REPORT

on unleashing the potential of cloud computing in Europe
(2013/2063(INI))

Committee on Industry, Research and Energy

Rapporteur: Pilar del Castillo Vera

Rapporteurs for the opinions (*):
Lidia Joanna Geringer de Oedenberg, Committee on Legal Affairs
Judith Sargentini, Committee on Civil Liberties, Justice and Home Affairs

(*) Associated committees – Rule 50 of the Rules of Procedure
## CONTENTS

<table>
<thead>
<tr>
<th>Motion</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION</td>
<td>3</td>
</tr>
<tr>
<td>EXPLANATORY STATEMENT</td>
<td>17</td>
</tr>
<tr>
<td>OPINION OF THE COMMITTEE ON LEGAL AFFAIRS*</td>
<td>20</td>
</tr>
<tr>
<td>OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS*</td>
<td>25</td>
</tr>
<tr>
<td>OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION</td>
<td>32</td>
</tr>
<tr>
<td>RESULT OF FINAL VOTE IN COMMITTEE</td>
<td>38</td>
</tr>
</tbody>
</table>

(*) Associated committees – Rule 50 of the Rules of Procedure
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on unleashing the potential of cloud computing in Europe

(2013/2063(INI))

The European Parliament,

– having regard to the Commission communication of 27 September 2012 entitled ‘Unleashing the potential of cloud computing in Europe’ (COM(2012)0529) and the accompanying working document,


– having regard to its resolution on a new digital agenda for Europe: 2015.eu¹,

– having regard to Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme,

– having regard to the Commission’s proposal of 25 January 2012 for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011),

– having regard to the Commission’s proposal of 19 October 2011 for a Regulation of the European Parliament and of the Council establishing the Connecting Europe Facility (COM(2011)0665),


– having regard to the work by the European Telecommunications Standards Institute (ETSI) on a cloud standards mapping;

–


of the sale of consumer goods and associated guarantees\textsuperscript{1},

– having regard to Directive 95/46/EC of Parliament and of the Council 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\textsuperscript{2},

– having regard to Directive 2000/31/EC of Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market \textsuperscript{3},


– having regard to Rule 48 of its Rules of Procedure,

– having regard to the report of the Committee on Industry, Research and Energy and the opinions of the Committee on Legal Affairs, the Committee on Civil Liberties, Justice and Home Affairs and the Committee on the Internal Market and Consumer Protection (A7-0353/2013),

A. whereas while remote computing services in various forms, now commonly known as ‘cloud computing’, are not new, the scale, performance and content of cloud computing constitute a significant advancement in information and communication technologies (ICT);

B. whereas cloud computing has nonetheless attracted attention in recent years owing to the development of new and innovative large-scale business models, a strong push by cloud vendors, technological innovations and increased computing capabilities, lower prices and high-speed communications, as well as to the potential economic and efficiency benefits, including in terms of energy consumption, that cloud services offer all kinds of users;

C. whereas the deployment and development of cloud services in sparsely populated and remote areas can contribute to reducing their isolation, while at the same time pose particularly serious challenges given the insufficient availability of necessary infrastructure;

D. whereas the vendor benefits of cloud services consist of e.g. service fees, monetisation of underutilised and excess computing resources, economies of scale, the possibility of a captive customer base (so called lock-in effect) and secondary uses of user information, such as for advertising, with due regard for the requirements of personal data privacy and protection; whereas a lock-in effect can have competitive disadvantages that nevertheless can be dealt with through reasonable standardisation measures and better transparency on intellectual property licensing agreements;

\textsuperscript{1} OJ L 171, 07.07.1999, p. 12.
\textsuperscript{2} OJ L 281, 23.11.1995, p. 31.
\textsuperscript{4} OJ L 167, 22.06.2001, p. 10.
E. whereas the user benefits of cloud services consist of potentially lower costs, ubiquitous access, convenience, reliability, scalability and security;

F. whereas cloud computing also entails risks for users, in particular as regards sensitive data, and users need to be aware of those risks; whereas if cloud processing is done in a particular country, the authorities of that country can have access to the data; whereas this should be taken into account by the Commission when issuing proposals and recommendations regarding cloud computing;

G. whereas cloud services oblige users to hand over information to the cloud storage provider, a third party, raising issues relating to the continued control over and access to the information of individual users and its protection against the provider itself, other users of the same service and other parties; whereas encouragement of services which allow for the user and only the user to hold keys to the information stored, without the cloud storage providers themselves being able to access that information, could solve some of the issues pertaining to this problem;

H. whereas the increased use of cloud services provided by a limited number of large providers means that increasing amounts of information is aggregated in the hands of those providers, thus magnifying their efficiencies but also increasing the risks of catastrophic losses of information, of centralised points of failure that could undermine the stability of the internet and of access to the information by third parties;

I. whereas the responsibilities and liabilities of all the stakeholders involved in cloud computing services should be clarified, in particular as they apply to security and to respect of data protection requirements;

J. whereas the market for cloud services appears bifurcated along consumer and business lines;

K. whereas for business users, standardised cloud services can, if they meet the particular needs of the user, be an attractive means of converting capital cost to operating expense and of enabling fast availability and scaling of additional storage and processing capacity;

L. whereas for consumers, the fact that providers of operating systems for various types of consumer devices, in particular, are increasingly steering consumers – through the use of default settings, etc. – towards using proprietary cloud services, means that these providers are creating a captive consumer-base and aggregating the information of their users;

M. whereas the use of external cloud services in the public sector has to be weighted carefully against any increased risks with regard to information on citizens and against the ensured performance of public service functions;

N. whereas, from a security perspective, the introduction of cloud services means that the responsibility for maintaining the security of information belonging to each individual user is shifted from the individual to the provider, thereby raising the need to ensure that service providers have the legal ability to provide secure and robust solutions for communication;
O. whereas the development of cloud services will increase the amount of transmitted data and the demand for bandwidth, higher upload speeds and more available high-speed broadband;

P. whereas the achievement of Europe’s digital agenda targets, in particular broadband uptake and access for all, cross-border public services and research and innovation goals, is a necessary step if the EU is fully to reap the benefits that cloud computing has to offer;

Q. whereas there have recently been developments involving security breaches, in particular the PRISM spying scandal;

R. whereas there is a lack of server farms on European soil;

S. whereas the Digital Single Market is a key factor in attaining the targets of the Europe 2020 strategy, which would provide a significant boost in efforts to meet the objectives of the Single Market Act and respond to the economic and financial crisis affecting the EU;

T. whereas EU-wide broadband provision, universal and equal access to internet services for all citizens, and a guarantee of network neutrality are the essential prerequisites for the development of a European cloud computing system;

U. whereas the Connecting Europe Facility is intended, among other things, to increase broadband uptake in Europe;

V. whereas cloud computing should stimulate the integration of SMEs through the reduction of market entry barriers (e.g. by decreasing IT infrastructure costs);

W. whereas it is essential for a European cloud computing system that EU legal standards on data protection are guaranteed;

X. whereas the development of cloud computing should help promote creativity for the benefit of both rights-holders and users; whereas, furthermore, distortions in the Single Market should be avoided in the process and consumer and business confidence in cloud computing should be boosted;

General

1. Welcomes the Commission’s communication on unleashing the potential of cloud computing in Europe and approves the Commission’s ambition to develop a coherent approach to cloud services, but considers that, in order to achieve the ambitious goals set out by the strategy, a legislative instrument would have been more adequate for some aspects;

2. Underlines that policies enabling high-capacity and secure communications infrastructure are a crucial element for all services relying on communications, including cloud services, but highlights that, owing to the limited budget of the Connecting Europe Facility, support for broadband deployment needs to be supplemented with assistance provided under other Union programmes and initiatives, including the European Structural and Investment Funds;
3. Underlines that cloud services must offer security and reliability commensurate to the increased risks flowing from the concentration of data and information in the hands of a limited number of providers;

4. Underlines that Union law should be neutral and, absent compelling reasons of public interest, not be adapted to either facilitate or hinder any legal business model or service;

5. Stresses that a strategy on cloud computing should encompass collateral aspects such as the energy consumption of data centres and related environmental issues;

6. Emphasises the vast possibilities that having access to data from any device connected to the internet offers;

7. Stresses the obvious interest, from a dual perspective, for the EU in having more server farms on its soil: in terms of industrial policy, it would allow for enhanced synergies with the roll-out objectives for Next Generation Access Networks (NGA) set out in the digital agenda, and in terms of the Union’s data protection regime, it would foster trust by ensuring EU sovereignty over the servers.

