e|s|b Rechtsanwälte

Dresden Stuttgart Berlin Leipzig Prag

DATA PROTECTION, DATA SECURITY AND COMPLIANCE

DR. J. BÜCKING

VERNE GLOBAL

VERNEGLOBAL.COM

FOREWORD

In the field of international jurisprudence, there are many different ways of looking at an issue and a variety of different legal systems. This is exemplified by the difference between case-based Anglo- American common law and the European civil law approach, based on codified statute law. Similarly, the US approach to storing data stands in marked contrast to the European approach. The former involves dispersing data to multiple data centres distributed around the country (or indeed globally) with the aim of maximising resistance to attack and obfuscating data location. The latter insists on continuous access to and control over technical and organisational security measures, including where data is located. There is one thing, however, on which all are agreed – in this day and age, legally watertight storage and provisioning of business-critical information is no longer a legal nicety, and compliance with relevant standards requires proper backup and archiving processes. Since 2013, a series of revelations on mass surveillance carried out by a range of organisations, but particularly the NSA, have highlighted the importance of protecting both business and personal data. Data protection has become a core issue for business. Few people really understand the details of the business and personal liability risks that these issues give rise to. Non-compliance in this area can have fatal consequences for businesses. Legal consequences have ranged from potentially invalidating shareholders' formal approval of the board's activities (as required under German company law), to sackings and removal of the CEO's authority. Companies can also find themselves inadequately insured or even uninsured against such 'cyber-risks'. This white paper offers an overview of liability- related risks and looks at how an appropriate system of IT security management can limit these risks. The focus of the paper is on Iceland's status as a data haven for cloud services and data backups and archiving, viewed from the perspective of German data protection law.

PART 1: IT SECURITY OBLIGATIONS AND LIABILITY

Back in the good old days, the fate of a company was decided by its assets, raw materials, staff skill levels and order books. Today, its key operational resources are more likely to be the availability of information and its ability to protect that information. Studies show that failure of key IT systems for as little as 10 days is sufficiently damaging to a company that the chances of it exiting the market within 5 years are as high as 50%[1]. 93% of companies which suffer total data centre failure for 10 days or more file for bankruptcy within a year[2]. 70% of companies faced with catastrophic data loss are forced to close up shop within 18 months[3]. Other surveys have found that as many of 90% of companies which suffer business-critical data loss are forced to cease operations within two years[4]. Despite this, only 35% of SMEs have detailed plans for dealing with an IT disaster[5].

GENERAL IT LIABILITY RISKS

Given that availability of business data can be a matter of life or death for businesses and public sector organisations, it follows that they have a legal duty to ensure that they have in place effective risk and information management systems, which need to include meticulously documented internal control mechanisms. Under their corporate governance obligations, ultimate responsibility for ensuring compliance with this legal duty falls to senior managers. Monitoring and notification obligations are also incumbent on compliance, IT security and data protection officers. As well as protecting their IP, one of the key incentives for companies in safeguarding their information resources is to ensure that they are properly equipped for any future legal disputes with competitors, public authorities, staff etc. over issues such as contracts, liability, product quality or consequential damages. This requires documentation which is able to satisfy the rules of evidence. In the digital age, the key factor in determining the admissibility of documentation as evidence in such disputes is IT security. Proper risk management is therefore an essential component of a robust business strategy. In an era of outsourcing, cloud computing, widespread industrial espionage and mass surveillance, risk management needs to encompass information and communication management systems.

INDUSTRIAL ESPIONAGE

According to recent reports from reliable sources ranging from Europol and the German Ministry for Economic Affairs to German IT association Bitkom, the NSA alone stores data from 20 million German phone calls and 10 million German internet connections daily[6]. This level of surveillance is not aimed purely at preventing terrorism – it is also used to further business interests. The latest revelations suggest that domestic intelligence agencies may even have been complicit in allowing foreign business interests to obtain confidential business information[7].

