

Ursula Widmer/Latha R. Nair

Issues of Data Protection in the Context of Outsourcing From Switzerland and the EU to India

With the latest developments in information technology, outsourcing of business operations has become a practice with Swiss and European corporations. One of the preferred destinations for outsourcing is India, for various reasons including its cutting edge technology know-how, cheap labour force and good English skills. Outsourcing of business process operations from India involves transfer of personal data from Europe to a data processor in India and, therefore, requires caution. While Switzerland and the EU countries have data protection laws, India does not have any specific law and protects data only in a limited manner through some existing legislation. Hence, European data exporters have to enter into a contract which will have adequate clauses for protection of their data. This article examines the legal issues arising out of the export of personal data from Switzerland and EU countries to India and the safeguards to be observed when so doing. In order to appreciate the legal implications fully, the legal position in India vis-à-vis protection of data is also examined.

I. Indian BPO Industry and the Need for Data Protection

In June 2005, India came under global scrutiny due to the alleged data theft by an employee of one of the Business Process Outsourcing (BPO) companies, Infinity e-Search in northern India. The theft was revealed by a sting operation conducted by an undercover reporter from the Sun, a UK tabloid which photographed the employee accepting the money in return for a CD allegedly containing information relating to 1000 British nationals. The media and industry reactions to the theft mainly debated two issues – firstly, whether India's data protection laws are adequate and secondly, whether the incident could be disregarded, since similar instances are commonplace around the world.

The debates still continue between those with differing views on these issues, while the fact remains that, due to the sheer number of BPOs in India, it can really be called a back office of global businesses. A survey conducted by the National Association of Software and Service Companies (NASSCOM) showed that BPO units are mushrooming at the rate of one per week. Even India's information technology service majors such as Infosys, TCS and Wipro have established their own outsourcing arms so as not to miss out on a share of this booming market.¹

Outsourcing back-end processes from India has, therefore, become something of a trend among Swiss and EU companies as a means of reducing their operating costs. India is a preferred destination for BPO business for a number of reasons including its cutting edge technologies, massive manpower, relatively cheap labour and good English skills. However, India does not yet have specific legislation for the protection of personal data. The foreign companies outsourcing their back office operations from India do so by entering into contractual agreements with the BPOs. Such agreements usually contain clauses regulating data protection and protec-

tion of confidentiality of data processed by the BPOs on behalf of such companies. Data is the lifeline of financial institutions, banks, marketing institutions, the health industry, telecommunication companies and other businesses. Technologically processed data is one of the most valuable investments made by such businesses and, therefore, needs to be protected not only in the interest of those businesses but, in particular, also in the interest of the individuals concerned (customers, business partners, patients, telephone subscribers, credit card holders etc.). Against this background it is interesting to look into the question of how data is protected in India and how safe personal data maintained by a foreign company in the hands of an Indian BPO really is (see IV. below).

II. Data Protection in Switzerland

1. Statutory Conditions for the Disclosure of Data Outside Switzerland

The processing of personal data by private individuals and companies in Switzerland is regulated by the Federal Law on Data Protection, or DPL.² Unlike the legislation of the EU, the Swiss DPL not only applies to the data of natural persons but also to the data of legal persons.

As part of its general provisions on data protection, such as the obligation to collect data in a lawful manner, limitation of processing to specified purposes, the adequacy and relevance of the processing in relation to the purposes and the accuracy of the data, the DPL contains a regulation in Art. 6 concerning the disclosure of data outside Switzerland.

Art. 6 para. 1 DPL states that personal data may not be disclosed outside Switzerland if the privacy of the individual concerned would be seriously jeopardised by so doing. Serious jeopardisation of this kind is assumed in cases where the country concerned does not have a level of data protection equivalent to that of Switzerland. Although not specifically stated in the DPL, it is generally acknowledged that when the data protection in the country concerned is not equivalent, jeopardisation of the privacy of the individual concerned can be avoided by means of appropriate contractual agreements with the recipient of the data and the disclosure of the data outside Switzerland may be lawfully effected. However, such disclosure must occur in the context of lawful data processing that is compliant with the other data protection requirements.

The outsourcing of data processing to third parties is

▷ Dr. Ursula Widmer, Bern, and Latha R Nair, New Delhi. Further information about the authors on p. 32.

