



Workshop 3

Businesses, when data culture becomes a competitive advantage

The question of ownership of personal data is at the heart of this year's Forum d'Avignon. We heard earlier that the control of personal data is a strategic issue. That's true both for individuals – it is part of their digital identity – and for businesses, which now see capturing, using and unlocking the value in data as crucial to their development.

Data control is critical for the individual. The volume of personal data that is now collected, processed and stored makes it possible to know a great deal about each of us. It is possible to draw up a very precise profile and – depending upon the kind of data captured – develop predictive models that will reveal more about our religious faith, political opinions, lifestyle, sexual orientation, tastes, habits and many other intimate aspects of our personal life.

For businesses, the issue of confidence becomes even more critical when seeking to build a lasting relationship with customers. Companies must overcome all the doubts or fears that could stymie the development of data use as a lever for the creation of value for both citizens and companies.

#1 The law is not explicit about the ownership of personal data, but sets out fundamental data use ethics.

The law doesn't directly address the question of personal data ownership. Copyright, which contains an element of heritage, doesn't confer ownership rights over all personal information or data. It protects the way the data is structured and organized, but not the information contained. An exception occurs, however, when that information has protection in its own right, such as the titles of works of art protected by copyright, or when the information is part of a database protected by law sui generis.

In this context, on 9 September 2014 the Conseil d'Etat published a study entitled *Le numérique et les droits fondamentaux* (Digital technology and human rights), which rejects property law as the basis for regulation of personal data use (Proposal No 1). Instead, it favors the idea that the individual has rights over personal data, as in German law. According to the Conseil d'Etat, "*Recognition of ownership rights would be insufficient to balance the relationship between individuals and businesses and would complicate the state's regulatory function. Unlike property rights, the right to 'informational self-determination', a concept established by the German Constitutional Court in 1983, is a right of individuals whose effect is to 'guarantee in principle the ability of the individual to decide upon the communication and use of his or her personal data'*".

¹ For example, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 relative to the protection of individuals in respect of personal data and the free circulation of those data. OJEU 23 Nov., n° L 281, p. 31

² Harvard Law Review Vol IV, December 15, 1890, N°5, P 193

#2 How can ethical use of data be a competitive advantage for businesses?

At a time when privacy issues are a growing concern for citizens, more and more businesses take them into account in their customer communication, seeking to demonstrate their commitment to privacy. Legal considerations aside, compliance with regulations for protection of personal data is an effective way for companies to demonstrate their social and ethical responsibility. Implementation of best practice in respect of personal data protection unquestionably confers competitive advantage on companies in every sector but also protects against reputational risk.

Starting from the premise that it is cheaper to retain a client than win a new one, companies deploy strategies to maintain and sustain customer loyalty. These depend heavily upon confidence, which can only be built and maintained by taking into account the two fundamental values of knowledge and

It is the concept of a right to the protection of personal data¹ which gives the individual legal means to control how his or her data are used. Those who hold data have duties to the individuals whose data they hold, and face penalties if they fall short. These duties cover transparency, information, protection, confidentiality, and data deletion.

As long ago as 1890, two American academics, Samuel Warren and Louis Brandeis, published an article in the Harvard Law Review² entitled *The Right of Privacy* which drew upon the common law concept of implied trust. This concept requires the receiver of confidential information to protect the interests of the person entrusting him or her with that information - that is, to use the information in the interest of the provider, and not in his own interest.

This notion of implied trust, inspired by Roman law, is more relevant than ever because it makes those holding data about others the guardians and protectors of the data. But it does not prevent the holder profiting from the data, because the very purpose of the trust mechanism is to enable the owner of an asset to entrust it to a third party so that another can benefit.

These rules, no matter the legal system on which they are based, contain the concept of trust. The data are shared on the assumption that their use will respect the interests of those whose personality they reveal - a concept reflected in the need for consent or to inform, as well as in the concept of trust. The aim is to establish ethical rules to win and sustain the confidence of the individual whose personal data will be used by a third party.

recognition. Knowledge includes the customer history. That is, his or her interactions with the various arms of the business, as well as product information. Recognition is the personalized response of the business to the customer: you have to know your customer to provide a targeted response or anticipate his or her wants.

Two factors have strengthened consumer expectations in respect of trust and transparency. One is the constant evolution of technology over the past decade. That is compounded by the excessive gap that still too often exists between companies' data protection commitments, whether voluntary or obligatory, and the reality of data use. Companies that respond to consumer expectations will enhance their credibility. We see this with our clients, who frequently ask us, in Europe and around the world, to help them define and implement best practice in personal data protection compliance. Typical initiatives include certificated audits, adoption of binding corporate rules, coaching of data privacy officers and embedding privacy by design.

