March 2012

Antonio Viñal & Co. ABOGADOS

AVCONEWS #4

• BARCELONA • LISBON • MADRID • MILAN • ISTANBUL • VIGO •

THE NEW EU DATA PROTECTION PROPOSAL: GETTING READY WITH THE SPANISH EXAMPLE

Wouldn't it be nice...

...if all 27 EU Member States were binded by the same rules on data protection, instead of having to cope with 27 different laws? Till now, non-EU companies with EU subsidiaries or branches have dealt with this situation in two different ways: 1) complying with the requirements pursuant to each local law; 2) establishing one set of rules throughout from their European head office. The first option is costly and time-consuming; the second one, a recipe for disaster.

The present situation derives from Directive 95/46/EC, which all EU Member States transposed into national law. While a certain degree of harmonization is assured by this method, it also leaves space for each national Parliament to decide on how to implement its provisions or even to incorporate new ones. As a consequence, all 27 legislations vary greatly on certain issues and define different standards of security measures or impose different fines for non-compliance.

However, the new proposed legislation adopts the form of a Regulation, which is directly enforceable in any EU Member State. This will undoubtedly simplify formalities and reduce expense, but a change of this nature raises a relevant question: what will happen with the rulings issued by each of the national Data Protection Authorities (DPAs) and the jurisprudence of the national Courts?

And more importantly still: how should companies prepare? In this update we'll compare the new issues introduced by the proposal with the present situation in Spain. Companies

THE NEW EU DATA PROTECTION PROPOSAL: GETTING READY WITH THE SPANISH EXAMPLE

that already process data in Spain will ensure a smoother transition, as many aspects of the proposal are already covered by the Spanish legislation.

Help me, Rhonda

So which are the new issues companies have to look out for?

1.- New or modified definitions. The Regulation modifies or introduces several definitions that can affect companies in many ways. Specifically, companies that collect health related data should pay special attention to such definitions as "genetic data" or "data concerning health"; multinationals should know which is their "main establishment" and whether they have to appoint a "representative".

2.- Consent. The question being not only how to obtain it but ensuring that it is given freely. Furthermore, the proposal expressly states that the controller shall bear the burden of proof of such consent.

3.- Rights of data subjects. The Regulation allows data subjects a greater control over their own data, including the obtaining of a copy of such data and strengthens the right to be forgotten, especially in the online environment. As regards the exercise of the data subject's rights, it also establishes a one month deadline for controllers to inform data subjects on whether action has been taken.

4.- Designation of a representative. This is mandatory for companies not established in the EU but which process data of subjects residing in the EU, with several exceptions (i.e., the company is established in a third country that offers an adequate level of protection according to the Commission, or it employs less than 250 people).

5.- Data breaches. Companies now have to notify data breaches to their DPA within 24 hours of becoming aware of it and to the data subject "without undue delay".

6.- Data protection impact assessment. Companies that carry out activities that present specific risks to the rights and freedoms of data subjects shall carry out an impact assessment. The Regulation defines these activities as relating to the analysis and prediction of a natural person's economic behavior or health; information on sex life, health and race; monitoring publicly accessible areas; processing genetic, biometric or children's data.

7.- Appointment of a data protection officer (DPO). Such appointment is mandatory when companies have 250 employees or more, or when the core activity consists of systematic monitoring of data subjects.

8.- International data transfers. The Regulation acknowledges binding corporate rules, which are presently

THE NEW EU DATA PROTECTION PROPOSAL: GETTING READY WITH THE SPANISH EXAMPLE

not accepted in every EU Member State.

9.- Creation of the European Data Protection Board. One of its principal tasks to will be "ensure the consistent application of the Regulation", which will affect in no small way the powers of national DPAs and their rulings and interpretations so far.

10.- Remedies, liabilities and sanctions. Data subjects can lodge complaints with any national DPA and seek judicial remedy before the Court of the Member State where the company processing its data has an establishment or where the data subject resides. Another significant change is the sharp rise in sanctions, which can now reach up to € 1,000,000 or 2% of worldwide turnover in the case of an enterprise.

I know there's an answer

So the all important question at this stage is: how do we best prepare for these changes?

Companies already processing data in Spain may have a partial answer to this due to the specific requirements of the Spanish Data Protection Act. Let's take a look at the relevant points introduced by the regulation and see how they compare to the Spanish Act:

1.- Data breaches and data protection impact assessment. Data controllers in Spain must have a Code of Practice (CP) laying down the rules and standards with regard to security measures. All employees must acknowledge its existence and abide by its rules. Depending on the type of data processed the CP will include stricter security measures, such as relevant procedures in case of a data breach. Likewise, biannual data protection audits are compulsory in certain cases.

2.- Appointment of a DPO. Again, such an appointment is already mandatory when processing certain data.

3.- Binding corporate rules. These are already acknowledged by the Spanish DPA.

4.- Liabilities and sanctions. Sanctions are amongst the highest in Europe, and can reach up to € 600,000, ensuring a higher degree of compliance, or at least a greater worry over data protection than most European countries.

So to summarize things up, it might not all be "good vibrations", since it remains to be seen to what degree the new requirements will be offset by the savings afforded by a single piece of legislation. It is clear, however, that companies will have to rethink their approach to data protection, especially their security measures and procedures. And if your company is already active in Spain, you might want to look at how well you're complying there as you might find some useful tips.