1 See Cover Stories of August 2004, "Can BPOs handle the Challenge?" by Jeevan M. Thankappan and Bijesh Kamath at the link <http://www.nc-india.com>.

2 Federal Law on Data Protection (DPL) of 19.6.1992. The DPL also applies to the processing of personal data by the Federal Administration and to institutions and organisations of the Confederation. Data processing by cantonal authorities and public institutions and organisations in the cantons is subject to cantonal law.

Issues of Data Protection in the Context of Outsourcing From Switzerland and the EU to India

permissible as a general principle under Art. 14 DPL if the outsourcing customer (the data controller) ensures that the third party commissioned to provide outsourcing services (the data processor) processes the data only in the manner that the data controller itself is entitled to do, and if no statutory duties of secrecy stand in the way of the outsourcing.

Under the statutory criteria, outsourcing the processing of personal data is, therefore, permissible under Swiss law if the requisite precautions regarding data protection have been laid down in the outsourcing contract.

2. Official Standard Contract

Switzerland's Federal Data Protection Commissioner recently published a standard contract for the outsourcing of data processing outside Switzerland.³ This standard contract is intended to be a tool, but has no binding legal effect, unlike the standard clauses that the European Commission defined in its Decisions on the transmission of data to third countries. The parties are not obliged to use the Data Protection Commissioner's standard contract. It is also possible to fulfil the data protection requirements whilst using differing contractual regulations, particularly where the question of an equivalent level of protection is concerned.

In Swiss data protection law, unlike that of the EU, there is no procedure, either, for establishing once and for all whether or not the data protection of a particular country is equivalent to that of Switzerland. The Data Protection Commissioner publishes a list with such information, but it is not binding. So, for instance, if a court action is brought against a company by an affected individual on the grounds of violation of Art. 6 DPL, the court may in its ruling deviate from the assessment of the Data Protection Commissioner in its own judgement as to whether or not the third country in which the data disclosure took place has equivalent data protection.

3. Duty of Notification

Art. 6 para. 2 DPL stipulates a duty of notification as regards disclosure of personal data outside Switzerland. Under the provisions of Art. 5 lit. b of the Ordinance on the Federal Law on Data Protection, or ODPL,⁴ the duty of notification applies explicitly with respect to the outsourcing abroad of the data processing. However, this

duty of notification applies⁵ in the case of disclosure of data to a country with equivalent data protection only if sensitive personal data⁶ or personality profiles⁷ are disclosed.

The Federal Data Protection Commissioner must be notified before the data is disclosed,⁸ although there are exceptions in cases where the disclosure outside Switzerland takes place in the context of a statutory duty or the individuals concerned are aware of the disclosure.

III. Data Protection in the European Union

1. EC Directive

Directive 95/46/EC⁹ (Directive) governs the protection of individuals with regard to the processing of personal data and the free movement of such data. The objectives of the Directive are (i) to protect individuals with respect to the processing of personal data and (ii) to ensure the free flow or movement of data within the EU and its member states. These two objectives may sound contradicting since it is difficult to protect privacy rights and, at the same time, ensure free movement of data. This applies both in relation to personal data transfer within the EU between the member states, but especially in the case of data transfer to third countries.¹⁰

The issue of the export of personal data to third countries is dealt with in Chapter IV of the Directive. Member states of the European Union must ensure that when personal data is transferred to third countries for processing, such third countries ensure an adequate level of protection.¹¹ Adequacy of the level of protection offered by a third country under the Directive must be assessed in the light of all the circumstances surrounding the data transfer such as nature of the data, purpose and duration of the processing operation, country of origin and country of final destination.¹² If it is found by the Commission that a third country does not ensure an adequate level of protection, member states must prevent any transfer of data to such country.¹³

However with the authorization of the member state concerned, it is permissible for a company in a member state to transfer personal data to a third country which does not have an adequate level of protection, provided the data controller (the data exporter in Europe wishing to outsource business) takes adequate safeguards with respect to the protection of privacy, in particular through contractual agreements.¹⁴ The member states must inform the Commission of such authorization when given.¹⁵

2. Standard Clauses Issued by the European Commission

Art. 26 (4) of the Directive states that within the framework of the procedure described in Art. 31 (2) of the Directive, the Commission may decide that certain standard clauses represent adequate protection such that data can be transferred into a country that does not offer an adequate level of protection. In its Decision 2002/16/EC of 27.12.2001,¹⁶ the Commission defined standard clauses for the data transfer to data processors. The parties must not deviate from these clauses, as the contract will otherwise not fall within the ambit of Art. 26 (4) of the Directive and the data transfer will only be permissi-

3 The text of the contract is available on the website of the Federal Data Protection Commissioner at <http://www.edsb.ch/e/themen/ausland/outsourcing.htm>.

