BEUC The European Consumer Organisation

The Consumer Voice in Europe

EU CLOUD COMPUTING STRATEGY

BEUC Position Paper

Contact: **Guillermo Beltrà – digital@beuc.eu**

Ref.: X/2013/014 - 28/02/2013

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • Fax +32 (0)2 740 28 02 • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Summary

The European Commission's Cloud Computing Strategy lacks ambition and is a missed opportunity because it fails to provide guidance on the most important consumer issues related to cloud computing. The European Consumer Organisation (BEUC) has identified a number of actions which need to be undertaken in order to build a consumer-friendly legal and policy framework for cloud computing.

Contractual aspects of cloud computing

- Modernisation of the consumer law *acquis* should continue via traditional non-optional legislation and not via optional instruments, which are a kind of self-regulation where businesses can decide whether they want to be subjected to European law.
- Implementation of the provisions contained in the Consumer Rights Directive on pre-contractual information and formal requirements applicable to cloud computing services.
- Reform of the European legal framework on legal guarantees to adapt it to the challenges of the digital economy encompassing specific rules on the conformity of cloud-computing services and consumers' rights in instances of non-functioning service. This could be done via a new Directive on digital content products or within the framework of an eventual revision of the 1999 Consumer Sales Directive.
- Guidance on transparency requirements and unfair contract terms to clarify the application of the Unfair Contract Terms legislation to cloud computing contracts. BEUC believes special attention must be paid to common contract terms which do not comply with the data protection and other existing EU legislation, ensuring the effective application of consumer law such as the Rome I and Brussels I regulations.

Data protection

- EU data protection law should apply to any data processing activity related to the offering of goods and services to data subjects residing in the EU or the monitoring of their behaviour, irrespective of whether the data controller and/or processor is established in the EU.
- The applicable law for specific processing operations should be the law of the country of residence of the data subject.
- The US-EU Safe Harbour Agreement should be reviewed urgently as it does not sufficiently guarantee the protection of personal data, while its enforcement remains ineffective.
- Transfer of an EU resident's personal data to a third country must be subject to the 'adequacy mechanism' to ensure that the third country provides an adequate level of protection as compared to the EU, while Binding Corporate Rules and Standard Contract Clauses could be used exceptionally, subject to strict safeguards and conditions.

- Any request for the transfer of EU residents' personal data to law enforcement authorities of third countries should require prior authorisation by the Data Protection Authority of the country of the data subject's residence.
- Codes of conduct in the field of data protection should be submitted for approval to the Article 29 Data Protection Working Party and offer a higher level of protection than the legal framework. They should be backed up by suitably robust auditing or testing procedures while providing for independent complaint handling, robust sanctions and effective consumer redress.

Interoperability and portability

- The necessary standards to allow full interoperability among cloud computing services of similar nature need to be developed.
- Policymakers need to ensure cloud providers do not 'lock-in' consumers to the service, either by lengthy contracts or making it technically cumbersome to switch.
- Automatic transfers of data between compatible cloud services should be encouraged in order to facilitate switching between competing providers.

Copyright

- The EU needs to undertake the necessary reform of copyright law, including a revision of the Copyright Directive 2001/29 in order to foster innovation and promote creativity to the benefit of both authors and consumers alike.
- The existing system of platform and territorial release windows for the distribution of audiovisual content is outdated. There should be a single date release of content for all types of distribution, both off and online.
- Flexible licensing systems are necessary to aid the emergence of innovative legal offers.
- The current systems of copyright levies are outdated with respect to the reality of cloud computing and must be phased out.

Liability of Internet Service Providers

- The European Commission should address the legal uncertainty regarding cloud computing service providers and ensure they also are included in the scope of Article 14 of the e-Commerce which defines the conditions for the liability of hosting providers.
- Injunctions against cloud computing service providers for IPR infringements should not result in a general monitoring obligation.
- Specific safeguards should be introduced against abusive notice and action requests for the removal of illegal content.

Net Neutrality

- An analysis of the relationship between cloud computing and net neutrality is necessary.
- Consumers must be able to access any cloud service using any telecom operator's access to internet services.
- Commercial agreements between telecom operators and cloud providers must be fully compliant with competition law and it must be verified that they do not discriminate between competing cloud service providers.

Introduction

The European Commission's Cloud Computing Strategy lacks ambition and is a missed opportunity because it fails to provide guidance on the most important consumer issues related to cloud computing. Cloud computing is a very important technological development, one which consumers are increasingly taking up. Regulating it correctly involves addressing a series of cross-cutting issues in multiple areas such as data protection, copyright or consumer protection and contract law, all the while providing for a neutral internet.

Developments in cloud technology can and are already providing numerous benefits to consumers. Cloud computing is a paradigm shift whereby consumers are increasingly placing their data and computing with remote services and therefore away from their own devices. Cloud services allow consumers to benefit from larger storage capacities, more convenience and more ubiquitous access to their data and preferred services. They also offer a potential increase in the reliability and security of their data and allow consumers to interact with other people in very innovative ways.

