International Briefing

January 2018

Editorial

Caro Lettore,

ormai è tutta una questione di dati!

Mentre ci affanniamo a combattere contro l'invasione dei dati nelle nostre vite, il sistema legale affronta il tema della digitalizzazione delle imprese:

Cosa devono sapere gli amministratori delle società tedesche in tema di protezione dei dati sui clienti, fornitori e partner commerciali? Quando si è tenuti a designare un responsabile per la protezione dei dati? Qual è il quadro giuridico emergente in materia di prodotti correlati alle auto connesse ("smart cars")?

A queste e molte altre domande fornisce risposta la presente edizione della nostra Newsletter. Questo numero contiene, inoltre, indicazioni relative ai nuovi obblighi in materia di trasparenza alla luce della IV Direttiva Antiriciclaggio e all'introduzione di un registro elettronico centrale...

Da ultimo...siamo felici di informarLa che BEITEN BURKHARDT è stato nominato Studio tedesco dell'anno per il settore dell'energia e da gennaio aprirà un nuovo ufficio ad Amburgo!

Buona lettura,

Matthias W. Stecher, M. C. J.
Coordinatore dell´Italian Desk

Content

I. Data Protection, Compliance, and Liabilities – Why Directors Must Care

At a recent discussion on the pitfalls of investing in foreign markets, a US private equity manager voiced his biggest surprise: the personal liability that the director of a German company faces in Germany if he or she breaches their broad duties and obligations vis-à-vis the company. Indeed, this potential liability does exist and the fact that one is not actively involved in managing the company rarely provides a defence against claims.

What, however, does this have to do with data protection?

In short, the director of a limited liability company needs to observe all statutory, contractual (by way of the articles of association), or other (by way of shareholders' resolution) obligations in connection with managing the company. One of the obligations is the monitoring of legal developments and changes that affect the company's business, organisation or legal requirements. Accordingly, the new European General Data Protection Regulation (hereinafter GDRP) is a legal development that any director of a limited liability company needs to keep abreast of, review and implement. This is all the more true, because the fines that can be imposed under the GDRP are severe and can amount to up to EUR 20 million or 4% of the global turnover. A company faced with such a fine may rightfully examine whether the director has fulfilled his or her obligations in readying the company for the coming GDRP.

The good news: the GDRP will only enter into force on 25 May 2018. The bad news: potentially, there is much to be done.

A diligent director will have a clear roadmap for implementing the changes required for compliance with the GDRP, will have created deliverables with his team and – in general – will not be surprised by the content of the GDRP. The Data Protection Agency of Lower Saxony has gone so far as to state: Data protection is an issue for the director.

However, reality often looks quite different: we note that knowledge about the GDRP is often limited to data protection specialists. We have therefore identified the major issues businesses need to examine their current practices and possibly amend these practices by 28 May 2018 – or install new practices.

Why did the EU create the GDRP, at all? The current data protection law within the EU is based on Data Protection Directive 95/46/EC. Obviously, there has been significant technical progress since 1995.

Also, the Directive only established a minimum standard, leading to a wide range of data protection laws and no unified standard. To tackle these differences the EU has classified the new data protection rules as a regulation, which requires no transformation by Member States; at the same time, the GDRP contains elements of a directive, as Member States need to adapt a wide range of laws, in order to ensure compliance with the GDRP rules. As an example of the magnitude of the changes that this involves, more than 300 acts need to be amended or have been amended in Germany alone.

How should one go about complying with the impending changes caused by the GDRP?

An initial assessment of data practices should be the first step on the road to compliance with the new data processing regime. The GDRP requests that businesses draw up records of data processing activities (Article 30 GDRP) outlining all data processing operations. This not only relates to customer data, but to all third party data, which is the object of processing. This includes the data of employees, suppliers, consultants and others. Special care is advised when collecting or processing data related to minors, as more stringent protection applies. Likewise, more stringent protection applies to sensitive personal data, such as religion, political persuasion, health or sexual orientation. The data processing directory is not required for enterprises und undertakings with less than 250 employees – this exemption is intended to carve out SMEs. However, this *de minimis* exception does not apply, if the data processing is not occasional. There is hardly a situation, where processing is only occasional. In all likelihood, at least some processing will occur on a regular basis.

