

Position Paper

Unleashing the Potential of Cloud Computing in Europe Cloud Strategy of the European Commission

12 March 2013

Page 1

The Federal Association for Information Technology, Telecommunications and New Media (BITKOM) represents more than 1,700 companies in Germany. Its 1,200 direct members generate an annual sales volume of 135 billion Euros annually and employ 700,000 people. They include providers of software and IT services, telecommunications and Internet services, manufacturers of hardware and consumer electronics, and digital media businesses. BITKOM campaigns in particular for a modernization of the education system, for an innovative economic policy and a future-oriented Internet policy.

Summary

BITKOM welcomes the European Commission's strategy 'Unleashing the Potential of Cloud Computing in Europe' ('EU Cloud Strategy') published in its Communication dated 27 September 2012. BITKOM has developed comments and proposals which aim to make the EU Cloud Strategy a success. The comments and proposals can be allocated into five categories which BITKOM considers to be important success factors.¹

- Standardisation in cloud computing
- Legal framework for cloud computing (mainly data protection law and contract law)
- Use of cloud computing in public administration
- Infrastructure for cloud computing and
- International cooperation in cloud computing.

The comments and proposals of BITKOM can be summarised as follows:

- Standardisation, certification and codes of conduct in cloud computing
BITKOM emphasises the importance of standardisation to support interoperability (between different clouds and between cloud applications and traditional IT systems), for data portability and to define data protection and security levels. In this context, the Association welcomes the appointment of a Steering Board for the European Cloud Partnership (ECP). BITKOM expects further standardisation projects in cloud computing to have a significant influence on the European cloud market and is therefore prepared to support the Steering Board in its work. A certification scheme should also be implemented in the realm of a standardised EU data protection regime for cloud computing. Further expectations or industry-specific requirements of cloud users should be agreed on by the cloud providers by voluntary self-regulations or codes of

German Association
for Information Technology,
Telecommunications and
New Media

Albrechtstr. 10 A
10117 Berlin-Mitte
Germany
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Contact

Dr. Mathias Weber
Head of Department
IT-Services
Tel.: +49.30.27576-121
m.weber@bitkom.org

Nils Hullen, LL.M.
Head of Brussels Office
Tel.: +32.2.6095-321
n.hullen@bitkom.org

President

Prof. Dieter Kempf

Management

Dr. Bernhard Rohleder

¹ Pillars 1 to 3 follow the Key Actions 1 to 3 of the EU Cloud Strategy. BITKOM considers pillar 4 to be decisive; in the EU Cloud Strategy, the infrastructure is only given passing mention. BITKOM's pillar 5 refers to Chapter 4 of the EU Cloud Strategy's additional political initiatives).

Position Paper

EU Cloud Strategy

page 2

conduct, in order to maintain the necessary flexibility and limit the administrative burden, informing customers transparently about the conditions of the cloud service at the same time.

■ Legal framework for cloud computing

BITKOM welcomes a practical approach to the harmonisation of data protection and privacy within the EU based on the General Data Protection Regulation. Clear rules about data processing are essential - in particular with regards to the allocation of accountability and responsibility.

BITKOM considers the European Commission's announcements about model contract terms to be extremely useful for cloud contracts and expressly welcomes this move. Model contract terms should not be obligatory requirements under European contractual law for cloud computing contracts.

■ Use of cloud computing in public administration

BITKOM calls for public administrations to take a leading role in the implementation of cloud computing. BITKOM encourages the development of a strategy paper, a phased plan and a governance framework regarding implementation for administration clouds in the EU countries.

■ Infrastructure for cloud computing

A high-speed broadband infrastructure serves as the basis for cloud computing. In order to efficiently accelerate the development of high-speed networks beyond previous achievements using competitive means, it is essential to provide a corresponding regulatory environment and use all synergies for the development of the network.

■ International cooperation in cloud computing

Due to the small domestic markets, European coordination in relation to legal requirements and standards is required, but not sufficient on a global scale. BITKOM proposes a revival of the transatlantic economic partnership and support of the cloud working group Transatlantic Economic Council to create a joint legal cloud framework.