4 Ordinance on the Federal Law on Data Protection (ODPL) of 14.6.1993.

5 Art. 7 para. 2 ODPL.

6 Art. 3 lit. c DPL defines sensitive personal data as data concerning 1) religious, philosophical or ethical, political or trade union beliefs or activities, 2) health, sexuality or racial origin, 3) social security measures, 4) administrative or criminal proceedings and sanctions.

7 Art. 3 lit. d DPL defines personality profiles as collections of data which allow the appraisal of essential characteristics of the personality of a natural person.

8 Art. 6 para. 2 DPL.

9 1995 OJ L 281/31.

10 See Peter Blume, CRi 2005, 71 ff.

11 Art. 25 (1) Directive.

12 Art. 25 (2) Directive.

13 Art. 25 (4) Directive.

14 Art. 26 (2) Directive.

15 Art. 26 (3) Directive.

16 2002 OJ L 6/52.

Issues of Data Protection in the Context of Outsourcing From Switzerland and the EU to India

ble if the authorization of the member state of the data exporter has been obtained in accordance with Art. 26 (2) of the Directive.¹⁷

Thus, if data exporters in EU member states wish to ensure, through contractual agreement avoiding authorization procedures of individual member states, adequate protection in respect of data processing by an outsourcing provider in a third country that does not have an adequate level of protection within the meaning of Art. 25 (1) and (2) of the Directive, then the standard clauses defined in the Decision of the Commission must remain unchanged. There is no leeway for negotiation in this respect.

IV. Data Protection in India

Prior to the alleged data theft in 2005 (see I. above) over a dozen employees of a Pune-based BPO unit, Mphasis, had been arrested by the Indian police for allegedly stealing credit card identities belonging to certain foreign nationals and attempting to siphon off huge amounts from these credit card accounts. The incident made headlines and was a topic of debate at a political level in India. The reactions from the Indian government included the possibility of introducing a new data protection law in India. Currently data is protected in a very limited way in India under some statutes.

1. Indian Copyright Act, 1957

The Indian Copyright Act, inter alia, protects original literary, dramatic and artistic works as well as cinematograph films and sound recordings. The definition of a literary work also includes databases and the owner of a literary work has the right to certain acts under the statute, including reproduction of the work in any material form including the storing of it in any medium by electronic means, issuing of copies of the work to the public, performing the work in public, communicating it to the public.

Section 16 of the Act clarifies that all copyrights arise out of the Act alone and that there is no concept of common law copyright in India; however, the section also states that this does not prevent any person from initiating an action for breach of trust or confidence.¹⁸ In other words, even if one is not able to claim copyright in a work under the Act, the Act does not prevent the aggrieved party from filing an action aimed at restraining a defendant from breach of trust or confidence in the contents of the work.

However, since copyright law is concerned with protection of the originality of expression in a work rather than the contents of the work, any data protected under the Act would be protected only for the originality in the manner or arrangement of the data. Hence, no protection can be claimed for data per se under the Copyright Act and the protection offered is very limited to that extent. Nor can protection be claimed for maintaining the confidentiality or privacy of personal data.

It would appear, therefore, that in a case where violation of copyright in the data was established, the remedies under Indian copyright law are confined to breach of copyright in the literary work (which is the data arranged in a particular form) and not privacy rights.

2. Information Technology Act, 2000

The Information Technology Act (the "IT Act") was enacted in the year 2000 with the main purpose of providing legal recognition for transactions carried out by means of electronic commerce. The definition of data covers a representation of information, knowledge, facts etc. prepared or processed in a computer system in any form or stored internally in the memory of the computer.

Under Section 43 (b) of the Act, penalties by way of damages up to 10,000,000 Indian Rupees (approximately USD 200,000) are prescribed against any person who without the permission of the owner "downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium".

