International Chamber of Commerce
The world business organization

ICC comments on EU General Data Protection Regulation Issues

The following ICC comments deal with on-going EU Data Protection Regulation matters relevant to related future discussions by the European Parliament and the European Council. The three points outlined in this paper represent specific points of the EU General Data Protection Regulation that raise concern among global business. ICC aims to provide recommendations for improvement of those. ICC likely will have further comments in the future. The language in the Regulation proposal is currently in the process of modification, and while these ICC comments reflect the European Commission proposal available at this time, they should also be relevant to conversations of proposed amendments in the future.

The EU General Data Protection Regulation (Regulation) intends to replace the 95/46 Data Protection Directive (Directive). The Directive always had two main purposes 1) Protecting the right to privacy of natural persons, and 2) Making certain not to prohibit or restrict the free flow of data.[1] Furthermore, the first recital for that Directive references the objectives of the formation of the European Union, which include "ensuring economic and social progress by common action to overcome the barriers which divide Europe."[2] Subsequently, the dual purposes of protecting human rights, while also promoting innovation and economic progress, have been the defining goals of European Union data protection and privacy efforts for the last two decades.

These purposes are reflected as goals in the Regulation, but it is not clear the provisions of the document uniformly further both of those aims. We take as a starting point for our comments key objectives set forth in the recitals to the Regulation: a more effective and less administratively burdensome data privacy regulation that will allow for new business models while providing credible and accountable data protection, the responsibility for which is shared across stakeholders. We support those goals. Significant concerns arise, however, as we review the Articles which seek to implement those objectives.

A number of Articles merely transpose existing requirements of the Directive and some improve on the current state of the Directive. However, too often the proposal contains vague terms and consequently allows too much room for interpretation. In some cases this can lead to difficulty measuring the impact of the regulation on Controllers and Processers. One example of this lack of specificity is the many mentions of implementing and delegated acts. The lack of specificity in the subject matter leads to a lack of legal clarity in understanding obligations, while undue specificity in the Regulation will result in implementation challenges, given likely constraints on the flexibility needed to accommodate innovations in technology, business models and deployments. These constraints may also inadvertently hamper the development of small and medium-sized solution providers as they will often need to tailor their offerings to service niche markets.

Overall, the failure to provide legal certainty or clarity of requirements in a number of instances, compounded by the potential of limited flexibility of implementation, serves to disadvantage the EU in terms of global competitiveness by chilling innovation and weakening the ability to attract facilities and investment.

The problem is not the desire for credible, accountable and effective data protection, but rather the failure to provide details that allow obligations to be properly understood, coupled with constraints on implementation that limits needed operational flexibility. The balance of this paper highlights these

[1] 95/46 Directive, Article I, Sections 1 and 2
[2] Id, Recital 1

concerns as we address a number of issues in the Draft Regulation which are of specific ICC competence, including: 1.) The need for improved and streamlined methods to allow for international data transfers, 2.) A request for focus on reducing administrative burdens, 3.) Proposals for increasing harmonization to create a predictable set of rules and expectations. The focus on these three issues should not be interpreted as ICC support for other provisions in the Draft Regulation. There are many other issues with the document, which require study and thoughtful modification. This paper focuses on the above three categories of issues to bring specific focus to these areas of substantial concern for the global business community.

Finally, this paper calls out potential unwarranted burdens which might be imposed because of such lack of clarity and limited flexibility. These burdens will be costly to both business and the region in terms of out-of-pocket compliance costs as well as lost economic growth and commercial opportunity. . Not only may these unwarranted burdens needlessly increase costs or drive businesses away from the region, but the privacy benefits of these administrative burdens are suspect.

As we emerge from the worst recession since the great depression we must limit such needless economic burdens, maximize our ability to marshal economic growth, promote job opportunities and optimize commercial opportunity. We must also consider the potential impact of such regulatory constructs on Cloud Computing and other technology and business initiatives that can reduce cost, drive new markets, and benefit consumers.

