11

IBM Position on the proposed data protection regulation

IBM welcomes the Commission's ambition to create a single, harmonized and modern set of data protection rules for the single market. By creating conditions for both privacy and innovation to flourish, a revised EU data protection framework that is robust, balanced and future-proof could boost economic and social growth. Crucially, however, privacy and competitiveness do not present an "either / or" choice. Rather, Europe has an historic opportunity for global leadership with a regulation that both renews its commitment to privacy and embraces innovation.

The current draft regulation fails to grasp that opportunity. Rather, it takes a step backwards for competitiveness at a time of economic crisis. Newly proposed obligations are too vague or too complex to be properly understood – or complied with. New constraints on implementation would remove the flexibility European businesses need to innovate and thrive. Nor are IBM's concerns limited to the information technology sector in which we participate. Rather, we are concerned about the draft's consequences for all our clients. Today, every sector -- finance, insurance, logistics, media and advanced manufacturing – must make efficient use of technologies and data to compete in a global economy.

The failings of the current draft appear to stem from an overriding concern with the world of social media. The issues raised by social media are, of course, important; however, draft's proposed solutions have broad and serious consequences for technological innovations of many kinds, on the one hand, and on established means of providing IT services on the other. Many requirements are overly prescriptive, which undermines technological neutrality and fails to take into account differences among business types and models. Other requirements are entirely vague, such as those in the many areas of "delegated acts." Most fundamentally, the regulation fails to balance the legitimate interests of people and businesses *of all sectors* or take into consideration the contexts in which data is processed.[1] In sum, the draft's rigid approach to protecting data privacy threatens Europe's ability to address its most difficult societal and economic problems.

General Observations

Harmonisation is good, but not at any cost. Industry recognizes the benefits of greater harmonization. In fact, it has called for more harmonisation for many years. In this draft, however, these benefits are outweighed by the administrative burden and subse-

[1] The right to data protection is not an absolute one but needs to be balanced with other freedoms and benefits, e.g. freedom of expression and communication, the right to protect intellectual and other property, the rights to pursue scientific and social progress, and the right to run a business. European Union Agency for Fundamental Rights, http://fra.europa.eu/en/theme/data-protection-privacy.

quent costs the draft regulation would impose on business. Much of this burden, in our view, fails to actually increase the protection of the user.

A balanced and effective approach to privacy takes risk into account. The draft regulation assumes that "one size fits all." That is, it does not appropriately recognize the importance of context and how it affects potential consequences to users. All data are not equal; nor is all processing. Yet the draft fails to make meaningful distinctions. As an especially problematic example, Article 4 of the proposed Regulation substantially extends the scope of data covered by the existing Directive. As a result, all obligations of the Regulation would apply to this very broad category of data, irrespective of the context of the data processing or its purposes. By overburdening individuals and organizations, this regulation will endanger Privacy by courting widespread flouting of an overbroad law.

European industry needs for legal certainty and predictability: The current legal framework[2] has been in place for the last 17 years. We, and presumably the drafters, anticipate the new framework will last for a similar period of time or even longer. The shift from a directive to a regulation removes the availability of national courts to review and interpret the regulation. The final text must, then, provide for a high degree of legal certainty and predictability. With its [49) delegated and implementing acts, the draft does anything but.

Especially where sanctions are potentially large, regulators need discretion to make them appropriate: The draft's "one-size-fits-all" approach would apply the same large monetary sanctions to all violations regardless of their severity, the culpability of the violator, or the harm to individuals. In some cases, other sanctions, such as specific performance, may be more effective and appropriate than fines. Moreover, the level of sanctions considered, inspired by competition law, is prohibitive. Data Protection Authorities need to have discretion to enforce based on the facts of each case.

On Administrative burden

The European Commissioner estimates that, once implemented, the new data protection regime will save industry 2,3 billion each year. This assessment fails to take into account the additional burden and costs imposed by new provisions. Rather, our own assessment suggests that costs for business will increase dramatically for the following reasons:

- The range and specificity of detail required in new obligations, including new requirements for documentation, will create significant and needless burdens. These requirements need to be flexible to address different business models and levels of data risk for different businesses.

- The draft's approach to Data Protection Impact Assessments present a major burdens for business. Their content and scope, and the need for prior notification or approval will needlessly increase cost and unduly impede both innovation and the timely provision of services.

---

2 1995/46/ Directive

- The scope of the definition of breach and associated notification requirements, especially the concepts of notification within a reasonable timeframe, mitigating effects of safeguards (encryption, etc) and potential for harm or adverse impact will pose issues of practicability and undue burden. This burden extends not only to business but also to the regulators and data subjects who will be subjected to a constant stream of notifications about "breaches" that pose no significant risk of harm.
- The draft regulation would impose a significant new burden on employers across the EU with respect to processing of employment data. The proposed consent provisions will prevent or substantially impede the legitimate processing of employee data (e.g. salary, pension plan, skills and training, leave benefits). Business in Europe will be substantively disadvantaged in competing globally and employees' opportunities for advancement diminished by these unworkable restraints. Article 82 further undermines the regulation's aim of harmonization by allowing member states to introduce additional domestic rules on employment data. Instead of a unified approach employers will face a maze of complexity from 27 additional regimes.

On Processor/Controller relationship

The current legislative framework clearly distinguishes between the role of a data controller and that of a data processor. The draft regulation would fundamentally change this concept – and inject confusion into well-settled contractual relations – by establishing joint liability between all data controllers and data processors. Freedom to negotiate between contractual parties is a firmly established principle and practice throughout the European economies. Where obligations are directly imposed on the processor by law, the processor can no longer rely on the controller's assertions related to the nature of the data (which may not, in fact, be accessible to the processor) and will thus have a need to "know" the data subject. Furthermore, the processor may be less willing to accept the controllers' processing requirements as sufficient based on their interpretation of their obligations to secure the data. This blurring of lines between the two parties' roles would impose unnecessary additional burden and render current business practices impossible. The clear roles under the current legal framework should be maintained to avoid confusing established consumer relationships and posing new impediments to jobs and growth.

On Analytics

Today data is generated from all kinds of sources and activities, from the digitization of traditional business records to entirely new kinds of data generated online or by sensors embedded in products and infrastructure. At the same time, advances in mathematics and technology make it possible to extract more predictive insights from such data. Together, these accelerating trends create new and powerful opportunities to address important societal and business challenges. Some examples: While individual research institutions can work for years on a cure for Alzheimer's, results come much faster when analytics are applied these institutions combine available data sets. Patient-centric health systems rely on abundant data that is accessible at multiple points of care and operations. That is the promise of today's business analytics: extracting insights from proliferating data to help individuals, organizations and entire societies get smarter.
IBM does not believe that realizing the promise of analytics requires the sacrifice of personal privacy. There is no greater threat to analytics than this short-sighted notion.

When analytics programs fail to protect privacy, they create distrust that harms both the organization responsible and of this emerging – and promising – technology.

However, we are concerned that the current wording of Article 20 of the draft puts legitimate use of analytics (or here profiling) at risk. Provisions relating to "profiling" should not prevent businesses from being able to evaluate and analyze data and use such data predicatively for legitimate business purposes, including identity verification and fraud detection and prevention.