Position Paper

EU Cloud Strategy

page 3

Contents Page

1. Preliminary remarks about BITKOM's B2B focus.....	4
2. Promote standardisation in cloud computing.....	5
3. Practice-orientated legal frameworks for cloud computing	5
3.1 Harmonisation of data protection suitable for data processing	5
3.1.1 Standardisation of the data protection rules for cloud providers	6
3.1.2 Improving technical data privacy	6
3.1.3 Clear regulations for data processing	6
3.1.4 Applicability of standard contractual clauses	7
3.1.5 Introduction of internationally applicable law - elimination of legal grey areas	8
3.2 Flexibility through codes of conduct and certification.....	8
3.3 Contract law for cloud computing	11
3.3.1 Cloud contracts have their own requirements.....	11
3.3.2 Indispensable elements of cloud computing contracts	11
3.3.3 Plea for fair model contract clauses suitable for SMEs.....	11
3.3.4 Regulations required for legal "ancillary conditions" in cloud computing ..	12
3.3.5 Addressing consumer protection in cloud computing contracts.....	12
3.3.6 Rejection of mandatory contractual requirements under European contract law for cloud computing contracts	13
3.4 Providing access to content - suggestions and comments	13
4. Public Sector - advancement of a shared leadership role of the public industry through a European cloud partnership	13
4.1 Focus on open standards.....	14
4.2 Supporting the acceptance of electronic documents	14
5. Infrastructure - development of broadband for cloud computing	15
6. Position of Europe in cloud computing and international cooperation	15

Position Paper

EU Cloud Strategy

page 4

1. Preliminary remarks about BITKOM's B2B focus

BITKOM suggests that the content and language of the key actions and associated political steps planned by the Commission should be clearly separated into the

- Business-to-Consumer (B2C) and
- Business-to-Business (B2B)

fields of communication and business and that this should also be documented through a fully standardised use of terminology. BITKOM therefore proposes the introduction of the terms

- "consumer" be used for private consumers of cloud services and
- "companies" for commercial consumers

BITKOM is fully aware that a number of the measures planned by the Commission apply equally to both B2C and B2B; for instance in the case of "mobile banking", the health industry, communication with authorities and also with regards to copyright law.

Nevertheless, only a clear distinction between both areas will provide the opportunity to initiate target group-specific measures, identify the benefits for the respective user groups and communicate the achieved results in a targeted and comprehensible way.

A separation also appears to be appropriate due to the fact that, in their role as consumers and citizens, private individuals have different expectations and requirements when it comes to the service quality of cloud services with regards to availability and system stability, in comparison with companies in the B2B environment. The same is true of data protection, data privacy and compliance.² Unlike consumers, companies are also required to observe a far greater number of legal requirements when using IT systems and therefore also cloud services, e.g. commercial and fiscal archiving requirements and obligations regarding the recognition and avoidance of risk.

These specific requirements are to be taken into consideration with various supplementary EU measures adjusted for both user groups.

In contrast, the differentiation between major and small-scale companies made in the EU document appears to be less appropriate. As small firms in particular gain access to major opportunities in the global market through the use of a cloud, they essentially have the same requirements as major companies, e.g. with regard to data protection, data privacy and compliance. Furthermore, the same legal regulations apply to small firms as major companies. BITKOM there-

² Saving holiday photos in the cloud, a mobile music download by an end consumer or the voluntary publication of private information on Facebook tend to have a different degree of privacy requirements than the processing of data critical to companies or authorities. Increased requirements in these cases can, for instance, be fulfilled through anonymisation, pseudonymisation of personal information, through the high quality of the encryption algorithms used or the legal security of the processes.

Position Paper

EU Cloud Strategy

page 5

fore suggests that small and medium-sized firms should not be additionally overburdened with bureaucratic regulations.

As cloud computing is of greater macroeconomic importance in the B2B environment and the problems in this area need to be dealt with the most urgently, BITKOM has focused on the B2B environment in this response.

2. Promote standardisation in cloud computing

Standardisation to support interoperability (between different clouds and between clouds and cloud applications and traditional IT systems), for data portability and to define data privacy and security levels is required for the further development of the cloud market.

