Business Analytics, Big Data, and the Cloud

Regulatory requirements when mining information treasure
Big data and cloud computing are bringing corporate data management back into the picture. They have the potential to facilitate the generation of further profit contributions from the virtually unlimited quantities of data in companies. But there is also a risk of violating regulatory requirements and causing a new data scandal to erupt. So the question is how to exploit this potential and what the limits are.

The market research institute Gartner puts the two topics of big data and cloud computing on its list of the top 10 IT trends for the current year 2012. The faster and more comprehensive analysis of corporate data (business analytics) which they make possible is expected to create a new foundation for forecasts and decision-making. This is indicated by the fact that the worldwide market for business analytics tools in 2011 exceeded the figure of US$12 billion.

**Business analytics, big data, and cloud computing**

We frequently lump together under the concept of big data a number of different technologies which eliminate the limitations in the evaluation of business data which once existed. On the one hand, there are new methods enabling the organization of data by distributing extremely large data quantities across a scalable environment of server clusters and processing them in a complex series of parallel operations (example Hadoop). SAP, on the other hand, combines this method with the use of innovative in-memory technologies in its database technology HANA (high performance analytic appliance) developed in 2010, which uses the RAM, which is much faster than the hard drives previously utilized, as storage for the analysis evaluation. The bottom line is that it is now possible to evaluate far larger quantities of data much more rapidly.

The so-called cloud, on the other hand, is the general term for the virtualization and distribution of computing and storage capacity. Originally, a separate physical server system with its own storage capacity was dedicated to a business application. But since the operation of these systems had to assure full availability even during peak load times (e.g., during close-out of the monthly accounts in the accounting department of a corporate group), the capacities (computing, storage) were designed very generously, even extravagantly, from a cost standpoint. The first wave transferred these physical systems to virtualized servers so that a number of business applications shared one system, making more efficient use of resources. The development of the cloud has now reached the point that the physical location of these virtualized server systems can be selected at will thanks to networking. Customers profit from low costs, the ability to adjust immediately the capacities being used, and the availability at any place.

**Fundamental scenarios for the use of business analytics**

The fundamental scenarios for the use of business analytics tools have not changed in the wake of these technologies, but the power they have for shedding light on the steadily rising flood of corporate data in a short time (real time) certainly has. Essentially, a distinction can be made between two use scenarios
Strategy

in the company: the analysis of customer data for the purpose of increasing revenue (Scenario 1) and the analysis of corporate data for the purpose of enhancing performance (Scenario 2).

The analysis of current customer data with the aid of business analytics tools is especially useful for any company offering highly standardized products to address a mass market, such as is the case for telecommunications providers. As a rule, these providers have at their disposal a large number of discrete customer data records which can no longer be broken down into homogeneous customer segments using “on-board aids” such as spreadsheet programs and addressed specifically in the sense of marketing. Moreover, in the case of transaction-oriented service providers such as banks and telecommunications companies, an extremely large volume of transaction data (records about phone use, so-called call data records, or purchasing patterns revealed by the statements of the credit card data) derived from the attributes of customer data records in the contract data (so-called master data such as place of residence or age) is available.

When analysis methods are employed to enhance corporate performance, the intent is to screen all of the performance data created during production for efficiency potential. We can think here about the derivation of important performance indicators in real time such as those logically arising from the cause and effect chains of balanced scorecard management. The improvement in forecast capability and the speed at which this information becomes available can lead to massive improvements in the management of the production and logistics value chain. In addition, complex scenarios for the comparison of various alternative actions can be calculated and help to prepare the basis for difficult management decisions in advance.

Regulatory requirements

The factor common to both of these usage scenarios is that the potentially great benefits the company might obtain from the analysis are countered by the risk of loss in the private sphere of specific people, customers, or employees. The German Federal Constitutional Court recognized this problem as early as 1983 and elevated the individual’s basic right to control his or her personal information to a constitutional principle in its so-called census decision.

In Germany, the Federal Data Protection Act (BDSG) as most recently revised in 2009 represents the current framework for handling personal data collected, processed, and used in IT systems or manually. Moreover, the various German states also have data protection laws on the books, although they are of little interest for commercial, non-public companies, and there are more specific regulations for certain sectors in special acts such as the Telecommunications Act (TKG) or the Telemedia Act (TMG) for service providers.

