Data Security Council of India (DSCI)
Response to

A Comprehensive Approach on Personal Data Protection in the European Union

Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Region

The above approach from the European Commission addresses the new challenges for the protection of personal data based on the inputs received from various stakeholders during the 2009-10 when it launched the review process for updating the Data Protection Directive 95/46. In the above paper, EC highlights the key objectives of the comprehensive approach to data protection.

DSCI is pleased to submit its views on the following:

1. The Global Dimension of Data Protection (Reference – section 2.4)
   - Core data protection elements for international agreements
   - Improving and streamlining the current procedures
   - Clarify the adequacy procedures

Global Privacy Principles

DSCI strongly believes that there is a need of global privacy standards that focus on the core principles of privacy as against the bureaucratic, complex and cumbersome procedures being observed. The importance of Transborder Data flow in the globalized economy has increased dramatically. Almost every industry sector dealing with trade in goods and services make use of data flows. Rapid globalization of the world economy along with advancement in Information Technology allows companies to reap benefits through trade in services. Transborder Data Flow facilitates business process streamlining, improves market access, and maintains business relevance in fast-evolving business landscape.

*DSCI recommends* addressing of divergence in the regulatory approaches to reduce hindrances to the free flow of data. This should be aimed at reducing bureaucratic control, enhancing harmonization of global privacy principles, standards, and best practice codes that have bearings on Transborder Data flow, while addressing privacy and security concerns. Privacy requirements of countries can be addressed by such a global set of privacy principles and should not be constrained by local laws.
Binding Corporate Rules | Improving and streamlining the current procedures

Extending BCRs to Service providers

Global data flows are the norm as can be seen from a number of scenarios. Multinationals operating across the globe transfer data of their customers, suppliers, and employees through a mutual recognition of BCRs as provided by European Commission to Data Controllers. However, we believe that the concept of BCRs applicable to MNCs should be extended to service providers as well. Whether they are e-commerce, banking, travel, hospitality or IT/BPO service providers, they should be treated as a global service provider, who should declare their BCRs. Much the same way an MNC can demonstrate and ensure data privacy accountability, service providers will be able to demonstrate.

**DSCI recommends that the facility of Binding Corporate Rules should be extended to the global service providers**

Adequacy assessment | Clarify the adequacy procedures

DSCI recommends review of adequacy assessment from the one based on privacy law conforming to EU Data Protection Directives to more encompassing and flexible, which respects the legal evolution for data protection in the third countries. It should be limited to adhere to the core principles of data protection rather than a similar legal framework.

**Encompassing and flexible adequacy assessment**

Indian Govt, recently, amended the Information Technology Act, which has a section protecting sensitive information under lawful contracts. The cap on the compensation has been removed, making organizations accountable for maximum possible liability for failure to protect the information. These provisions promise the required protection to data travelling to India as a part of outsourcing.

**DSCI recommends that the adequacy norms should be flexible to qualify for this kind of legal steps taken by third countries, reflecting the legal culture of respective countries while assuring the protection. If there are national laws that enforce the implementation of security practices for protecting personal information, with punishments for non-compliance; and recognize the importance of contracts for the same, such legal frameworks should be deemed to be adequate.**

Secondly, the adequacy norms also take the self regulatory initiative of industry into the account. DSCI, an industry initiative set up by India IT and BPO industry through NASSCOM, is establishing itself as a Self Regulatory Organization for data protection. DSCI, with its Privacy Framework (DPF), recommends privacy principles and advocates privacy practices. It is in the process of establishing assessment of practices followed by service providers.

**DSCI recommends that the availability and strength of such SROs should be factored into the adequacy assessment and should be recognized by the adequacy assessment process.**
2. Self Regulatory Initiative and EU Certification Scheme  
(Reference – section 2.2.5)

Self Regulation

DSCI strongly believes that recognition of self regulatory initiatives of data controllers by European Union balances the interest of business while assuring privacy. It is an effective way of enforcement of data protection rules. Self regulation enabled by organizational, sectoral, functional, technological and professional codes address specific, granular and dynamic requirements of technology enabled transformation. It represents managed compliance approach rather than strict legal enforcement based approach. However, DSCI feels that the acceptance of self regulation should also consider the self regulatory initiative of service provider (data processor) industry. This way the dynamism of privacy protection will be ensured in complexity of current business practices characterized by global sourcing. The universal principles of privacy, adherence to best practices, due diligence for privacy, privacy impact assessment, adoption of privacy enabled technologies and inculcating ‘privacy by design’ in organization's culture should be promoted by the self regulatory initiative. The self regulatory initiative should be in a position to evaluate the practices adopted by the industry and empowered to take the corrective action in case of any compromises.