8. Underlines the importance of digital literacy among all citizens, and urges the Member States to develop concepts of how to promote the safe use of internet services, including cloud computing;

The cloud as an instrument for growth and employment

9. Emphasises that, given the economic potential of the cloud for increasing Europe’s global competitiveness, it can become a powerful instrument for growth and employment;

10. Stresses, therefore, that the development of cloud services, in the absence or insufficient availability of broadband infrastructure, risks widening the digital divide between urban and rural areas, which will make territorial cohesion and regional economic growth still harder to achieve;

11. Highlights that the Union faces multiple, simultaneous pressures on GDP growth at a time when the scope to stimulate growth from public funds is limited by high debt and deficit levels, and calls on the European institutions and the Member States to mobilise every possible growth lever; notes that cloud computing can become a transformative development in all sectors of the economy, with special relevance in areas such as health care, energy, public services and education;

12. Stresses that unemployment, including youth and long-term unemployment, has reached unacceptably high levels in Europe and is likely to remain high in the near future, and that determined and urgent action is needed at all political levels; notes that e-skills and digital education actions in cloud computing development can, consequently, be of extraordinary importance in order to tackle the rising unemployment, especially among young people;

13. Underlines the need for greater e-skills among users and for training to show the benefits that cloud computing can offer; recalls the need to create more qualification schemes for specialists managing cloud computing services;
14. Highlights that SMEs are at the heart of the EU’s economy and that more actions are needed to promote the global competitiveness of EU SMEs and to set the best possible environment for the uptake of new promising technological developments, such as cloud computing, which can have a high impact on the competitiveness of EU businesses;

15. Insists on the positive impact of cloud computing services on SMEs, in particular those established in remote or outermost areas or facing economic difficulties, as such services contribute to the reduction of fixed costs for SMEs by allowing the rental of computing power and storage, and calls on the Commission to consider an appropriate framework allowing SMEs to increase their growth and productivity, as SMEs can benefit from reduced upfront costs and better access to analytics tools;

16. Encourages the Commission and the Member States to communicate the economic potential of cloud computing to SMEs in particular;

17. Points out that the EU must take advantage of the fact that this technology is at a relatively early stage and must work towards developing it in order to benefit from the economies of scale which it is expected to offer, thereby revitalising the Union’s economy, particularly in the ICT sector;

The EU market and the cloud

18. Stresses that the internal market should remain open to all providers complying with Union law, as the global free flow of services and information increases the competitiveness of and opportunities for Union industry and benefits Union citizens;

19. Regrets the indications of massive, pervasive and indiscriminate governmental access to information related to Union users stored in third-country clouds, and calls for cloud service providers to be transparent about how they manage the information that consumers make available to them through the use of cloud services;

20. Insists that, in order to counter the risk that information is accessed directly or indirectly by foreign governments, where such access is not allowed under Union law, the Commission shall:

   (i) ensure that users are aware of this risk, including by supporting the European Network and Information Security Agency (ENISA) in activating the public interest information platform in the Universal Service Directive, and

   (ii) sponsor research in and commercial deployment or public procurement of relevant technologies, such as encryption and anonymisation, enabling users to secure their information in an easy way;

   (iii) involve ENISA in verifying the minimum security and privacy standards of cloud computing services offered to EU consumers and, in particular, to the public sector;

21. Welcomes the Commission’s intention to establish an EU-wide certification system that would provide an incentive for developers and providers of cloud computing services to invest in better privacy protection;
22. Calls on the Commission, in cooperation with Union industry and other stakeholders, to identify areas where a specific Union approach could prove particularly attractive globally;

23. Emphasises the importance of ensuring a competitive and transparent Union market in order to provide all Union users with secure, sustainable, affordable and reliable services; calls for a simple, transparent method to identify security flaws in such a way that service providers on the European market have a sufficient and appropriate incentive to remedy such flaws;

24. Underlines that all cloud providers operating in the Union must compete on an even playing field, with the same rules applicable to all;

Public procurement, and procurement of innovative solutions, and the cloud

25. Stresses that the take-up of cloud services by the public sector has the potential to reduce costs for public administrations and provide more efficient services to citizens, whilst the digital leverage effect to all sectors of the economy would be extremely beneficial; points out that the private sector can also take advantage of those cloud services for the procurement of innovative solutions;

26. Encourages public administrations to consider safe, reliable and secure cloud services in IT procurement, while underlining their particular responsibilities with respect to protection of information relating to citizens, accessibility and continuity of service;

27. Calls, in particular, on the Commission to consider making use of cloud services, where appropriate, in order to provide an example to others;

28. Calls on the Commission and the Member States to speed up the work of the European Cloud Partnership;

29. Calls on the Commission and the Member States to make cloud computing a priority area for research and development programmes, and to promote it in the public administration sector as an innovative e-government solution of public interest, as well as in the private sector as an innovative tool for business development;

30. Stresses that the use of cloud services by public authorities, including by law enforcement authorities and EU institutions, requires special consideration and coordination between the Member States; recalls that data integrity and security must be guaranteed and unauthorised access, including by foreign governments and their intelligence services without a legal basis under Union or Member State law, prevented; stresses that this also applies to the specific processing activities of certain essential non-governmental services, in particular the processing of specific categories of personal data, such as by banks, insurance companies, pension funds, schools and hospitals; stresses, furthermore, that all of the aforementioned is of particular importance if data is being transferred (outside the European Union between different jurisdictions); takes the view, therefore, that public authorities, as well as non-governmental services and the private sector, should, as far as possible, rely on EU cloud providers when processing sensitive data and information until satisfactory global rules on data protection have been introduced, ensuring the security of
sensitive data and of data bases held by public entities;

**Standards and the cloud**

31. Calls on the Commission to take the lead in promoting standards and specifications supporting privacy-friendly, reliable, highly interoperable, secure and energy-efficient cloud services as an integral part of a future Union industrial policy; stresses that reliability, security and protection of data is needed for consumer confidence and competitiveness;

32. Stresses that standards are based on examples of best practices;

33. Insists that standards should enable easy and complete data and service portability, and a high degree of interoperability between cloud services, in order to increase rather than limit competitiveness;

34. Welcomes the mapping of standards that has been entrusted to ETSI, and highlights the importance of continuing to follow an open and transparent process;

**Consumers and the cloud**

35. Calls on the Commission to ensure that consumer devices do not make use of cloud services by default and are not restricted to specific cloud service provider;

36. Calls on the Commission to ensure that any commercial agreements between telecommunications operators and cloud providers are fully compliant with EU competition law and that they allow consumers full access to any cloud service, using an internet connection offered by any telecommunications operator;

37. Reminds the Commission of its as yet unexploited prerogative, under Directive 1999/5 (the RTTE Directive), to require that equipment incorporates safeguards protecting users’ information;

38. Calls on the Commission and the Member States to raise consumer awareness of all risks related to the use of cloud services;

39. Calls on the Commission to ensure that consumers, when prompted to accept or otherwise offered a cloud service, are first given the information necessary for an educated decision, particularly when it comes to the jurisdiction covering the data stored in these cloud services;

40. Stresses that the information thus provided should identify, among other things, who the ultimate provider of the service is and how the service is financed; stresses, furthermore, that if the service is financed by using users’ information to target advertising or enable others to do so, this should be disclosed to the user;

41. Stresses that the information should be in a standardised, portable, easily comprehensible and comparable format;

42. Calls on the Commission to explore appropriate measures to develop a minimum
acceptable level of consumer rights in relation to cloud services, covering issues such as privacy, data storage in third countries, liability for data losses and other matters of significant interest to consumers;

43. Calls on the Commission and the Member States to adopt specific measures on the use and promotion of cloud computing in relation to open access and open educational resources;