Apart from records of processing activities, the GDRP requires a wide range of informational items to be disclosed to the data subject at the time of collecting data. This includes, *inter alia*, the duration of the intended data storage, the revocability of consent, and the transfer of data outside the EU. In practice, this will require the modification of data protection declarations, consent forms and information displayed in connection with third party plug-ins.

The GDRP retains the fundamental approach of requiring either statutory permission or consent to process data (the term "process" includes collection and storage). Consent granted by the data subject pursuant to the current legal framework will, in general, remain valid under the GDRP, providing the manner in which the consent has been given is in line with the conditions set out in the GDRP. This requires urgent attention: data processing based on consent may run afoul of the GDRP's concept of consent! The sooner the current consent mechanism is adapted to bring it into line with the GDRP, the more data can be processed under the new law. Looking back at our initial thought: a director who does not have a clear plan on how to evaluate the current consent mechanism in data processing may breach his duties as a director and not be compliant with the GDRP.

The GDRP also introduces a new concept to mitigate the risks inherent with data processing: a data protection impact assessment. Such an assessment needs to be in writing and identify whether the type of processing used, in particular where new technologies are involved, is likely to result in a high risk to the rights and freedoms of natural persons. Where such a risk is likely, an impact assessment of the envisaged processing operations is required. In effect, the GDRP requires an examination of data processing types, and, if risks are apparent, an assessment of risks and benefits. Commencing certain types of data processing without such an analysis may be a violation of the GDRP and thus also be a breach of the obligations of a director.

The GDRP further introduces the concept of data portability in Article 20 GDRP. This provision gives the data subject the right to demand the transfer of personal data collected by one controller to another controller in a machine-readable format. In essence, a data subject can demand that pictures posted on one social network can be transferred to another, or that their sales history be transferred from one merchant to another. Data therefore needs to be structured in a way that allows such transfers.

The last few months have also shown that data protection breaches may have been covered up or not have been readily disclosed. As a safeguard against this, the GDRP requires the data protection authorities to be notified, even where there is only a suspicion of data breach.

To underscore the importance of adherence to the GDRP, the EU has decided to increase fines dramatically, as mentioned above. Word of mouth has it that the data protection authorities have also increased personnel and are preparing diligently for the monitoring of adherence to the GDRP and enforcement of the new rules. A director is therefore well advised to keep abreast of developments, to install a team that is responsible for managing the process and to drive the necessary change.

For a first overview, you can download the BB data protection app from the Apple App Store

We are available to discuss any further steps that may be needed to help your or your client's organisation meet the legal requirements of the GDRP.

Prof. Dr Hans-Josef Vogel,
Lawyer,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Dusseldorf

II. Preparing for the GDPR – the data protection officer

It is well known that the General Data Protection Regulation ("GDPR") will apply as of 25 May 2018 and will affect all data processing that relates to the European market. The GDPR introduces numerous new data compliance related obligations for data controllers as well as for data processors located anywhere in the world, if such data processing affects data subjects in the European Union. One of the compliance questions often asked by international clients relates to the issue of whether or not to designate a data protection officer ("DPO"): What is the specific role of the DPO and do I have to designate one? Here is a brief overview.

What is the role of a DPO?

According to the GDPR, the data protection officer is the Person who will inform and advise the controller or processor and data processing employees of their obligations under EU or local data protection provisions and monitor compliance with GDPR and other applicable data protection laws.

Is a DPO mandatory?

