WRANGU

ePrivacy
DIRECTIVE *VS.* REGULATION

DIRECTIVE

- Directive required local regulations for implementation.

ePrivacy Directive complements the Data Protection Directive (DPD)

REGULATION

- Regulation is self-executing and is legally binding across the EU. The regulation will create consistent and uniform application across the EU.

ePrivacy Regulation complements the General Data Protection Regulation (GDPR)

ePrivacy Regulation is *lex specialis* and GDPR is *lex generalis* meaning if the two come in conflict over some provision, the ePrivacy Regulation will govern.

EXPANDED SCOPE

- The ePrivacy Directive concerned the protection of electronic communications networks and services to end-users.

- The ePrivacy Regulation applies to providers of electronic communication services and publicly available directories as well as those who use electronic communications to send direct marketing or make use of processing and storage capabilities or collection information stored processed on terminal equipment.

The regulation will cover end-users located in the EU.

IOT

- The ePrivacy Directive does not contemplate IoT.

N/A

- The principle of confidentiality should apply to current and future means of communication including machine-to-machine communications.

‘OTT’

- The Directive governs publicly available electronic communications networks and services.

- The Regulation extends the privacy protection of the directive by including ‘over the top’ (OTT) communication services like Zoom and instant messengers, like WhatsApp.

OTTs are entities that offer communication services through the users’ internet connection.

METADATA

- No regulation of metadata.

N/A

- The new regulation will cover not only the content of communications but also the metadata such as “numbers called, the websites visited, geographical location, the time, data and duration when an individual made a call.”

Metadata is information derived from the electronic communication other than the content of the communication.

COOKIE WALLS, CONSENT FATIGUE & WHITELISTS

- The Directive required protection against unwarranted intrusion into the privacy sphere. Users need to be provided with clear and comprehensive information when using cookies including the right to refuse. The Directive limited cookies that did not require consent to those that are strictly necessary for the legitimate purpose of enabling the use of a specific service requested by the end-user.

- Requirements are similar to the Directive and does not require consent for non-privacy invasive cookies. The Regulation includes new ideas to address the deluge of information and consent fatigue. Recital 20a addresses the issue of ‘consent fatigue’ when ubiquitous uses of tracking cookies overloads end-users with consent requests, which can lead to a situation when “consent request information is no longer read and the protection offered by consent is undermined.”

The ePrivacy Regulation seeks to address this by allowing users to provide consent to the use of certain types of cookies for certain service providers through whitelists.

DIRECT MARKETING

- Safeguard against intrusion into privacy by unsolicited communications for direct marketing. Direct marketing is ok to offer similar products or services as what was sold but must provide an opt-out.

Direct marketing is not allowed without the consent.

- Rules stay pretty much the same, it’s okay to allow the use of contact information for messages within the context of an existing customer relationship. Direct marketing communications require consent of the end-users before direct marketing communications are sent to them.

When end-users have provided consent, they must still be able to withdraw it at any time.

ENFORCEMENT PROVISIONS

- Created a requirement that the Directive be enforced by the national supervisory authority to “have sufficient powers and resources to investigate cases of non-compliance...including powers to obtain any relevant information” and has the power to impose sanctions.

- Retains the national supervisory authority with the ability to investigate noncompliance and raises the level of fines equal to that in the GDPR:

€20 million

or

4% of global turnover

WRANGU

AMSTERDAM | LONDON

Wrangu provides flexible software solutions for integrated risk, security and privacy management. Founded in 2016, Wrangu’s mission is to deliver software solutions that enable clients to solve their risk and compliance challenges efficiently and with true transparency.