While cloud services potentially bring about many tangible and varied benefits to consumers, they also come with numerous risks. For instance, as consumers subscribe to complex cloud contracts, they are exposed to unbalanced contract terms, loss of control over their personal data without sufficient information of who is processing their data and what are their rights in case their data is misused or their access to the cloud computing service is not of the quality that they would expect. Without resolving key consumer issues related to the cloud, consumer trust will not flourish. Unfortunately, the European Commission's strategy fails to achieve this objective.

1. Contractual aspects of cloud computing services

Under key action 2, the Commission proposes measures to ensure fair and safe contracts for cloud computing services. The Commission describes the current situation as characterised by a lack of legal certainty, a proliferation of unbalanced contracts with cloud providers who "use complex contracts or service level agreements with extensive disclaimers" (Communication, point 3.2.) and the resulting risk of unfair contract terms being imposed on consumers having led to a lack of confidence in digital and a reluctance to use these services.

To tackle these problems, the Commission proposes several measures, most significantly the use of the proposed regulation on a Common European Sales Law (CESL) and to establish a complementary optional contract law instrument to cover aspects outside the CESL proposal. In addition, model contracts for business-to-consumer (b2c) transactions should be developed with industry.

Whilst we share the Commission's analysis of the problem, namely that consumers need protection from unbalanced contract terms in order to foster trust in cloud services, the measures outlined by the Commission in its Communication to address these problems are misguided. By relying on merely optional measures which industry can use or avoid according to their preference, the Commission pushes the very concept of consumer protection to the point of absurdity: the EU will protect consumers by relying on industry self-discipline to use fair contract terms according to an optional model – or to continue to exploit the current legal uncertainty and

use unfair, non-transparent contracts. Instead, BEUC calls for a solid regulatory legal framework for consumers, which requires the modernisation of the current consumer law acquis via non-optional legislation. The recently adopted Consumer Rights Directive (CRD)[1] - which is not even mentioned by the Commission in its analysis on the situation regarding b2c contract terms - addresses important contract law areas such as pre-contractual information, formal requirements and the right of withdrawal.

BEUC is against regulating consumer rights by optional means. Optional regimes such as the proposed CESL would give traders the possibility to decide which level of protection consumers benefit from. This is unacceptable from a consumer policy perspective.

This fundamental flaw becomes even more prominent in digital contracts, including those for cloud computing services, as an online business providing these services across borders will be able to decide between modern European rules or national legislation, which is, as acknowledged by the European Commission in Recital 17 of the CESL proposal[2] often unclear in terms of consumer rights in this sector. As a result, businesses may well avoid the specific obligations of the CESL or those of a complementary optional measure as nobody will oblige them to apply these standards and consequently consumers will not benefit from the modern rules that are so urgently needed.

On the contrary, **consumers need clear legislation applicable to all contracts and not dependent on an opt-in or opt-out choice for business**. BEUC believe that the traditional harmonisation of mandatory consumer law must remain the regulatory choice for the EU, as has been the case over the last three decades.

BEUC's proposal

Instead of trying to build consumer confidence on the goodwill of business, the Commission should continue with modernising the consumer law acquis. Below we provide an overview of the current EU legal framework regarding the contractual aspects of cloud computing b2c contracts and make proposals on how the three main areas of concern can and should be appropriately addressed:

[1] Directive 2011/83/EU, 25 October 2011

[2] Recital 17: "*In order to reflect the increasing importance of the digital economy, the scope of the Common European Sales Law should also cover contracts for the supply of digital content. The transfer of digital content for storage, processing or access, and repeated use, such as a music download, has been growing rapidly and holds a great potential for further growth but is* ***still surrounded by a considerable degree of legal diversity and uncertainty.*** *The Common European Sales Law should therefore cover the supply of digital content irrespective of whether or not that content is supplied on a tangible medium.*" (emphasis added)

1) Pre-contractual information and formal requirements

The CRD introduced a harmonised system of pre-contractual information for on-line distance contracts, which would apply to cloud computing services. Additionally, this Directive includes rules on the way such information shall be provided to the consumer, complementing the transparency requirements of the 1993 Unfair Contract Terms Directive and the relevant sector-specific legislation (see recital 11 CRD[3]).

Furthermore, it is crucially important that Article 5.1(h) of the Consumer Rights Directive[4] is effectively enforced so that cloud service providers comply with the obligation to disclose the necessary information related to the interoperability of their services with other services.

These rules, which must be transposed before December 2013 to national legislation, will certainly improve consumer conditions when purchasing digital products or accessing cloud computing services. However, additional measures should be envisaged to ensure the correct implementation of this legislation by service suppliers. An example includes the standardisation of key information as proposed in the 2012 Consumer Agenda[5]. This initiative should take into account all the relevant pre-contractual information of Articles 5 and 6 of the CRD and indicate the way this information shall be presented to consumers while fully respecting the new rules introduced in the CRD on formal requirements.