Companies may choose to designate a DPO on voluntary basis at any time. However, according to Article 37 of the GDPR, a controller or processor must designate a DPO if its core activities are large scale operations of (1) regular and systematic monitoring of data subjects or of (2) processing of special categories of data (Article 9) or personal data relating do criminal convictions and offences (Article 10). However, Member States may establish other requirements related to the designation of a DPO under national law. Germany, for instance, requires companies to nominate a data protection officer if they employ ten or more persons to process personal data, if their processing of data is subject to a data protection impact assessment (Article 35) or if the data processing is for the purposes of transmission or market research.

"If core activities consist of large scale processing..."

The GDPR requirement to designate a DPO is based on the principle that, if the core activities of a controller or processor relate to data processing, this in particular may impact on the fundamental rights and freedoms of natural persons. The term "core activities" means the key operations necessary to achieve the controller's or processor's goals. However, necessary support functions, such as paying wages for employees or operating standard IT and corresponding IT support activities are not considered "core activities".

Further, a DPO is only mandatory under Article 37 of the GDPR if such activities will be carried out on a large-scale basis. However, the GDPR does not define what constitutes large-scale processing. The Article 29 Data Protection Working Party ("WP29") recommends in its *Guidelines on Data Protection Officers* (WP 243) that factors like the number of data subjects concerned, the volume of data and the range of different data items being processed, the duration or permanence of the data processing activity and the geographical extent of the processing activity be taken in to consideration. According to WP29, examples of large-scale processing include the processing of customer data in the regular course of business by insurance companies or banks, processing of personal data for behavioural advertising by a search engine or the processing of data by telecommunications service providers.

Only systematic monitoring or processing of sensitive data trigger the DPO obligation

Not all large-scale data processing will trigger the obligation to designate a DPO, even if this processing is a core activity. The GDPR refers only to regular and systematic monitoring and processing of special categories of data, both on a large-scale basis. The WP29 interprets "regular" as "ongoing or occurring at particular intervals for a particular period" and/or "recurring or repeated at fixed times" and/or "constantly or periodically taking place". To be "systematic" processing must occur according to a system, be pre-arranged, organised or methodical, take place as part of a general plan for data collection or be carried out as part of a strategy. Profiling and scoring activities, location tracking and monitoring of wellness and fitness would therefore be considered regular and systematic within the meaning of Article 37 of the GDPR. Any large-scale processing of sensitive data as defined in Article 9 of the GDPR, including health data, data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, would require the designation of a DPO.

What about the processor?

Article 37 applies to both the controller and the processor. Each must comply with the requirements set out by the GDPR and in some cases both must nominate a DPO.

May I designate a single DPO for several entities?

Article 37 (2) of the GDPR allows a group of undertakings to designate a single DPO, provided that she or he is "easily accessible from each establishment". This is linked to the role of the DPO, which requires the DPO to have a sound command of the entity's local language and be easy for staff and local authorities to contact directly. The WP29 recommends that the DPO be located within the EU in order to comply with the easy access requirement.

What is the Risk?

Any non-compliance with the requirement to designate a DPO is subject to administrative fines up to EUR 10 million or up to 2 % of the total worldwide annual turnover of the preceding financial year of the undertaking, whichever is higher.

But isn't there an App for this...?

Our recently launched BEITEN BURKHARDT Data Protection App provides helpful tools to help you determine whether or not your organisation is required to designate a DPO under the GDPR. The app will be available in the English language soon.

Dr Axel von Walter,
Lawyer, Licensed Specialist for Copyright and Media Law, Licensed Specialist for Information Technology Law,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Munich

III. A German Law Perspective on "Smart Cars"

Two main branches of German law affect automated or "smart cars", namely data protection law and liability under the Federal Road Traffic Act. In both fields, the statutory provisions have been amended recently.