**Intellectual property, civil law etc. and the cloud**

44. Urges the Commission to take action to further harmonise laws across the Member States in order to avoid jurisdicitional confusion and fragmentation and to ensure transparency in the digital single market;

45. Calls on the Commission to review other EU legislation to address gaps related to cloud computing; calls, in particular, for clarification of the intellectual property rights regime and for a review of the Unfair Commercial Practices Directive, the Unfair Contract Terms Directive and the E-Commerce Directive, which are the most relevant pieces of EU legislation that apply to cloud computing;

46. Calls on the Commission to establish a clear legal framework in the field of copyright content in the cloud, especially with regard to licensing regulations;

47. Acknowledges that the advent of the storage of copyright works by cloud computing services should not compromise the right of European right holders to receive fair compensation for the use of their work, but questions whether these services can be considered to be on par with traditional and digital recording and storage media and equipment;

48. Calls on the Commission to investigate the different types of cloud computing services, how the cloud storage of copyrighted works affects the royalties systems and, more specifically, the ways in which private copying levies that are relevant for certain types of cloud computing services are imposed;

49. Calls on the Commission to promote the development, jointly with stakeholders, of decentralised services based on free and open-source software that would help harmonise practices across cloud providers and enable EU citizens to regain control over their personal data and communication, for example by means of point-to-point encryption;

50. Stresses that, owing to uncertainties regarding applicable law and jurisdiction, contracts are the main tools for establishing relations between cloud providers and their customers, and that there is therefore a clear need for common EU guidelines in that field;

51. Calls on the Commission to work together with the Member States to develop EU best practice models for contracts, or ‘model contracts’, that will ensure complete transparency by providing all terms and conditions in a very clear format;

52. Calls on the Commission to develop, together with stakeholders, voluntary certification schemes for provider security systems which would help to harmonise practices across
cloud providers and which would make clients more aware of what they should expect from cloud service providers;

53. Stresses that, owing to jurisdiction problems, EU consumers are in practice unlikely to be able to seek redress from cloud services providers in other jurisdictions; calls, therefore, on the Commission to provide adequate means of redress in the consumer services area, since there is a strong imbalance of power between consumers and providers of cloud computing;

54. Calls on the Commission to ensure the speedy implementation of Alternative Dispute Resolution and Online Dispute Resolution and to make sure that consumers are equipped with adequate means of collective redress against security and privacy breaches as well as against illegal contract provisions for cloud services;

55. Regrets the current lack of effective remedies for users in case of breach of contract;

56. Calls for systematic consumer information regarding the processing activities of personal data to be included in contract proposals, as well as for users’ consent to be compulsory before the terms of a contract may be changed;

57. Calls on the Commission, within the framework of its expert group discussions, to require cloud providers to include in contracts certain key clauses guaranteeing the quality of the service, such as obligations to update software and hardware where necessary, to determine what happens if data is lost, and to determine the time it would take to resolve a problem, or how rapidly the cloud service could take down offending materials, should the cloud user make such a request;

58. Recalls that where a cloud provider uses the data for a purpose other than that agreed on in the service agreement, or communicates data or uses it in a way contrary to the terms of the contract, he should be considered data controller and should be held liable for the infringements and breaches incurred;

59. Stresses that cloud services agreements must set out, in a clear and transparent manner, the duties and rights of the parties concerning data processing activities by cloud providers; points out that the contractual arrangements shall not entail a waiver of the safeguards, rights and protections afforded by Union data protection law; urges the Commission to come forward with proposals to restore the balance between cloud service providers and their customers as regards the terms and conditions used by cloud services, including provisions to:

- ensure protection against arbitrary cancellation of services and deletion of data;

- guarantee a reasonable chance for customers to recover stored data in cases of cancellation of service and/or removal of data;

- provide clear guidelines for cloud providers to facilitate the easy migration of their customers to other services;

60. Highlights that the role of the cloud service provider under current Union legislation needs
to be determined on a case-by-case basis, as providers can be both data processors and data controllers; calls for the terms and conditions for all users to be improved through the development of international best practice models for contracts and through the clarification of where the service provider stores data and under which area of law within the EU;

61. Highlights that particular attention must be given to situations in which the imbalance in the contractual situation between the customer and the cloud provider leads the customer to enter into contractual arrangements imposing standard services and a contract to be signed in which the provider defines the purposes, conditions and means of the processing; stresses that, in such circumstances, the cloud provider should be considered data controller and become jointly liable with the customer;

**Data protection, fundamental rights, law enforcement and the cloud**

62. Takes the view that access to a safe internet is a fundamental right of every citizen and that cloud computing will continue to play an important role in this aspect; reiterates, therefore, its call on the Commission and the Council unequivocally to recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights;

63. Reiterates that, as a general rule, the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context;

64. Stresses that Union data protection law, since it is technologically neutral, already now fully applies to cloud computing services operating in the EU and must, therefore, be fully respected; stresses that the opinion of the Working Party of the Article 29 (WP29) on Cloud Computing should be taken into account as it provides clear guidance for the application of Union data protection law principles and rules to cloud services, such as the concepts of controller/processor, purpose limitation and proportionality, integrity and data security, the use of subcontractors, allocation of responsibilities, data breaches and international transfers; underlines the need to close any gaps in the protection as regards cloud computing in the ongoing review of the Union data protection legal framework based on further guidance by the European Data Protection Supervisor and the WP29;

65. Recalls its serious concern about the recent unveiling of US National Security Agency surveillance programmes, and of similar programmes operated by intelligence agencies in various Member States, in the recognition that, should the information available up to now be confirmed, these programmes entail a serious violation of the fundamental right of EU citizens and residents to privacy and data protection, as well as of the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, and the freedom to conduct business;

66. Reiterates its serious concerns about the compulsory direct disclosure of EU personal data and information, processed under cloud agreements, to third country authorities by cloud

---

1 Particularly in the case of consumers and SMEs using cloud services.
providers subject to third country laws or using storage servers located in third countries, and about direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

67. Regrets that such access is usually attained by means of direct enforcement by third countries authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;

68. Stresses that such practices raise questions of trust as regards non-EU cloud and online service providers, and as regards third countries that do not rely on international instruments for legal and judicial cooperation;

69. Expects the Commission and the Council to take such measures as are necessary to solve this situation and to ensure the respect of the fundamental rights of EU citizens;

70. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches;

71. Stresses that cloud services that fall under third country jurisdiction should provide users located in the EU with a clear and distinguishable warning of the possibility that their personal data may be subject to intelligence and law enforcement surveillance by third country authorities under secret orders or injunctions, followed, where applicable, by a request for the data subject’s explicit consent for the processing of personal data;

72. Urges the Commission, when negotiating international agreements that involve the processing of personal data, to take particular note of the risks and challenges that cloud computing poses to fundamental rights, in particular – but not exclusively – the right to private life and to the protection of personal data, as laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; urges, furthermore, the Commission to take note of the negotiating partner’s domestic rules governing the access of law enforcement and intelligence agencies to personal data processed through cloud computing service, in particular by demanding that such access for law enforcement and intelligence authorities only be granted with full respect for the due process of law and on an unambiguous legal basis, as well as the requirement that the exact conditions of access, the purpose of gaining such access, the security measures put in place when handing over data and the rights of the individual, as well as the rules for supervision and for an effective redress mechanism, be specified;

73. Stresses its serious concerns about the work carried out within the Council of Europe’s Cybercrime Convention Committee with a view to developing an additional protocol on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 on ‘trans-border access to stored computer data with consent or where publicly available’ in order to ‘facilitate its effective use and implementation in the light of legal, policy and technological developments’; calls on the Commission and the Member States, in view of

---

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp
the forthcoming consideration by the Committee of Ministers of the Council of Europe, to ensure the compatibility of the provision of Article 32 of the Convention on Cybercrime, and its interpretation in the Member States, with fundamental rights, including data protection and, in particular, the provisions on trans-border flows of personal data, as enshrined in the EU Charter of Fundamental Rights, the EU data protection acquis, the European Convention of Human Rights and the Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing (‘Convention 108’), which are legally binding upon the Member States; calls on the Commission and the Member States to reject firmly any measure that would put the application of these rights at risk; is alarmed by the fact that should such an additional protocol be endorsed, its implementation could result in unfettered remote access by law enforcement authorities on servers and computer systems located in other jurisdictions, without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process;