The next relevant provision is Section 66 of the Act, which defines 'hacking' and prescribes punishment for the same. Anyone who with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Hacking is a criminal offence under the Act and is punishable with imprisonment for up to three years or with fines which may extend to Indian Rupees 200,000 (approximately USD 4,000) or both.

A review of the above sections will reveal that, although the IT Act was originally enacted for an entirely different purpose, it does have a few provisions¹⁹ that may be interpreted in favour of parties affected by any breach of privacy or other violation of their data.

3. Amendments to the IT Act, 2000?

What is indeed interesting is that in August 2005, the Press Information Bureau of the Government of India, on behalf of the Ministry of Communications and Information Technology, issued a press release on the report of the Expert Committee on amendments to the IT Act, 2000.²⁰ The press release states that the amendments proposed by the Expert Committee were in the wake of the recent developments nationally and internationally, particularly with respect to the provisions related to data protection and privacy in the context of BPO operations, liabilities of network service providers, computer related offences, regulation of cyber cafés etc. In view of the recent concerns about the operating provisions in the IT Act relating to 'data protection and privacy', in addition to contractual agreements between the parties, the Committee is proposing certain amendments, which are:

¹⁷ See *Gerlind Wisskirchen*, CRi 2004, 171.

¹⁸ Section 16 – No copyright except as provided under the Act: No person shall be entitled to copyright or any similar right in any work, whether published or unpublished, otherwise than under and in accordance with the provisions of this Act or of any other law for the time being in force, but nothing in this section shall be construed as abrogating any right or jurisdiction to restrain a breach of trust or confidence.

¹⁹ Especially, the definition of 'hacking' in Section 66 is too broad to include a breach of privacy as well. The relevant part in the section is "affects it injuriously by any means".

²⁰ See the "Report of the Expert Committee on Amendments to IT Act, 2000" at <http://www.mit.gov.in/itact2000/index.asp>. The link gives the Press Release, Summary of the Proposed Amendments and the Full Text of the Report of the Expert Committee.

Issues of Data Protection in the Context of Outsourcing From Switzerland and the EU to India

- ▷ An additional section to ensure reasonable security practices and procedures for sensitive information by any body corporate;
- ▷ Gradation of the severity of computer-related offences committed dishonestly or fraudulently, and punishment thereof;
- ▷ An additional section for breach of confidentiality with intent to cause injury to a subscriber.

a) Purpose of the Amendments

Nevertheless, closer examination of the proposed provisions reveals that the amendments do not deviate from the initial objectives of the IT Act and that the amendments propose only few safeguards for data protection in addition to what would be provided in the contract between the parties. Also, since the press release issued by the Ministry indicated that the amendments are intended to cover the issue of data protection raised by the recent incidents in India, it appears that the Indian government may not wish to enact a separate law for data protection in the near future at least, contrary to promises that were being made.

b) The Need of Data Protection Legislation

India is today viewed as one of the information technology majors. The increasing number of technology-related crimes in India in recent years merely reflects the growth of the Indian information technology industry.²¹ Critics of the incidents relating to the recent data thefts in India say that the media exaggerated and hyped up these incidents and that similar incidents also occur in other parts of the world. However, these incidents raise serious issues concerning the security of foreign data with Indian BPO companies and are a reminder to the government of the lack of a specific Indian law for data protection. The fact that some of the developed countries who are outsourcing business from India do not have specific legislation on data protection is neither a justification nor an excuse for trying to wish this issue away. It has been suggested that India has a 'robust data protection law' in the shape of the IT Act, 2000 and it is therefore not necessary to enact separate legislation in this area.²² However, the IT Act, 2000 does not prescribe any rules relating to crucial aspects of data protection such as the processing of personal data, the conditions under which data may be collected from an individual, the precautions to be taken while collecting data, confidentiality and security of processing of the data collected, etc.

Even the proposed amendments to the IT Act which deal with data protection appear to constitute nothing more than 'patches' to the Act and certainly seem incongruous. The purpose of the IT Act as originally drafted was not to protect data, and the law-makers need to be mind-

ful of that. When the world is moving towards sui generis protection of data, India must do the same, especially since such a move would be more convenient and conducive to foreign companies when outsourcing business to India.

