NEWS BRAZIL DESK

Noerr

December 2014

INTERNATIONAL DATA PROTECTION

in Brazil, Germany and Poland

Dear readers,

In recent years, Brazil has experienced expanding internet access and smartphone usage. This has largely made the country not only one of the biggest markets for social networking websites and games but also for growing e-commerce ventures. One of the most important challenges in the digital economy era is the protection of personal data. Both Brazilian and foreign online companies are well advised to familiarize themselves with the privacy obligations and provisions impacting data handling set forth in the new Brazilian Internet Act.

Germany and Poland have data protection laws harmonised with EU rules, which affect virtually any collection, processing and transfer of personal data. This includes not only direct marketing and e-commerce practices but also intragroup data transfer and post-merger integration matters. Indeed, the outsourcing and integration of certain business operations, such as human resources management or the operation of software applications, often requires the transfer of personal data concerning employees and customers to a shared service centre. As a result, the companies involved should conduct thorough data protection analyses in order to ensure solid legal compliance.

Against this background, this newsletter offers an overview of international online data protection in Brazil, as well as of data privacy and international data transfer in Germany and Poland.

We hope you enjoy reading this issue of our newsletter.

Yours sincerely,

Holger Alfes, Alexander Liegl & Luiza Saito Sampaio

Brazil

Personal Data Protection in Brazil

Currently, there is no specific privacy law enacted in Brazil, since the respective bill of law is still in process. However, personal data protection principles are guaranteed by the constitutional fundamental rights to privacy and intimacy and to communications secrecy and certain legislation has been passed on that basis earlier this year.

Law No. 12,965/2014 (the "Brazilian Internet Act" or so-called *Marco Civil da Internet*), which entered in force on June 23, 2014, specifically regulates the collection, maintenance, treatment and use of online personal data. The Brazilian Internet Act is applicable to (i) Internet users, (ii) Internet connection providers, i.e. those promoting the transmission of data packages in the Internet by means of IP addresses authentication or assignment, and (iii) Internet application providers, i.e. those providing a set of features which can be accessed by a computer or any device connected to the Internet.

Privacy Requirements

Internet connection and application providers are only allowed to process personal data upon express consent by the user. Terms and conditions or any agreements between providers and users must contain clear and complete in-

formation regarding the collection, use, storage, protection and treatment of personal data.

Personal data, connection or access registration information or private communications may not be disclosed to third parties, unless the user expressly consents thereto or if required by judicial order.

Mandatory Retention Provisions

Internet connection providers must store connection registrations (i.e. information concerning the date and time a connection begins and ends and the IP addresses used) under secrecy for one year. Similarly, Internet application providers have the obligation to keep registrations of access to Internet applications under secrecy for six months.

While Internet connection providers are prohibited from storing information regarding the access to Internet applications, Internet application providers, such as search engines and social media websites, are not allowed to keep access registration related to other Internet applications except if the user previously consented thereto.

Application of the Brazilian Internet Act to Foreign Companies

Pursuant to Article 11 of the Brazilian Internet Act, whenever the collection, storage or treatment of connection or access logs, personal data or private communications by Internet connection or application providers occurs in Brazil, Brazilian regulations must be observed.

In other words, Brazilian law may be applicable to foreign companies offering services to Brazilian users or who, directly or indirectly through another company pertaining to their economic group, maintain offices in Brazil.

In case a foreign company is fined in Brazil due to breach of legal obligations related to the storage of connection or access logs or privacy requirements, the Brazilian subsidiary or establishment will be held jointly liable.

Noerr Brazil Desk

Embedded in a leading European law firm, Noerr Brazil Desk provides advice and support to Brazilian companies wishing to invest or already conducting business in Germany and Central and Eastern Europe (CEE) countries, as well as to European companies having an established presence in Brazil or contemplating entering the Brazilian market.

We work as a gateway to a comprehensive range of legal advisory services and tax solutions offered by our firm in Germany and CEE. In Brazil, we rely on a network of experienced “best friends” law firms.