74. Underlines that particular attention must be paid to SMEs which increasingly rely on cloud computing technology when processing personal data, and which may not always have the resources or the expertise to address security challenges adequately;

75. Stresses that the qualification of data controller or processor needs to be reflected in an appropriate manner by the actual level of control it has over the means of processing, in order that the responsibilities for the protection of personal data with the use of cloud computing are clearly allocated;

76. Stresses that all the principles laid down in EU data protection law, such as fairness and lawfulness, purpose limitation, proportionality, accuracy and limited data retention periods, must be taken fully into account by cloud computing service providers when processing personal data;

77. Underlines the importance of having effective, proportionate and dissuasive administrative sanctions that may be imposed on cloud computing services that do not comply with EU data protection standards;

78. Stresses that, in order to define the most appropriate safeguards to implement, the data protection impact of each cloud computing service must be assessed on an ad hoc basis;

79. Stresses that a European cloud service provider should always act in conformity with EU data protection law, even if this conflicts with instructions by a client or controller established in a third country, or when the data subjects concerned are (solely) residents of third countries;

80. Stresses the need to address the challenges raised by cloud computing at an international level, in particular as regards government intelligence surveillance and necessary safeguards;

81. Stresses that EU citizens subject to intelligence surveillance by third country authorities should benefit from at least the same safeguards and remedies as are available to citizens of the third country concerned;
82. Regrets the approach in the Commission’s communication whereby it fails to mention the risks and challenges attached to cloud computing, and urges the Commission to continue its work on cloud computing by developing a more holistic communication on cloud computing that takes into account the interests of all stakeholders, and that contains, alongside a standard reference to the protection of fundamental rights and compliance with data protection requirements, at least the following:

- guidelines to ensure full compliance with the EU’s fundamental rights and data protection obligations;
- limitative conditions under which cloud data may or may not be accessed for law enforcement purposes, in compliance with the EU Charter of Fundamental Rights and with EU law;
- safeguards against illegal access by foreign and domestic entities, for instance by amending procurement requirements and applying Council Regulation (EC) No 2271/96\(^1\) to counteract foreign laws that may result in massive illegal transfers of the cloud data of EU citizens and residents;
- proposals on how to define the ‘transfer’ of personal data and on how to update standard contractual clauses that are tailored to the cloud environment, as ‘cloud computing’ often involves massive flows of data from cloud clients to cloud providers’ servers and data centres, involving many different parties and crossing borders between EU and non-EU countries;

83. Calls on the Commission to explore the adequacy of a review of the EU-US Safe Harbour Agreement, in order to adapt it to technological developments, especially with regard to aspects linked to cloud computing;

84. Instructs its President to forward this resolution to the Council and the Commission.

EXPLANATORY STATEMENT

All over the world companies are increasingly realising the gain of productivity they can achieve by easily accessing the best performing business applications and/or drastically boosting their infrastructure resources at affordable costs. In this regard, estimates from the European Commission calculate that by 2014 cloud revenue can reach 148.8 billion and that 60% of all server workloads will be virtualized.

The economic and commercial prospects of the cloud are indeed promising and there is consequently a business case for its development, which in practical terms means that with or without Europe’s intervention cloud computing will continue to develop in one way or another.

In the past the Union institutions have taken some welcome but small steps, such as when the European Commission published the 2010 Communication ‘Towards interoperability for European public services’ and the ENISA report on the main security issues related to the cloud.

Consequently the presentation of the Commission’s Strategy for cloud computing is welcomed. However, we must not forget that when developing any strategic framework of action, and in particular this future cloud computing strategy, we have to try and be as horizontal as possible without taking for granted any circumstances that might not seem to directly affect its development.

Accordingly, infrastructure policies are crucial: strong fixed and mobile communication networks are prerequisite in order to grasp the full potential of the cloud and consequently the rapporteur regrets that the Connecting Europe Facilities communication and more specifically the proposed regulation on Guidelines for Trans European Telecommunications Networks, which are welcome steps that have the capacity of boosting much needed investment into broadband networks in Europe, will not be able to perform adequately if they are not provided with proper financial resources.

On the other hand, due to the strong commercial nature of cloud systems, the future strategy must address a wide number of aspects that range from technological issues related to cloud systems development, management and elastic scalability, without forgetting the flexibility that any ICT development needs in order not to hamper innovation when addressing standardisation matters, to non-technical issues such as legal aspects related to data privacy and security that pose a major obstacle towards wide uptake of cloud infrastructures.

With regards to these last aspects: the proposed data protection regulatory framework now being debated in Parliament is welcomed due to the urgent need -as demanded in Parliament’s own initiative report on a Digital Agenda for Europe- to adapt the 1995 regime to the digital society. It is however crucial that the final outcome does not impede the development of new and state of the art cloud services, and promote its uptake. In this respect it is important that the data protection framework establishes a clear delimitation of the roles and responsibilities of the controller and processor-. Furthermore, the recently proposed directive on network and information security is also welcomed.
These are crucial aspects; we must not forget that the Cloud, due to its outsourced nature, adds an extra feature of insecurity to our perception of security and data protection. In this respect, the World Economic Forum has noted that 90 percent of suppliers and users of cloud services think that risks to privacy are a ‘very serious’ impediment to wide adoption of cloud computing.

In addition, Europe should stimulate research and technological development in the area of cloud computing. Europe’s excellent background in key research and development aspects, such as GRIDs and Service Oriented Architectures, can give the EU a competitive advantage. Consequently, Horizon 2020 should play a major role.

With regards to the concrete action lines of the Commission’s communication, the following can be underlined:

1. Cutting through the jungle of standards:

   This is a fundamental aspect. At the end of the day users must be able to change their cloud provider in a fast and secure manner. In other words: complete portability, a high degree of interoperability and open specifications are essential. Efforts must be invested in eliminating the lock-in of customers. Consequently the mapping of existing standards entrusted to ETSI is, at this stage, a good start. But it must be guaranteed that the process is as open and transparent as possible. Also the Rapporteur believes that cloud standards are by definition of a global nature, and no region of the World can go about globally-applicable standards in isolation. Europe must focus on maximizing the opportunities for its SMEs and consumers in the global market. We need standards that have the capacity of becoming worldwide standards.

   In addition ENISA can also play an important role and the Rapporteur agrees that it should assist the development of EU-wide voluntary certification schemes for cloud computing, meeting the deadline set in the Communication of establishing a list of such schemes by 2014.

2. Safe and Fair Contract Terms and Conditions.

   In spite that the Common European Sales Law deals with ‘digital content’ contracts for consumers and small firms, an instrument might be needed to deal with other aspects, specially data location and transfer -utmost account should be taken of the Article 29 Working Party opinions-, and common contractual terminology.

   The underlying principle in this key action should nevertheless be that the cloud offers different services and business models ’One size does not fit all’. Consequently, when establishing ‘safe and fair contract terms’, it is clear that contracts between business and consumers are of a substantially different nature than those between businesses. Likewise, challenges public administrations face when embracing cloud services differ greatly from those of regular consumers. In other words, different clouds respond to different needs and challenges. Contract law should however be able to accommodate all aspects,
3. Promoting Common Public Sector Leadership through a European Cloud Partnership.

The Rapporteur believes that the public sector, including the Commission itself, must take the lead. Not just because of the gain of productivity that can be achieved by easily accessing the best performing applications and technologies at affordable costs, but because in addition citizens would be able to benefit from more efficient and innovative public services. By way of an example, the prospects with regards e-health, education and transport services are enormous.

The cloud partnership is a welcome tool, however we must move up a gear. There is an urgent need for a high degree of coordination and to avoid the serious risk that in a near future the public sector market will be even more fragmented, as with the eID, where no real coordination took place when Member States starting to develop their different national systems.