International Data Flows/Transfers

Today's Information Society is global by definition. ICT-enabled commerce is its growth engine and data is the currency of the digital economy. Whether through Cloud Computing, Big Data or the Internet of Things, cross-border data transfers are an essential element of new technologies, business models, economic opportunities and societal interactions. For any nation or region to remain competitive – meaning it is viewed by the investment community as a desirable place to invest or do business – innovation must be allowed to flourish. This innovation is not just new technology, but also includes new business models and services based on global data flows. The ability to use and transfer data is a crucial factor in the EU's current and future commercial competitiveness and ability to attract global investment. As the EU considers a Regulation, it must do more to enable cross-border data flows in keeping with the needs of the information age.

Enabling international data flows does not mean diminished respect for privacy or the protection of data. It does, however, require more flexible and adaptable approaches, including finding new and appropriate solutions to address specific concerns in a narrowly tailored manner. The Regulation should implement compelling public policy, while limiting needless burdens or unintended consequences. This means removing bureaucratic hurdles to information flows. As industry, we have supported recognizing different mechanisms for privacy accountably; for example, broadening the concept of adequacy decisions to include more flexible negotiations with countries, regions or sectors to provide adequate protections for international data transfers. These more flexible agreements could provide reduced administrative burdens on organizations transferring data, while still providing a mechanism to enforce the requirements for processing the data according to the standards of the data protection regulation.

One need is to improve the current suggestions regarding the accountability-based transfer regime. This accountability model would allow controllers and processors to demonstrate they will subject themselves to certain commitments on the processing of the data, no matter where the data resides, without being overly prescriptive as to how. The concept of obligations flowing with the information has been established in Canada for years under the Personal Information Protection and Documents Act (PIPEDA) and has roots in the OECD Guidelines.

An accountability-based system should use some of the transfer mechanisms described in the Regulation, which include Binding Corporate Rules (BCRs), standard clauses and derogations. However, the Regulation should look to streamline and harmonize the notification and approval

requirements for Binding Corporate Rules and Model Contractual Clauses (MCCs) mechanisms, which would reduce the burden on companies while offering adequate levels of data protection. BCRs are currently too narrow in scope (applying only to intra-group transfers and to controllers), and too long and costly in their implementation to realize their full potential. Another effective mechanism to pursue is encouraging industry sector Codes of Conduct, which would operate at the global level in place of regional or sectoral-specific approaches. Such a Code of Conduct would allow any company in that industry to subject itself to the obligations in the Code, and then have the ability to transfer the data outside of the EU.

By way of an example, an approved BCR company may transfer personal data from an EU member state to its office in Australia. However, there is no provision to transfer data across different organizations when each has had its BCR certified. Each of these organizations has been found to have adequate practices and yet information transfers would require new proofs of adequate protection which, because they are redundant, add costs while adding nothing to the actual protection of privacy. As we consider the world of cloud computing and global trade, information transfers occur not only just within groups of companies in the same corporate family, or with their agents "processing" data on their behalf. New legal instruments must reflect those realities to enable the EU to capture the economies of scope and scale reflected by today's reality as well as access to new markets which these technologies and trading practices facilitate.

Administrative Burdens

We welcome the goal of making the framework more efficient by reducing the unnecessary administrative burdens, such as the elimination of notification obligations. Removal of such administrative burdens has the potential to result in more effective privacy protection as organizations working to comply can focus resources on managing personal data appropriately, instead of processing paper-work. However, the Regulation introduces several new and substantial administrative obligations that are not narrowly tailored to achieve compelling public policy objectives. These obligations will make the regulation less efficient and effective. These new obligations will likely increase burdens on the controllers and processors, and there is no demonstration they will increase privacy protection for the data subject.

One example of such an unnecessary documentation obligation is the requirement in the Regulation that all "processing operations" need to be documented by an organization. This obligation is ill-defined at the outset and risks creating unnecessary and overly detailed paper trails, which could impose substantial costs with no commensurate benefit. Instead of focusing on creating paperwork, we recommend the Regulation concern itself with outcomes.

