POHLMANN & COMPANY

International Compliance Update

4/2015

Our "International Compliance Update" portrays current developments and trends in international compliance legislation, jurisdiction and practice with a focus on their relevance for Germany.

Canada

A brief History of Anti-Corruption Enforcement Activities in Canada

Stefan Hoffmann-Kuhnt

- While enforcement actions for violations of anti-corruption legislation against individuals and companies have become frequent occurrences in the United States and in Europe, Canadian Authorities have been slow to follow their southern neighbors' practices.
- After enacting its *Corruption of Foreign Public Officials Act*[1] ("**CFPOA**") in 1998 it took a long time for Canadian law enforcement to secure its first guilty pleas.
- Until today there have only been three corporate entities that pleaded guilty under the act as well as the conviction of just one individual.

[1] SC 1998, c 34 ("CFPOA")

>>>

Also in this issue:

S. Bartsch / M. Erhard | **Business Partner Checks and Data Protection**

Subscribe to the International Compliance Update here.

The first conviction dates back to the year 2005 when Hydro-Kleen Systems Inc.[2] was fined a small amount of CAD[3] $25.000 after it plead guilty of paying bribes of $28.300 to a US Immigration official. It is remarkable that the amount of the fine was less than the amount of the bribe actually paid.

The Niko Resources Case

It then took almost another six years until the next case was settled with a guilty plea by Niko Resources Ltd.[4], a Calgary based natural gas company, in June 2011. Niko Resources had been providing improper benefits to public officials from Bangladesh including the provision of a vehicle worth around $190.000 as well as improper travel and accommodation expenses. The resulting fine for Niko Resources was already substantially higher at $9.5 million. Noteworthy from the Niko Resources case is that the settlement also contained a three year probation term including an obligation for Niko Resources to implement an anti-corruption compliance program[5] which in turn was subject to periodic independent review. The description of the court's view of what steps Niko Resources should undertake to implement its anti-corruption compliance program show that their expectation was quite similar to what today is required in other international frameworks for effective Compliance Programs such as the World Bank Group's Integrity Compliance Guidelines[6] or the U.S. Foreign Corrupt Practices Act ("**FCPA**") Resource Guide[7]. Here is an excerpt of the Niko Resources Probation Order:

- Development of a rigorous anti-corruption compliance Code of Conduct
- Nomination of a senior corporate executive to implement and oversee the compliance program
- Issue policies governing: gifts, hospitality, entertainment and expenses, customer travel, political contributions, charitable donations and sponsorships, facilitation payments and solicitation
- Implementation of a system of internal accounting controls designed to ensure that the company makes and keeps fair and accurate books, records, and accounts
- Ensuring strong Tone from the Top
- Regular corruption risk assessment followed by gap analysis in order to ensure that the compliance standards and procedure are updated at least annually
- Training and communication measures including periodic training for all directors, officers and employees as well as, where appropriate, agents and business partners
- Institute appropriate due diligence and compliance requirements pertaining to the retention and oversight of all agents and business partners
- Provide guidance and advice to directors, officers and employees
- Provision of safe and confidential whistleblowing facilities including the protection of any whistleblowers as well as responding to any concerns raised
- Ensuring appropriate disciplinary measures to address violations of the Code of Conduct

>>>

[2] R v. Watts, [2005] A.J. No. 568
[3] CAD = Canadian Dollar. All amounts denoted as $ in this article refer to CAD
[4] R v. Niko Resources Ltd., 2001
[5] Niko Probation Order: http://www.cba.org/CBA/advocacy/PDF/Niko%20Probation%20Order.pdf
[6] WBG ICG: http://siteresources.worldbank.org/INTDOII/Resources/Integrity_Compliance_Guidelines.pdf
[7] FCPA Resource Guide http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf

The Griffiths Energy International Case

The third case settled to date is that of Griffiths Energy International Inc.[8] where the incoming new management discovered evidence of bribery and self-disclosed its findings to the Canadian- as well as US Authorities. Also based in Calgary, the oil and gas company had been making "consulting" payments of more than $2 million to a company controlled by the wife of the ambassador of the central African Republic of Chad while negotiating for oil concession rights. Griffiths paid a fine of $10.35 million – only slightly more than Niko Resources, even though the bribes paid were in excess of 10 times higher than those paid by Niko Resources. Reasons for this more lenient sentence can be attributed to the full and extensive cooperation with authorities[9]. Given that there are no obligations for self-disclosure under Canadian law and there was no preceding case that could indicate whether leniency would be applied by the courts, the management of Griffiths Energy took a leap of faith disclosing all of their findings to the Public Prosecution Service of Canada as well as to the Royal Canadian Mounted Police ("**RCMP**"). Even legally privileged communication between Griffiths Energy and its previous outside legal advisors was handed over, underscoring management's commitment to full cooperation with law enforcement. Furthermore it is noted in the statement of facts that Griffiths Energy had taken steps including the adoption of a robust anti-corruption compliance program and the strengthening of internal controls.