BITKOM welcomes the fact that the Steering Board appointed for the European Cloud Partnership (ECP) on 19.11.2012 intends to arrange for the development of a list of existing cloud-relevant standards, which are currently under review, by the European Telecommunications Standards Institute (ETSI) as part of their work programme. A report in the form of a cloud computing standards roadmap is scheduled to be released by the Commission in 2013.³

BITKOM expects further standardisation projects in cloud computing to have a significant influence on the European cloud market. BITKOM is therefore prepared to contribute its appraisals and experiences and participate in discussions and round tables held by the Steering Board.

3. Practice-orientated legal frameworks for cloud computing

3.1 Harmonisation of data protection suitable for data processing

BITKOM welcomes the harmonisation of the data protection framework within the EU. Data controllers and processors both should from a General Data Protection Regulation.

In addition to the aspect of uniformity and the scope of application, particular attention should also be given to ensuring that the future Regulation does not create any new hurdles and that it removes existing uncertainties for cloud computing in applicable law. Therefore, the following issues should be taken into consideration:

- the improvement of data protection by technical means,
- the adoption of clear rules regarding data controllers and processors, and
- the elimination of legal grey areas.

³ This will implement significant recommendations and conclusions which are covered in the following study: The Standardisation Environment for Cloud Computing - An analysis from the European and German point of view, including the 'Trusted Cloud Technology Programme' Study by Booz&Co. und FZI for the Federal Ministry of Economics and Technology (BMWi), February 2012, available to download from <http://www.trusted-cloud.de/de/878.php>

Position Paper

EU Cloud Strategy

page 6

3.1.1 Standardisation of the data protection rules for cloud providers

In principle, BITKOM very much welcomes the proposal of a General Data Protection Regulation. BITKOM suggests the following:

- The complete harmonisation of European regulations should apply to all processors offering services in Europe, irrespective of whether these providers also act as data processors in a Member State.
- During this process, the data processing by a cloud provider should be subject to the supervision of the authorities of the Member State in which the cloud provider is domiciled - regardless of the customer (responsible for the processing) and regardless of the Member State where they are domiciled - . In the case of cloud providers which are not headquartered in a Member State, it should also be the case that only one supervisory authority should be responsible and this should be determined according to objective criteria. It must be guaranteed that the participating users and providers are not confronted with different interpretations by the supervisory authorities.

3.1.2 Improving technical data protection

BITKOM encourages the improvement of the technical data privacy enhancing tools in the current draft of the General Data Protection Regulation.

IT technology is a key “enabler” of data protection. Privacy can be effectively increased through encryption, pseudonymisation and anonymisation. Data stored and processed in the cloud with a sufficient level of encryption could be treated like non-personal data by the cloud provider with no further risk. However, technical data protection is time-consuming and often costly. The legislator needs to create the right incentives in order to make use of technical data protection. This perspective should be taken into account in the review of the European data protection framework. Incentives should be provided for the pseudonymisation and anonymisation of personal data, emplacing the fact that anonymous data is not personal data, and creating facilitated conditions for the processing of pseudonymised data, as is already the case under German data protection law⁴.

3.1.3 Clear regulations for data processing

- Clear regulations for data being processed on behalf of a controller - particularly for the clear definition of responsibilities of the processor and the controller - are also crucial for the further development of cloud computing. The relevant provisions proposed in the General Data Protection Regulation do not structurally fit with some forms of cloud computing, and would therefore hamper it. In order to achieve practicality, it should be made clear that data processing on behalf of a controller is permitted in general. The relevant articles should be carefully revised, taking account of the following points:
- A clear distinction should continue to be made between the responsibility of controllers and processors, and the processor should only be responsible for the processing of data within the contractually defined limits. This also includes the provisions regarding the security of the processing. Only the con-

⁴ See German Federal Data Protection Act (Bundesdatenschutzgesetz), Article 5 (3).

