a software application enabling access to the Internet”
  - Such choices are binding on, and enforceable against any “third parties”, i.e. any party other than the user and the browser, including “first party” publishers.
- Periodic reminders of the right to withdraw consent.

- Impact of Article 9 on digital advertising:
  - Consent means GDPR-consent.
  - Respecting/acknowledging browser settings, such as DNT would be legally required.
  - General browser settings could be overridden by more specific consents, obtained, e.g. through consent banners or other technical means.

- Browsers and other apps enabling access to the internet to offer “the option to prevent third parties from” interfering with a device.
- “Upon installation,” the user would have to choose general settings **allowing or rejecting tracking for advertising purposes**, or select an intermediary position. Users may not complete installation before making a choice.
- Browsers must inform users about privacy implications of their choice in a way that does not “dissuade end-users from selecting higher privacy settings and [that includes] **relevant information about the risks** associated to allowing third party cookies […] **including the compilation of long-term records** of individuals’ browsing histories **and use of such records to send targeted advertising.**”
- Browsers are ***required*** **to offer ability to block** all third party cookies by default, but merely ***encouraged*** **to “provide easy ways […] to change the privacy settings** at any time [and] to allow the user to make exceptions” or whitelist certain websites and their third parties.

- Impact of Article 10 on digital advertising:
  - Third parties may be technically blocked by a large amount of users.
  - General settings may not be able to be overcome through legally valid consents as a technical matter if browsers block cookies and other forms of tracking.
  - Consent may thus have to be expressed at a technical level through the browser (even if legally valid consent is obtained through other means).
  - But because browsers aren't required to provide such functionality, it may be difficult for users to provide such technical consent.
- Breach of Article 10 can be fined with penalties as high as 10,000,000 EUR or 2% of global annual turnover (whatever is higher).