[8] R v. Griffiths Energy International, [2013] A.J. No 412
[9] https://www.cba.org/ABC/ladefense/Pdf/Griffiths_Amended_Statement_of_Facts.pdf

The Nazir Karigar Case

So far the only CFPOA case against an individual which ended in a conviction[10] and a three year imprisonment was the case against Nazir Karigar[11], a business man from Ottawa who was indicted on charges of planning to pay bribes to Indian public officials on behalf of Cryptometrics Canada Ltd in a plot to influence purchasing decisions of Air India for a $100 million contract to supply facial recognition software. Karigar himself exposed the bribery scheme to the authorities after his relationship with Cryptometrics had broken down. He unsuccessfully tried to obtain immunity, the sentence of three years compared to the maximum sentence of five years imprisonment however indicates that a certain level of leniency for his cooperation with the authorities was applied by the court.

With the small number of cases brought against companies and/or individuals under the CFPOA in the first 10 years after the act was published it comes as no surprise that Canada has been criticized by the OECD due to its weak enforcement efforts. This criticism had become stronger in particular after Canada ratified the UN Anti-Bribery Convention in 2007. It was only in 2008, that a special unit to investigate white collar crime was created within the RCMP. Starting off with only just over a dozen investigators at its inception, this unit is said to have grown to more than 100 specially trained investigators. Nevertheless the number of individuals and companies under investigation for CFPOA violations is increasing steadily. It is furthermore important to note the fact that CFPOA violations in Canada are exclusively prosecuted under the Canadian criminal law, which does not provide for Deferred Prosecution Agreements or Non-Prosecution Agreements as it is standard practice in the United States. This causes investigations to be more complex and lengthy compared to those conducted in the United States.

>>>

[10] R v. Karigar [2013] O.J. No. 3661
[11] http://www.thelitigator.ca/litigator/wp-content/uploads/Karigar-Sentencing-Decision.pdf

Important Amendments to the CFPOA

An important milestone in the development of the Canadian legal anti-corruption framework was the adoption of Bill S-14[12] in June 2013, which brought a number of changes to the CFPOA as follows:

- Increase of the maximum penalty from previously five years imprisonment and unlimited fines to a new maximum of fourteen years imprisonment and unlimited fines;
- Introduction of a Books and Records Offence, punishable by a maximum of 14 years and unlimited fines for falsifying records or disguising payments related to bribery;
- Application of Act to all businesses, eliminating a previous exclusion of non-profit organizations or charities;
- Elimination of exception for "Facilitation Payments" – however this elimination did not come into force together with the rest of Bill S-14 but rather will follow a separate timetable still to be announced by order of the Governor in Council;
- Strengthened Extraterritoriality of the Act, where the Government of Canada can now exercise jurisdiction over all persons or companies that have Canadian nationality, regardless of where the alleged bribery offence took place;
- Exclusive authority to lay charges under the Act is given to the RCMP.

These amendments to the CFPOA have made parts of the Canadian anti-corruption legislation more consistent with the US FCPA. Under Canadian law conditional and absolute discharges as well as conditional sentences of imprisonment are not available for crimes punishable by a maximum sentence of fourteen years. Therefore the increase of the maximum term of imprisonment to fourteen years represents a significant increase in severity of penalties under the CFPOA.

