

Keeping darkness out of the cloud

By Viviane Reding, European Justice Commissioner

Cloud computing conjures up images of floating zeroes and ones – data liberated from the desktop and drifting effortlessly from one server to the next. Consumers and companies benefit from storing information on remote servers, no matter where they are, and then pulling it back when they need it. Our societies have been transformed as users embrace social networks, blogs, newsfeeds and shared bookmarks that are kept in the cloud. Companies cut costs by outsourcing data storage tasks.

But is there a dark lining to the cloud? While this lofty world holds much economic promise and consumer benefits, it also raises new challenges for policymakers. Consumers who store data in the cloud risk losing control over their photos, contacts and emails. Data is whirling around the world: a UK resident who creates an online personal agenda could use software hosted in Germany that is then processed in India, stored in Poland and accessed in Spain.

The European Commission takes data protection and privacy very seriously. Data protection is a fundamental right in the European Union. We have rules on how data should be protected so users know what they are signing up to when they use social networking sites. The cloud's security is essential for consumer confidence.

The EU's data protection rules are more than 15 years old. They have stood the test of time, but now they need to be modernised to reflect the new technological landscape. The Commission is reviewing ideas from consumers and businesses on how to move forward. As the EU Commissioner in charge of data protection, I will propose changes to the 1995 Data Protection Directive later this year.

One idea is “privacy by design” – building privacy-enhancing technologies into products and services. Data protection is a “must have” feature for individuals and society in general. A cloud without robust data protection is not the sort of cloud we need. These features should be well-integrated in the design of cloud computing products and services, from the very start of the business processes. This is not about giving an unfair advantage to European companies or holding back cloud computing in Europe. The real winners will be those manufacturers and service providers – no matter where they are from – that understand the competitive advantage of having built-in privacy features.

The underlying approach should be a “cloud-friendly” environment. But a cloud without clear and strong data protection is not the sort of cloud we

need. Having cloud-friendly rules can only help technology companies – many of which in Europe are small businesses – to know exactly what is allowed and what is not. This may mean simpler, harmonised measures, such as the registration forms for notification purposes. We also want to encourage self-regulatory initiatives. Codes of conduct or codes of practice like the "binding corporate rules" for international data transfers are good solutions.

Regulatory certainty is essential: companies must know what the rules are about the flow of data within the EU and at a global level. For example, the implementation of the EU's Data Protection Directive differs across Member States. We need to clarify when this reflects an unavoidable difference of culture and legal tradition, or when it is merely an avoidable obstacle to the rules of the Single Market. I plan to work with EU Member States and Data Protection Authorities to address this challenge.

As the centre of gravity in our digital world shifts from the desktop to the cloud, we also have to keep a careful watch over individuals' privacy and the right to personal data protection. In the cloud, personal data is processed and stored far from where a user lives. This raises important questions for policymakers. Who is in charge of protecting our information kept in remote server farms in the four corners of the globe and transferred from one to another in milliseconds? The cloud is borderless so the question of how to effectively protect our personal data online is also global. I call on companies to ensure that data is protected and secure.

Transparency must be ensured. Today's tech-savvy individuals need to be able to trust the internet to reap its full benefits. They need to be guaranteed control of their personal data, of the possibility to switch cloud providers easily, and their right to delete their personal data at wish: *the internet needs to learn how to forget*.

"The right to be forgotten" is not merely about deleting all data. Just like in real life, when you use web-based services, you cannot assume that no records exist of your past actions. What matters is that any data records are made irreversibly anonymous before they are used again.

We cannot afford foot-dragging in this area. As EU Commissioner for Fundamental Rights, I look forward to speaking with European and US companies in Davos later this week about our rethink of the general data protection rules in Europe. When considering policy for the cloud, our feet are firmly on the ground: the goal is to ensure that well-tested rules evolve naturally to serve the globalised 21st century.