It is crucial that consumer representatives are closely involved in any such initiative, not just industry representatives as suggested by the Communication on Cloud Computing.

2) *Legal guarantees*

According to a recent empirical study of the European Commission[6] the most important problems experienced by consumers are related to the lack of effective remedies in case of lack of conformity with the contract (e.g. one-third reported problems with access and 18% to quality). These concerns are not addressed in the Commission's Communication.

As no EU harmonisation yet exists for a lack of conformity of services in general, nor for digital content, BEUC calls for a reform of the European legal framework on legal guarantees to adapt it to the challenges of the digital economy by providing a legal solution to such frequent consumer frustrations. Therefore the European Commission should update the current consumer acquis to cover digital products such as cloud computing. This could be done via a new Directive on digital content products or within the frame of an eventual revision of the 1999 Consumer Sales Directive. The rules included in chapters 10 and 11 of the CESL could serve as a basis with appropriate adaptations.

---

[3] This Directive should be without prejudice to Union provisions relating to specific sectors, such as (…) privacy and electronic communications (…).
[4] Directive 2011/83/EU, 25 October 2011
[5] COM(2012) 225 final, 22 May 2012
[6] Europe Economics (2011), 'Digital content services for consumers: Assessment of problems experienced by consumers' available at http://ec.europa.eu/justice/newsroom/consumer-marketing/events/digital_conf_en.htm

3) Unfair contract terms

In contrast to the 1999 Consumer Sales Directive, the legislation on unfair contract terms fully covers contracts for the supply of cloud computing services. However, it is often uncertain how these rules should apply in the digital environment. Consumers are very often confronted with a flow of disclaimers, contractual terms and mentions, which are difficult to both access and understand. The length and complex legal jargon make it impossible for consumers to understand what the real legal implications of the contract are.

It is essential that the terms and conditions of cloud computing business to consumer contracts are drafted in plain and intelligible language and easy to find on the trader's website so consumers can understand what they are agreeing to.

Additionally, these contracts often include unfair clauses such as terms excluding the trader's liability in case of damages or lack of conformity of the service with the contract terms, allowing unilateral changes of terms, conditions or the characteristics of the product at the supplier's entire discretion, within their jurisdiction and/or with mandatory arbitration clauses.

With most cloud computing services, the business to consumer contracts also include terms which do not comply with data protection legislation or unfairly reduce the rights of the consumer - such as with terms authorising the processing of more data than is necessary for the provision of the service or disclosure to third parties without further information. Additionally, terms may allow for the transfer and storage of personal data to third country jurisdictions without safeguards.

In addition, there are concerns in relation to jurisdiction and choice-of-law clauses. Many cloud computing providers subject their contract terms and conditions to the law of an American state and limit complaint submission in binding arbitration schemes or before US courts therefore ignoring the protection granted to EU consumers under Rome I[7] and Brussels I[8] regulations.

Most providers also include clauses disclaiming any kind of liability for the lack of functionality of the service in their contract terms. These types of clauses are frequently accompanied by terms which aim to exclude direct and indirect liability for damage(s) caused to the consumer[9].

In this respect, the European Commission should address the lack of enforcement, in particular with respect to data protection obligations, but also to the lack of transparency and unfairness of cloud computing contract terms. This could be done by way of guidance on transparency requirements and fairness of consumer contracts. This would help clarify the application of unfair contract terms legislation to digital content contracts, including those for the provision of cloud computing services and should include examples of terms which may be considered unfair under the 1993 Unfair Contract Terms Directive.

---

[7] Regulation (EC) 593/2008 of 17 June 2008 on the law applicable to contractual obligations.

[8] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[9] Bradshaw S., Millard C. and Walden I., 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', Queen Mary University of London – Legal Studies Research Paper N° 63/2010.

BEUC has recently produced a position paper on contractual aspects of digital content contracts where we address these concerns[10].

BEUC demands:

- The modernisation of the consumer *acquis* should continue through mandatory legislation and not through optional instruments.
- Implementation of the Consumer Rights Directive provisions on pre-contractual information and formal requirements that apply to cloud computing services.
- A reform of the European legal framework on legal guarantees to adapt it to the challenges of the digital economy, encompassing specific rules on conformity of cloud-computing services and the consumer's rights where there is a lack of functionality of the service. This could be done via a new Directive on digital content products or in the framework of an eventual revision of the 1999 Consumer Sales Directive.
- Guidance on transparency requirements and unfair contract terms to clarify the application of the UCT legislation to digital content contracts, including for cloud computing services. Special attention needs to be paid to common contract terms which do not comply with the data protection legislation or existing legislation at EU level ensuring the effective application of consumer law such as the Rome I and Brussels I regulations.

[10] BEUC position paper, 'Digital Products: EU consumers need clear rights', X/2012/099 -10/12/2012.

