**New EU e-Privacy Regulation (ePR)**

**What could it mean for you?**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10 JAN.</td>
<td>4 APR.</td>
<td>15 MAY</td>
<td>21 JUN.</td>
<td>1 JUL.</td>
<td>11-12 OCT.</td>
</tr>
<tr>
<td>European Commission adopts proposed e-Privacy Regulation</td>
<td>Article 29 Working Party adopts opinion</td>
<td>Maltese Presidency of the EU Council adopts progress report</td>
<td>Rapporteur Marju Lauristin (S&amp;D, Estonia) presents draft report to European Parliament LIBE committee</td>
<td>Estonian Presidency of the EU Council takes forward e-Privacy proposal</td>
<td>European Parliament LIBE committee to adopt draft report</td>
</tr>
</tbody>
</table>

### Debate

#### PROPOSAL

**EU Commission**

- Proposed ePR

**Article 29 Working Party**

- EU national data protection authorities

**EU Council**

- Progress report

**EU Parliament**

- Draft LIBE report

### SCOPE

- **M2M**

- Certain provisions of the proposed ePR (e.g. the obligation to respect the confidentiality of communications) would not only apply to traditional telecommunications service providers. In line with the definition of electronic communications services (ECS) contained in the proposed European Electronic Communications Code (EECC), they would also apply to:
  - over-the-top (OTT) communication apps such as messaging, webmail and voice/video calling services; and
  - machine-to-machine (M2M) communication services.

### CONFIDENTIALITY OF COMMUNICATIONS

- ECS providers would generally have to collect users’ consent to process electronic communications data, which includes:
  - content (e.g. the message contained in an email); and
  - metadata (i.e. the who, what, where and when the email was sent).

  Providers would have to remind users of their right to withdraw consent every six months.

### ONLINE TRACKING

- Software permitting electronic communications (e.g. operating systems, browsers and other applications) would have to require users, upon installation, to choose whether they want to prevent third parties from storing information on their device (e.g. third-party cookies) or processing information stored on their device (e.g. a social media app accessing a user’s photos). The proposed ePR would not prohibit so-called “tracking walls”, which prevent access to websites or apps by users who refuse to be tracked.

### DEVICE TRACKING

- The tracking of users through the collection of signals “emitted” by their devices (e.g. to count the number of people in an area) would be allowed on condition that a clear and prominent notice is displayed to the public. Users’ consent would not be required. However, users would have to be informed about how they could stop or minimise collection.

### ENFORCEMENT

- Data protection authorities (DPAs) in the EU member states would become responsible for supervision and enforcement of the proposed regulation.

- Companies that breach the law would face fines of up to €20m or 4% of worldwide annual turnover (whichever is higher).

---

This infographic is a snapshot of the current ePR debate. It is published by Cullen International’s Digital Economy service which tracks regulation in Europe at EU and national levels. © Cullen International - July 2017.