Consisting of Brazilian and German qualified lawyers, the Noerr Brazil Desk team offers its clients:

- Cultural awareness
- Effective exchange of information in Portuguese, German and English
- Excellent knowledge of the German, CEE and Brazilian jurisdictions
- In-depth market knowledge of Brazil, Germany and CEE
- Interdisciplinary solutions and industry know-how ranging from automotive, banking and finance, energy, health care to machine building and real estate

Penalties for Data Protection Violation

Regardless of further civil, criminal or administrative penalties applicable in case of data protection violation, the following sanctions set forth in Article 12 of the Brazilian Internet Act can be applied:

(i) Warning including a deadline for the adoption of corrective measures;

(ii) Fine of up to 10% of the revenues of the economic group in Brazil in the previous fiscal year, excluding taxes;

(iii) Temporary suspension of the providers’ activities; and/ or

(iv) Prohibition of the providers’ activities.

Exemption of liability for content generated by third parties

Internet connection providers are not liable for damages caused by user-generated content. Internet application providers’ liability is restricted to user-generated damaging content which they failed to timely remove after a judicial order or, in the specific case of non-authorised sexual content or nudity, after the request by the injured users or their legal representative.

Germany

Personal Data Protection in Germany

The German Federal Data Protection Act (*Bundesdatenschutzgesetz*, the “BDSG”) transferred the terms of the EU-Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (“EU Data Protection Directive”) into German law. It stands in a long tradition of German privacy regulation starting as early as 1970, when the data protection act of the state of Hessen, the world’s first general data protection act, was enacted.

The purpose of the BDSG is not to protect data as such but to protect individuals against their right to privacy being impaired through the handling of their personal data. Accordingly, it goes beyond just imposing data security measures and rather seeks to limit the collection, processing and use of per-

sonal data upfront and subjects it to strict requirements.

Legal Requirements

According to the BDSG any collection, processing and use of personal data is prohibited, unless it passes a two-step-test.

In a first step it is to be verified, whether the "ban with permit reservation" (so called "*Verbot mit Erlaubnisvorbehalt*") set forth in Sec. 4 para. 1BDSG is passed. According to said Sec. 4 para. 1 BDSG, the collection, processing and use of personal data is only lawful if it is permitted or ordered by the BDSG or other law, or if the data subject (i.e. the person to whom the data relates) provided consent.

The BDSG contains a number of permissions which apply depending on the specific type of data in question and the purposes and scope of the intended collection, processing or use.

Transfers permitted by the BDSG include transfers which are conducted as a means to pursue own commercial purposes of the transferring entity, if and to the extent it is necessary to safeguard legitimate interests of the transferring entity and provided there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of such transfer (see Sec 28 para. 1 sentence 2 no. 2 BDSG).

In a second step, it is to be verified, whether data is transferred to a recipient (shared service centre) that is located in a country which is neither a member state of the European Union ("EU") nor of the Agreement on the European Economic Area ("EEA") and, if this is the case, whether such country provides – from a European perspective – for an adequate level of data protection (see Sec. 4b para. 2 sentence 2 BDSG).

Privacy Protection Safeguards

The European Commission ("EC") issued a list of countries, in which the level of data protection is deemed adequate due to the rules of law applicable in those countries. To date, Brazil does not fall under this category. Argentina and Uruguay are the only South American countries included in the list.

If the recipient is located in Brazil, the data protection supervisory authorities may nonetheless authorize a transfer of personal data to such a recipient, if the data controller adduces adequate safeguards with respect to the protection of privacy and exercise of the corresponding rights. Such safeguards can in particular result from contractual clauses or binding corporate regulations.

These contractual clauses are standardized EU contractual model clauses of the EC which – if used verbatim – make a case-by-case authorization of the transfer with respect to the second step by the data protection supervisory authorities even superfluous.

There are two types of EU contractual model clauses. One type is to be used in a controller to processor relationship where the personal data is processed by the shared service centre only for and as instructed by the respective transferring group entity.

The other type is to be used in controller to controller relationships in which the receiving entity has a certain discretion regarding the scope and purpose of the use of personal data it receives from the transferring entity.

The EU contractual model clauses to be used in Germany must – unlike in other EU countries – often be supplemented with additional clauses to ensure that also the first step of the test mentioned above is passed.

Risks of non-compliance

Failure to comply with the rules of the BDSG may result in fines of up to EUR 300,000 per case or even in criminal penalties.