4. Protection of Data Via Contracts

The Indian statute governing contractual agreements is the Indian Contract Act, 1872. It is possible for a data exporter from Europe to enter into a contract under this Act with an Indian BPO company for outsourcing of the former's business activities to India. There does not appear to be anything inconsistent with the Indian Contract Act in the standard contract of the Swiss Data Protection Commissioner or the standard clauses defined by the European Commission. The contract must mention the specific duties and obligations of both parties involved. Many companies operate their business in India by entering into such contracts. Such contracts specify the terms and conditions under which data is to be used, processed and dealt with by the Indian company. Hence, a well-drafted contract with an Indian BPO should take care of most of the concerns of a data exporter regarding safety of its data.

It is therefore important for a data exporter to negotiate the contractual clauses with the data processor/BPO in India in order to achieve a balance between maximum business benefits and adequate protection of personal data. The data exporter must bear in mind that until such time as India enacts legislation that offers sufficient and adequate legal protection for personal data, any uncertainty regarding doing business with an Indian data processor/BPO is a matter of negotiation of the relevant contract using appropriate legal expertise and advice.

V. Is it Safe to Export from Europe to India?

Since India does not have any law for the protection of data and since the existing legislation offers only limited protection, the safety of data exported from Europe to India would be a matter of concern for any data exporter. However, one has to find alternatives so that business transactions do not suffer. As seen before, a well-drafted contractual agreement covering inter alia, the protection of data and obligations connected thereto would be the only option in the circumstances for a data exporter to India.

1. Drafting of contracts

a) Required Minimum Content

Under the terms of both the standard contract published by the Swiss Federal Data Protection Commissioner and the standard clauses of the Commission in Decision 2002/16/EC, it is the following points that are to be regulated as precisely as possible in the outsourcing contract in question:

- ▷ *Definition of the exported data:* The categories of data must be described, in particular when the data concerned is sensitive data within the meaning of the data protection legislation of the data exporter or the EC Directive.²³

21 Recent examples are the case of the attempted sale of a pornographic video clipping that resulted in dismissal of the CEO of baze.com, an auction portal owned by e-bay Inc., and the case of a multi-media clipping transmitted via mobile handsets where the naked body of a woman was morphed with a famous Bollywood actress.

22 See e.g. "India has a robust data protection law" by Na. Vijayashankar (Naavi) dated June 24, 2005 on http://www.naavi.org/cl_editorial_05/edit_june_24_05_01.htm.

23 Art. 8 Directive.

Issues of Data Protection in the Context of Outsourcing From Switzerland and the EU to India

- ▷ Definition of the *categories of persons concerned*, i.e. those to whom the exported data refers.
- ▷ Definition of the *processing operations* according to their nature, scope and purpose. In particular, it must also be established which persons the data processor may allow to access the data and/or to which persons it may pass on the data on behalf of the data exporter.
- ▷ Definition of the *organisational and technical security measures* that must be taken in connection with the data transfer by the data exporter and the data processing by the data processor.

b) Additional Contract Points

In addition to regulation of the above-mentioned essential points in establishing a definition of the data covered by the contract and the processing thereof, the following points must also be taken into consideration in connection with the contractual regulation of the outsourcing of data processing activities:

- ▷ *Reciprocal guarantees* by the parties that on the one hand the data transfer by the data exporter and the agreed data processing by the data processor are compliant with the data protection law of the data exporter and fulfill all conditions required by such law in relation to the data transfer (e.g. duties of notification to the data protection authorities, notification to/consent of the persons concerned etc.), and that on the other hand the data processor can comply with all the provisions of the contract under the laws of its own country;
- ▷ *Responsibilities and procedures* designed to safeguard the rights of the persons concerned, such as their right to information, correction of incorrect data, deletion of data, blocking of onward transfer of data to third parties;
- ▷ *Duties of notification*, e.g. in the event of breach of the agreed security measures or of enquiries/measures on the part of the authorities;
- ▷ In the event that the data processor is dealing with data relating to more than one data exporter, there should be special and adequate provisions in the contract regarding the *separation and protection of sensitive personal data and trade secrets*;
- ▷ The data processor should be sure to employ *skilled labour* in operations being carried out for the European company;
- ▷ The data processor should take all reasonable steps to maintain the *confidentiality* of all the information and personal data provided by the data exporter for processing. Such reasonable steps should include, but not be limited to:
 - verification of the background of the employees to check for any criminal record;
 - appropriate confidentiality clauses in the employment contracts with the employees;
 - instructing employees before they start any processing with regard to the sanctity of the data and the legal reasons for maintaining the confidentiality thereof, and the security policies;
 - creating and establishing in-house practices for