The Rapporteur believes that in order to fully reap the benefits of cloud technology and maximise use of resources, the public sector should be the motor due to its size and presence in almost every sector across Europe. We must insist that public administrations undergo their ‘digital switchover’, and start, in a proactive manner, coordinating their initiatives immediately.

Likewise European institutions must also without further delay start evaluating the possibilities and challenges that cloud technology has to offer them. Due to the many complex questions that must be answered (budgetary structural constraints, possible lack of market development, clarification of internal security aspects etc), the Institutions must elaborate a strategy for the European institutions.

Cloud computing and the Digital Single Market

The full development of cloud computing has a strategic importance in the completion of the digital single market. In that sense the cloud strategy touches upon many aspects that affect the need for higher convergence, and eventually, harmonisation, in order to eliminate all the existing barriers in for example: broadband deployment, spectrum allocation, consumer protection, IPR, data protection, specific product regulations, and payment transactions.

Consequently, the development of the Cloud in Europe has an extraordinary potential of becoming a powerful accelerator to the completion of the digital single market.
23.9.2013

OPINION OF THE COMMITTEE ON LEGAL AFFAIRS*

for the Committee on Industry, Research and Energy

on unleashing the potential of cloud computing in Europe
(2013/2063(INI))

Rapporteur (*): Lidia Joanna Geringer de Oedenberg

(*) Associated committee – Rule 50 of the Rules of Procedure

SHORT JUSTIFICATION

Your rapporteur welcomes the Commission’s Communication, but considers it appropriate, in order to ensure that upcoming legislation will be operative, to call on the Commission to make certain provisions more stringent and to look at the problem together with all other legislation that may assist in eliminating barriers and unlocking its full potential.

Cloud computing has a huge potential and should provide benefits for business, citizens and the public sector but, as a new model of networked computing, poses some legal and contractual risks. Among other concerns, such as security or supplier lock-in, there is major concern among both service providers and users regarding the lack of standardisation which would be required for a single market across Europe, the diversity of relevant legislation across Europe, currently unclear contract provisions and the lack of clear rules on intellectual property rights (IPR).

Recent research shows that 48 % of managers in both the private and the public sectors are aware that the implementation of cloud computing can speed up and facilitate their work. More than half of them have not, however, introduced any procedures to minimise business risks such as identity theft.

The biggest threat in the cloud are so called ‘insiders’, those working in the establishments

1 The size of the global market is expected to rise steeply, from USD 21.5 billion in 2010 to USD 73 billion in 2015; cloud computing is expected to boost GDP by between 1 and 2 % in Europe’s five biggest economies; it is expected to add 11.3 million jobs to the worldwide economy by 2014 (data taken from International Data Corporation (IDC) worldwide and regional IT cloud services forecast for 2011-2015 and Federico Etro, The Economics of Cloud Computing, 2011).
providing cloud services, who have access to customer data, followed by other tenants of the service provider in the cloud, notably in case of a breakdown of isolation mechanisms.

The EU digital single market remains fragmented due to differing legal regimes among the Member States, and when it comes to IPR only a limited level of harmonisation has taken place in the wake of the Copyright Directive. Action must therefore be targeted to address the issue of cloud services that depend on a uniform IPR regime to cross borders. The proposals on collective rights management and the private copy levy must take into account the development of new technologies, in particular cloud computing services, and clarify the rules for securing IPR in a digital environment.

According to the recent Commission public consultation on cloud computing, the legal regime was unclear to respondents in 90% of cases. There is general confusion among stakeholders regarding rights and responsibilities in cross-border cloud computing situations, in particular with regard to matters relating to liability and jurisdiction. Coupled with the fragmentation of the internal market, this calls for further harmonisation of laws across the Member States, in particular by eliminating gaps and weaknesses in applicable EU legislation, notably the Unfair Commercial Practices Directive and the Unfair Contract Terms Directive in terms of consumer protection, and the E-Commerce Directive when it comes to exemptions from private copy levies.

Consumers and SMEs who want to make use of public clouds are often faced with ‘take-it-or-leave-it’ contracts, most often tick-box agreements. The Commission should therefore, together with the Member States, consider introducing clearer rules or model contracts. There is a need for guidelines and standardised model contract schemes setting out the key terms and conditions that are important to users, while increasing transparency.

Cloud users should furthermore be able to evaluate any cloud service offer on the basis of standardised procedures regarding the security and warranties provided by the service, so-called Service Level Agreements (SLA). A voluntary certification scheme enabling users to evaluate and compare, in a simple manner, the level of conformity to standards, interoperability and the security systems of cloud services should therefore be implemented at European level, taking into account the differences encountered in these respects at the three different levels of service: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The first case concerns security equipment, supply lines, data, etc. In the second case, responsibility for security largely lies with the client, who should adequately protect their data. In the third, responsibility lies with the supplier.

The provision of adequate means of redress for users when it comes to cloud computing service providers is necessary, in particular in the consumer service area. Owing to jurisdictional problems, European consumers are currently in practice unlikely to be able to seek redress from the service provider. The Commission should therefore speed up the implementation of Alternative and Online Dispute Resolution and forms of collective redress in order to facilitate the solving of conflicts in this area faced by users, without putting too much additional pressure on national courts.
SUGGESTIONS

The Committee on Legal Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Urges the Commission to take action to further harmonise laws across the Member States in order to avoid jurisdictional confusion and fragmentation and to ensure transparency in the digital single market;

2. Notes the urgent need for a clear and uniform European legislation for cloud computing to ensure a competitive European environment, increasing innovation and boosting growth;

3. Calls on the Commission to review other EU legislation to address gaps related to cloud computing; calls, in particular, for clarification of the intellectual property rights regime and for a review of the Unfair Commercial Practices Directive, the Unfair Contract Terms Directive and the E-Commerce Directive, which are the most relevant pieces of EU legislation that apply to cloud computing;

4. Notes the importance of considering the legal framework for cloud computing with the current review of the EU Data Protection rules, ensuring clear rules with regard to the processing of personal data; notes the importance of free movement of such data in a secure legal framework, resulting in greater data interoperability and, more importantly, greater confidence for users;

5. Points out that the right to privacy is a fundamental right and, therefore, that new cloud computing services must be developed in a manner that ensures a high level of personal data protection in line with the fundamental rights and basic freedoms of the Union;

6. Calls for the establishment of a European seal to show, where the personal data of European citizens is transferred to third countries, that the businesses and third countries involved comply with EU law and uphold the fundamental right to privacy;

7. Calls on the Commission to take the necessary steps to develop European cloud computing that upholds the principles and values of the EU, and to foster cooperation between private operators for the same purpose;

8. Calls on the Commission to establish a clear legal framework in the field of copyright content in the cloud, especially with regard to licensing regulations;

9. Acknowledges that the advent of the storage of copyright works by cloud computing services should not compromise the right of European right holders to receive fair compensation for the use of their work, but wonders whether these services can be considered to be the same as traditional and digital recording and storage media and equipment;

10. Calls on the Commission to look into the different types of cloud computing services, how the cloud storage of copyrighted works affects the royalties systems and, more
specifically, the ways in which private copying levies that are relevant for certain types of cloud computing services are imposed;

11. Stresses that, owing to uncertainties regarding applicable law and jurisdiction, contracts are the main tools for establishing relations between cloud providers and their customers, and that there is therefore a clear need for common European guidelines in that field;

12. Calls on the Commission to work together with the Member States to develop European best practice models for contracts, or ‘model contracts’, that will ensure complete transparency by providing all terms and conditions in a very clear format;

13. Highlights the importance of cloud computing services for SMEs, in particular those established in remote or outermost areas or facing economic difficulties, and calls on the Commission to consider an appropriate framework to allow SMEs to increase their growth and productivity, as SMEs can benefit from reduced upfront costs and better access to analytics tools;

14. Calls on the Commission to develop, together with stakeholders, voluntary certification schemes for provider security systems which would help to harmonise practices across cloud providers and which would make clients more aware of what they should expect from cloud service providers;

15. Calls on the Commission to promote the development, jointly with stakeholders, of decentralised services based on free and open-source software (FOSS) that would help harmonise practices across cloud providers and enable European citizens to regain control over their personal data and communication, for example by means of point-to-point encryption;