Another example is the requirement for Privacy Impact Assessments (PIAs). PIAs are a useful tool as part of the accountability measures and are most effectively implemented when they allow flexibility for an organization to tailor the assessment to their particular organization and business processes. Mandating prescriptive PIAs could run counter to the many different methods organizations across the globe have put in place to assess privacy (and security) impact. As privacy risks are typically contextual and often technology-specific, this level of flexibility is important to create a dialogue between privacy compliance staff within companies, and the technologists and business people who develop the innovations that process personal data in new ways.

To make the PIA most effective, it is often integrated into existing product development processes. Also, as the PIA is a critical document to allow for an open and thorough conversation between lawyers, compliance staff and developers at a company, the Regulation should not create the burden of mandating companies to turn over the PIA to the supervisory authorities. Any such requirement to provide the PIA will likely result in the legal staff treating every PIA as a potential regulatory filing and create a chilling effect on the open dialogue necessary between product developers and legal staff for a robust PIA. This consideration of legal risk has the potential to create delay in the review process, and impede the ability of the privacy compliance staff to effectively design in privacy at the earliest stages in product/service/programme development. Such a requirement would also potentially have a

negative impact on intellectual property protection goals so critical to global competitiveness. Furthermore, the scope of potential requirements to file PIAs that could be subject to prior notification or approval is both overbroad and extensible through delegated acts and DPA lists. This lack of legal certainty and potential delay could negatively impact both innovation and investment. Even worse, as a result, the PIA may become detached from existing product development process, and hence lose its relevance and effectiveness in building in privacy protection mechanisms in the end product or service.

Industry supports a Privacy-by-Design principle as a necessary component of any accountability programme. However, organizations should have freedom to implement the processes which best fit their organization, and to implement them without concern that they will have to provide the process documentation to the supervisory authority. Mandating specific requirements around privacy-by-design is unlikely to be effective, given the broad application of the Regulation to various industries and sectors.

Bureaucratic documentation requirements, coupled with the potential for unreasonably large fines (based on revenue from business activity having nothing to do with the European Union) will have the effect of creating substantial disincentives for companies to bring new and innovative business opportunities to the European Union, while having limited impact on accomplishing the goals of the Regulation. Instead, the Regulation should focus on allowing the Data Protection Officer (DPO) the ability to put in place appropriate and accountable controls processes.

Harmonization

We support the European Commission's goal of enhancing the single market by increasing harmonization on data protection rules across the 27 Member States. A regulation is directly applicable in all Member States. It does thereby address one of the most obvious problems with the current legislative framework - the diverging implementations of the current 95/46 Data Protection Directive by Member States. In choosing the legal instrument of a Regulation, we would like to point to the importance of an instrument which should outline the rules in a horizontal and technology neutral manner. This horizontal instrument should not be supplemented by additional legal instruments focused on specific technologies or services as this would not provide the necessary legal certainty.

Another important modification necessary to help achieve technology neutrality is for the draft to clarify the relationship between the e-privacy Directive and the Regulation. Provisions in the two documents, including data breach obligations, are not harmonized. Therefore, there is a risk organizations may be subject to conflicting requirements and to different supervisory authorities. The relationship between the two documents should be clarified in the text.

Moreover, further work on the concept of "main establishment" could greatly assist in reaching the goal of allowing organizations the efficiency of operating in a single market. The introduction of this concept of a one-stop-shop for data protection issues will not only increase legal certainty, but also reduce administrative burdens, and create an incentive for DPAs to move to a mutual recognition model. However, the current language in the Regulation needs further clarification to ensure this one-stop-shop will actually work. Clarity is especially required in terms of how to apply the model to enterprises with presence in multiple jurisdictions.

One necessary clarification is further definition of how to determine an organization's "main establishment". One possibility to provide further definition is for the Regulation to provide specific criteria to determine the location of the main establishment. The Regulation should also clarify that the "main establishment" designation is available to organizations with headquarters outside of the European Union. Further, a "main establishment" should not be directly tied to the definitions of "Controller" and "Processor" in the Regulation. A large multi-national company may have a structure where there are many separate Controllers and where they may also act as a Processor, depending upon the organizational structure and type of business.

