



16- POINT

**ACTION PLAN FOR
CLOUD COMPUTING IN EUROPE
PRESENTED BY EUROCLOUD**

<http://www.eurocloud.org/>

A 16-POINT ACTION PLAN FOR CLOUD COMPUTING IN EUROPE PRESENTED BY EUROCLOUD

EuroCloud, the European organisation for cloud computing and software-as-a-service (SaaS), held its first pan-European member Congress in Luxembourg in July 2010. Attendees took part in a series of participative workshops throughout the day, moderated by EuroCloud board members and including contributions from selected subject matter experts. The workshops had the task of drawing up the elements of the EuroCloud action plan.

Workshop participants consisted of a diversified group of information and communications technology (ICT) experts, from service providers and software developers to investors and integration partners. This diversity was a key factor in obtaining a clear and well-structured set of principles.

The meeting concluded with agreement on a 16-point plan to help European businesses benefit from cloud computing. The action plan, set out in this document, specifies the next steps to create trust and success in cloud computing in Europe by activities such as:

- promoting best practice by highlighting cloud success stories and working with others in the industry to establish pragmatic standards;
- facilitating cloud as a vehicle for IT-enabling SMBs and SMEs in the European marketplace, and fostering the development of new skills needed to take full advantage the opportunities afforded by cloud computing;
- working with authorities to ensure the best possible legal and institutional framework to protect and provide maximum value to business users of cloud computing; for example, by clarifying the legal framework for cross-border data flows in a cloud computing environment;
- Continuing to develop EuroCloud's role as a community for collaboration and networking among industry players to bring the best possible cloud solutions to market in Europe and beyond.

The findings of each of the EuroCloud Congress workshops are set out below.

SECURITY AND CERTIFICATION

There is a clear trend towards cloud adoption among businesses and individuals. The will is there to change to this new model of computing. But we must recognise that, for all except industry insiders, cloud computing is new and unfamiliar. Thus our key goal as an industry is to build trust in the cloud.

Security is one of a larger set of issues that can be collectively grouped under the general heading of trust. That trust can only be built on better understanding and communication. Customers need guidance to help them understand and objectively evaluate the risks and benefits.

THE NEED FOR CERTIFICATION

A fundamental requirement in the cloud environment is that providers must offer visibility into their processes. With an internal IT infrastructure, the enterprise can see what is happening and knows what its risks are. With a cloud provider, the customer cannot know what lies behind the service unless the provider tells them.

The value of certification is that it provides a framework and a common language for understanding what a provider has to offer, so that the customer can make a more informed judgement about the suitability of the proposition for their needs. When coupled with a third-party auditing process, this offers additional comfort that the provider meets a recognised standard.

A number of separate initiatives are under way to create standards, best practice guidelines and certifications for various aspects of cloud computing and SaaS, while data centres already have to conform to established audit standards such as SAS-70 and ISO 27001. With no industry-wide co-ordination, there is a danger of prospective cloud buyers being confused by the advent of too many separate initiatives and competing or overlapping standards.

BENEFITS OF CERTIFICATION

- To be able to evaluate cloud providers, customers need to know what to ask for. As a baseline, a recognised industry certification can offer a commonly agreed checklist of questions.
- At the moment, customers are devising their own questionnaires to send to providers. This creates an unnecessary duplication of effort both for customers in drawing up the questionnaires and then for providers understanding how to answer each one. Some form of standardisation on a common list of questions or an accepted external audit/certification will help reduce this extra cost on both sides.
- A certification checklist that's agreed by the industry will help providers to help themselves. It will ensure they can identify any gaps in their infrastructure or processes and fix them ready for certification. Reputable participants in the industry will benefit from measurements that help identify those who don't play by the rules.

However it is important to sound a note of caution. Certification and audit processes should not become so burdensome or inflexible that they block innovation and competition, especially on the part of smaller players and new market entrants. Certification must be designed to work across the spectrum, from the smallest provider up to the very largest.

SECURITY IN THE CLOUD

Security is often cited as a concern. It is self-evident that the public cloud is an environment that is exposed to more potential threats than a typical enterprise network secured behind a well-maintained firewall. However the industry must drive home the argument that security in the cloud can often be stronger and deeper than security in a conventional infrastructure because of the steps providers take to counter those threats. Two factors contribute to this:

- The provider has to ensure the security of each individual customer's data within its own infrastructure. Customers have to be confident their data will not be accessed by other customers or become commingled with other data in a way that compromises integrity or compliance. Therefore in addition to controlling access at the perimeter, the provider also invests in extensive internal measures to keep each customer's data secure and logically separate.
- Increasingly, security is getting too difficult for individual enterprises to keep up with the required skills, knowledge and expertise. Because cloud providers pool resources across their customer base, they have more accomplished security.
- A cloud provider typically invests a higher percentage of its revenue on security compared to the percentage of budget that an enterprise IT operation spends. The benefit of this spend is shared across the provider's whole customer base, yielding a much higher "return on security investment" or ROSI.