Position Paper

EU Cloud Strategy

page 7

troller can determine how important the data is for them and how it needs to be protected. The allocation of responsibilities between the controller and processor (Art. 22, 24, 26, 27, 28 of the Regulation) is not sufficiently clarified in the draft.⁵

- In addition to the contractually agreed obligations, processors should only be responsible for those obligations in their field of activity, e.g. taking the required protection measures (e.g. by privacy by design) and implementing appropriate security systems.
- Accordingly, customers who receive prior confirmation, in the form of corresponding certifications⁶, that relevant security standards will be adhered to can rely on this certification without being required to fulfil their own additional control obligations. The purpose of the certificate is the legally required review of the contractor by the customer on the basis of a standardised requirements catalogue.⁷ The ability to interchange between the customer's review and a certificate should be enshrined in law.
- It should be made easier to draw up contracts with processors (cloud providers) should be introduced if their own service providers can provide evidence of suitable certificates or binding corporate rules (e.g. for the maintenance of operational equipment). In these cases, problem analyses by the service provider would also be permissible, even if they are domiciled in such a third country. Two further conditions apply to the permissibility of problem analyses by the service provider in an otherwise non-secure third country: Firstly, the transfer and possible recognition of personal data is only a technically unavoidable event within the scope of a problem analysis. And secondly, a problem analysis is required, for instance in order to maintain and guarantee operations.

As the law stands, this would only be possible within a direct contractual relationship between all controllers and any of the processor's service providers which might be involved.

3.1.4 Applicability of standard contractual clauses

BITKOM suggests that the European Commission clarify the fact that the standard contractual clauses of European cloud providers can also be used for contractual relationships within the EU. The standard contractual clauses should be revised or amended so that they can also be used by European cloud providers who want to use sub-contractors outside of the EU.

By the end of 2013, the Commission will work together with the stakeholders to set up model terms for cloud computing to be used in service agreements between cloud providers and commercial cloud users, thereby accounting for the

⁵ The responsible party and processor are named at the same time in numerous regulations. In the sense of a clear allocation of responsibility to the responsible party, the reference to the processor needs to be deleted from the corresponding regulations.

⁶ The response deals with certification matters in details in sub-chapter 3.2.

⁷ Proposal of the Working Group of the Trusted Cloud Initiative of the Federal Ministry of Economics and Technology Cf.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

Position Paper

EU Cloud Strategy

page 8

development of EU legislation in this area. This measure is very welcome, as binding standard contractual clauses in data processing are an important instrument for the contractual definition of IT services in compliance with the law. They will also shorten and simplify contractual negotiations, thereby reducing costs for the participants. The use of standard contractual clauses is a particularly essential prerequisite when exporting personal data to third countries, which is common in cloud computing services. However, there are often circumstances where a European supplier has the personal data of its European customers processed by sub-contractors in third countries⁸. At the moment the European supplier is, however, not permitted to use the EU standard contractual clauses when dealing with its non-European sub-processors.⁹ This means that a non-European cloud provider is given a standard procedure which states that they can process data on behalf of a European customer (for the processor) using non-European sub-contractors, while a European cloud provider would not be permitted to do the same. This puts European cloud providers at a competitive disadvantage.

European cloud providers should therefore be able to use the same standardised contractual clauses for both customers and sub-contractors in and outside of Europe. This would cut down on competitive disadvantages, reduce bureaucratic red tape and also lead to increased transparency and legal clarity.

3.1.5 Introduction of internationally applicable law - elimination of legal grey areas

BITKOM proposes a transatlantic initiative to remove legal grey areas which have resulted from the introduction of internationally applicable law. Conflicting legal obligations in American and European legislation represent significant legal uncertainty, not only for cloud providers but also all companies which process data on both sides of the Atlantic. Both sides should work towards a common understanding which defines the circumstances under which companies can be asked to release personal data to fight terrorism. Obligations under respective data protection law should then be amended correspondingly.

3.2 Flexibility through codes of conduct and certification

BITKOM suggests making it easier for cloud customers to exercise discretionary and monitoring powers when using cloud services - by promoting codes of conduct¹⁰ and their recognition as proof of compliance with the cloud customer's

⁸ For instance, the memory capacity offered there is used.