The BDSG contains a prohibition concerning the use of personal data which includes a provision allowing consent: “The processing and use of personal data shall be admissible only if this Act or any other legal provision permits or prescribes them or if the data subject has consented” (Section 4 (1) BDSG). Unless a company has obtained the consent of the data subject, it is dependent on legalization based on a law when using available data related to individuals.

Scenario 1: Analysis of customer data to increase revenue

The primary provision for the collection and analysis of customer data is Section 28 (1) number 1 BDSG which permits the storage, modification or use of personal data as a means of “fulfilling one’s own business purposes” so far as it is in accordance with the purposes of a contract (admissibility element 1) or, pursuant to number 2, “necessary to safeguard justified interests [of the company] and there is no reason to assume that the data subject has an overriding legitimate interest” (admissibility element 2).

The question which now arises for the businessman is, of course, how these two alternatives can be realized in practice. With regard to the meaning of “business purposes”, a fairly broad interpretation of the term will arise from the viewpoint of the professionals in a marketing department. After all, the custo-
mers benefit if all of the information about them available to the company is analyzed for the purpose of offering them products which are an exact fit to their wishes and needs; indeed, this cannot be viewed as anything but a special service. For example, why would a bank see anything wrong with taking the analysis of the transactions on a customer's account showing that a large sum had recently been paid out from a building society contract and, in response, sending him or her suggestions for investment of the money?

However, lawmakers see the danger of increasing third-party control over the customers' data in such cases and have defined the concept of business purposes very restrictively so that consumers are protected from such unsolicited cross- and up-selling offers. Consequently, companies may act solely on the basis of an existing, concrete contractual relationship. If a customer has acquired a claim to consulting services along with the product, the provider is free to offer these services to the customer. If, however, it is a matter of offering additional products which would require the establishment of a new contractual relationship, approaching the customer is prohibited pursuant to Sections 4 (1), 28 (1) number 1 BDSG. Correspondingly, the legitimation for analysis of the customer data for the purpose of identifying such sales potential is lacking.

Telecommunications companies make use of this distinction between consulting and marketing by offering options with their rate plans. Pointing out to a subscriber that he or she had very high costs in the previous month is then within the scope of the existing contractual relationship and legitimizes the offer of the appropriate flat rate option. However, it is possible to argue in this case as well that the selection of such an option modifies the existing contract, which means that the marketing character is overriding.

Storage of data in a customer relationship management (CRM) system can be regarded as legitimate with respect to specific customer preferences, provided that the idea of service plays an especially significant role. We could think here of the preferences which guests in higher-class hotels express as a way to assure their well-being in the event that they return for another stay.

Safeguarding justified interests

If the processing of data for the purposes of a contract is prohibited, the second admissibility element pursuant to Section 28 (1) number 2 BDSG concerning the “safeguarding of justified interests” may legitimize the action. However, the company's justified interest in the processing of the data must be related to a concrete processing or utilization purpose. A bank which issues credit cards, for example, might claim a justified interest of this nature which would override the data subject's protected interests if it creates payment profiles intended to prevent misuse.

Actual practice has also shown that this norm, which requires a weighing of the various circumstances, leaves a lot of room for interpretation. However, legal precedents are in agreement that a compilation of customer data going beyond the master contract data – information from consultations, transaction data – and its assessment with the specific aim of increasing revenue is not permissible. Any data mining of a compilation of data in the form of a data warehouse in particular lacks any justified interest because the purpose of the processing could not be concretely stated at the point in time the data are stored.

In summary, we can say that the analysis of personal data for the purpose of increasing revenue is subject to narrow limits. Unless the company has obtained the customers’ consent in advance in accordance with Section 4 (1) BDGS, companies may use the information in their possession solely for the purpose of the contract or, under certain circumstances, for preparation of an offer for special consulting or other services or for the detection of fraud.