DSCI Privacy Framework (DPF) and DSCI Security Framework (DSF) evolved by Indian IT and BPO industry have the potential to qualify as an industry code. DSCI believes its security and privacy practices expand the measures prescribed under the model contractual clauses and will like the European Union to recognize these frameworks for data processors. This will provide an additional layer of comfort towards the protection of data flows. DSCI has been evolving a mechanism to provide independent assessment of service providers (data processor), which will further augment the comfort.

*DSCI recommends that self-regulation of service providers, through an independent SRO like DSCI, should be accepted by the European Union to enable global data transfers without any hindrance.*

Privacy Certification / Seal

The commission’s recognition of the need for privacy seals for ‘privacy-compliant’ processes, technologies, products and services is a welcome step. This will enable the data subject’s capability to take a trust decision while performing electronic and physical transactions. However, DSCI believes that the coverage of the privacy certification and seal should be extended to match the global nature of transactions. It can rely on the self regulatory initiative of the industry for certifying, rating or providing a seal to a process or service.

DSCI believes that its endeavor for improving privacy culture and practices of service provider industry through its privacy and security frameworks, practices and its ability to evaluate service providers will enable it to partner with any mechanism Commission proposes for certifying, rating or providing a privacy seal.

*DSCI recommends that the mechanism for privacy certification or seal should take help of the self regulatory initiatives of both data controller and service provider industry in order to extend the coverage to global data flows.*
3. Enhancing Data Controllers’ Responsibility
(Reference – section 2.2.4)

DSCI agrees with the proposal that Accountability should form one of the privacy principles, and that the appointment of data protection officer and privacy impact assessment should be made mandatory. DSCI Privacy Framework (DPF) includes Accountability as one of the privacy principles, among others.

DPF focuses on a set of best practices that include privacy impact assessment too. Service providers, implementing the privacy principles through the best practices approach promoted by DPF, will be able to provide data protection assurance to their clients, namely data controllers. A number of implementations have demonstrated that DPF along with its data-centric methodology identifies privacy risks, which are then addressed through the best practices.  

**DSCI recommends** that Accountability be included as one of the privacy principles as it will make data protection more effective without placing administrative burden on data controllers.
**DSCI engagement with EU**

Data Security Council of India (DSCI) has engaged with the European Union during the last 2 years and responded to its earlier notices. The following submissions have been made by DSCI:

1. To AEPD, Spain prior to the Privacy Commissioners Conference in November, 2009 on extending of BCRs to the service providers. Response was sent in July 2009
2. The questionnaire in so far as it related to international data transfers to third countries was submitted to the EU in August 2010

**About NASSCOM**

NASSCOM is a global trade body with its seat in India and over 1200 members focusing on software products and services, of which over 250 are global companies from the US, UK, EU, Japan and China. NASSCOM has been instrumental in maintaining India’s leadership position in the global offshore IT-BPO industry, by encouraging its members to build and uphold highest standards in particular with regard to data security concerns.

**About Data Security Council of India (DSCI)**

Data Security Council of India (DSCI), a section 25 not-for-profit company, was setup as an independent Self Regulatory Organization (SRO) by NASSCOM, to promote data protection, develop security and privacy codes & standards and encourage the IT/BPO industry to implement the same. DSCI has developed Best Practices for Data Protection that are in line with global standards and cover emerging disciplines of security and privacy. While its immediate goal is to raise the level of security and privacy of IT and BPO service providers to assure their clients and other stakeholders that India is a secure destination for global sourcing, DSCI also promotes these best practices for domestic industry segments like Banking, Telecom and E- governance.

**For further information, please contact:**

Dr. Kamlesh Bajaj  
Chief Executive Officer  
DATA SECURITY COUNCIL OF INDIA (DSCI)  
3rd Floor, Niryat Bhawan | Rao Tula Ram Marg | New Delhi - 110057, India  
P: +91-11-26155071 | F: +91-11-26155070 | M: +91-9910501633  
E: kamlesh.bajaj@dsci.in