⁹ Cf.: Clause 23 of Directive 2010/87/EU. A European cloud provider who wishes to assign processing tasks to sub-contractors must use the standard contractual clauses defined in Commission Directive 2010/87/EU. However, they cannot transfer the clauses directly. As the standard contractual clauses only permit the direct export of data to non-European sub-processors by the processor (cf. Clause 5 of the Commission Directive 2010/87/EU), a European cloud provider, as the processor, needs to convince their customers that it has adopted the standard contractual clauses in their own contracts with non-European sub-processors. Only when the legal regulations have taken such data privacy agreements sufficiently into account can the cloud provider sign the contracts. This data privacy agreement concluded directly between customers and sub-processors, which could be very high in number depending on the amount of sub-contractors, would then of course also need to be concluded according to the internal European data privacy agreements with which the customer and cloud provider legally secure those processing services allocated to the European cloud provider itself

¹⁰ Negotiated agreements at community and association levels are to be given priority over individual negotiated agreements by companies.

Position Paper

EU Cloud Strategy

page 9

due diligence and monitoring obligations. Voluntary certificates with standardised and transparent testing procedures should be established by expert third parties to provide evidence that the monitoring obligations have been fulfilled by processors. Finally, data protection requirements within the scope of cloud services need to be developed further and a corresponding certification framework is also required.

- Cloud customers who upload personal data and other sensitive data to the cloud are responsible for ensuring that this data is adequately protected in accordance with security needs. The level of protection required depends on the risks posed to the rights and freedoms of those affected by the specific processing. In addition to the type of data involved, a decisive factor is the context of the data processing in terms of content and infrastructure. In order to fulfil this responsibility, cloud customers need to select and assess their service providers carefully. To make their selection, they need information which allows them to evaluate the suitability of a provider for their data processing needs. It is often impossible for cloud customers to fully cope with these monitoring obligations themselves, as the very nature of a cloud infrastructure means that it is not bound to a specific location.
- A good way to provide more transparency and support for cloud customers in fulfilling their monitoring obligations is a harmonised system of qualitatively comparable types of evidence, e.g. industry-specific codes of conduct and certifications which confirm that the data processing complies with legal regulations - and the special requirements of the respective company or specific industry - and provide evidence of this to the affected party.
- Such a system would make it easier, both for the affected party uploading their data to a cloud and also the responsible party using their cloud for company data, to identify which evidence is useful, appropriate and relevant to their situation.¹¹
- The recognition of submitted voluntary agreements as evidence that monitoring obligations have been fulfilled by the processor avoids the need for on-site monitoring.
- There are some circumstances where the provider or customer requires special evidence of compliance with the data protection regulations or special provisions for a high level of data privacy and data protection. For this purpose, corresponding evidence in the form of certificates needs to be encouraged and recognised.
- To meet this target, the certification should provide an analysis of appropriate depth and width. The requirements of the individual cloud customer or user vary widely - depending on the context. "General" certificates would therefore be more confusing than useful. It is therefore essential to develop a generally applicable certification framework and identify industry-specific requirements within the scope of this framework, which would then be tested for certification purposes.

¹¹ This would optimally support the assertion of the right of self-determination by affected parties and the acceptance of responsibility by the responsible agent.

Position Paper

EU Cloud Strategy

page 10

- To minimise the external certification costs for companies, the certification should be designed as a retrospective review of internal data privacy processes. The documentation of the internal processes and certification should also be based on the same principles.
- Certification options should follow a consistent, objective standard which enables a comparison of the providers and their data protection measures. The test criteria for awarding the certificate should be standardised and established on the basis of legislation for the European internal market. Test criteria should be identified in a process involving both data protection authorities and representatives of data processing providers and users.¹² Options should be provided which take the protection requirements for the data into account.¹³ The certificate should be issued by qualified private bodies. The suitability of the certifying body should be verified by means of accreditation. The certifying body should be liable for inaccurate certifications.¹⁴ When specifying certifications, cost-effectiveness for cloud providers should also be taken into account, along with the required minimum standards of quality.
- The requirements for the accreditation of certifying bodies should be established by representatives of the data privacy authorities and representatives of the customers and data processors. The accreditation should apply to the entire scope of the General Data Protection Regulation and should be implemented by suitable and, in particular, professionally qualified and independent bodies. The EU General Data Protection Regulation should in principle stipulate the requirements for accreditation bodies, but should leave the selection of the accreditation bodies to the Member States.
- In addition to data privacy, there are also a series of other topics where it makes sense to give providers the opportunity to declare their own legal eligibility for the service they provide. In addition to the negotiated agreement under data privacy law, a self-declaration can contain statements regarding compliance with national legal systems, interoperability, data portability and service quality and can therefore replace redundant certificates and the expenses associated with certification.
- In the case of certification, it is important that standards and certifications are based on existing approaches generally accepted in the industry, such as ISO 27001, which can then be supplemented with essential cloud specifics. This creates a significant advantage in terms of speed while at the same time avoiding additional competition-related costs resulting from new certifications.