2. Data Protection

Cloud computing services create a number of important data protection risks, mainly a lack of control over personal data as well as insufficient information with regards to how, where and by whom the data is processed and sub-processed.

Cloud computing services store and process the personal data of individual citizens, be it through governments or companies who offer services on the cloud, or directly through services such as email, social networking, etc. Therefore, a key question is whether the current legal framework provides appropriate safeguards to protect individuals' personal data in the cloud. The data protection challenges are not cloud computing specific, but have been intensified by the nature of cloud computing and the fact cloud services are increasingly being purchased by European consumers.

The problems related to a lack of transparency, compliance with the key principles of data protection (including purpose limitation and data minimisation) and the uncertainty of the distinction between data controllers and data processors also apply to cloud computing and are addressed in the draft proposal for a Data Protection Regulation. BEUC has provided extensive comments on the draft Regulation[11].

Therefore we focus here on the specific problems related to applicable law, the transfer of data to third countries and codes of conduct as identified in the Communication on Cloud Computing[12].

Applicable law and jurisdiction

Cloud computing is based on the concept of location independence, which implies information and personal data is transferred across jurisdictions. As a result, it is difficult to determine which law applies to a specific cloud computing service.

Under the existing Directive 95/46[13], for EU data protection legislation to apply the cloud provider must either be established in the EU or use equipment in an EU Member State. However, cloud computing services may escape compliance with EU law, even if targeted towards EU citizens for the simple reason that the conditions set out in EU legislation are not met. For instance, the definition of what constitutes “equipment” in the online environment is problematic and can offer cloud providers a means of avoiding EU legislation.

BEUC strongly believes that any data processing activity related to the offering of goods and services to data subjects residing in the EU, or the monitoring of their behaviour must comply with EU law, irrespective of whether the data controller or processor is established in the EU. It should be noted that the offering of goods and services also includes so-called online ‘free services’, which are based on monetising the secondary use of consumers’ data, while the “monitoring of behaviour” shall include tracking and profiling carried out by controllers outside the EU. For these provisions to deliver benefits to European consumers, effective enforcement mechanisms and procedures need to be in place.

[11] BEUC position Paper on Data Protection Regulation proposal X/2012/039 - 27/07/2012.
[12] Communication COM(2012) 429 final ‘Unleashing the Potential of Cloud Computing in Europe’.
[13] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

As regards the national law to apply to a specific processing operation, it should be that of the country in which the consumer resides. When dealing with the issue of applicable law, it is essential to keep in mind that the main aim of the EU Data Protection Framework is to protect the rights of data subjects. In practice, when there is an element or factor closely related to the EU which helps protect the interests of EU citizens, the legislator[14] and the judge[15] often decide in favour of EU law.

International transfers

Directive 95/46 prohibits the transfer of personal data to countries which do not ensure an adequate level of protection. Articles 25 and 26 provide for the transfer of data outside the EU only if the country of destination provides an adequate level of protection. However, with cloud services it is very common that data is not always stored and processed in the same location within the provider's network. It is therefore virtually impossible to know in real time where the data is located, stored or transferred.

The draft Data Protection Regulation recognises the new reality and abandons the principle that personal data may not be transferred without an adequate level of protection, setting instead a number of principles which must be fulfilled when personal data is transferred outside the EU. In the absence of an adequacy decision, the draft Regulation allows for the transfer of data provided that the controller or the processor have adhered to appropriate safeguards. Such safeguards will be provided by Binding Corporate Rules (BCRs), standard data protection clauses approved by the European Commission or adopted by a Data Protection Authority (DPA).

The Communication on Cloud Computing foresees specific actions with regards to the international transfer of data. In particular, the review of standard contractual clauses and the approval of Binding Corporate Rules for cloud providers have been identified as priority actions.

Standard contractual clauses as adopted by the EU Commission for the purpose of framing international data transfers between two controllers, or one controller and a processor, are based on a bilateral approach. Such clauses are useful for Business-to-Business (b2b) transfers. However, approvals are often restricted to a single contractual document covering a defined set of transfers, which makes the concept completely unworkable for multiple and evolving transfers.

As regards Binding Corporate Rules, these constitute a code of conduct for companies which transfer data within their own corporate group. It is important that BCRs are binding and enforceable upon all members of the corporation and that implementation requires approval by the supervisory authority.

[14] See Article 12 of the Distance Selling Directive (Directive 97/7/EC), Article 6(2) of Directive 93/13 on Unfair Terms in Consumer Contracts and Article 7(2) of Directive 99/44 on certain aspects of the sale of consumer goods and associated guarantees and article 6 of the Rome I Regulation (Regulation 593/2008/EC).

[15] See ECJ jurisprudence on the Rome Convention; e.g. Ingmar GB Ltd. and Eaton Leonard Technologies Case C-381/98.

