Data Security Council of India
Position Paper
AEPD Joint Proposal for a Draft of International Standards
On the Protection of Privacy with regard to
the processing of Personal Data

In light of the upcoming meeting of the AEPD Working Group on the above proposal on June 11, 2009, the Data Security Council of India (DSCI) is delighted to share its views with the Working Group Members on the proposed EU International Standards.

1. AEPD WG brief for the June 11 meeting

It is understood that the WG will consider the following:
- Clarify the role of document
- Review controller/processor notions
- Review filing system
- Reduce bureaucratic requirements
- Set accountability principles
- Adapt concept of sensitive data
- Promote international data transfers, if recipient offers an adequate level of data protection
- Inform individuals of security breaches
- Broaden supervisory authority concept
- Enhance international cooperation
- Encourage proactive measures
- Analyse relevant law

⇒ DSCI would welcome clear rules and standards on outsourcing, international data transfers, and the role of self-regulatory organizations

2. Outsourcing and International Data Transfers

It is good to see a clear message that outsourcing of processing by a responsible person or entity is an organizational decision; hence it will not attract application of openness principle, and will not require consent of data subjects.

The document accepts that “the establishment of a uniform framework to regulate international data flows must be considered one of the essential aspects in setting international standards”. But then it goes on to state (para 14 Explanatory Note) that data can not be transferred to States where those principles, rights and guarantees, i.e. establishment of a level of privacy protection similar to that of these standards, are not respected. However, in the next para it states that “as these standards refer not only to States, but also to organizations, this reference must be understood to refer to the provisions contained in Part VI of the standards, as there may be the case that, even when the laws of the State where the receiver of the international transfer is established do not provide similar guarantees to the standards, these guarantees might be offered by that recipient by virtue of agreements entered into with the transmitter of the information, or through binding corporate rules.”

It further states that as per this standard, the level of data protection in the recipient State should be “similar”, and not “adequate”, “equivalent” or “equal”. This is a positive development. The responsible person or entity transferring data will be required to verify the level of protection foreseen
in the destination State or organization. However, in addition the supervisory authority too is required to analyze the concurrence of these requisites in the destination State or organization.

This ends up nearly retaining the status quo. Verification of “similarity” of data protection in the recipient organization by the responsible person or entity is not enough; supervisory authority too has to analyze the concurrence of these requisites in the destination organization.

➤ **DSCI welcomes the improvements in the Standards, but recommends the following additional points for inclusion:**

1. Once a responsible person or entity/independent body verifies that the level of protection by the recipient in the destination State is similar to that in his own State, there should be no need for the supervisory authority to verify the same. International data transfers should begin.

2. Countries with data protection laws and/or rules should be recognized as ensuring an adequate level of protection of personal data. Current system for assessing third countries is too cumbersome and lengthy – it verifies the equivalence of a third country law with the Directive. Even with “similar”data protection instead of “adequate”, supervisory authorities are required to verify that recipient affords data protection. This should not be the case.

3. What would be the new position of supplier organizations based outside EU ?. Currently termed as ‘inadequate’ country, there are provisions made by way of standard contractual clauses to facilitate cross-border data flows involving personal data. Will the more generic requirement of “recipient affording a similar level of protection to that one provided in the document” as mentioned in 14.1, ease the cross-border data flows?

4. Para 13 on Provision of services may be made more explicit by stating that responsible person or entity/independent body may obtain assurance (for example, an auditor’s report), contractual obligation, or other representation (for example, written annual confirmation) to ensure that the supplier guarantees a level of protection similar to that contained in this Document.

3. **Self-Regulatory Organizations (SROs) – Role clarification**

Part VI on Compliance and Monitoring encourages States to promote better compliance with applicable laws on data protection through proactive measures and monitoring. The proposed proactive measures include the implementation of procedures to prevent and detect breaches; appointment of data protection officer with powers for exercising supervisory functions; training programs for members of the organization for understanding the applicable laws of data protection; conducting of independent audits to verify compliance on the applicable laws on data protection; including the design of secure systems that protect privacy of persons; implementation of privacy impact assessments.

Regulatory/supervisory authorities of administrative nature are expected to be created, in keeping with these standards, which are impartial, and independent. Self-Regulation systems can also be established as provided for in para 22 of the Explanatory Memorandum. Self-Regulatory Organizations (SROs) are, however, expected to exercise authority, the fulfillment of which should be mandatory for those who submit to their jurisdiction to seek settlement by invoking alternate dispute resolution process(es), namely, mediation, conciliation or arbitration under obligatory or voluntary terms. Authorities are expected to resolve claims, and complaints of data subjects at no cost.