¹² Cf.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

¹³ For instance, medical data or data subject to business confidentiality need to be secured using higher-quality privacy measures than the address data of an online gambling website.

¹⁴ Cf.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

Position Paper

EU Cloud Strategy

page 11

3.3 Contract law for cloud computing

A European cloud strategy and the measures derived therefrom represent an opportunity to reduce contract law expenses for international cloud computing contracts.

When discussing the further development of the legal framework for cloud contracts it is, however, important not to forget that the companies have already established a functioning practice for designing cloud contracts on the basis of national legal systems.

3.3.1 Cloud contracts have their own requirements

The design of cloud contracts must take diverse requirements into account and draw up contractual agreements, which partly are already known from other legal arrangements. However, it would not be reasonable to impose existing parameters on cloud computing business models, which were designed for other contractual circumstances. In this sense, a comparison between cloud computing and outsourcing and between the respective applicable legal requirements is not constructive. Cloud services are usually very specific and are limited to a certain clearly-defined purpose. They do not require any prior procurement procedure and are not associated with the transfer of personnel.

Likewise, the European Common Sales Law is unsuitable for cloud contracts and is not appropriate as a legal basis for such contracts. It is questionable whether downloading digital content from the internet should even be regarded as a cloud service. Business relationships in cloud computing are predominantly based on rental and services agreements. Moreover, it is currently impossible to foresee when and whether the Regulation on a Common European Sales Law will even come into force. Support for the drawing up of cloud contracts would, however, only help in practice, if it is provided quickly and enables both appropriate and easy-to-understand contract design.

3.3.2 Indispensable elements of cloud computing contracts

Certain contractual elements are essential for cloud computing business relationships. These include, for instance, the definition of service parameters in Service Level Agreements (SLAs) and the assignment of tasks and responsibilities to cloud providers and cloud users respectively. SLAs can also be used to assess when and to what extent the agreed cloud services were provided properly and whether warranty claims or contractual penalties can be asserted. If the European Commission were to propose examples of balanced SLAs, this would certainly be helpful in contract practice.

3.3.3 Plea for fair model contract clauses suitable for SMEs

Contractual conditions for cloud contracts, both in the areas of B2B and B2C, should answer questions about storing, returning and passing on the data after the end of the contract, the release and integrity of the data, data privacy, the storage location of data, the apportionment of data responsibility between the cloud provider and the cloud user, liability for disruptions of the cloud service and for the loss of data, the involvement of sub-contractors and the settlement of disputes arising from the cloud business relationship. It would therefore be of great assistance in contract practice and a useful guidance, if the European Commission were to publish considerations regarding the contractual regulation

Position Paper

EU Cloud Strategy

page 12

of these questions in the form of model contract terms. Due to the different ranges of interests, model terms, which are independent of each other, should be created for contracts with consumers (B2C) and contracts between companies (B2B). A cloud customer's commercial status could be used as the distinguishing criterion. If the cloud customer is acting as a business, the B2B rules apply. In both situations, such model clauses should also be based on the regulations for service and rental contracts in order to adequately represent the typical contractual conditions in cloud computing. The provisions should, however, not be too complicated, would need to be suitable for adaptation according to the respective cloud business model and must be optional for the contractual parties of the cloud contract.

When the EU draws up model contract terms, it is also important to ensure that these are compliant with the relevant legislation of the Member State and should, for instance, not fail in a legal review of terms and conditions within the Member State. It is essential that the cloud provider has legal certainty regarding the effectiveness of the model contract terms.

When seeking fair contractual conditions in cloud computing for small companies (and consumers), it is important to remember that small companies are often also cloud providers. In order not to jeopardise this, it should be ensured that the stipulations under contract law in cloud model contracts can also be fulfilled by small companies and do not overburden them.