OTHER TRUST ISSUES

Having reliable access to their data and retaining governance over its handling is just as important to customers as keeping it safe from unauthorised access.

Service level agreements provide assurances on the availability of data. As well as publishing their own SLA metrics, providers must disclose SLAs from subcontractors in the service chain, such as data center and backup providers, and their impact on their own service level commitments to customers. It is important to remember that the sensitivity of the data stored varies between applications and through the lifetime of the data. Some providers offer various options for availability and service levels, depending on the requirements at each point in the data lifecycle.

Customers should always be able to recover their data. Getting data out is as critical as the operational issues while it is under the provider's control. Is there a trusted mechanism for the customer to access its data without interference of the provider? They

may wish to keep a separate back-up or to test other platforms. A customer may decide to move to an alternative provider, or the provider may terminate its service. There should be a mechanism for getting data back, either if the provider fails (for example through bankruptcy), or if the customer stops paying. It should be noted that some countries, including France and Luxembourg, are preparing legislation on the question of returning data after a provider fails.

Data protection legislation requires customers to handle data in a certain manner, including keeping it stored within the regulated area (such as the EU or an individual national jurisdiction), and complying with archiving and retention rules. It is their responsibility in law to ensure compliance. Customers should be able to specify the compliance parameters and rely on providers to obey them and provide an audit trail of the actions taken.

Data handling regulations must be respected not only during storage and processing but also for back-ups, archiving, disaster recovery, upgrades and other processes that potentially involve data transfers.

In summary, when entering a relationship with a cloud provider, customers must be satisfied with arrangements for the entirety of the data lifecycle, from the moment of creation and the act of sharing, through transfers from one home to another, potential separation and divorce on occasion, and ultimately archiving and deletion.



RECOMMENDATIONS FOR ACTION

Failures of trust damage the industry's reputation and increase the risk of regulation being imposed on cloud providers without full consultation. It is up to the industry to take a lead to ensure wide awareness of best practices among both customers and providers. As well as collaborating with others within our own industry, we should seek to emulate and build on best practice knowledge accumulated by industries in other fields that have been here before.

ACTION POINT 1

EuroCloud should work with others in the industry to educate and inform customers on how to work with SaaS and cloud providers to ensure their data is stored and handled correctly throughout the data lifecycle.

ACTION POINT 2

EuroCloud should provide guidance to help the industry and its customers understand the value and relevance of certifications and standards relating to cloud computing and SaaS.

ACTION POINT 3

EuroCloud should collaborate with the rest of the industry, with user interest groups and with public agencies, to produce useful standards for best practice guidelines, certification and auditing of cloud and SaaS providers.

SERVICE LEVELS AND CUSTOMER EXPERIENCE

Much of the discussion about cloud computing has focused on the initial buying decision in relation to conventional 'on-premise' computing, with an emphasis on comparing factors such as cost, functionality/capability and security. But the as-a-service model of cloud computing means that the relationship is ongoing rather than happening at one moment in time. Thus it's just as important (if not more so) to also make a thorough examination of the customer experience to be expected after the contract begins.

The service level agreement (SLA) is the part of the contract that sets out the boundaries and understandings within which the service will operate. An SLA should be more than just a set of numbers. It's a structure that helps define the relationship between a customer and a provider, and success should be judged by the performance delivered. For example, Amazon doesn't offer the thick, detailed SLA contracts favoured by traditional software providers, but it still performs at service levels that are higher than those of the traditional, large, well-known companies. It is a matter of looking beyond the technology and understanding the service parameters from a customer's perspective.

The goal for providers is to ensure they are managing the service in the right way and that their customers are having the right experience in terms of the business output that's delivered. The main consideration when sitting down to think about SLAs is to ask, what is your application doing? What is your customer trying to accomplish with your solution?

The customer experience is not defined only by SLAs. Our industry should perhaps put more focus on risk management and accountability. If we give customers more understanding of the risk factors, greater transparency into processes, and better visibility into performance data, it can help them assess the risk for themselves and make their own decisions on how they manage it. This includes understanding what will happen in the event of a failure and what steps the customer can take until the service is restored.