Data protection law

The constant communication of automated cars with their environment creates a great amount of technical[1] and personal data[2], which may reveal information about the driver´s social environment, preferred locations and driving style. Numerous companies from various branches are keen on using such data, e. g. car manufacturers to improve their products, car service stations and workshops to offer individual inspection intervals and insurance companies to offer "pay as you drive" rates to customers.[3]

However, processing the large magnitude of data generated by automated cars may contradict fundamental data protection principles, in particular the principles of data reduction and data economy.[4] It is therefore vital that the purposes of such data collection and processing be defined and restricted in advance, and controls be placed on access to such data by data controllers. Limiting collectable data to that, which is actually necessary for the purposes of the processing, will only be successful if car manufacturers and service providers ensure the principles of privacy by design and by default[5] are already implemented at the conception phase. One possibility would be, for example, to establish an expiry date for non-personal data, so as to decrease the probability that it can be subsequently personalised as a result of the increasing amount of collected and stored data.[6]

Liablity

After the revision of the Vienna Convention on Road Traffic in 2014, the German legislator followed three years later with a law designed to address the legal issues raised by the use of highly and fully automated cars[7]. A precondition for the functionality of automated cars is the exchange of information with businesses (Car-to-Business), other cars on the road (Car-to-Car)[8] and road infrastructure (Car-to-X).

In addition, the involvement of automated cars in traffic situation may move the liability for car accidents from the driver towards the manufacturer. The new section 63a (1) of the Federal Road Traffic Act reacts to this development and requires car manufacturers to equip automated cars with data recorders (so-called black boxes), which use data from satellite navigation systems to record when and where the automated system was active and whether the system requested the driver to take back control. As a result, it may become possible to clarify whether a driving mistake or a system failure led to a car accident, so that liability may be linked to either the driver or the manufacturer of the automated system. Recorded data must generally be stored for six months and, in case of a car accident, for three years. While section 63a (2) of the Federal Road Traffic Act requires the car owner to submit the recorded data to the authority responsible for imposing penalties for traffic violations upon request, the conditions for this transmission are not clearly determined. The legislator has not clarified whether minor or only severe violations trigger this transfer obligation, leaving the data subject in an uncertain position towards the authorities.

Dr Andreas Lober,
Lawyer,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

[1] For example weather or road conditions.
[2] For example current position of the car, acceleration and speed, frequency of recent destination.
[3] Some insurance companies already offer telematics standard rates depending on the individual driving style.
[4] Sec. 3a of the Federal Data Protection Act and, as of 25 May 2018, Article 5 (1) (c) GDPR.
[5] See Article 25 GDPR.
[6] vbw, Die bayerische Wirtschaft, Position Paper – Automatisiertes Fahren – Datenschutz und Datensicherheit, p. 12.
[7] Core elements of a highly and fully automated car are that the automated system is able to manage the driving task, including car steering and complying with traffic rules independently, and that the system can be overridden and deactivated at any time by the driver (Sec. 1a (2) of the Federal Road Traffic Act).
[8] Also known as Vehicle-to-Vehicle (V2V).

IV. New Transparency Requirements for German Companies

New national central register: ownership structures and beneficial owners must be notified

"The German Government tightens up its fight against money laundering!" This was the goal for the implementation of the EU's Fourth Money Laundering Directive in Germany. One of the most essential components of this Directive is the new central electronic transparency register. All legal entities and business partnerships must inform the register about their ownership structure and, in particular, the identity of any beneficial owners.

Companies affected had until 1 October 2017 to comply with this registration obligation.

The transparency obligations apply to any legal entities governed by private law, any registered partnership or other "corporate structures", including trusts and unregistered foundations and similar corporate structures. The goal of the German legislator is to store information about the beneficial owner and to ensure transparency with respect to the natural beneficial owners behind each company. In the future, every Member State of the European Union will have a central transparency register. The transparency registers of the individual Member States will be connected to each other.

Who is a beneficial owner?