According to the US-EU Safe Harbor Agreement, transfers to US organisations who adhere to the Agreement's principles can lawfully take place under EU law as the recipient organisations are assumed to provide an adequate level of protection of the transferred data. BEUC points out that Safe Harbour fails to meet the standards of EU law and does not guarantee the protection of personal data of European consumers as a fundamental right. Safe Harbor is based on companies' self-certification of compliance with the principles, which should not be sufficient for the transfer to take place. BEUC calls for a revision of the Safe Harbour principles as a matter of urgency.

Access to personal data for law enforcement purposes

Controllers operating in the EU must be forbidden to disclose without prior approval personal data to a third country if so requested by a third country's judicial or administrative authority. BEUC regrets that the proposed Data Protection Regulation does not include a provision that clearly states that in cases where a third country requests the disclosure of personal data, the controller or processor has to obtain prior authorisation for the transfer from its local supervisory authority[16].

This provision is especially relevant with regards to data disclosure to US authorities. The US uses instruments such as the Foreign Intelligence Surveillance Act (FISA) and the Patriot Act to collect data about the political activities of foreign individuals who may have no links whatsoever to the US and they do so via companies with offices in the US.

Codes of conduct

The Commission's Communication on Cloud Computing identifies the development, together with relevant industry actors, of a code of conduct for cloud computing providers as a specific action. This intends to support uniform application of data protection rules and it may be submitted to the Article 29 Data Protection Working Party for endorsement.

Although BEUC considers that the existing data protection Directive establishes an effective framework within which self-regulation and co-regulation in the field of data protection can be developed, we regret the approach of the European Commission in the cloud computing Communication. Firstly, the Commission has excluded consumer groups and civil society organisations from the range of stakeholders providing feedback on the issue of data protection - a fundamental right for European citizens. A code of conduct which does not comply with these governance principles does not have sufficient legitimacy. Secondly, despite the requirement under the Directive 95/46 requires for any code of conduct to be submitted to the Article 29 Data Protection Working Party for approval, the Commission has decided to make such submission only optional, thus giving industry the green light to develop 'soft' self-regulation to deal with personal data, without any assessment of compliance with the legal framework by Data Protection Authorities.

[16] A similar provision appeared in the leaked draft version but was deleted following the pressure by a number of stakeholders, including the US federal Trade Commission. http://edri.org/files/12_2011_DPR_USlobby.pdf

Codes of conduct can be endorsed if they amount to added value for consumers' rights by offering a higher level of protection than the legal framework; are backed up by suitably robust auditing or testing procedures; and provide for independent complaint handling, robust sanctions and effective consumer redress.

Certification

BEUC supports the establishment of EU certification schemes, including a European Privacy Seal, as long as clear certification criteria are developed and the administration is entrusted to independent, third party organisations. The establishment of a Certification Authority for the issuing of the seals and the accreditation of specially trained and tested independent experts who carry out the primary evaluation of the products would provide for additional safeguards.

The development of EU certification schemes and privacy seals could become an effective means of ensuring 'privacy compliant' or even 'privacy enhancing' IT products, websites, companies and services. It will also provide an incentive for developers and providers of such products and services to invest in better privacy protection, while allowing users to make an informed and quick choice. However, it is important to clarify that the granting of a seal would not simply certify compliance with the law, but provide an added layer of protection.

BEUC demands:

- EU data protection law should apply to any data processing activity related to the offering of goods and services to data subjects residing in the EU or the monitoring of their behaviour, irrespective of whether the data controller and/or processor is established in the EU.
- Applicable law for a specific processing operation should be the law of the country of residence of the data subject.
- The US-EU Safe Harbour Agreement should be reviewed urgently as it does not sufficiently guarantee the protection of personal data and its enforcement remains ineffective.
- Transfers of an EU resident's personal data to a third country must be subject to the adequacy mechanism, while Binding Corporate Rules and Standard Contract Clauses could be used exceptionally, subject to strict safeguards and conditions.
- Any request for the transfer of EU resident's personal data to law enforcement authorities of third countries should require prior authorisation by the Data Protection Authority of the country of the data subject's residence.
- Codes of conduct in the field of data protection must ensure a high take up of the industry, be submitted for approval to the Article 29 Data Protection Working Party and offer a higher level of protection than the legal framework, be backed up by suitably robust auditing or testing procedures and provide for independent complaint handling, robust sanctions and effective consumer redress.

3. Interoperability and Portability

Interoperability and compatibility of cloud computing services is crucial for consumers. Consumer choice and competition within the cloud will only flourish if there are enough interoperable services so that consumers can easily shop around and port their data along when they switch providers. Consumer choice is crucial in order for consumer trust in the cloud to develop. Interoperability is also important to enable consumers to retain ownership of their data and exercise their right to data portability.

Data portability should be understood as the right to recover and/or to shift information and data from one cloud to another. Cloud services of the same nature need to be compatible and facilitate the exchange of data amongst competing services.