3.3.4 Regulations required for legal “ancillary conditions” in cloud computing

A legal need for regulations exists for legal “ancillary conditions” in cloud computing, i.e. regulations which define specific requirements for data and the management of data (processing, use, access and the storage of data). These requirements would need to be standardised across Europe and optimised for data processing by way of cloud computing.

For example, data privacy (liability of the cloud provider in the event of the loss of data), the insolvency security of the data (correct return of data in the event of the provider's insolvency), data privacy and archiving requirements have not yet been standardised across the EU or geared towards cloud applications.

3.3.5 Addressing consumer protection in cloud computing contracts

As already mentioned, there is a significant difference between cloud contracts between companies (B2B) on the one hand and cloud contracts with customers (B2C) on the other hand.

In the case of cloud computing contracts for B2C business transactions, the interests of the consumer and the means of the cloud provider need to be appropriately balanced. In doing so it should be taken into consideration that the cost benefits for cloud services can only be realised if these services retain their character as easily scalable standard services. Moreover, it must be guaranteed that contractual conditions in B2C cloud contracts are consistent with national consumer protection law and therefore provide legal certainty. At the same time, standardised contract terms must ultimately be suitable for use in their respec-

Position Paper

EU Cloud Strategy

page 13

tive scope of application. These requirements are particularly important if small and medium-sized companies are acting as cloud service providers. The special benefit of standardised contract terms is, after all, unification and the opportunity to create an extensive field of application.

3.3.6 Rejection of mandatory contractual requirements under European contract law for cloud computing contracts

The creation of model B2B and B2C contract terms is to be welcomed. However, setting mandatory European contract law has to be avoided, as it would not be suitable. The complexity of individual cloud business models requires considerable flexibility in drafting contracts and opposes to obligatory legislation. Consequently, there cannot be any standard and firmly predefined legal "cloud contract".

3.4 Providing access to content - suggestions and comments

Improved flexibility and modernisation of collecting societies are required in order to promote the creation of value with cloud music services in a European internal market. The regulation of their de-facto monopoly through state supervision and controls should also not exclude their subsidiaries.

We therefore consider the problems addressed by the current draft directive regarding collective rights management in Europe to be the future roadmap for the creation of a European internal market for creative content. However, the spheres of activity addressed in the draft are not far-reaching enough.¹⁵

4 Public Sector - advancement of a shared leadership role of the public industry through a European cloud partnership

In a Position Paper¹⁶ developed jointly with VOICE - Verband der IT-Anwender e.V. (Association of IT Users), BITKOM has called for the increased use of cloud computing in the public sector. The recommendations in this Position Paper are consistent with Key Action 3 in the EU strategy. The comments and references apply to the situation in Germany and would need to be verified for the other EU countries.

Cloud computing provides excellent solutions for the diverse requirements of public services. However, the opportunities have barely been exploited by the public sector. Concerns about security and data privacy, along with procurement and budgetary law, have prevented the broad application of cloud computing in public administration. Furthermore, the strategic direction has yet to be determined in many areas.

Functioning pilot projects in the public sector can act as important primers and benchmarks for the economy. They build confidence in the new technology and increase their acceptance.

¹⁵ For further details please refer to the detailed response regarding the current Draft Directive:

http://www.bitkom.org/de/themen/59922_73400.aspx

¹⁶ Cf.: BITKOM/VOICE, February 2012, "Empfehlungen für den Cloud Computing-Standort Deutschland" (recommendations for cloud computing in Germany as a location)

Position Paper

EU Cloud Strategy

page 14

BITKOM calls for the public sector to take a leading role in the implementation of cloud computing. BITKOM encourages the development of a strategy paper, phased plan and governance framework regarding the implementation of administration clouds in the EU countries.

4.1 Focus on open standards

The public sector must set an example by committing to standards for public administration, enable interoperability between cloud services by using the standards and processes, indicating and calling for adherence to standards when tendering public cloud projects and increasing investment into cloud computing.

Confidence in cloud providers can only be created through open standards. Open standards are being developed internationally and must be taken into account by the relevant national bodies. The statements in Section 2 also apply to the public sector.