Each natural person, who holds or controls more than 25% of a company's capital shares or voting rights or exercises control in a similar manner is regarded as a beneficial owner. This also includes indirect control. The new transparency obligations apply to agreements between several shareholders. In addition, greater transparency is required for trust relationships and voting trust agreements. The beneficial owner's place of residence is irrelevant. Foreign beneficial owners of a German GmbH (limited company), who have their place of residence abroad, will therefore have to be report their ownership to the German transparency register. Administrators of foreign trusts, who have their place of residence in Germany, must also report their details to the transparency register.

Obligations for companies

The companies affected are obligated to gather, keep and update the details of their beneficial owners. Accordingly, the beneficial owners are obligated to provide the companies with the relevant information. The obligations also apply where the beneficial owner's place of residence is abroad. The obligation to send information to the transparency register applied for the first time from 1 October 2017.

Impending penalties

Simple cases of non-compliance with the information obligations can lead to fines of up to EUR 100,000.00. Serious, repeated or systematic violations can lead to fines of up to EUR 1 million or double the amount of the economic advantage gained from the violation, which may even exceed EUR 1 million. Violations of the companies' obligations to provide information on the corporate structure of the shareholders, as well as beneficial owners, carry administrative fines. Here the "naming and shaming" approach is used: in the future all decisions on fines will be published on the websites of the competent authorities, including the names of the persons responsible.

Exceptions

To the extent that the details of the beneficial owners are already accessible from documents or other public registers, registration under the transparency register shall be deemed to be fulfilled. In this case it is sufficient that the information can be gathered from other public registers. Where companies are unable to determine the beneficial owners, despite investigations, the companies are entitled to provide the transparency register with the name of their legal representative as the "beneficial owner". How extensive such investigations must be in order to use this legal representative exception will depend on the individual case.

Access to the transparency register

Generally, the transparency register is a publicly accessible register. Every person with a "legitimate interest" is entitled to information. Although the plan is to treat the right to access the register restrictively, it is unclear to what extent this will be put into practice.

Conclusion

Companies and their corporate bodies as well as direct and indirect shareholders are required to immediately comply with the new obligations. Now that the transparency register is up and running, all companies and other associations in Germany should verify whether they need to register or take further action. If you are interested in further information, please do not hesitate to contact BEITEN BURKHARDT.

Dr Maximilian Degenhart,
Lawyer,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Munich

V. BEITEN BURKHARDT opens in Hamburg

BEITEN BURKHARDT shall open a representative office in the Hanseatic City of Hamburg as of January 2018. A a total number of nine lawyers will move either fully or in part-time to the Hamburg office. "In our view this opening is another logical strategic step as BEITEN BURKHARDT maintains offices where our clients are settled and where we can provide the best advisory quality. In Hamburg, just as in all our other offices, we shall offer the entire range of commercial law and business consultancy services, and we will certainly continue to advise our clients across practice groups and offices", says Frank Obermann, Managing Partner of BEITEN BURKHARDT.

The business landscape of Hamburg features an extremely diversified broad range of industry sectors. Large and medium-sized companies from industries such as aeronautics and transport, healthcare, energy and media business as well as the public sector but also financial and insurance services are domiciled in Hamburg. This mix of trades and industries matches perfectly the portfolio of BEITEN BURKHARDT and will substantially contribute to further develop our industry-focussed consultancy.

Including Hamburg BEITEN BURKHARDT is represented with five German offices, one office in Brussels and China respectively and two offices in Russia.

VI. BEITEN BURKHARDT is Law Firm of the Year for Energy Law

BEITEN BURKHARDT has been awarded the title Law Firm of the Year for Energy Law by the leading German language legal market publication JUVE.

The energy law practice group was delighted when the winner was published on 26 October 2017. BEITEN BURKHARDT continuously strengthened and developed regulatory advice, particularly in the energy industry, working together with all players at the energy law market: energy producers, power suppliers and marketers, as well as grid and storage operators (electricity, gas and heat). The practice group members also work together with energy service providers, project developers and industrial firms, as well as financial investors and financing banks.