[12] http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/1/s14-e.pdf

The Integrity Framework

Quite separate from its efforts to strengthen the CFPOA, the Canadian Government issued in 2012 the *Public Works and Government Services Canada* ("**PWGSC**") Integrity Framework for procurement and real property transactions designed to exclude companies that have been convicted for certain offences from contracting with the Canadian Government. This Integrity Framework was modified in March 2014 to further tighten its debarment regime. Many organizations criticized the Integrity Framework for being excessively severe and even counterproductive in the fight against corruption, as it did not provide for mechanisms to consider remediation efforts taken in response to violations, nor did it give any incentive for companies to self-report. Due to its retrospectivity, companies that had already been penalized for a violation in the past and had reformed itself to become strong advocates of anti-corruption activities would still be subject to debarment from public contracts. Another aspect that drew criticism was the fact that the Integrity Framework did not specify any monetary threshold, e.g. linking the amount of bribes paid to the severity of the resulting penalty. Therefore the consequences for a company that paid a relatively small bribe would be the same compared to a company that had paid several million dollars of bribes. Criticism of the Integrity Framework was so strong, including from Transparency International, the Canadian Bar Association, the Canadian Council of Chief Executives and the Canadian Chamber of Commerce, it was only a matter of time until PWGSC issued a further modification to the Integrity Framework. As a result the Integrity Framework was finally replaced in June 2015 by the current Integrity Regime[13].

>>>

[13] See Government of Canada's Integrity Regime: http://www.tpsgc-pwgsc.gc.ca/ci-if/ci-if-eng.html

The Integrity Regime

Applicable to all federal procurement transactions irrespective of the dollar amount, this Integrity Regime provides for a ten year debarment of bidders that have been convicted of or plead guilty to specific listed offences within the last three years or where their affiliates or the members of their board of directors have been charged or convicted of such listed offences. The list of offences includes crimes such as corruption, collusion, bid-rigging, tax evasion, money laundering, bribing of foreign officials, falsification of books and documents or insider trading to name just a few. Bidders that have been convicted or plead guilty to similar foreign offences are also debarred under the Integrity Regime, however the Integrity Regime now provides for a possible assessment to verify whether the foreign conviction had followed due process if compared to Canadian legal processes.

The debarment of ten years can now be reduced to five years, provided that the bidder can demonstrate that they cooperated with the law enforcement authorities and have taken sufficient actions to remediate the infraction. The new Integrity Regime also takes a somewhat less strict approach to violations committed by affiliates, whereby the determining factor is now whether the entity in questions had any legal or de facto control over the entity that had committed the violation.

Under the new Integrity Regime there is still no minimum Dollar threshold for the judgement of violations and also no concessions offered for self-reporting of offences.

Where a US company prosecuted under the FCAP will in many cases be able to avoid a guilty plea or a conviction by agreeing to the terms of a Deferred Prosecution Agreement, their Canadian competitors do not have such avenue. It furthermore can be argued that the absence of DPA's is viewed as a deterrent to self-reporting and will also lead to much prolonged legal proceedings, as companies try hard to avoid the consequences of a guilty plea or conviction, particularly if their target clients are governmental bodies governed by the Integrity Regime.

Stefan Hoffmann-Kuhnt
is President and Managing Director of Pohlmann & Company's new Canadian office in Montreal. His areas of expertise include the implementation of effective, business-related and risk-based compliance processes and tools.

Germany

Business Partner Checks and Data Protection

Sebastian Bartsch / Dr. Max Erhard

- Anti-corruption laws in numerous countries include extraterritorial reach and wider definitions of legal terms such as corruption, bribery or public official and impose corporate liability for unlawful conduct of business partners.
- In order to mitigate such risks, all relevant business partners should be subject to a risk-based integrity check ("**Business Partner Check**").
- Accordingly, compliance efforts of a company should account for certain restrictions and limitations in order not to lead to violation of the law itself.

A good business relationship is largely based on mutual trust and integrity. Against this background and the background of so many fraud and corruption (and other white collar crimes) cases around the world, a company's integrity plays an ever increasing role as an economic factor. Unlawful conduct of business partners eventually represents a considerable, unpredictable risk for companies. In this context and mainly in regard to liability aspects, the focus of companies has shifted towards compliant behavior of business partners. Especially anti-corruption laws in numerous countries include extraterritorial reach and wider definitions of legal terms such as corruption, bribery or public official and impose corporate liability for unlawful conduct of business partners (i.e. inter alia FCPA and the UK Bribery Act).

In order to mitigate such risks, all relevant business partners should be subject to a risk-based integrity check ("Business Partner Check"). The definition of "relevant business partners" depends in large parts on a company's overall risk profile and the intended business relations.