#3 No substantive data ethics without a data culture

Data ethics must be based upon behavior, hence the importance of developing a data culture. This can serve several goals, which sometimes converge and at other times conflict. Companies will seek to grow market share, by accelerating the transformation

#4 From data culture to data governance: practices and regulatory changes in Europe

The aims of those involved in data culture vary, but are all linked to governance. The ethical regulation of data will be based upon technical and legal tools enabling individuals, citizens and consumers to retain control over their data.

On the legal front the European Commission, promoting stricter rules on data protection, has taken the initiative. A draft regulation under discussion, intended for implementation in 2017, aims to bolster consumer confidence in online services and use of digital technologies more widely, and simultaneously underpin the single European market.

The challenge for businesses is now to structure their data management around regulation, security and certification, as means to strengthen confidence and thus enhance value, performance and differentiation. Future European regulations will add two new fundamental requirements to the fundamental principles set out in Directive 95/46 and will transform business practices. These are the principle of data minimization and the new principle of accountability, which will impose on a business the obligation to justify the internal mechanisms put in place to ensure compliance with digital technology and freedom regulations. A business will not only have to respect the law, but set out and document what it does to ensure ongoing compliance.

³ Isabelle Falque Pierrotin, « Data la nouvelle ruée vers l'or », Enjeux Les Echos, March 2013

#5 Data culture is also knowing how to share, to avoid the emergence of natural monopolies

Analysis of big data provides a return on the investments of data-collecting businesses, but also spurs growth in data available which in turn enhances the quality of the information obtained and the power of these same businesses. This process creates high barriers to entry and raises the profile of the dominant business or businesses.

of the internet user into online shopper, reader, or brand ambassador, but also by improving data security to reassure the customers who entrust them with their data. The data protection regulator, as guardian of personal freedoms, will see data culture as a way to enhance conformity with the rules.

This proposed regulation will oblige businesses to build compliance with data protection law into their operations. Keen to simultaneously enhance customer loyalty and benefit from the digital revolution, companies must henceforth be able to show that they have implemented tools and procedures enabling them to provide legal and operational protection for data entrusted to them by employees, customers, suppliers and others. That will enable them to contain their exposure to penalties which will be significantly enhanced (the latest version of this draft regulation foresees fines of up to 5% of worldwide turnover).

Investment in data management and compliance with the regulatory framework is becoming unavoidable, but this investment should confer an advantage on those who get on with it. It should help develop a climate of confidence that will enable companies to arm themselves against reputational risk, at a time when informed consumers are well aware of the privacy failings of social networks.

“If companies want to build lasting innovation which won't be rejected by users, they must guarantee that personal data will be protected. It's not a cost, it's an investment.”³

By using data in ways that respect the law and ethics, businesses using personal data will be able to develop and durably promote their expertise.

In such situations, markets are generally rebalanced in either of two ways:

- ▶ Regulations are introduced to force the dominant player to share his key asset and facilitate competition;
- ▶ The risk of declining confidence can cause users to switch to more agile rivals, who sometimes use disruptive technologies.

An ethical data culture then becomes essential for these new competitors, conferring an advantage and protecting them until they in turn become market dominant...

Ernst & Young Société d'Avocats

EY Société d'Avocats is one of the French leading firms in tax and law. Through our membership in a global organization, we put our expertise to serve a sustainable and responsible performance. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

Ernst & Young Société d'Avocats
Registered with the Hauts-de-Seine Bar (France)
Member of Ernst & Young Global limited

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 Ernst & Young Société d'Avocats.
All Rights Reserved.
Photos: © Gettyimages

Studio EY France - 1409SG114
SCORE France N° 14-045

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and it is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey-avocats.com

Contacts

Fabrice Naftalski

Attorney at law Partner, Ernst & Young Société d'Avocats
EMEIA Head of IPIT Law Practice / CIPP/E, CIPM & EuroPrise Legal Expert
Tél. : +33 (0)1 55 61 10 05
E-mail : fabrice.naftalski@ey-avocats.com

Bruno Perrin

Partner, Ernst & Young et Associés
Telecom Media Technology Leader in France
Tél. : +33 (0)1 46 93 65 43
E-mail : bruno.perrin@fr.ey.com

Louisa Melbouci

Marketing Manager – Telecom Media Technology
Tél. : +33 (0)1 46 93 76 47
E-mail : louisa.melbouci@fr.ey.com