COMPONENTS OF SLAS

As an industry, we do need to work towards common understanding of what is meant when we say SLA, and towards a common vocabulary or taxonomy of terms and concepts used when discussing service levels and customer experience.

- An SLA should always refer to performance levels (ie quality of service) rather than simply whether a service is up or down (ie availability of service).
- SLAs set the bar for customer experience – 99.5% allows for a large chunk of downtime, more than is tolerable for mission-critical applications.
- It is important to be aware of how SLA compliance is measured. Service availability is typically monitored by checking for a response every ten minutes, but for many instances, this is too long an interval

- Many customers just want to use the software as needed. They don't really care when exactly it's up or down or what problem has caused a service level failure, so long as it's there when they want it. Business context and usage patterns are an important element of risk assessment.
- Some customers demand transparency at a more granular detail – not just performance but also covering other aspects of service management such as governance and compliance. Thus a service contract may include specifications for where data is stored or how long it is archived, for example.

Behind the service to the customer, the cloud often contains multiple levels of SLAs – especially at higher levels of solution such as platform as a service and software as a service, which may themselves be built on or incorporate other cloud services as part of their infrastructure. As the manager of the solution, the provider has to have internal support and policies in place so that it can be proactive at managing risk and ensure it remains in control when one of these third-party services has a glitch.



RECOMMENDATIONS FOR ACTION

Growing dependence on cloud computing across society increases the systemic risk of any potential failure and it is inevitable this will lead to government regulation, in the same way that other crucial infrastructure providers such as banking and telecoms are regulated today. The industry must take a lead now in defining best practice for service levels and customer experience that can form an effective basis for future regulation.

ACTION POINT 4

EuroCloud should work with the industry to promote best practice benchmarks for customer-vendor engagements, including actions when a service deteriorates or fails.

ACTION POINT 5

EuroCloud should work with industry and stakeholder customers, such as government, to promote best practice around more granular transparency in SLAs, focused on customer risk management.

ACTION POINT 6

Industry participants should work with initiatives such as the EU's SLA@SOI project to further standardization in service level monitoring, with the future aim of enabling an elastic system of dynamic service level provisioning.

THE LEGAL FRAMEWORK FOR CLOUD AND SAAS PROVISION

Cloud computing opens up new possibilities, especially across national boundaries, and it is important that the legal framework doesn't obstruct that potential, especially if such obstructions prevent European businesses from enjoying the same market reach and freedoms as their competitors enjoy in large national economies such as the US, China and India, where there is a single legislative framework.

Much of the existing legal framework within which cloud computing has to operate was designed in the past. Existing laws often relate to earlier generations of information and communications technology, and sometimes make implicit assumptions based on those earlier architectures that no longer apply to cloud computing, or which introduce unforeseen difficulties. In particular, problems can arise when a cloud service crosses national boundaries – an everyday occurrence in the globally connected cloud computing environment, but an exceptional event for earlier generations of computing, which were designed to serve a single enterprise from a fixed location. Sometimes the implications of certain laws may not be recognised until a breach or an event occurs that results in an investigation. Such factors have created a legal minefield for cloud providers attempting to offer services in Europe that go beyond a single national jurisdiction.

Fortunately, the European Commission is seeking input from stakeholders to help it shape EU policy, rather than taking a top-down approach to shaping the agenda. Within the context of defining how to pursue the Digital Agenda, the Commission is currently in the process of defining its cloud computing strategy. This provides a welcome opportunity to focus on the barriers that currently exist within the context of seeking resolution.

Specific issues that need action include the following points.

- The industry must make its voice heard when governments are drafting digital economy laws, to ensure that the impact of obligations and restrictions imposed on providers do not have unintended consequences for the flexibility, cost-effectiveness and competitiveness of cloud services that can be made available to European businesses.
- The industry sometimes has difficulty communicating with policy makers because of the lack of a common vocabulary and context for cloud computing. More use of cloud computing by government may help policy makers to better understand the context of their decisions.
- Harmonisation is needed to prevent situations where, as in the case of data retention legislation, providers offering services that cross national borders can find themselves obeying the law in one jurisdiction by a course of action that simultaneously violates the law in another jurisdiction.