In German law, statutory requirements concerning the collection, storage, changing, transfer and usage of personal data ("**Use of Personal Data**"; "**Datenverwendung**") can be found in the Federal Data Protection Law ("**Bundesdatenschutzgesetz"** or "**BDSG**"). Accordingly, compliance efforts of a company should account for certain restrictions and limitations on the Use of Personal Data in order not to lead to violation of the BDSG (or other applicable law) itself. There is hardly any present case law on these issues. So it offers only limited guidance[1].

Regarding the legitimacy of the Use of Personal Data, one can differentiate between "if" and "how to" use such personal data. Although this differentiation may not always be quite definite, the distinction nonetheless offers a good guidance in practice.

"If" to use personal data

Article 4 (1) of the BDSG prohibits collection, processing and usage of personal data, if there is no permission or order by the BDSG, another specific legal regulation or consent or approval of the person concerned ("**Verbot mit Erlaubnisvorbehalt**").

However, regulations outside the legal framework of the BDSG that may include such an approval or order do not apply to Business Partner Checks. At times, the prohibitions mentioned in the related EU regulations and Article 17 et seq. of the German Foreign Trade and Payment Act ("**Außenwirtschafts-**

[1] Solely the Federal Finance Court of Germany (BFH) has already dealt with a similar topic, the admissibility of data protection for the examination of internal employees on the basis of terrorist lists, BFH, Judgement of 19 June 2012; File number VII R 43/11.

gesetz" or "**AWG**") are actually seen as bases for permission for conducting the necessary sanctions and embargo list checks.[2] This, however, is not an acceptable practice. The above mentioned norms imply a certain availability and knowledge of personal data (i.e. knowing the identity of the business partner), but they do not regulate the admissibility and scope of collection of personal data. Therefore, they do not meet the constitutional requirements imposed by the principle of legal certainty regarding the Use of Personal Data and consequently are not sufficient as a legal basis for permission[3].

Basis for permission of the BDSG

The central permissions for the Use of Personal Data during Business Partner Checks can be found in Article 28 (1) of the BDSG. The regulation mentions three alternatives of admissibility (No. 1 to 3). These alternatives can individually justify the admissibility of the Use of Personal Data but are not to be applied simultaneously.

The general precondition for admissibility of all three alternatives is the sole Use of Personal Data for one's own business objectives (Article 28 (1) Sentence 1 of the BDSG). This highlights the ancillary nature of the Use of Personal Data for business purposes. The Use of Personal Data for Business Partner Checks prior to a business transaction can clearly be assumed to be of such nature.

Additionally, the intended purpose of the Use of Personal Data has to be clearly defined (Article 28 (1) Sentence 2 of the BDSG). This definition consequently applies to and thereby limits future use of the collected personal data. The individual requirements of the three alternatives of admissibility under Article 28 (18) Sentence 1 No. 1 to 3 of the BDSG are as follows:

- The basic requirement of the permission set out in No. 1 is that the obtained personal data is necessary for the justification, realization and termination of contractual or similar legal obligations with the person concerned. In this context, the central limitation to the Use of Personal Data is the criterion of necessity. Necessary is only what is actually needed in order to fulfil the rights and obligations which are arising from the legal relationship. This may be assumed with regard to the sanctions list check, this being an obligation that is immediately connected with the execution of business. Further checks, especially concerning corruption risks, can hardly be deemed necessary under No. 1.

- No. 2 only permits the Use of Personal Data, if the personal data is needed in order to serve a legitimate interest of the responsible entity (i.e. the company using the personal data) and if this is not outweighed by the interest of the person concerned. A legitimate interest is every actually existing interest, that is justified by the state of affairs and that is endorsed by the legal system of the responsible entity. Such an interest is immanent to Business Partner Checks. Its purpose is the prevention of criminal offences by the company's employees and therefore subsequently the prevention of a legal responsibility of the company itself. Simultaneously, it fulfills the board's obligation to ensure that the company and its employees act within the scope of legal requirements ("**Legalitätspflicht**"). This interest has to be weighted up against the interest of the person concerned. The more intense the intrusion into the constitutionally protected general right of personality (privacy) of the person concerned is, the more likely this person's interest will outweigh any legitimate interest of a company. Therefore, defining clear boundaries for Business Partner Checks is crucial.

>>>

[2] Peters/Schwab, RDV 2006, 196, 196; Meyer/Macke, HRRS 2007, 445, 459.

