Brussels, 22 March 2018

Plea of European Telecom DPOs and Heads of Privacy on e-Privacy Regulation

As Data Protection Officers (DPO) and Heads of Privacy of Europe's leading telecommunications operators, we are working full speed ahead to bring our companies in compliance with the General Data Protection Regulation (GDPR) as of 25th May 2018. We consider the GDPR as an opportunity to further enhance the privacy of our customers and users in an increasingly digitised society.

Yet the novel regulation, which overhauls the mid '90s EU privacy framework to establish modern and future-proof rules for all sectors and organisations, will need to cohabit with an obsolete e-Privacy Directive from 2002 that specifically governs the handling of telecommunications data with more restraining conditions than for any other sector of the economy.

Our companies deeply value and support the fundamental principle of confidentiality of communications. We are in the business of providing European customers with trusted, dependable services to connect with other people. The principle of confidentiality enshrined in the e-Privacy Directive is set to remain an unwavering pillar of our operations.

This is fully compatible with the necessity to bring the rules allowing for the legal processing of communications data in line with what is permissible under the GDPR. Stricter rules for communications "metadata" artificially push telcos into a dumb pipe scenario that assumes their role in the economy should simply be to deliver telecommunications and internet traffic, in disregard for our ambition to tap into the potential of data analytics to optimise our investment in cutting-edge infrastructure and to innovate in services with high social benefits such as smart mobility.

The proposed reform of the old directive into a new e-Privacy Regulation is falling short of that ambition. Instead of affording to telecom providers the same flexibility, and related accountability, granted to the processing of personal data by the GDPR, the proposal perpetuates the current disparity as it makes the processing of any metadata conditional upon user consent (hence the difficulty to rely on sizeable and consistent datasets for analytics) or full anonymisation of the data at hand (hence the loss of valuable information that enable meaningful analytics[1]).

As digitisation is leading to an increasing convergence of markets and technologies and the creation of converged services, regulatory harmonisation for all sectors and services in the EU should be a primary objective of law-making. In our view, the GDPR is the best instrument to achieve this harmonisation in the field of privacy. As far as the protection of personal data is concerned, the GDPR should cover all providers and services in the same way, all the more when they process the same type of data such as location data.

Our view as privacy professionals is that metadata are inherently no more or less sensitive than other specific kinds of data, e.g. financial data or medical data. Location data – an eminent example of metadata – is explicitly defined as personal information in the GDPR. The nature, scope, context and purpose of the processing is what actually determines the degree of sensitivity of the information, according to the risk-based approach that constitutes a fundamental principle of the GDPR.
We are convinced that this risk-based approach as well as the basic principles applicable to personal data in the GDPR, should hold valid for metadata too. Purpose limitation, data minimisation, storage limitation, integrity and confidentiality: all these principles ensure high standards of privacy protection and keep organisations accountable towards their users and customers.

[1] see also Recital (17) of the proposal, which acknowledges that the displaying of traffic movements over time by processing location metadata would not be possible with anonymised data, due to the needed identifier.

Accountability does not clash with flexibility. On the contrary, flexible mechanisms to process data in the absence of user consent substantially shift the responsibility of legal compliance to organisations that wish to use those data and encourage their responsible behaviour. Although consent is an option for processing customer data in the context of an existing contractual relationship, this is not the most suitable solution for analytics operations that require large datasets in order to work and do not need to rely on fully identifiable data to perform those analysis. Other mechanisms, coupled with strong safeguards like pseudonymisation and opt-out options, could be much more appropriate.

The GDPR already provides for important safeguards regarding information, transparency, right to object, possibility to withdraw consent at any time, the need for Privacy Impact Assessments and heavy sanctions for infringing companies. By adding an additional layer of protection, the future e-Privacy Regulation could in fact have a negative impact on European consumers, by reducing the ability for telecom operators in Europe to create the best in class products and services for them.
For the reasons above, we DPOs and Heads of Privacy call upon EU decision-makers to pursue a bold alignment of the e-Privacy Regulation with the GDPR with regard to the lawful processing of data. If more flexible grounds for handling metadata were introduced, European telcos could finally make the most of the data economy, still in full respect of people's confidentiality.

The data analytics possibilities that would originate from such flexibility would allow telecoms to use location metadata to better plan their investment decisions and to rollout and upgrade their networks to provide citizens with high-quality and reliable connectivity. Improved customer service and the provision of datasets to public authorities for high-value societal purposes (such as smart mobility tools that allow local authorities to map urban traffic and reduce congestion accordingly) are among the many applications that would be enabled by a truly future-proof e-Privacy Regulation.

We remain at the disposal of EU lawmakers to contribute to a regulatory framework that reconcile the protection of citizens' privacy and confidentiality with the opportunities offered by the data economy to develop world-class communication networks and services in Europe.

Signatories:

A1 Telekom Austria Group – Judith Leschanz, Group Data Protection Officer

BT – Sarah Blacker, Chief Privacy Officer

Deutsche Telekom – Claus-Dieter Ulmer, Global Data Privacy Officer

KPN – Rachel Marbus, Data Protection Officer

OTE – Kostas Megas, Group Data Protection Officer

Proximus – Olivier Moumal, Data Protection Officer

PT Portugal – Vítor Fernandes, Data Protection Officer

Swisscom – Nicolas Passadelis, Head of Data Governance

TDC Group – Christian Fröhlich, Head of Telecom & Competition Law

Telefónica – Manuel Crespo de la Mata, Data Protection Officer

Telenor – Nicholai Kramer Pfeiffer, Group Privacy Officer

Telia Company – Hele Jonsson, Group Chief Privacy Officer

TIM – Roberto Fermani, Head of Privacy

Vivacom – Georgi Sredkov, Data Protection Officer

Vodafone – Mikko Niva, Group Privacy Officer