The exercise of the consumer's right to data portability might require a distinction between different types of cloud services[17]. Depending on the nature of each cloud service, the type of data that will be important for consumers to port when they switch providers will vary. For instance, for general storage services it is evident that consumers need to be able to easily switch providers and take all their documents along with them. For specific storage files, such as online photo platforms, consumers should be able to easily switch providers while moving the photos along with additional layers of information they have gathered, e.g. albums, tags, comments and so on. For other services where consumers do not own the content they consume, such as video or music streaming platforms, what is relevant for consumers to be able to port to a competing service is the preferences, playlists and other personalisation they may have made with the other service used.

Empowering consumers through easier switching

Exporting the data from one cloud provider to a new one is far from easy for consumers. Moving from one cloud service to another is very often a task which requires advanced technical skills in order to fulfil the complex procedures providers put in place to prevent the loss of customers.

Cloud users need to be able to extract their data from a cloud with the same ease with which it entered. Cloud providers should not complicate the process consumers must follow to recover their data and delete their account. To spur competition, this process should be user-friendly and straightforward. This will facilitate switching and allow consumers to easily choose the most convenient service for them. Therefore, there should not be any contractual or technical restrictions in place.

Furthermore, the possibility for automatic data transfers should be considered. In many cases, and this will be increasingly the case as consumers move more of their data onto the cloud, the quantity of data which needs to be transferred is so large that it is impractical for consumers to use their broadband access to download and then re-upload their data to the new provider's servers. This is particularly the case when we take into account that for most European consumers, the upload

[17] From a consumer perspective, cloud services can be regrouped around different general categories, such as: storage services, both general (for any types of files) and specific (only music, only images, only video, etc); streaming platforms, social networks, web-based email, location-based services, and so on.

bandwidth provided in their broadband access services is rather limited. Therefore it is important that cloud service providers are able to devise automatic transfers of data when consumers decide to switch providers. This would also add efficiency to the entire system as the data would only be transferred on the upper layers of the internet without the need to push it down to the consumer's devices and then back up again to the new providers' servers.

Interoperability and compatibility of cloud services is also crucial to avoid vendor lock-in situations, where consumers, cannot switch because it is either technically very complicated and cumbersome for them to do so or because they are contractually locked into the service. Avoiding lock-in situations is also important to prevent barriers to market entry, for consumers to fully benefit from the increasing variety of cloud services and to foster innovation and competition in this emerging market. Therefore, BEUC calls on the European Commission to enact the standards necessary to allow for full interoperability among competing cloud services.

BEUC demands:

- The necessary standards to allow for full interoperability among competing cloud services of the same nature need to be developed.
- Policy makers need to ensure that cloud providers do not lock-in consumers to the service with lengthy contracts or by making it technically cumbersome to switch.
- Automatic transferal of data between compatible cloud services should be encouraged in order to facilitate switching between competing providers.

4. Copyright

The Commission's Communication lacking in ambition

BEUC's assessment of the Cloud Computing Strategy is that it falls short in ambition and represents another lost opportunity for the EU to define clear priority actions necessary to reform current copyright law and establish a Digital Single Market.

Over the past five years, a number of consultations were launched at EU level and a number of reports published which helped identify the main challenges in creating a Digital Single Market for online content. The 2008 Green Paper on Copyright in the Knowledge Economy[18], the 2009 Reflection Paper on Creative Content[19], the 2010 EU Digital Agenda[20], the Monti Report on the Future of the Single Market[21] and the EU IPR Strategy[22] have all identified the same problems.

We expect the European Commission to propose concrete reforms of copyright law that will help the EU to develop a future-proof framework which balances the rights of creators with the rights of consumers and the general public.

Need for a coherent and forward looking EU copyright agenda

Cloud computing has the potential to facilitate consumer access to content. With countless new opportunities arising from the ways in which content is accessed and distributed, the need has arisen to rethink the European legal framework, achieve a fair balance between different stakeholders and promote innovation as well as cultural diversity. The current copyright framework continues to fail to keep pace with rapid digital developments.

Consumers should be able to benefit from the realisation of a truly competitive Internal Market, access diverse online content of the highest quality and at a fair price. Authors are entitled to have their rights protected and receive fair compensation for the use of their works on the internet. Copyright law should aim to foster innovation and promote creativity to the benefit of both authors and consumers. At the same time, it is important to provide the necessary incentives for the development of new business models allowing for the simultaneous distribution of content across the EU and via multiple channels.

The remaining territorial restrictions and fragmentation along national borders result in Europe's culture staying locked at a national level. We fully agree that European cultural diversity must be safeguarded; however European creative works should not remain locked within national borders. The fostering of cultural diversity requires access to diversity.