16. Stresses that, owing to jurisdiction problems, European consumers are in practice unlikely to be able to seek redress from cloud services providers in other jurisdictions; calls therefore, on the Commission to provide adequate means for redress in the consumer services area, since there is a strong imbalance of power between consumers and providers of cloud computing;

17. Calls on the Commission to ensure a speedy implementation of Alternative Dispute Resolution and Online Dispute Resolution and to make sure that consumers are equipped with adequate means of collective redress against security and privacy breaches as well as against illegal contract provisions for cloud services.
### RESULT OF FINAL VOTE IN COMMITTEE

<table>
<thead>
<tr>
<th>Date adopted</th>
<th>17.9.2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Result of final vote</strong></td>
<td></td>
</tr>
<tr>
<td>+:</td>
<td>23</td>
</tr>
<tr>
<td>-:</td>
<td>0</td>
</tr>
<tr>
<td>0:</td>
<td>0</td>
</tr>
<tr>
<td><strong>Substitute(s) present for the final vote</strong></td>
<td>Eva Lichtenberger, Angelika Niebler, József Szájer, Axel Voss</td>
</tr>
<tr>
<td><strong>Substitute(s) under Rule 187(2) present for the final vote</strong></td>
<td>Olle Schmidt</td>
</tr>
</tbody>
</table>
19.9.2013

OPINION OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS*

for the Committee on Industry, Research and Energy

on unleashing the potential of cloud computing in Europe
(2013/2063(INI))

Rapporteur(*): Judith Sargentini

(*) Associated committee – Rule 50 of the Rules of Procedure

SUGGESTIONS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Reiterates that alongside the potential and benefits of ‘cloud computing’ for businesses, citizens, the public sector and the environment, in particular in terms of cost reduction, it entails significant risks and challenges, particularly for fundamental rights (including privacy and data protection) and by increasing impact in case of disruptions, whether they are caused by malfunction, malpractice, criminal action or hostile action by another country;

2. Takes the view that access to a safe internet is a fundamental right of every citizen and that ‘cloud computing’ will continue to play an important role in this aspect; reiterates, therefore, its call on the Commission and the Council unequivocally to recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights;

3. Reiterates that, as a general rule, the level of data protection in a ‘cloud computing’ environment must not be inferior to that required in any other data-processing context;

4. Stresses that Union data protection law, since it is technologically neutral, already now fully applies to cloud computing services operating in the EU and must, therefore, be fully respected; stresses that the opinion of the Working Party of the Article 29 (WP29) on
Cloud Computing\(^1\) should be taken into account as it provides clear guidance for the application of Union data protection law principles and rules to cloud services, such as the concepts of controller/processor, purpose limitation and proportionality, integrity and data security, the use of subcontractors, allocation of responsibilities, data breaches and international transfers; underlines the need to close any gaps in the protection as regards cloud computing in the ongoing review of the Union data protection legal framework based on further guidance by the European Data Protection Supervisor (EDPS) and the WP29; considers that not all sensitive information is personal data, and therefore urges the Commission to propose guidelines to protect non-personal sensitive data in a cloud context, particularly in the case of government data and of data from organisations such as banks, insurance companies, pension funds, schools and hospitals;

5. Recalls that where a cloud provider uses the data for a purpose other than that agreed on in the service agreement, or communicates data or uses it in a way contrary to the terms of the contract, he should be considered data controller and should be held liable for the infringements and breaches incurred;

6. Stresses that cloud services agreements must set out, in a clear and transparent manner, the duties and rights of the parties concerning data processing activities by cloud providers; the contractual arrangements shall not entail a waiver of the safeguards, rights and protections afforded by Union data protection law; urges the Commission to come forward with proposals to restore the balance between cloud service providers and their customers as regards the terms and conditions used by cloud services, including provisions;

– ensuring protection against arbitrary cancellation of services and deletion of data;
– guaranteeing a reasonable chance for customer to recover stored data in case of cancellation of service and/or removal of data;
– providing clear guidelines for cloud providers to facilitate the easy migration of their customers to other services;

7. Highlights that the role of the cloud service provider under current Union legislation needs to be determined on a case-by-case basis, as providers can be both data processors and data controllers; calls for the terms and conditions for all users to be improved through the development of international best practice models for contracts and through the clarification of where the service provider stores data and under which area of law within the EU;

8. Highlights that particular attention must be given to situations in which the imbalance in the contractual situation between the customer and the cloud provider leads the customer to enter into contractual arrangements imposing standard services and a contract to be signed in which the provider defines the purposes, conditions and means of the processing\(^2\); stresses that, in such circumstances, the cloud provider should be considered

---


\(^2\) Particularly in the case of consumers and SMEs using cloud services.
‘data controller’ and become jointly liable with the customer;

9. Stresses that the use of cloud services by public authorities, including by law enforcement authorities and EU institutions, requires special consideration and coordination between the Member States; recalls that data integrity and security must be guaranteed and unauthorised access, including by foreign governments and their intelligence services without a legal basis under Union or Member State law, prevented; stresses that this also applies to the specific processing activities of certain essential non-governmental services, in particular the processing of specific categories of personal data, such as banks, insurance companies, pension funds, schools and hospitals; urges the Commission to issue guidelines for these organisations to follow when using cloud services to process, transmit or store their data, including the adoption of open standards to prevent vendor lock-in, and a preference for open source software to improve transparency and accountability of the services used; stresses, furthermore, that all of the aforementioned is of particular importance if data is being transferred (outside the European Union between different jurisdictions); takes the view, therefore, that public authorities, as well as non-governmental services and the private sector, should, as far as possible, rely on EU cloud providers when processing sensitive data and information until satisfactory global rules on data protection have been introduced, ensuring the security of sensitive data, and of data bases, held by public entities;

10. Recalls its serious concern about the recent unveiling of US National Security Agency surveillance programmes, and of similar programmes operated by intelligence agencies in various Member States, in the recognition that, should the information available up to now be confirmed, these programmes entail a serious violation of the fundamental right of EU citizens and residents to privacy and data protection, as well as of the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, and the freedom to conduct business;

11. Reiterates its serious concerns about the compulsory direct disclosure of EU personal data and information, processed under cloud agreements, to third country authorities by cloud providers subject to third country laws or using storage servers located in third countries, and about direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

12. Regrets that such access is usually attained by means of direct enforcement by third countries authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;

13. Stresses that such practices raise questions of trust as regards non-EU cloud and online service providers, and as regards third countries that do not rely on international instruments for legal and judicial cooperation;

14. Expects the Commission and the Council to take such measures as are necessary to solve this situation and to ensure the respect of the fundamental rights of EU citizens;

15. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches;
16. Stresses that cloud services that fall under third country jurisdiction should provide users located in the EU with a clear and distinguishable warning of the possibility that their personal data may be subject to intelligence and law enforcement surveillance by third country authorities under secret orders or injunctions, followed, where applicable, by a request for the data subject’s explicit consent for the processing of personal data;

17. Urges the Commission, when negotiating international agreements that involve the processing of personal data, to take particular note of the risks and challenges that cloud computing poses to fundamental rights, in particular – but not exclusively – the right to private life and to the protection of personal data, as laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; urges, furthermore, the Commission to take note of the negotiating partner’s domestic rules governing the access of law enforcement and intelligence agencies to personal data processed through cloud computing service, in particular by demanding that such access for law enforcement and intelligence authorities only be granted with full respect for the due process of law and on an unambiguous legal basis, as well as the requirement that the exact conditions of access, the purpose of gaining such access, the security measures put in place when handing over data and the rights of the individual, as well as the rules for supervision and for an effective redress mechanism, be specified;