Data protection supervisory authorities may further prohibit non-compliant processing activities which may require swift and costly amendments of business processes already implemented.

Poland

Personal Data Protection in Poland

In Poland, the Act on the Protection of Personal Data of 1997 (Journal of Laws of 2014, Item 1182, the "Polish DPA") implemented the EU Data Protection Directive. The Polish DPA applies to the processing of personal data in both manual and electronic records. It must be observed by any public and private entities processing (collecting, amending, using, erasing etc.) personal data.

These entities are recognised as data controllers, who decide on the scope and purpose of data processing. Additionally, with respect to electronic services, the Act on Electronic Services of 2002 (Journal of Laws of 2013, Item 1422, as amended) sets out detailed and specific regulations.

Brazilian companies must comply with Polish data protection regulations on the same basis as Polish companies, if they are involved in the processing of personal data by technical means located in Poland. In case of a Polish subsidiary of a Brazilian undertaking, these regulations will be binding for the entity seated in Poland.

Restrictions on Data Transfer to Brazil

As a rule, when data of a Polish data subjects is transferred outside the EEA, certain formalities have to be observed by the data controller. The type of formalities will depend on the safeguards on which the personal data transfer is based.

In principle, the dataflow outside the EEA is allowed, if the destination country ensures an adequate level of protection. As mentioned above, since Brazil is not included in the list of countries where the level of data protection is deemed adequate, any transfer of personal data from Poland to Brazil may only take place subject to the prior consent of the Polish Inspector General for the Protection of Personal Data (*Generalny In-*

spektor Ochrony Danych Osobowych, "GIODO") and provided that the data controller ensures adequate data protection safeguards.

Amendments to the Polish DPA

Same as in Germany, ensuring of adequate data protection safeguards can be in practice done by (i) integrating EU contractual model clauses of the EC in an agreement between a data controller and another data controller or data processor, and (ii) adopting binding corporate rules.

Currently, even if the transfer relies on the EU contractual model clauses of the EC or binding corporate rules, the prior consent of GIODO is required. However, as of 2015, due to the newest amendment to the Polish DPA, those undertakings bound by EU contractual model clauses of the EC or binding corporate rules will be relieved from this requirement. In the case of adoption of binding corporate rules, a prior approval by GIODO will still be required before the processing of personal data based on such rules can start.

In all other cases, the formal consent of GIODO will be required. This shall be taken into account, since in practice it takes several months to obtain such a consent. In addition, GIODO issues its approval at its exclusive discretion.

Alternatives

Alternatively, a transfer of personal data to Brazil can take place upon a written consent by the concerned data subjects (for instance, the customer of a Brazilian online shop). Such consent shall relate specifically and clearly to the transfer of data outside the EEA. Additionally, it must be given freely.

Another alternative refers to data transfers required to perform a contract between the data controller and the data subject. If an international data transfer is performed on such basis or upon the data subject's consent, neither GIODO's notification nor its consent will be required.

Polish DPA Sanctions

A breach of the Polish DPA would give rise to criminal liability, including a prison sentence of up to three years. In practice, the criminal charges are very unlikely.

However, GIODO may issue an administrative decision, which can be much more severe for the company. The authority may require a situation be reversed to a state compliant with Polish data protection law. In extreme cases, the non-compliant company may have to erase the data base containing personal data.

For further information please contact:

Noerr Brazil Desk

Dr. Holger Alfes, LL.M.
Rechtsanwalt (Germany)
Attorney-at-law (New York)
T +49 69 971477-231
holger.alfes@noerr.com

Prof. Dr. Alexander Liegl
Rechtsanwalt (Germany)
T +49 8928628-266
alexander.liegl@noerr.com

Luiza Saito Sampaio, LL.M.
Advogada (Brazil and Portugal)
T +49 69 971477-414
luiza.saitosampaio@noerr.com

Tobias Kugler
Rechtsanwalt (Germany)
T +49 69 971477241
tobias.kugler@ noerr.com

Katarzyna Ziółkowska
Radca prawny (Poland)
T +48 22 579 30 60
katarzyna.ziolkowska@noerr.com

www.noerr.com