4.2 Supporting the acceptance of electronic documents

For the seamless flow of electronic administration processes, it is necessary to accept electronically produced documents and papers which, under some circumstances, can be saved in a cloud environment such as an electronic safe and can then be re-submitted for administrative purposes.

The crossover from the previous hybrid management of files to full electronic document management is an inter-disciplinary challenge at all levels of administration and for all specialist departments.

The coexistence of electronic and paper documents makes electronic workflows more expensive and slows them down.

The use of electronic signatures is an important basis for document management systems at the various administration levels and the joint signature process in the case of multi-level administrative decisions. Electronic signatures guarantee the integrity, authenticity and a verifiable signature and time stamp function within the organisation. Archiving also needs to be verifiable in the long term. On the other hand, regulations and laws should be simplified to reduce the complexity of processes so that electronic documents can be easily used. For instance, the principles of e-invoicing with no signature could be established as a basis for electronic documents. An internal or official checking process with an audit trail is sufficient for authenticity and integrity - which would lead to significant process improvements. An example of this is ZUGFeRD, the new standard for electronic invoices which is favoured by BITKOM.

Position Paper

EU Cloud Strategy

page 15

5 Infrastructure - development of broadband for cloud computing

From the point of view of BITKOM, those locations where cloud services can be accessed quickly, securely and easily will benefit in international competition. A modern broadband infrastructure is therefore a basic requirement and also forms the basis for the broad use of cloud-based innovations in economics, science and society. The development of new infrastructures is of extreme importance for society and economic policies in Europe.

Saving and processing data seamlessly requires high transfer capacities and, consequently, an infrastructure which is available via broadband in both areas of high population and rural regions. In recent years, previous attempts to improve the broadband provision using infrastructure programmes have led to the significant reduction of so-called “dead zones”. Nevertheless, providers still face the challenge of making huge investments into the infrastructure.

In order to efficiently accelerate the development of high-speed networks beyond previous achievements using competitive means, it would be essential to provide a corresponding regulatory environment and make use of all synergies for the development of the network. Regulation must not represent a risk for investments and should instead take its impact on investments and jobs into account to a greater extent than ever before.

6 Position of Europe in cloud computing and international cooperation

BITKOM strongly supports the international cooperation announced in sub-chapter 4.2 of the EU Cloud Strategy. Such cooperation is particularly significant when it comes to boosting the growth of European IT companies. It is generally known that internationalisation remains a hurdle which IT companies face at a relatively early stage to facilitate long-term growth. Due to the small domestic markets, the European coordination regarding legal requirements and standards is required, but not sufficient on a global scale. BITKOM proposes a revival of the transatlantic economic partnership and support of the cloud working group Transatlantic Economic Council to create a joint legal cloud framework. In such a transatlantic economic agenda, cloud computing would take a key position, as it is set to be the central economic platform of the future. The development of a transatlantic cloud market defined by low transaction costs and a high level of confidence will define the formative infrastructures of the 21st century.

The EU should make use of its leading role in the areas of data privacy and security in international committees and develop its strengths in the areas of software as a service and business process as a service in a targeted way. In this sense, sub-chapter 4.2 should be supplemented to include specific measures:

- Support the Transatlantic Economic Council's cloud working group to permanently establish a shared cloud perspective:
All legislative and regulatory measures which affect cloud computing should be regularly submitted to the Transatlantic Economic Council for review of the effects on the transatlantic economic zone.

Position Paper

EU Cloud Strategy

page 16

- **Strengthen convergence efforts between the legal systems:**
In the long term, the convergence of cloud computing legal standards is an important goal. For this purpose, government representative on both sides should be involved in ongoing legislation processes from an early stage.
- **Strengthen bridging mechanisms such as “Safe Harbor”:**
Bridging mechanisms, which make differences between the legal systems more economically friendly, are of strategic importance. This high significance is currently insufficiently reflected in political work. BITKOM urges the further development of Safe Harbor, which in particular involves stronger implementation and control mechanisms on both sides of the Atlantic.
- **Establish joint research focus points in the field of cloud computing to support the convergence of cloud policies in the medium term (data privacy, encryption, logging data access, standardisation)**
- **Support the multilateral and bilateral discussions by the EU regarding cloud computing matters.**