This successful development of the practice group convinced the JUVE awarding body in its decision. Providing reasons, the JUVE team said: "The expansion of the Berlin office propelled the law firm to the forefront of energy law. Now the law firm can provide advice to its numerous new, also international, clients more comprehensively than ever. The approach pays off: The team is well positioned on the consultant list of large energy suppliers."

Dr Maximilian Emanuel Elspas, head of the energy law group, is particularly delighted that the "successful work of the previous years has been honoured with this prize. Such an award motivates the entire team." Frank Obermann, Managing Partner at BEITEN BURKHARDT, adds "that this award is a symbol of BEITEN BURKHARDT's continuing development. The whole law firm is pleased about the honour. Moreover, the recognition confirms BEITEN BURKHARDT's successful strategy to focus on industries."

VII. L'Italian Desk

l'Italian Desk è nato per rispondere alle esigenze delle società italiane interessate ad espandere la propria attività sul mercato tedesco, nonché di quelle che in Germania abbiano già avviato la propria impresa.

Viceversa, assistiamo anche imprese tedesche che intendano internazionalizzare il proprio business in Italia e quelle già attive nel Belpaese.

I nostri esperti operano a Monaco di Baviera e a Düsseldorf. I membri dell'Italian Desk gestiscono le pratiche in italiano.

Ai nostri clienti italiani forniamo un'assistenza multidisciplinare, così da poter far fronte a richieste che implichino l'intervento coordinato e organizzato di differenti competenze professionali.

In particolare, prestiamo consulenza nell'ambito di operazioni societarie straordinarie, di operazioni immobiliari, nella costituzione di società e nella definizione di programmi d'investimento, nonché in ambito finanziario e fiscale.

Please note

This publication cannot replace consultation with a trained legal professional.

If you no longer wish to receive this newsletter, you can unsubscribe at any time by e-mail (please send an e-mail with the heading "Unsubscribe" to **ItalianDesk@bblaw.com**) or any other declaration made to BEITEN BURKHARDT.

Imprint

This publication is issued by
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH

Ganghoferstrasse 33, D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich /
VAT Reg. No.: DE811218811

For more information see:
https://www.beiten-burkhardt.com/en/references/imprint

Editor in charge

Thomas Seipel

Your Contacts

Beijing • Suite 3130, 31st floor • South Office Tower • Beijing Kerry Centre • 1 Guang Hua Road • Chao Yang District • Beijing 100020
Susanne Rademacher
Tel.: +86 10 8529-8110 • Susanne.Rademacher@bblaw.com

Berlin • Kurfuerstenstrasse 72-74 • 10787 Berlin
Dr Christian von Wistinghausen
Tel.: +49 30 26471-351 • Christian.Wistinghausen@bblaw.com

Brussels • Avenue Louise 489 • 1050 Brussels
Dietmar O. Reich
Tel.: +32 2 6390000 • Dietmar.Reich@bblaw.com

Dusseldorf • Cecilienallee 7 • 40474 Dusseldorf
Dr Claudio G. Chirco
Tel.: +49 211 518989-144 • Claudio.Chirco@bblaw.com

Frankfurt am Main • Mainzer Landstrasse 36
60325 Frankfurt am Main
Dr Detlef Koch
Tel.: +49 69 756095-408 • Detlef.Koch@bblaw.com

Moscow • Turchaninov Per. 6/2 • 119034 Moscow
Falk Tischendorf
Tel.: +7 495 2329635 • Falk.Tischendorf@bblaw.com

Munich • Ganghoferstrasse 33 • 80339 Munich
Matthias W. Stecher
Tel.: +49 89 35065-1431 • Matthias.Stecher@bblaw.com

St. Petersburg • Marata Str. 47-49, Lit. A, Office 402
191002 St. Petersburg
Natalia Wilke
Tel.: +7 812 4496000 • Natalia.Wilke@bblaw.com

You will find further interesting topics and information about our experience on our website.