- The pre-existing state of rules and directives governing data protection must be reviewed to ensure they are consistent across the EU and fit with the reality of cross-border data flows in a cloud computing environment.
- In the banking industry, the physical location of money is not usually a material factor. Contracts between banks and their customers are governed based on where the customer is located. Given the economies of scale and other advantages that can flow from greater flexibility in the location of data and processing by cloud providers, there may be a case for building a similar legal framework for data in the EU, focusing on the contractual agreement between providers and customers rather than the physical location of data.
- We need recognition that small businesses consuming cloud computing often have no control or visibility into where their data is being stored or processed, even though they are legally responsible for how the data is handled. There is a vivid need for greater awareness of the impact of legislation and for additional steps to enable more proactive risk management.
- We must recognise that legislation governing B2C services (offered to the general public) has to be more stringent on providers than is necessary for B2B services (offered only to businesses). Consumers cannot be expected to make complex risk assessments, whereas businesses have more resources to assess and manage risk for themselves (and often want to have this choice).
- There is confusion regarding certification of data centres, with some providers and customers using the US audit standard SAS 70, while others prefer ISO 27001. It was noted that regulation is expected later this summer relating to certification alternatives and replacements.



RECOMMENDATIONS FOR ACTION

EuroCloud can play a role in helping raise awareness in the marketplace, promoting infrastructure skills and lowering the barriers to adoption of cloud computing. At the same time, we must highlight the consequences of policies and legal frameworks where they act against the interests of EU businesses or citizens wishing to benefit from adopting cloud computing.

Realizing that policy cannot be formed in a vacuum, it is incumbent on our industry to work to establish standard best practices and frameworks that can, if necessary, be translated into law. If the industry is able to do a good job of self-regulation, then that minimises the need for regulation to be imposed by law. On the other hand, if we do not act in a timely manner, we risk an incident giving rise to the imposition of legal requirements without consultation.

Meanwhile, our industry already has to work within a legal framework inherited from past generations of ICT. We must engage policy makers in a constructive review of the law and its implementation to find ways of removing the obstacles to a truly EU-wide digital market, for which cloud computing can be a crucial enabler.

ACTION POINT 7

EuroCloud must work with government and other authorities to fine-tune the regulatory framework (notably on data protection and data retention) to enable cross-border data flows for B2B cloud computing.

ACTION POINT 8

EuroCloud and the cloud computing industry must raise awareness of the benefits that flow from harmonisation of policy frameworks throughout Europe, and should work to develop and adopt consistent best practices as a demonstration of the industry's ability to achieve effective self-regulation

ACTION POINT 9

EuroCloud should begin to develop a position on whether data law should govern jurisdiction of customer contracts rather than physical location of data and processing, especially in B2B contracts.

FOSTERING AND RECOGNISING INNOVATION

As a disruptive paradigm, cloud computing is changing the way ICT is being used by companies. At the same time, these changes are introducing new fears and doubts regarding security, quality of service, data protection and other matters. In order to increase the pace of cloud computing adoption, we have to embrace these fears and doubts as new opportunities emerge for innovating and creating new business.

THE VALUE CHAIN OF SUPPORTING AND FINANCING R&D

Despite the fact that the majority of companies have the goal of continuing to improve and develop their products and solutions by investing in research and development (R&D), they have difficulties to clearly identify the value chain of R&D. Companies are also having difficulty to identify the most efficient methodology to incorporate the results of R&D in their products, maximizing investments in product differentiation and innovation. Small and startup companies, usually working within small budgets, have the need to concentrate their R&D efforts on supporting existing products. For investors, it's also more secure, from a perspective of return on investment, to invest in products and solutions that are ready to be commercialised instead of putting funds into R&D efforts.

INNOVATION AS A CONTINUOUS PROCESS THAT SHOULD BE ENCOURAGED

Following the previous topic, it is remarked that the culture of innovation, based on structured R&D plans, should be promoted and encouraged. It's important to focus these efforts not only on companies but also on consumers. Companies should search for innovative solutions having customers' problems and needs in their horizon. On the other hand, customers should have the culture of searching and demanding for more innovative products and solutions.

HOW TO ADAPT ASYMMETRIC RHYTHM OF R&D IN THE UNIVERSITIES AND COMPANIES?

R&D centres in companies and universities have different rhythms and methodologies for organizing their R&D projects. Usually, companies have to work in small time frames, always having to focus the work on return on investment and product incorporation. This methodology is different from the one used by academic research projects, where time and product orientation are not mandatory requirements. The promotion of R&D ventures between companies and academic institutions is recognised as being a key factor for increasing knowledge transfer and the development of new and innovative products.



RECOMMENDATIONS FOR ACTION

There is huge potential from cloud computing to foster business innovation and enable R&D, as well as its impact on cultural development, new forms of education, and other fields of endeavour. The industry must raise awareness of the role that it can play and seek to facilitate European innovation.

ACTION POINT 10

Because of their low cost of adoption and rapid deployment, cloud based technologies are innovation enablers. EuroCloud can help diffuse best practices to encourage take-up of cloud services for business innovation and R&D.