18. Stresses its serious concerns about the work carried out within the Council of Europe’s Cybercrime Convention Committee with a view to developing an additional protocol on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 on ‘trans-border access to stored computer data with consent or where publicly available’ in order to ‘facilitate its effective use and implementation in the light of legal, policy and technological developments’; calls on the Commission and the Member States, in view of the forthcoming consideration by the Committee of Ministers of the Council of Europe, to ensure the compatibility of the provision of Article 32 of the Convention on Cybercrime, and its interpretation in the Member States, with fundamental rights, including data protection and, in particular, the provisions on trans-border flows of personal data, as enshrined in the EU Charter of Fundamental Rights, the EU data protection acquis, the European Convention of Human Rights and the Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing (‘Convention 108’), which are legally binding upon the Member States; calls on the Commission and the Member States to reject firmly any measure that would put the application of these rights at risk; is alarmed by the fact that should such an additional protocol be endorsed, its implementation could result in unfettered remote access by law enforcement authorities on servers and computer systems located in other jurisdictions, without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process;

19. Underlines that particular attention must be paid to small and medium-sized enterprises which increasingly rely on ‘cloud computing’ technology when processing personal data, and which may not always have the resources or the expertise to address security challenges adequately;

http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp
20. Stresses that the qualification of data controller or processor needs to be appropriately reflected by the actual level of control it has over the means of processing, in order that the responsibilities for the protection of personal data with the use of cloud computing are clearly allocated;

21. Underlines the importance of digital literacy among all citizens, and urges the Member States to develop concepts of how to promote the safe use of internet services, including cloud computing;

22. Stresses that all the principles laid down in EU data protection law, such as fairness and lawfulness, purpose limitation, proportionality, accuracy and limited data retention periods, must be taken fully into account by cloud computing service providers when processing personal data;

23. Underlines the importance of having effective, proportionate and dissuasive administrative sanctions that may be imposed on ‘cloud computing’ services that do not comply with EU data protection standards;

24. Stresses that, in order to define the most appropriate safeguards to implement, the data protection impact of each cloud computing service must be assessed on an ad hoc basis;

25. Stresses that a European cloud service provider should always act in conformity with EU data protection law, even if this conflicts with instructions by a client or controller established in a third country, or when the data subjects concerned are (solely) residents of third countries;

26. Stresses the need to address the challenges raised by cloud computing at an international level, in particular as regards government intelligence surveillance and necessary safeguards;

27. Stresses that EU citizens subject to intelligence surveillance by third country authorities should benefit from at least the same safeguards and remedies as are available to citizens of the third country concerned;

28. Regrets the approach in the Commission’s communication whereby it fails to mention the risks and challenges attached to cloud computing, and urges the Commission to continue its work on cloud computing by developing a more holistic communication on cloud computing that takes into account the interests of all stakeholders, and that contains, alongside a standard reference to the protection of fundamental rights and compliance with data protection requirements, at least the following:

- guidelines to ensure full compliance with the EU’s fundamental rights and data protection obligations;

- limitative conditions under which cloud data may or may not be accessed for law enforcement purposes, in compliance with the EU Charter of Fundamental Rights and with EU law;

- safeguards against illegal access by foreign and domestic entities, for instance by
amending procurement requirements and applying Council Regulation (EC) No 2271/96\(^1\) to counteract foreign laws that may result in massive illegal transfers of the cloud data of EU citizens and residents;

– proposals to guarantee net neutrality and service neutrality in order to prevent commercially motivated discrimination against specific cloud services;

– proposals to guarantee that access to legal content will not be harmed by actions against illegal content;

– proposals on how to define the ‘transfer’ of personal data and on how to update standard contractual clauses that are tailored to the cloud environment, as ‘cloud computing’ often involves massive flows of data from cloud clients to cloud providers’ servers and data centres, involving many different parties and crossing borders between EU and non-EU countries;

– measures to address the existing imbalance in the cloud services market between service providers and most of the users of their services;

– measures promoting research on how current EU legislative frameworks and international agreements fit particular cloud computing services scenarios, measuring both the economic and the environmental impact of cloud computing, as few studies have yet been made on these aspects.

RESULT OF FINAL VOTE IN COMMITTEE

<table>
<thead>
<tr>
<th>Date adopted</th>
<th>18.9.2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result of final vote</td>
<td></td>
</tr>
<tr>
<td>+:</td>
<td>43</td>
</tr>
<tr>
<td>-:</td>
<td>3</td>
</tr>
<tr>
<td>0:</td>
<td>1</td>
</tr>
<tr>
<td>Members present for the final vote</td>
<td></td>
</tr>
<tr>
<td>Substitute(s) present for the final vote</td>
<td></td>
</tr>
<tr>
<td>Alexander Alvaro, Cornelis de Jong, Mariya Gabriel, Marian-Jean Marinescu, Salvador Sedó i Alabart, Janusz Wojciechowski</td>
<td></td>
</tr>
<tr>
<td>Substitute(s) under Rule 187(2) present for the final vote</td>
<td></td>
</tr>
<tr>
<td>Nuno Teixeira</td>
<td></td>
</tr>
</tbody>
</table>
OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Industry, Research and Energy

on unleashing the potential of cloud computing in Europe (2013/2063(INI))

Rapporteur: Sabine Verheyen

SUGGESTIONS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Industry, Research and Energy as the committee responsible, to incorporate the following suggestions into its motion for a resolution:


– having regard to Directive 95/46/EC of Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data3;


---

1 OJ L 304, 22.11.2011, p. 64.
5 OJ L 304, 22.11.2011, p. 64.
society,

A. whereas the Digital Single Market is a key factor in achieving the targets of the Europe 2020 strategy providing a significant boost in attaining the objectives of the Single Market Act and responding to the economic and financial crisis affecting the EU;

B. whereas EU-wide broadband provision, universal and equal access to Internet services for all citizens, and a guarantee of network neutrality are the essential prerequisites for the development of a European cloud system;

C. whereas the Connecting Europe Facility is intended, among other things, to increase broadband uptake in Europe;

D. whereas the benefits of cloud technology lie in cost savings, the creation of jobs and new business opportunities, flexibility (adaptation of data-storing capacity according to needs), mobility (of workers, enterprises and citizens), enhanced competitiveness through potential economies of scale, and the innovation potential of new services, eventually leading to economic benefits, particularly for SMEs (small and medium-sized enterprises).

E. whereas cloud computing should stimulate the integration of SMEs thanks to the reduction of market entry barriers (e.g. decreases in IT infrastructure costs);

F. whereas it is essential for the European cloud system that European legal standards on data protection be guaranteed;

G. whereas the development of cloud computing should help to promote creativity for the benefit of both rights-holders and users; whereas, furthermore, distortions in the Single Market should be avoided in the process and consumer and business confidence in cloud computing should be boosted;

1. Is aware of the major economic, social and cultural potential of cloud computing and welcomes the Commission’s initiative of launching a comprehensive cloud strategy, thereby addressing the attendant legal issues;

2. Emphasises the vast possibilities in having access to data from any device connected to the Internet;

3. Underlines that the longer-term strategic dimension of cloud computing should be fully acknowledged and supported as an opportunity to relaunch the European economy (incorporating research and development, and the use of cloud technology in industry, for instance);

4. Insists, however, on the problems related to the use of cloud computing, by helping enterprises to identify, choose and put into practice cloud solutions adapted to their needs and by supporting the development of the access to high-speed broadband Internet;

5. Underlines that fears related to the loss of control of data by the user and the dependence on external providers generated by data outsourcing may undermine users’ confidence in

---

1 OJ L 167, 22.06.2001, p. 10.
cloud computing; insists, therefore, on the fact that data protection must be thoroughly ensured in order to create and maintain both public and private users’ confidence in cloud computing;

6. Underlines, in particular, the need to ensure the adequate protection of sensitive data, such as, for instance, health-related data;

7. Considers that securing data portability, integrity, confidentiality, availability, reversibility and interoperability of services, platforms, and infrastructures forms a great challenge, given that all of these are essential for the stimulation of innovation and competition; calls on the Commission to ensure that cloud providers do not lock-in cloud users to their own services, and that users retain full control over their data and can switch to another service upon request, without undue delay, free of charge and without the loss of data; considers that overcoming these challenges is essential for building consumer, business and public sector confidence in cloud-based services and unleashing their full potential.