Scenario 2: Analysis of the company data for the purpose of enhancing performance

To the extent that companies want to utilize the rising flood of data fed by processes in production and logistics for the purposes of performance analysis and improvement, there are generally no statutory restrictions. After all, the BDSG protects personal data and does not concern itself with the data created during the production process.
If, however, personal data are collected as well (e.g., so that the performance of the specific employee can be assessed), there are restrictions which must be observed by the employer so that excessive surveillance is prevented. Continuous recording of data by the various enterprise systems such as time clocks or application log-ons, for instance, can open the door to comprehensive analysis of employee behavior. The automated processing of these data is subject to the co-determination rights of works councils and personnel representatives. The German Federal Labor Court is quite restrictive in its assumption that data processing “[is] intended to monitor the behavior or performance of employees” if it is possible to attribute the stored performance data to specific employees, regardless of the purpose for which these data were originally captured. In this case, it is possible to conclude a works agreement with the social partners entitled to co-determination which will legitimize the processing in the form regulated in the agreement.

Section 32 BDSG regulates data processing for the purposes of the employment relationship and declares the protection of employee data to be a general principle. It was incorporated into the act in 2009 in response to various data scandals in large corporations. When it is a question of safeguarding employer interests such as the extent to which they exercise their right to issue instructions or monitor the performance of the employees, such actions can be regarded as legitimate in accordance with the legal statute. However, total surveillance (e.g., with the aid of video recordings) is not permitted. There must be a distinction here between the idea of supervision (legitimate) and surveillance (not permitted), but this in turn leaves room for interpretation which can be clearly defined on the basis of a works agreement.

Private use of e-mail clients

One special regulatory feature occurs whenever employees use any means of communication which the employer has provided to them for their work (e.g., e-mail clients). If the employer allows or tolerates the private use of these means, the prevailing opinion is that it then acts as a telecommunications service provider within the sense of Section 3 number 6 TKG (German Telecommunications Act) with respect to the employees. The consequence of this opinion is that the employer would be bound by the secrecy obligation for telecommunications pursuant to Section 88 TKG and the data protection provisions of the TKG, thereby losing completely any access to the e-mails. Although higher labor courts have handed down deviating decisions in isolated cases, companies are urged to conclude and communicate works agreements covering this situation so that access to employees’ work is not completely excluded, e.g., in the event that an employee remains away from the company for a longer period of time (owing to vacation, illness, etc.).

In summary, we can say with respect to the second scenario – analysis of company data for the purpose of enhancing performance – that the evaluation of many types of data from production and logistics does not initially run up against any obstacles. This is where the exploitation of potential for efficiency with the aid of new technologies such as big data and cloud computing comes in. But since legal precedents prohibit data processing which can be used as surveillance, regardless of the actual intent of the company, the works agreements should be modified to take the new opportunities into account as a precautionary measure. Obviously a more in-depth and comprehensive analysis of production processes potentially enables the identification and assessment of the performance of individuals.
The dilemma of the cloud providers

As it is a German law, the BDSG applies only on the territory of Germany. But because there have been numerous and extensive modifications to adapt it to EU directives, we can already think in terms of a Europe-wide harmonization of data protection law. However, cloud providers who want to offer their services in both Europe and the USA are in a more difficult position because the applicable legal systems differ from one another.

There are no general American laws regulating data protection; it is up to the providers to regulate the protection in the specific contracts with their subscribers. But now the discussions are focusing more and more on the US Patriot Act, a federal law passed by the American Congress in 2001 as part of the measures adopted in the fight against terrorism. This act gives American government agencies the authority to force companies to surrender the customer data they have stored. The broad interpretation of the law's provisions by the Americans extends even to data stored in Europe and seeks to apply the obligation to companies whose headquarters are in Europe if they are affiliated with American companies in a corporate group. The cloud providers find themselves on the horns of a dilemma because they are now subject to two regulatory areas which contradict each other. The cloud providers can even be prohibited from disclosing the surrender of the customer data (a so-called gag order) so that the non-American customers do not even learn of the disclosure. As long as this contradiction has not been resolved, the customers have the alternative of storing data in encrypted form in the cloud. But this would mean that cloud computing in the sense of distributed processing would no longer be possible.

Björn Froese works as Management Consultant in Strategy, Innovation, Marketing and Sales (SIMS). Since earning his degree in industrial engineering and management in Berlin and Berkeley, USA, he has worked as a corporate consultant in the field of corporate finance, focusing on corporate transformation and transaction advisory. He has supported a number of very large transformation projects in Germany and abroad. His expertise has been completed by his earning a Master of Commercial Law at the University of Saarland, specializing in contract management.

Bjoern.Froese@detecon.com