October 2017

AK Position Paper

Proposal for a Regulation on Privacy and Electronic Communications (e-Privacy-Regulation)

COM (2017) 10

www.akeuropa.eu

About us

The Austrian Federal Chamber of Labour is by law representing the interests of about 3.6 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transperency Register under the number 23869471911-54.

The AK EUROPA office in Brussels was established in 1991 to bring forward the interests of all its members directly vis-à-vis the European Institutions.

Organisation and Tasks of the Austrian Federal Chamber of Labour

The Austrian Federal Chamber of Labour is the umbrella organisation of the nine regional Chambers of Labour in Austria, which have together the statutory mandate to represent the interests of their members.

The Chambers of Labour provide their members a broad range of services, including for instance advice on matters of labour law, consumer rights, social insurance and educational matters.

More than three quarters of the 2 million member-consultations carried out each year concern labour-, social insurance- and insolvency law. Furthermore the Austrian Federal Chamber of Labour makes use of its vested right to state its opinion in the legislation process of the European Union and in Austria in order to shape the interests of the employees and consumers towards the legislator.

All Austrian employees are subject to compulsory membership. The member fee is determined by law and is amounting to 0.5% of the members' gross wages or salaries (up to the social security payroll tax cap maximum). 816.000 - amongst others unemployed, persons on maternity (paternity) leave, communityand military service - of the 3.6 million members are exempt from subscription payment, but are entitled to all services provided by the Austrian Federal Chambers of Labour.

Rudi Kaske
President

Christoph Klein
Director

The AK's position in detail

In January 2017, the EU Commission published the proposal for a Regulation on privacy and electronic communications, intended as a replacement to the existing e-Privacy Directive in May 2018. The special rules contained within the Directive are to be seen as complementary to the General Data Protection Regulation (GDPR). In view of the enormous daily impact of electronic communications and the increasing monitoring of user behaviour, it is the declared goal of consumer protection to safeguard the confidentiality of electronic communications as well as the right to self-determination in the management of personal communication data more effectively than had been the case.

1. No commercialising of traffic and location data

The exploitability of traffic data will in the future exceed levels seen until now (network security, fee billing, marketing of communications services or provision of services with added value, each with prior consent of the user). From BAK's perspective, users must definitely maintain control over the use of their communication data for purposes other than communication transfer.

BAK demands: It must be clarified in Art. 6 that end user consent must be required, without exception, for data use that is irrelevant to the purposes of the service, not relying on the limited level of protection, which is afforded by the GDPR in individual cases. By no means Article 6 of the e-Privacy Regulation should allow to process electronic communications data based on 'legitimate interest' or further processing for 'compatible purposes'.

Some background: The EU Commission acknowledges that users "want to control the use of electronic communications data for purposes other than conveying the communication" (Recital 17). Accordingly, it should also be clarified in the draft that consent for other purposes from the individuals concerned must be obtained, without exception. Only in this way it is beyond doubt that data processors cannot rely on the lowest level of protection afforded by the General Data Protection Regulation, which is often subject to interpretation. It should be explicitly prohibited to use consumers' sensitive metadata for the "predominantly legitimate interests" of commercial providers or for a consent-free "further use" of data for purposes "compatible" with the original use. Otherwise, consumers' hitherto data protection level would be completely and unacceptably lowered.

2. E-Privacy can be distilled down to "Do not track!": Compulsory strict default settings for hardware and software

Consumers, as well as those tasked with protecting data across Europe, are complaining that thoroughly effective protection against one of the most insidious threats to privacy is

lacking: the spying on internet user behaviour. Data analysts outperform themselves by using algorithmic evaluation of surfing behaviour: Data mining, either through the classification of individuals according to their characteristics and preferences, or via predictions on their future behaviour; excavating ever larger mountains of data with analysis tools, signifies profits for internet companies, whilst heralding the loss of privacy by those concerned. Smartphones and web browsers must therefore be set to a low data use threshold.

BAK demands: The General Data Protection Regulation regulates technical data protection "by default" (the strictest possible default setting for devices and software). This provision must be implemented in Art. 8 and 10 - otherwise the law is void from the start.