To realize its full potential, the concept of “main establishment” needs to allow a large corporate organization to look to one Supervisory Authority for guidance and interpretation of the Regulation across the EU. Any concerns between the Supervisory Authorities must be addressed with effective mechanisms for “Co-operation and Consistency” as described in Chapter VII of the Regulation. Large and diverse multi-national companies are expected to interpret the provisions of the Regulation to comply, while they are focused on their primary missions of innovation and economic development. It follows then that it is reasonable to expect the Supervisory Authorities, who are among the leading substantive experts in the world, to produce consistent and uniform interpretations so as to realize the goals of harmonization and predictability which can be fostered by a true one-stop-shop system. Crisp definition criteria, and focus on co-operation and consistency within the framework of the objectives of eliminating unnecessary burdens and fostering innovation and growth, can remove any concerns about forum shopping or a regulatory race to the bottom, and can drive substantial efficiencies for regulators and companies. Focus will also be needed to make certain Supervisory Authorities have sufficient resources to provide consistent and uniform implementations. Currently, Supervisory Authorities have widely varying amounts of resources and capabilities. A close examination will need to be made of each Supervisory Authority’s capacity to determine the extent to which they can fulfil the “main establishment” goals.

Work on the concept of “main establishment” should be undertaken with a view toward global inter-operability and alignment. The EU privacy structure needs to work with non-EU regulatory regimes to allow for efficient and effective international data transfer. Specific focus should be made by the Commission and Parliament to analyze how the Draft Regulation can assist this interoperability and alignment.

Conclusion

This Regulation creates a unique opportunity to promote economic development across the European Union while furthering shared goals of protecting privacy. Predictability in how organizations will process personal data can drive trust and confidence in participation in the digital economy. However, the revised draft does not fully take advantage of the opportunity for clarity. Instead, it runs the risk of creating greater uncertainty, which could decrease investment in the European Union and weaken competitiveness. We urge the European Commission, the European Council and the European Parliament to look specifically at language to provide more clarity for decreasing the burdens on international data transfers, reducing counter-productive administrative burdens, and promoting harmonization.

:-:-:-:-:-:-:-:-:-:-:-:-:-:-:

The International Chamber of Commerce (ICC)

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.
The fundamental mission of ICC is to promote open international trade and investment and help business meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the 20th century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rule setting, dispute resolution, and policy advocacy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice. ICC also offers specialized training and seminars and is an industry-leading publisher of practical and educational reference tools for international business, banking and arbitration.
Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on relevant technical subjects. These include anti-corruption, banking, the digital economy, marketing ethics, environment and energy, competition policy and intellectual property, among others.

ICC works closely with the United Nations, the World Trade Organization and intergovernmental forums including the G20.

ICC was founded in 1919. Today it groups hundreds of thousands of member companies and associations from over 120 countries. National committees work with ICC members in their countries to address their concerns and convey to their governments the business views formulated by ICC.

ICC Commission on the Digital Economy

Business leaders and experts develop and promote the continued and stable growth of the Digital Economy, and further adoption of its underlying ICT foundation, through regulatory advocacy of key business positions and best practices through ICC's Commission on the Digital Economy.

Through its members who are ICT users and providers from both developed and developing countries, ICC is recognized in expert circles as the global consensus voice for private sector expertise on policy matters that drive the Digital Economy. It also provides the ideal platform for developing global voluntary rules and best practices for this area of interest to companies worldwide. Dedicated to the expansion of secure ICT-facilitated trade, ICC champions the liberalization and regulatory harmonization that are required to achieve a free flow of information across all borders.

ICC led and coordinated the input of business around the world to the United Nations World Summit on the Information Society (WSIS), Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda through its initiative, Business Action to Support the Information Society (BASIS http://www.iccwbo.org/basis).

International Chamber of Commerce
The world business organization
Policy and Business Practices
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org