[18] http://ec.europa.eu/internal_market/copyright/docs/copyright-infso/greenpaper_en.pdf
[19] http://ec.europa.eu/avpolicy/docs/other_actions/col_2009/reflection_paper.pdf
[20] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
[21] http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf
[22] http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_en.pdf

Access to content

Accessibility is the main advantage of cloud computing services for digital content. Consumers should be able to access content, no matter whether it is music, audiovisual or books from different devices at the location of their choice and irrespective of their nationality or place of residence. Consumers should be able to benefit from the establishment of a Single Market both online and offline.

Currently, the territorial management of copyright, in combination with the uncertainty as to the ownership of copyright and the complex licensing mechanisms, result in the fragmentation of the European market for creative content.

Rights holders have so far defended the position that territoriality of copyright and **market fragmentation** is an objective reason which justifies price discrimination. However, the recent ruling of the European Court of Justice in the Premier League case clearly stated that "a system of territorial licences for the broadcasting of football is contrary to EU law"[23]. This ground-breaking ruling of the ECJ and the categorical rejection of absolute territorial exclusivity confirms the incompatibility of current business models for online content with the Internal Market.

BEUC also considers both **platform and territorial release windows** to be outdated. Although beneficial to some intermediaries, broadcasters and distributors, the current system is incompatible with the Commission's commitment to establishing a digital single market, irrespective of the fact it is contrary to consumer choice and hinders the emergence of innovative business models for the online distribution of European works. BEUC calls for a single day and date release for all types of distribution, both off and online across Europe.

The main focus of EU policies should be the establishment of flexible licensing systems that allow for the emergence of innovative legal offers without excessive transactional costs and endless negotiations about license terms and tariffs.

Private copying and copyright levies

As consumers increasingly adopt and use cloud computing services, they replicate less, if any, content on their personal local devices, which is making the private copy levy concept less relevant. The majority of business models for legal content, such as those based on streaming, do not necessarily require consumer storage capacity in the terms of the private copying exception and therefore applying levies on the basis of memory size is unaligned with the manner in which music and audiovisual content is consumed. Furthermore, cloud based services make it possible to measure authorised uses of creative content allowing for precise, license-based remuneration of right owners.

BEUC strongly believes that the current systems of copyright levies do not correspond to the needs of the digital environment and are outdated with respect to the reality of cloud computing, as was stated by Mr Antonio Vitorino in his final

[23] Cases C-403/08 Football Association Premier League Ltd, v QC Leisure and C-429/08, Karen Murphy v Media Protection Services Limited;

recommendations following the copyright levies mediation[24]. BEUC calls for immediate EU action in order to reform the current systems of copyright levies and launch as a matter of urgency a reflection as to alternative systems of fair compensation. The more digital content consumers are able to acquire as part of licensing services, the less need there is for private copying compensation, as right holders will be directly and fairly compensated.

Our suggestions are clearly defined in our position paper[25].

BEUC demands:

- The EU needs to undertake the necessary reforms in current copyright law, including a revision of the Copyright Directive 2001/29 in order to foster innovation and promote creativity to the benefit of both authors and consumers alike.
- The existing system of platform and territorial release windows for the distribution of audiovisual content is outdated. There should be a single release date for content by all forms of distribution, both off and online.
- Flexible licensing systems are necessary to allow for the emergence of innovative legal offers.
- The current systems of copyright levies are outdated with respect to the reality of cloud computing and must be phased out.

[24] http://ec.europa.eu/internal_market/copyright/docs/levy_reform/130131_levies-vitorino-recommendations_en.pdf

[25] Copyright levies mediation- BEUC response to public consultation, X 2012/40.

5. Liability of Internet Service Providers

Clarification of scope of Article 14 of e-Commerce Directive

The e-Commerce Directive established a liability regime for Internet Service Providers (ISP) for illegal content. There is legal uncertainty as to the definition of hosting providers and namely the application to cloud computing service providers. The main difficulty relates to the definition of a hosting service under Art. 14, where it is defined as a service that "consists of the storage of information provided by the recipient of the service". However, the criterion of storage of information does not correspond to services, such as cloud computing services, where the storage is just one aspect of the entire package. As a result, national courts have adopted different interpretations and case law differs from one country to another, thus resulting in legal uncertainty.

Overall, BEUC does not consider revision of the e-commerce Directive provision on internet intermediaries necessary. On the contrary, the European Commission should address the legal uncertainty regarding cloud computing service providers and ensure they are also within the scope of Article 14 of the e-Commerce Directive (Art. 14). When clarifying the scope of application, due consideration of the impact on freedom of expression and communication is necessary.

Risk of injunctions remains

Both the Copyright[26] and the IPR Enforcement Directives[27] foresee the possibility for right holders to apply for injunctions against Internet Service Providers. Injunctions have been used widely for IPR infringements. The main problem relates to the fact that injunctions cease not only the infringement, but also prohibit future infringements. However, the prevention of future infringements may lead to a de facto general monitoring obligation for the hosting provider and therefore a conflict with Art. 15 of the e-Commerce Directive.

The European Court of Justice has recently ruled[28] that hosting providers cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical and audio-visual works. Such an obligation would fail the prohibition on imposing on providers a general obligation to monitor (Article 15 of the e-Commerce Directive). The Court also stressed that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.