Some background: Cookies (and other technologies) serve the investigation of surfing behaviour. According to the draft Regulation any use of "processing and storage" in terminals not performed by the user is basically prohibited, and it remains up to the user to declare consent (as in the deposit of cookies) or the provision of service desired by the user or necessary appraisal of web traffic. In future, user consent should be obtained from the browser's default setting. This should make annoying cookie banners on websites obsolete. "Do Not Track" is the name of a web technology that is offered as an option in modern browsers. When activated, websites visited are automatically notified that the saving of data for creation of a user profile is vetoed. According to the draft Regulation browsers need not be pre-set to the most data sensitive setting. Users should merely be offered a number of optional settings. As a result, the draft Regulation clearly rests behind legitimate consumer expectations and does not match the General Data Protection Regulation that obliges providers to a data protection-friendly default (privacy by default). A Eurobarometer survey undertaken by the EU Commission in 2016 indicated that around 60% of Austrians interviewed change their browser settings for data protection reasons anyway. The 40%, who apparently do not actively do so (above all the elderly and generally individuals with little internet user skills) should therefore be afforded a helping hand with data protection-friendly default settings.

3. No monitoring by "track and trace services" without consent from the concerned

This draft also opens up a surveillance gateway to consumers in their offline everyday life. Shops, that identify their customers (via their smartphones and WLAN or Bluetooth connections) and wish to track their movements or durations of stay, do not even have to seek their consent, according to the Commission's draft Regulation. A simple notice in the shop should suffice. 54% of consumers surveyed by the Federation of German Consumer Organisations (VZBV) categorically refuse to countenance such personal tracking. They believe that prohibiting such methods is the only adequate response to this development. Commercial track and trace services without the consent of those concerned are also completely unacceptable for BAK.

BAK demands: Art. 8 Para. 2 Z b and Para. 3 and 4 should be withdrawn without replacement.

Some background: X looks at a garment. Nice, but far too expensive. She continues, but then returns and reconsiders: Really? The ideas of purchase are disoriented. A few days later she enters another branch of the same clothing chain. "Your" garment appears on the monitor. "How do they know what I had been interested in …?" Fiction? No. In London, public refuse bins equipped with WLAN modules and screens already tracked the mobile phones of passers-by in 2013.

Smartphones transmit signals, in order to enable a telephone, internet, WLAN or Bluetooth connection. For example, these signals may be used commercially in order to track consumer traces in the offline world as well. They can recognise a consumer when he repeatedly enters a business and reconstruct his movements within that business. This concept designates the scanning of highly accurate device-related information as "track and trace services". Amongst their purposes are: "counting of individuals, data regarding the number of individuals waiting in a queue, delivery of personalised advertising, tracking of individuals over a period of time…". Such offline would according to the draft regulation occur without the consumer's consent. Consumers would merely have to be informed by a notice that they are entering a monitored area. Shops would only have to inform about the purpose of the tracking, the person in charge of it and what the concerned individual can do to stop or minimize the tracking and collection of personal data.

4. Provision of class action suit

Improved enforcement in regard to data protection violations is long overdue. The option for provision of class action in the national law exists in the General Data Protection Regulation. There is simply no reason why EU consumer associations may launch actions regarding consumer's data protections against several sectors, but not the telecommunications sector.

BAK demands: Introduction of a class action suit in Art. 21 for organisations assuming consumer and data protection interests.

5. Privacy concerns regarding the "Internet of Things"

More and more companies offer "smart" devices equipped with sensors and internet connection that permit deeper intrusions into consumers' lives. Access to operating data should not be limited to the manufacturer.

BAK demands: The right to self-determination by the purchaser of the device over all operating data that the purchased product issues, must be safeguarded.

Some background: The gathering of permanent operational information by cars, heaters, shoes, dolls, watches, toothbrushes etc., all integrated on the internet and collecting the behavioural data of the user (Internet of Things). This includes data that has a dubious personal connection, such that in traditional concepts bears no relation to any particular individual or data that is anonymised. Nevertheless, researchers confirm that with the aid of appropriate analytical

tools, such data can almost always be assigned to a particular individual. Cayla, "the spy in the children's room" is a demonstrable illustration of current protection requirements in private households. She is "almost like a real friend", we are told on the product website of the doll, that replies to questions via a Bluetooth connection and voice recognition and can forward interactions between the child and doll to the US manufacturer. The doll is an example of such problems that may arise from the rapidly developing networked household appliances regarding concealed interception and opaque data receiver or data use capabilities.

Should you have any further questions
please do not hesitate to contact

Daniela Zimmer
T: +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

and

Peter Hilpold
(in our Brussels Office)
T +32 (0) 2 230 62 54
peter.hilpold@akeuropa.eu

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Vienna, Austria
T +43 (0) 1 501 65-0

AK EUROPA
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54
F +32 (0) 2 230 29 73