➤ **DSCI welcomes the acceptance of self-regulation in the standards; but it seeks clarification as to whether SROs, if responsible for all these programs in a country, and if they fulfill the criteria of impartiality and independence, and enforceability; will be treated at par with statutory regulators by EU?**

➤ **While provision of service for a claim or complaint may be free to a data subject; an SRO should be free to charge a fee for dispute resolution between responsible person or entity and a service provider.**
Whether EU would accept online dispute resolution (ODR) mechanism, if implemented by SRO?

4. **Best Practices approach as a route to data security – BCRs for service providers**

DSCI considers the best practices approach as a practical and realistic way to enhance global adherence to data security standards. As such, DSCI advocates the mutual recognition of BCRs: if BCRs have been approved with regards to compliance requirements then they should be universally accepted. DSCI notes with satisfaction that the Article 29 WP adopted this recommendation in its meeting early this year.

DSCI believes that in today’s globalized world, 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, employees including their personal data. Social networking sites like Myspace, Facebook, Orkut etc store personal data of all signed-up users, with their data being in any of their data centres across the globe. SWIFT and IATA members retain financial and travel related data of customers, that contains personal data, in any of their data centres anywhere in the world. E-commerce transactions, google searches, amazon and ebay purchases all require personal data. And it is provided by individuals if they want to avail of the services provided by sites. Cloud computing with its attendant cost benefits provides services to customers from anywhere in the “cloud”. So, personal data of any country’s citizens is spread all over. **Hence, approach to data protection has to be based on a different paradigm** It is pointed out that in coming years technology would overwhelm the “adequacy” norm.

We believe that the concept of BCRs applicable to MNCs should be extended to service providers too. Whether they are e-commerce, banking, travel, hospitality or IT/BPO service providers, they should be treated as global service providers 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 the same. They may be required to follow the same process of approval as that for MNCs, as per the revised guidelines of Article 29 WP recommendations, and be then universally acceptable throughout the EU.

An MNC can implement BCRs to show compliance with the data protection requirements of a country in the EU - irrespective of where it is processed. Likewise, it should be possible for a service provider located in a non-EU country such as India to demonstrate compliance with data protection requirements of an EU country where the client is located, and/or where the data is originating, by following the best security and privacy practices and standards. Proper protection and privacy should be based on the tenet of best practices, in the form of BCRs, followed by service providers.

DSCI recommends that the concepts of BCRs should be extended to all service providers. They should be treated as global service providers who should declare their BCRs, which should be subject to the same process of approval as afforded to MNCs.

DSCI believes that the focus should be global rather than provincial.

5. **Accountability Principles – providing business with clear and simple rules**

APEC has defined **Nine Privacy Principles**, which enable accountability in the flow of data while preventing impediments to trade. They include the following principles:

1. Preventing harm
2. Integrity of Personal Information
3. Notice
4. Security Safeguards
5. Collection Limitations
6. Access and Correction
7. Uses of Personal Information
8. Accountability

APEC’s approach puts emphasis on the practical aspects of data flows. At the moment, APEC undertakes the so-called Data Privacy Pathfinder project, which aims at promoting consumer trust and business confidence in cross-border data flows. It includes the support to business needs, reduction of compliance costs, providing consumers with effective remedies, allowing regulators to operate efficiently, and minimizing regulatory burdens.

DSCI suggests that this practical approach by APEC may be considered by the EU as a route to ensure consumer trust and business confidence in cross-border data flows. It should be suitably incorporated in the EU Standards as a ‘Harms-based’ approach that emphasizes the following of best practices and international standards in cross-border data flows, rather than the process-oriented approach of the Directive to approve standard contractual clauses, BCRs, or other similar instruments by supervisory authorities. This will help reduce bureaucratic controls.

****

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)

Following the initiative of NASSCOM, the National Association of Software Services Companies of India (NASSCOM), DSCI was launched to work as a not-for-profit organization and an independent self-regulatory organization to promote the data security and data privacy standards and frameworks among the Indian IT and ITeS (IT enabled Services) companies. Business Process Outsourcing (BPO) is part of ITeS. DSCI is registered under Section 25 of the Companies Act in India.

The key objectives of DSCI are:
- To enable Indian IT/ITeS organizations to provide high standard of security and data protection by adopting the best practices.
- To develop, monitor and enforce an appropriate security and data protection standard for the Indian IT/ITeS industry that would be adequate, cost effective, adaptable and comparable to the global standards.
- To build capacity to provide security certification for organizations.
- To create a common platform for promoting sharing of knowledge about information security and data privacy; and foster a community of security professionals and firms.
- To create awareness among industry professionals and other stakeholders about security and privacy issues.

Presently, no other country has a self-regulatory organization to encourage IT/ITeS companies to follow standards.

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