- compliance with confidentiality requirements;
- having stringent policies regarding carrying mobile devices such as phones or notepads through which data may be transferred;
- immediate dismissal of and disciplinary action against any employee found to be breaching any of the policies or indulging in any practice that could jeopardise the safety of the data;
- ▷ A *security surveillance report* should be sent to the data exporter at periodic intervals;
- ▷ The data exporter should reserve the right to request the BPO to *review* the security measures in audits and require improvements or alterations if felt necessary;
- ▷ Provision of civil *remedies* and stipulation of liquidated *damages*;
- ▷ In the event of termination of a contract, the *exit clauses* should be worded appropriately so as to address effectively any issues relating to the in-sourcing of the data processing activities outsourced to the BPO and the protection of the personal data related therewith. Such terms should include the safe return and/or destruction of the personal data.

c) Implementation Prospects

It seems doubtful whether companies in the EU will be able to incorporate the standard clauses set out in Decision 2002/16/EC without modification into contracts with the BPOs. In particular, it may not be simple to achieve through negotiation the inclusion of the third-party beneficiary clause stipulated in the standard clauses, which provides that certain clauses can be enforced directly against the data processor by the persons whose data is being processed, nor the regulation allowing data protection authorities in the EU member state of the data exporters to carry out audits on the data processor's premises.²⁴ If it proves impossible to adopt the standard clauses unchanged, then the authorization of the respective authorities in the EU member state of the data exporter must be obtained for the data transfer.

For Swiss data exporters, there are no prescribed binding clauses, since the standard contract published by the Federal Data Protection Commissioner is no more than a recommendation. Swiss companies must therefore make a judgement at their own discretion as to whether or not the contract they have negotiated with the data processor delivers sufficient protection to fulfil the requirements of the Swiss Data Protection Law.

2. What Happens If There is a Breach of Contract by a Company Located in India?

Breach of contract by a BPO is not a hypothetical situation as we have seen from the data theft cases in India. However, if the contract makes provision for such eventualities, it would then be an issue of enforcement of the terms. Indian courts will interpret the contract as per the provisions of the Indian Contract Act, 1872 and the established case law. If the matter is tried before a court in Europe it is possible to have the judgment enforced in

²⁴ See Peter Blume, CRi 2005, 76.

Issues of Data Protection in the Context of Outsourcing From Switzerland and the EU to India

India under the Indian Civil Procedure Code, 1908.²⁵

However, a data exporter should be aware that the Indian legal system has its own delays in handing out justice to litigants. If the data exporter wants to make a delinquent employee criminally liable, it is possible to do so through Section 66 of the IT Act as well as through provisions of the Indian Penal Code. In criminal proceedings, the court also has the discretion to grant general damages which are nominal and special damages where injury is proved. If the contract has provided for liquidated damages, this will be duly considered by the court. If a judgment is entered against the accused and the accused is unable to pay the criminal penalty, then the court could enhance the duration of the sentence in lieu of a criminal penalty.

As far as civil remedies are concerned, if liquidated damages are provided for in the contract, the affected party may be able to claim them provided the injury is proved. In the absence of a provision for liquidated damages,

Indian courts rarely award heavy damages for civil injuries. In the event the court awards damages and the defendant refuses to pay the damages, the plaintiff could enforce the judgment by attachment and sale of any of the assets of the defendant. However, it is possible for the parties to put a limit on their liabilities in the event of breach of contract by way of a clause in the contract.

VI. Conclusion

India has been in the world's focus as a direct result of its fast-growing information technology industry and changing economy due to liberalisation. Outsourcing of business activities to India is more and more interesting for companies in Switzerland and Europe. While it is a fact that India does not currently offer adequate legal protection for personal data, this has not until now prevented data exporters from Europe from outsourcing some of their business processes to India. Safety of personal data may be ensured by data exporters through adequately negotiated and drafted contracts.

²⁵ See sections 13, 14 and 44A of the Indian Code of Civil Procedure, 1908.