EVERSHEDS SUTHERLAND

Data Privacy update
The ePrivacy Regulation

On the 10 February 2021, ambassadors in the Council of the European Union Permanent Representatives Committee (COREPER) announced it had agreed a negotiating mandate on a draft ePrivacy Regulation ("**the ePrivacy Regulation**"). The ePrivacy Regulation will update existing rules on the protection of privacy and confidentiality in the use of electronic communication services.

How have we got here?

The initial ePrivacy Directive from 2002 was an important legal instrument for privacy and confidentiality of communications, specifically with regard to rules for tracking and monitoring of communications.

The GDPR requires the EU to update this 2002 Directive. In January 2017, the European Commission published proposals for its reform. The recent agreement on the negotiating mandate has been long awaited to allow negotiations on the final text to progress.

The updated text is required to address confidentiality of modern day technological developments such as Voice over IP, web-based email and messaging services, machine-to-machine communication (Internet of Things), communication between individuals on publicly accessible networks (e.g. public hotspots/WiFi) and new techniques for tracking an individual's online behaviour.

What are the key changes?

The new ePrivacy Regulation will repeal the previous 2002 ePrivacy Directive. The ePrivacy Regulation acts as *lex specialis* to the GDPR by complementing it in certain areas; for example, many ePrivacy Regulation provisions will apply to both natural and legal persons, in contrast to the GDPR, which does not apply to personal data concerning legal persons.

The overarching purpose of the ePrivacy Regulation is to ensure that, as a general rule, electronic communications data must be confidential. Interference, such as listening, monitoring and processing of data by anyone other than the end-user, will be prohibited. However, the current draft of the ePrivacy Regulation does provide for permitted processing in circumstances such as:

- Ensuring integrity of communications services;
- Identifying malware/viruses; and
- Where the service provider is bound by domestic or EU law for prosecution of criminal offences or prevention of threats to public security.

Key areas of interest in the draft text include:

- Interception of electronic communications data by humans or machines without consent of the communicating parties, is prohibited. This may occur when someone other than the communicating parties listens, reads, scans or stores the content or its metadata for purposes other than exchange of communications or also where third parties monitor websites visited, timing of the visits and interaction without the consent of the end-user;
- Public hotspots and WiFi must ensure the confidentiality of electronic communications transmitted via publicly available services/networks;

- Metadata related to communications (e.g. location, time, date, duration), which can be considered almost as sensitive as the content of the communication itself, must also be kept confidential. However, with consent, metadata may be used to display, for example, traffic movement to help public authorities and transport providers develop infrastructure or monitor the spread of epidemics;

- To promote a trusted and secure Internet of Things, machine-to-machine data transmitted via a public network must be kept confidential;

- The collection of information from end-users terminal equipment, including hardware and software which may contain highly sensitive information such as photos and contact lists, should only be permitted with the end-users consent. Use of information without consent should be limited to situations that involve none or very limited intrusions of privacy; and

- Users must be given genuine choice to accept cookies or other similar identifiers. To avoid cookie consent fatigue, an end-user can give consent by whitelisting one or several providers in their browser settings.

The draft text of the ePrivacy Regulation states that the rules should apply regardless of whether the processing of electronic communications data or personal data of end-users who are in the EU takes place in the EU or not, or regardless of whether the service provider or person processing such data is established or located in the EU or not. In summary, the rules should apply when end-users are in the EU, opening the door to enforcement against companies for actions originating outside of the EU. Even if the processing takes place outside the EU or the service provider is established or located outside the EU, the rules still apply.

Where we go from here

It is important to remember the draft ePrivacy Regulations are subject to change before the finalized text is agreed and it will be some time before implementation. Therefore while it is prudent that organizations are aware of the future changes and be mindful of preparations they may need to take, no changes are required immediately.

The final text must now be negotiated by the Council of the EU and the European Parliament. Once this process is complete, the ePrivacy Regulation will be published in the EU Official Journal and enter into force 20 days later. It is currently anticipated that the introduction of the ePrivacy Regulation will have a two-year sunset period similar to the GDPR. If accepted by the Council of the EU and the European Parliament as part of the negotiation of the current draft, this will provide organizations with sufficient time in order to become compliant.

We will continue to monitor progress in this area and issue updates as more information becomes available.

For further information, please contact:

Ireland

Marie McGinley
Partner, Head of IP, Technology & DP

T: +353 1 6441 457
MarieMcGinley@
eversheds-sutherland.ie

Emma Quinn
Solicitor, IP, Technology & DP

T: +353 1 6644909
EmmaQuinn@
eversheds-sutherland.ie

Holly Traynor
IP, Technology & DP

T: +353 1 6441467
HollyTraynor@
eversheds-sutherland.ie

US

Michael Bahar
Partner, Co-Lead of Global Cybersecurity and Data Privacy

T: +1 202 383 0882
MichaelBahar@
eversheds-sutehrland.com

Brandi Taylor
Counsel, Cybersecurity and Data Privacy

T: +1 858 252 601
BrandiTaylor
@eversheds-sutherland.com

Margaret O'Brien
Associate, Cybersecurity and Data Privacy

T: +1 404 853 8070
MargaretOBrien
@eversheds-sutherland.com

eversheds-sutherland.com

02/21 6969327.2