---

[26] Article 8.3 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

[27] Article 11 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

[28] Sabam v Netlog Case 360/10. In the main proceedings, the injunction requiring the installation of a filtering system would involve monitoring all or most of the information stored by the hosting service provider concerned, in the interests of the copyright holders. Moreover, that monitoring would have to have no limitation in time, be directed at all future infringements and be intended to protect not only existing works, but also works that have not yet been created at the time when the system is introduced. Accordingly, such an injunction would result in a serious infringement of Netlog's freedom to conduct its business since it would require Netlog to install a complicated, costly, permanent computer system at its own expense.

BEUC is opposed to a wide interpretation of the provision on injunctions i.e. one which would require cloud service providers (falling within the scope of hosting providers) to monitor content and prevent future infringements. Such an expansive interpretation conflicts with the prohibition of general monitoring and therefore should be rejected.

Notice-and-action procedure

Hosting providers can only benefit from the limited liability provisions of the e-Commerce Directive when they expeditiously remove or disable access to illegal information as soon as they have actual knowledge or are aware of the facts or circumstances regarding the illegal information. This rule forms the basis for "notice-and-action" (N&A) procedures.

BEUC is strongly opposed to a horizontal approach with regards to notice and action procedures for all types of illegal content, including child abuse, defamation, health, gambling and intellectual property rights. Treating child abuse and user-created content in the same way is inappropriate.

BEUC has identified a number of principles which notice and action procedures should comply with:

- Validity of notices: every notice shall clearly identify the specific content concerned, provide evidence that the notice provider is entitled to act and demonstrate that the content is illegal.

- Actual knowledge: Only a court can confirm the illegal nature of content. Notification by third parties shall not suffice for the rule on the illegal nature of the content.

- Expeditious action: an action timeframe should be established for different types of content in order to provide hosts, notice and content providers with legal certainty.

- Safeguards against abuses: when the content has been taken down on the basis of an invalid notice or false information provided by the notice provider, the latter shall be liable for damages both to the host provider and the user or content provider.

- Notice and Notice: Upon receipt of a valid and substantiated notice, the host provider shall inform the content provider, who will be able to submit a counter-notice before any further action is taken. The notice-and-notice procedure should be used in cases which involve complex legal assessments, such as IPR related issues.

- Targeted action: notice and action requests should target specific content rather than resulting in bans on the operation of whole sites or systems and in general monitoring.

BEUC demands:

- The European Commission should address the legal uncertainty regarding cloud computing service providers and ensure they are also included within the scope of Article 14 of the e-Commerce Directive.
- Injunctions against cloud computing service providers for IPR infringements should not result in a general monitoring obligation.
- Specific safeguards should be introduced against abusive notice and action requests for the removal of illegal content.

6. Net Neutrality

BEUC regrets that the European Commission has not looked into the relationship between Net Neutrality and Cloud Computing in its Cloud Computing Strategy, therefore obviating the link between these two important issues for European consumers. In order to amend this, the relationship between and impact of cloud computing and net neutrality needs to be analysed and, where appropriate, specific guidance provided in the upcoming Commission recommendation on net neutrality.

Net neutrality is the principle that all electronic communications passing through a network are treated equally, independent of content, application, service, device, source or target. As consumers move their digital activities onto the cloud, they need to be able to fully exercise their right to an internet access service that is free of illegitimate discrimination. An internet access service they can buy and use to access no matter what cloud computing service is on offer to them on the internet.

In recent years, telecom operators have been consistently and increasingly violating this fundamental principle for their own commercial benefit and to the detriment of European consumers. There is a risk that telecom operators and cloud service providers undertake commercial agreements whereby the operator gives preferential treatment to the services of the cloud provider it is partnering with. It is crucial that these agreements are checked for compliance with competition law and, in order to respect the neutrality of the internet, it is verified that they avoid negative discrimination against competing cloud services. Similarly, if telecom providers wish to provide specific cloud services with premium access to higher qualities of service it must be ensured that other competing cloud services will not be discriminated against.

Furthermore, if net neutrality is not strongly protected, consumers will find themselves in the situation where they can only choose from certain cloud computing services depending on the telecom operator they have chosen to access the internet with, therefore severely reducing consumer choice.

The neutrality of the internet has also guaranteed a level playing field for market entrants and innovators who wish to launch a new service, ensuring that all of them have the capacity to reach the entire internet and its end-users and consumers. Without net neutrality, market entry for new comers is hindered and consumer choice risks being further reduced.

BEUC demands:

- An analysis of the relationship between and impact of cloud computing and net neutrality is necessary.
- Consumers must be able to access any cloud service using any telecom operator's access to internet services.
- Commercial agreements between telecom operators and cloud providers must be fully compliant with competition law and it must be verified that they do not negatively discriminate against competing cloud service providers.

END