[3] Cf. Pottmeyer, in: Witte, Praxishandbuch Export- und Zollmanagement, Teil 5 A.5.8.1; Breinlinger, ZD 2013, 267, 268 et seq..; Gola/klug/Körffer, in: Gola/Schomerus, Federal Data Protection Act, Article 4, Recital 8; Sokol, in: Simitis, BDSG Article 4, Recital 12 et seqq.. See also BFH, Judgement of 19 June 2012 File number VII R 43/11, Clause 7 et seqq.

- Lastly, No. 3 requires that the processed data is generally available and that no legitimate interest of the person concerned obviously outweighs. The majority of the Use of Personal Data in connection with Business Partner Checks can be assumed to fulfill these requirements. Even data bases that are liable to costs and are used additionally to internet search engines are classified as generally available sources. However, an obviously outweighing legitimate interest of the person concerned may always impose limitations that have to be met.

Approval of the person concerned

In many cases, part of Business Partner Checks will be to obtain the approval from the person concerned for the Use of Personal Data and thereby obtaining permission under Article 4 (1) of the BDSG. This, however, implies that the approval was in fact voluntarily granted by the person concerned (Article 4a of the BDSG). For this reason, the business partner cannot approve the Use of Personal Data on behave of a third party such as shareholders or directors. The approval will not be considered voluntary if it is granted under duress or obtained surreptitiously. Particularly, a potential economic predicament of the person concerned has to be considered during the Business Partner Checks. The presence of such a situation has to be examined on a case-by-case basis. This kind of predicament often exists, if the business opportunity offered by the data collecting party is crucial for the person concerned in order to secure this person's personal well-being[4]. However, even for such a case the interest of the party using the personal data may in particular cases outweigh the interest of the person concerned and therefore confirm the validity of the person's approval[5].

[4] Federal Constitutional Court (BVerfG), Decision of 17 July 2013 – 1 BvR 3167/08, Clause 18; Decision of 23 October 2005 – 1 BvR 2027/02, Clause 35.
[5] BVerfG, Decision of 17 July 2013 – 1 BvR 3167/08, Clause 18; Decision of 23 October 2006 – 1 BvR 2027/02; Clause 35.

"How" to use personal data

In regard to the question "how" to collect personal data, two principles must be applied. First, this is the principle of data minimization (Article 3a of the BDSG); secondly, the principle of collection of personal data directly with the concerned person (Article 4 (2) of the BDSG).

According to the principle of data minimization, only essential personal data may be used (so-called "need to know"). Therefore, too extensive collection of personal data in the course of Business Partner Checks is not permitted.

According to the principle of collection of personal data directly with the concerned person, required personal data has to be collected from the person concerned. However, in the context of Business Partner Checks certain exemptions may allow the collection of personal data via third parties. These exemptions include publically available sources (Article 4 (2) No.1, in connection with Article 4 (2) No. 3 of the BDSG) and the collection of personal data via third parties if this collection via third parties is essential for and required by the business purpose (Article 4 (2) No 2a of the BDSG). Both exemptions apply to checking sanctions lists, public registries and data bases.

>>>

Conclusion

Over the past years, Business Partner Checks have become compulsory for the majority of companies. However, data protection sets strict and legitimate limits to the Use of Personal Data. Substantiated and informed processes for Business Partner Checks have to simultaneously account for such restrictions and make use of the provided scope and leeway. In the end, efforts to protect the own company should not become legal infringements themselves.

Sebastian Bartsch
is Senior Consultant at Pohlmann & Company. He focuses on Compliance Risk Analyses, maturity analyses of Compliance Management Systems (CMS) as well as business partner reviews and the implementation of risk-based processes.

Dr. Max Erhard
is Associate at Pohlmann & Company in Frankfurt. He studied law at the Albert Ludwigs University of Freiburg and earned his doctorate with a thesis on a competition law topic.

Corporate. Compliance. Governance.

We'd like to know your areas of interest.

Please send us your suggestions via e-mail to:

update@pohlmann-company.com

Pohlmann & Company

Guiollettstrasse 37-39
D-60325 Frankfurt a.M.

P: +49 (0)69 260 1171 40

Nymphenburger Strasse 4
D-80335 Munich

P: +49 (0)89 217 5841 70

1000 Rue de La Gauchetière West 24th Floor
Montreal, QC H3B 4W5, Canada

P: +1 514 448 7487

www.pohlmann-company.com

update@pohlmann-company.com

Subscribe to the International Compliance Update here.

Imprint (Link)