Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

EU update

Kit Burden *, *Jeanne Dauzier*

DLA Piper UK LLP, United Kingdom

Keywords:
EU law
Intellectual property
Information technology law
Telecommunications law

A B S T R A C T

This is the latest edition of the DLA Piper column on developments in EU law relating to IP, IT and telecommunications. This news article summarises recent developments that are considered important for practitioners, students and academics in a wide range of information technology, e-commerce, telecommunications and intellectual property areas. It cannot be exhaustive but intends to address the important points. This is a hard copy reference guide, but links to outside web sites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

1. Portability

***Agnès Chavernoz**, Associate, DLA Piper Paris*

1.1. *Brussels reaches agreement on portability of online content services*

On 7 February 2017, the EU presidency and representatives of the EU Parliament reached an agreement on a draft Regulation enabling cross-border portability of online content services in the European Union.

If this draft Regulation is confirmed by the Council and the Parliament, it will enable European consumers to access and use online content services that they have acquired in any country of the European Union that they are travelling to.

This Regulation is deemed as the next significant step forward in creating a digital single market within the European Union, as the end date to roaming charges for travelers within the EU is nearing.

Scope of application

The new Regulation will apply:

- to online content which is provided against payment; or
- to free-of-charge online content if their broadcaster verifies the country of residence of their subscribers within the context of its provision of said content,

provided that such content i) is lawfully provided in the consumer's Member State of residence, ii) is provided on a portable basis, meaning that consumers can use and access the online content without a limitation to a specific location, and iii) is an audiovisual media services as defined by European law or a service whose main feature is the provision of access to works of broadcasting organizations.

Cross-border portability of online content will only be permissible in the context of temporary stays (such as holidays, business trips, etc.) and right holders will be able to require from the online content services provider that it verifies the consumer's country of residence in order to avoid abuse of its right to online content portability.

Any such verifications will need to be made in compliance with Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

For further information see: http://www.dlapiper.com/.

* *Corresponding author.* DLA Piper UK LLP, 3 Noble Street, London EC2V 7EE, United Kingdom. Fax: +44 (0) 20 7796 6666.
E-mail addresses: kit.burden@dlapiper.com (K. Burden); jeanne.dauzier@dlapiper.com (J. Dauzier).

http://dx.doi.org/10.1016/j.clsr.2017.04.002

Territorial localization of the provision of online content services

This draft Regulation constitutes a deviation from the traditional territorial approach of author's rights. In practice indeed, online content services are often licensed on a territorial basis as the online content services providers are only authorized by the concerned right holders to provide such content in a given territory. Under the draft Regulation, any provision of online content services to a European country where the consumer is temporarily staying will be deemed to occur in the consumer's country of residence, which means that the service providers will not need to obtain any particular authorization from the relevant right holders for the purpose of complying with their obligation to ensure portability of the content.

Moreover, the draft Regulation provides that the right to portability of online content cannot be waived by contract, either between the online content services providers and the relevant right holders, or between such service providers and the consumers. Contractual clauses designed to limit or prevent cross-border portability of online content services will be deemed unenforceable.

The draft Regulation is intended to apply nine months following its publication and will apply to the provision of online content services under contracts entered into before this date of application.

2. Privacy

2.1. *Europe: Artificial Intelligence, what can we learn from the GDPR?*

Giangiacomo Olivi, Partner, DLA Piper Milan, Andrea Batalla, Associate, and Santiago Carralero, Trainee, in DLA Piper Spain

Artificial Intelligence technologies ("**AIT**") is the term referred to any technology which enables both the collection of large amounts of information and taking autonomous decisions or actions. The AIT are closely related to data protection, especially when it comes to decisions that affect individuals. Data protection concerns arise from the volume of the information collected, how it is generated, the complexity of its processing and the new uses of said information. In this sense, the GDPR tackles several concerns related to AIT, as will be further developed.

Informed consent

Data subjects must give their explicit consent for the processing of their personal data. Additionally, data subjects must be able to understand the specific use and purposes of the corresponding organization for collecting and processing their personal data. It seems an easy and lawful principle but it must be noted that AIT are based on algorithms, which implies difficulties for organizations to explain to data subjects the reason of the decisions taken.

In relation to the explicit consent, we need to take into consideration the existence of the so-called "enriched data", which is the data resulting from the combination of different data, gathered on the basis of different legal grounds or gathered from different sources – such as the environment – that becomes personal data. In order to legally process the enriched data and bearing in mind that the consent provided is normally unambiguous for a specific processing, the organization shall increase the requests for consent in order to legitimately use it.

Accountability

The GDPR requires data controllers to demonstrate compliance, including obligations to carry out at an initial stage a data protection impact assessment for each risky process/product and to implement data protection by design and by default.

This implies an obligation for software developers and other parties that intervene in the creation and management of AI to integrate the data governance process with appropriate safeguards, including, for instance, data minimization and data portability (which should cover both the data provided knowingly by the data subject and the data generated by their activity).

Furthermore, the GDPR requires security measures that are "appropriate" to the risk, taking into account the evolving technological progress. This is particularly relevant when dealing with the potential risks of AI, which by definition evolve.

The application of the above principles will be key for all parties involved to limit their responsibility, or at least to obtain insurance cover for the data protection (and related data breach) risks. In this respect, the adherence to industry codes of conduct or other data protection adequacy certifications will also help.

Informed consent

Informed consent from the data subject is another key principle for the GDPR, as was already the case for most European jurisdictions. Such consent may not be easy to achieve within an AI scenario, particularly when it is not possible to rely upon predefined sets of instructions.

This is even more relevant if we consider that updated consent may not be easy to achieve for "enriched data", certain non-personal data that has become personal data (i.e. associated with an individual) through processing combined with other data gathered by the AI from the environment or other sources.

This may lead to a substantial increase in requests for consent (through simplified, yet explicit forms), even when personal data is not being used. Such an increase may not necessarily entail an equivalent increase in awareness of data protection – as was seen with the application of cookie regulations in certain European jurisdictions.

When dealing with AI, it may be that under certain circumstances parties involved will opt for a request of "enhanced consent", as is applied in Italy for certain contracts that impose clauses that are particularly unfavorable for the consumer. Such consent, however, will not per se exclude responsibility for the entity ultimately responsible for the data processing.

Security

Including appropriate safeguards to the processing of the personal data is mandatory. The large volume of data processed by AIT devices implies that many potential risks might arise as a consequence of the processing, storage or outsourcing of the personal data. Consequently, the GDPR establishes that any breach or leakage occurred shall be promptly communicated to the Data Protection Authorities, and in some cases, even to the affected data subjects.