8. Points out that Europe must take advantage of the fact that this technology is at a relatively early stage and work towards developing it, in order to benefit from the economies of scale which it is expected to offer, thereby revitalising its economy, particularly in the ICT sector;

9. Highlights the importance of cloud computing for SMEs – particularly those established in countries facing economic difficulties or in remote or outermost areas – as a means of combating their isolation and making them more competitive, as well as for public authorities, enabling them to make their services more efficient and flexible, and reduce costs and red tape;

10. Regrets that, in the field of cloud computing, differing legal requirements lead to a fragmentation of the Digital Single Market and to high transaction costs for cloud providers and users;

11. Accordingly, calls on the Commission to propose legislative measures concerning transparency requirements and to prevent abusive and unfair practices; calls, furthermore, on the Commission and the Member States to ensure that the consumer acquis applies to cloud computing services in a comprehensive and uniform fashion throughout the EU.

12. Welcomes the Commission’s steps towards developing EU-wide standard contractual conditions by taking into account national recommendations and best practices, given that both high security of services and legal certainty for cloud users and providers are important to further enhance the evolution of cloud services; believes, however, that this should not prevent the market from developing cloud services in response to the needs of consumers, businesses, or governments;

13. Deplores the proposal by Member States to cut the Connecting Europe Facility by EUR 8.2 billion in the coming multiannual financial framework (MFF);

14. Calls on the Commission to ensure a technology-neutral approach supported by open and interoperable standards, in order to maximise competition and consumer choice;
15. Welcomes the Commission’s intention to establish an EU-wide certification system which would provide an incentive for developers and providers of cloud computing services to invest in better privacy protection;

16. Underlines that users are not necessarily aware of the fact that the services they use rely on cloud computing; insists, therefore, on the need for users to be better informed on the treatment of their data, especially by whom, where and how their data are treated;

17. Underlines that the public sector plays a key role in the development of cloud computing; welcomes the establishment of the European Cloud Partnership and the conclusions adopted by its steering board after its first meeting; stresses the need to elaborate EU-wide and national recommendations and best practices for transferring public IT use to the cloud, while ensuring a high level of awareness on the question of security, especially where personal data are concerned;

18. Calls on the Commission to ensure, through the adoption of standard contractual clauses or binding corporate rules, that any transfers of an EU cloud user’s personal data to a third country must be subject to strict safeguards and conditions, in compliance with EU data protection legislation;

19. Calls on the Commission to explore the adequacy of a review of the EU-US Safe Harbour Agreement, in order to adapt it to technological developments, especially with regard to aspects linked to cloud computing;

20. Underlines that cloud computing raises the issue of determining the applicable law and defining the responsibilities of all involved parties in terms of implementation of EU data protection legislation, especially with regard to EU users’ stored data using cloud computing technology by companies established in third countries; calls, therefore, on the Commission and the Member States to ensure that any transfer to and processing of EU residents’ personal data by a cloud operator established in a third country takes place in accordance with EU data protection legislation; calls, furthermore, on the Commission and the Member States to ensure that EU-based cloud users are informed when cloud operators communicate their data to the law enforcement authorities of a third country; stresses, in particular, its concern in future trade agreements over the responsibilities of Internet service providers, which include data protection;

21. Calls on the Commission and the Member States to simplify legal cross-border access to content and services from the cloud, and to consider providing more flexible licensing systems; suggests that the Commission, during its ongoing revision of copyright rules, adopt specific proposals to ensure that the future applicable regime will promote the distribution and dissemination of cloud computing services and innovation;

22. Calls on the Commission to ensure that any commercial agreements between telecommunications operators and cloud providers are fully compliant with EU competition law and that they allow consumers full access to any cloud service, using an Internet connection offered by any telecommunications operator;

23. Draws the Commission’s attention to the highly strategic nature of the location of data centres and to the potential impact of having such locations based outside EU territory,
especially with regard to the storage of sensitive data or that of public bodies;

24. Calls on the Commission and Member States to make cloud computing a priority of research and development programmes, and to promote it in the public administration sector as an innovative e-government solution of public interest, as well as in the private sector as an innovative tool for business development;

25. Calls on the Commission to consult consumer organisations and industry on a regular basis and to take their observations into due consideration, particularly with regard to the establishment of contractual standards for cloud computing, and to report regularly to Parliament on the discussions and conclusions drawn by the expert group;

26. Encourages the Commission and the Member States to communicate the economic potential of cloud computing to SMEs in particular;

27. Calls on the Commission to propose measures for copyright levies that foster innovation and promote creativity for the benefit of both right-holders and users, and that ensure that digital content which is subject to a licensing agreement between service providers and right-holders and legally acquired by private individuals or businesses (with due regard to any attached restrictions on terms of business use), shall not be levied further by virtue of being uploaded to the cloud or stored in the cloud by a service provider, provided that the remuneration of right-holders has been effective;

28. Takes note of the technological fact that if cloud processing is done in a particular country, the authorities of that country, including the security services, have access to the data; notes that this has implications from an industrial espionage perspective; asks the Commission to take this into account when issuing proposals and recommendations regarding cloud computing;

29. Calls on the Commission, within the framework of its expert group discussions, to make mandatory for cloud providers the inclusion in contracts of certain key clauses guaranteeing the quality of the service, such as an obligation to update software and hardware where necessary, to determine what happens if data is lost, and to determine the time it would take to resolve a problem or how rapidly the cloud service could take down offending materials, should the cloud user make such a request;

30. Calls on the Commission and the Member States to adopt specific measures on the use and promotion of cloud computing in relation to open access and open educational resources;

31. Calls on the Commission to study and identify best practices within individual Member States regarding the potential savings which could be achieved in public expenditure through the use of cloud computing by the public sector, in particular by establishing new procurement models;
# RESULT OF FINAL VOTE IN COMMITTEE

<table>
<thead>
<tr>
<th>Date adopted</th>
<th>30.5.2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Result of final vote</strong></td>
<td></td>
</tr>
<tr>
<td>+:</td>
<td>33</td>
</tr>
<tr>
<td>-:</td>
<td>0</td>
</tr>
<tr>
<td>0:</td>
<td>2</td>
</tr>
</tbody>
</table>

**Members present for the final vote**
Claudette Abela Baldacchino, Pablo Arias Echeverría, Adam Bielan, Preslav Borissov, Jorgo Chatzimarkakis, Birgit Collin-Langen, Lara Comi, Anna Maria Corazza Bildt, Cornelis de Jong, Vicente Miguel Garcés Ramón, Evelyne Gebhardt, Malgorzata Handzlik, Stanimir Ilchev, Sandra Kalniete, Edvard Kožušník, Toine Manders, Hans-Peter Mayer, Sirpa Pietikäinen, Phil Prendergast, Mitro Repo, Zuzana Roithová, Heide Rühle, Christel Schaldemose, Catherine Stihler, Róża Gräfin von Thun und Hohenstein, Barbara Weiler

**Substitute(s) present for the final vote**
Jürgen Creutzmann, Ashley Fox, Ildikó Gáll-Pelcz, Anna Hedh, Roberta Metsola, Marc Tarabella, Kyriacos Triantaphyllides, Sabine Verheyen, Josef Weidenholzer
# RESULT OF FINAL VOTE IN COMMITTEE

<table>
<thead>
<tr>
<th>Date adopted</th>
<th>14.10.2013</th>
</tr>
</thead>
</table>
| **Result of final vote** | +: 41  
-:  0  
0:  1 |
| **Members present for the final vote** | Amelia Andersdotter, Josefa Andrés Barea, Jean-Pierre Audy, Ivo Belet, Jan Březina, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Jürgen Creutzmann, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Fiona Hall, Edith Herczog, Romana Jordan, Philippe Lamberts, Bogdan Kazimierczuk, Marisa Matias, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Herbert Reul, Jens Rohde, Paul Rübig, Salvador Sedó i Alabart, Francisco Sosa Wagner, Evžen Tošenovský, Ioannis A. Tsoukalas, Claude Turmes, Marita Ulvskog, Alejo Vidal-Quadras |
| **Substitute(s) present for the final vote** | Antonio Cancian, Rachida Dati, Ioan Enciu, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Werner Langen, Zofija Mazej Kukovič, Alajos Mészáros |