ACTION POINT 11

Regional and national governments and the EU should do more to make funding available to innovative start-ups and small businesses, especially those developing products and services for the large enterprise market.

ACTION POINT 12

EuroCloud should facilitate interaction between VCs, universities and entrepreneurs, participating in the emergence of a much-needed innovation ecosystem across Europe that will aid technology and skills transfer from universities and other research agencies to start-ups.

INDUSTRY ALLIANCES AND PARTNERSHIP

Visibility of what is happening in cloud computing across Europe is very poor, especially when compared to the US. Everybody is operating in their own domestic market and it is difficult to see what is happening in other national markets within Europe. There are many significant cloud and SaaS businesses in Europe but they are not as well-known as their US counterparts even in their own countries. The technology media is fragmented and coverage by journalists and analysts tends to concentrate on the better-known US vendors even if there is a larger or more relevant local equivalent. Different languages and cultures make it even harder to find accurate information by, for example, web searches or by reaching out in social networks.

These factors inhibit the ability of European businesses to expand across borders or to find partners in other countries. One of the key motivations for founding EuroCloud was to provide a forum where cloud and SaaS providers in Europe could link up and find each other.

Providers need to link up for a number of reasons. They may wish to team up to offer packaged services to vertical markets throughout Europe. They may simply need to compare notes, learn more about different technology implementations or business techniques, or converge on best practices. Smaller businesses need to understand how best to partner with larger, dominant technology firms and can benefit from alliances with others who have similar interests.



RECOMMENDATIONS FOR ACTION

A vital role for EuroCloud is to facilitate connections between members because we want to build partnership. It is essential to maintain our momentum by strengthening connections within and beyond the pan-European membership.

ACTION POINT 13

EuroCloud should build a membership marketplace to foster information exchange and partnership among its members.

ACTION POINT 14

EuroCloud must promote its own brand to raise awareness of its role as a rallying point for cloud and SaaS players in Europe.

INTERNATIONALISATION WITHIN EUROPE AND BEYOND

INTERNATIONALISATION

Web businesses are global by nature as they can be accessed anywhere around the world. This is the mindset of companies in the cloud computing space. Almost all companies that participated in this workshop discussion have an international presence. The ones that did not provide their solutions internationally were considering it, but felt more confident working in their own market.

Going global is a goal from day one for cloud computing companies mainly due to the opportunities to scale by reaching a wider market. However there are some barriers to expanding across borders, both within Europe and beyond. These range from language and cultural aspects to legal impediments.

COMMUNITIES

At least half of the workshop attendees had set up communities around their products and/or services offerings. Communities help to improve customer support and lower costs, as users help each other. They also help provide visibility and transparency, for example by showing how the service is running, which builds trust with their customers and end users.

EUROPE'S DIGITAL AGENDA

The Commission's Digital Agenda was welcomed by attendees as a catalyst for improving the cloud computing area and the business behind it. It was seen as an important initiative that would help providers in their efforts to expand across borders within Europe. Action to improve the digital infrastructure across Europe was highlighted and welcomed in particular. However some expressed doubts about the Commission's ability to deliver such a large list of actions. There were many priorities and it would need the assistance of industry to achieve them. EuroCloud can play a role in helping the European Union to prioritize and deliver these actions.



RECOMMENDATIONS FOR ACTION

EuroCloud has a crucial role to play in focusing attention on the European cloud industry and its successes, especially in highlighting examples where its customers have achieved business advantage and innovation through the use of the cloud. It should use its growing influence to encourage industry and government to adopt cloud services.

At the same time, the industry needs better infrastructure, more skills and lower barriers to enhance market success. Growing awareness of the benefits of cloud computing will help motivate investment in these areas.

ACTION POINT 15

EuroCloud should foster a community of the industry and its customers to highlight the success of cloud computing.

ACTION POINT 16

EuroCloud should work with other stakeholders to hold annual contests to celebrate innovation and best practice in cloud computing.

ABOUT EUROCLLOUD

EuroCloud (<http://www.eurocloud.org/>) is the first pan-European network of SaaS and cloud computing vendors and industry participants, with a presence today in more than 22 European countries. Through its diverse membership of vendors, integrators, supporting parties and industry experts, EuroCloud will promote cloud computing in Europe, sharing best practices, encouraging innovation and extending business within Europe and beyond. EuroCloud stands under the guidance of Pierre-José Billotte, president and founder of the former French ASP forum, now EuroCloud France.

For further information, please visit: <http://www.eurocloud.org/>