Joint declaration on the e-Privacy Regulation

After several years of deadlock in negotiations on the e-Privacy Regulation, the co-signatory organisations would like to express their position and concerns on recent developments.

We acknowledge that the regulation for electronic communications is a complex matter, as it must strike a balance between protecting the users' data and enhancing digitalisation as well as innovation.

However, we are worried that the text adopted by the Council could entail major negative spillover effects on the green and digital transformation advocated by EU leaders. While the energy sector is committed to protect data integrity as well as consumers' privacy and confidentiality, the current proposal might heavily undermine and delay Europe's 2030 climate & energy and 'Digital decade' objectives.

With regards to the trilogue negotiations, we encourage you to take in due account the following recommendations:

- **E-Privacy Regulation must not contradict DSOs' missions**

Distribution System Operators (DSOs) operate smart meters and provide essential services based on European and national legal obligations. Smart meters imply the collection of data from terminal equipment (meter) and use means to remotely communicate data (through electronic communication means). These smart meters then allow the DSO to fulfil its missions, which are among others to collect energy consumption data for billing obligations and to ensure stability and security of the network. The implementation of smart meters as a way to achieve the energy transition is largely encouraged at European and national level[1]. For this reason, both aspects, electronic communication and terminal equipment, should be covered by an exception regime. While compliance with legal obligations is an exception already foreseen for electronic communications (Article 6), this exception is missing for end-user's terminal equipment (Article 8). Therefore, Article 8 should encompass compliance with legal obligations to fully allow DSOs to fulfil their missions.

DSOs must guarantee the security and reliability of the energy system, thus **the legal grounds for permissible security software updates under Article 8 require further clarification**. Such updates do not have the possibility to be postponed and must be applied at any time for security reasons. Indeed, enacting the possibility to postpone security updates of smart meters might be particularly risky in the context of critical infrastructures where any delay could lead to a security gap and hamper the operation of the entire energy system. Any component of the energy system, including, but not limited to a smart meter system, is fundamentally distinct from any system for which an individual bears sole responsibility. The e-Privacy Regulation should therefore set forth an exception to the right of individuals to defer any software updates for smart metering devices.

- **E-Privacy should not hinder sustainable and innovative services**

The e-Privacy Regulation includes non-personal data in its scope but does not differentiate enough between the treatment of personal and non-personal data, which limits the collection of non-personal data in a disproportionate way.

[1] Article 19.2, Directive EU 2019/944 on common rules for the internal market for electricity

Besides, the new provisions on data collection would cause serious obstacles to the use of smart meters due to lack of information. For instance DSOs will not have enough availability of data suitable to evaluate and maintain the quality of supply and to adjust the network accordingly, undermining their capability to fulfil their service obligations. This would make innovation in the field of value-added services impossible and limit the sense of the ongoing smart meter rollout.

Therefore, e-Privacy would introduce barriers, first to provide current and future essential services and secondly, to encourage consumers' engagement in flexibility services provision and energy markets. We have serious concerns that the current text would limit the **choice of green services** as it **undermines viability** of innovative clean energy solutions: **the unavailability of smart metering information would hinder innovation and lead to a much less sustainable planet**[2].

- **The EU should ensure a secure and efficient digital environment in the energy sector**

Energy companies are already subject to strict legislation on data management and security with their assets being critical infrastructures. Besides, they are subject to horizontal regulation on personal data protection and perform DPIAs[3] that represent the highest level of consumer's protection. It should be underlined, that this obligation contributes to privacy protection to a much greater extent than costly and confusing limitation of collecting information from IoT devices under the proposed Art.8 of e-Privacy Regulation. **Consequently, companies that have DPIA process in place must be exempted from the e-Privacy Regulation, for the EU framework to be coherent and efficient.**

We are at your disposal for any clarification you may need.

Roberto Zangrandi Secretary, E.DSO	Kristian Ruby Secretary General, Eurelectric	Tomás Llobet Managing Director, ESMIG	Thomas Nowak, Carnot Consulting General, of European Heat Pump Association

[2] Role of smart meters in responding to climate change, by DELTA-EE; May 2019.

[3] A DPIA is a process that analyses the envisaged data processing, an assessment of the risks to the rights and freedoms of data subjects as well as the measures, safeguards, controls and mechanisms envisaged to address those risks. A DPIA process goes beyond helping data controllers to demonstrating compliance with the GDPR. It also supports data controllers in applying the principle of data protection by design: it allows them to anticipate potential impacts on the rights and freedoms of data subjects and implement stringent safeguards as soon as possible.