Germany is subject to a higher level of industrial espionage than any other EU member state. According to a Bitkom study[8], half of all businesses are affected. SMEs in particular are subjected to industrial espionage on a daily basis. One business in five has already suffered data theft, and this figure is on the rise. According to Bitkom, losses from espionage amount to €51 billion per year; at the global level, Europol estimates worldwide losses at €290 billion per year[9]. The Bitkom figure is largely made up of lost revenue as a result of the unauthorised use of stolen intellectual property, costs from patent infringements, and losses arising from failure, theft of, or adverse impacts on IT systems and operating procedures. Theft of sensitive digital documents, IT sabotage, and eavesdropping on electronic communications are the most frequent crimes. Despite this, fewer than half of German businesses are adequately protected. Though awareness of the problem is increasing, studies nonetheless show that 25% of SMEs do not have a security strategy in place. The average annual spend on IT security by SMEs is just €3,300[10].

In addition to attacks (espionage or sabotage) and IT disasters, there are other ways of losing data. European companies with more than 50 employees lose an average of 552 man hours per year as a result of IT downtimes and business data recovery measures[11]. In the US, 140,000 disk drives suffer total failure each week[12]. 6% of all PCs suffer data loss each year[13]. 31% of PC users have already lost all of their files as a result of an event beyond their control. 34% of companies do not test their tape backups – 77% of those that do discover errors[14]. According to a 2014 study by the Ponemon Institute, the average cost of a data disaster was $7.2 million or $214 per record lost[15]. Forrester Research puts the average cost of a data disaster at $1.4 million. It takes businesses an average of 18.5 hours following a data disaster before they are able to resume their key business processes[16].

HOW SAFE HARBOR WAS KNOCKED OUT

In principle, it would make sense to outsource the maintenance of data and systems to specialised companies and external data centres. However, five of the world's ten largest server farms are located in the US, a country that has become increasingly suspect. Transmitting data to international clouds always requires legal legitimation. Especially for transfers to unsafe 'third countries', as the EU had rated the US in terms of privacy law, most companies had been using the 'Safe Harbor' self-certification. Until recently, many companies were still using 'Safe Harbor' certification to provide legal cover for data export to the US. Quite apart from the need for a legal cause to do so, transferring data to the US (being an 'unsecure third country' in terms of data protection) had only been permissible where the recipient ensures that data is subject to an adequate level of protection, which has to be confirmed by the relevant certification. However, the (effectively decisive) statement by the 'Article 29 Data Protection Working Party' (the independent advisory body of the European Commission in data protection issues) had already raised massive doubts about the effectiveness of 'Safe Harbor', as this certification in its current form was no longer seen as suitable to guarantee an adequate level of data protection – and hence 'Safe Harbor' was also no longer able to give the 'cloudsourcing' companies and their decision-makers a clean bill of health from a liability perspective. As a result, the 'Safe Harbor' principle had been criticised as inadequate also at the level of the various national data protection agencies (in Germany, for example, by the Düsseldorfer Kreis as a leading body of the Federal Commissioner for Data Protection), and now, on October 06, 2015 also the European Court of Justice (ECJ) has effectively declared this regulation invalid[17] for the exchange of data between the US and the EU. In its ruling the court stated that the US, being a 'third country' without a data protection level matching the EU level, was not providing adequate protection for personal data, not even under 'Safe Harbor'. By October 2015, 4410 US companies had been certified under 'Safe Harbor', including the major cloud providers such as Microsoft, Apple, Adobe and Google.

Accordingly, when transmitting data to the US, the entity responsible for data processing may with immediate effect no longer rely on self-certification under the 'Safe Harbor' principles, but has to either verify compliance with legality criteria individually for each data transfer, use the EU standard contractual clauses ('Model Clauses') for commissioned data processing, or adopt Binding Corporate Rules (BCR) and have those approved by the competent data protection supervisory authorities. Yet, the viability of those two variants is questioned by the ECJ ruling (more details further down). However, these three options have so far been the basis for many well-known Cloud providers to allow a transmission of data to the US. Now, trade associations and the German government plan to jointly develop a strategy against industrial espionage, but building national or European Cloud structures is costly and will take time – time that the industry doesn't have in light of the massively increasing attacks.

PRIVACY SHIELD – A LEGALLY ROBUST SUCCESSOR?

The fate of the substitute solution to 'Safe Harbor' announced by the EU Commission on January 20, 2016 under the working title 'Privacy Shield' is unclear. After 'Safe Harbor' had become obsolete, especially the industry had pushed for a swift political solution between the EU and the US.

The Commission arrives at the result that the legal framework of the EU/US Privacy Shield meets the requirements defined by the ECJ in its 'Safe Harbor ruling', seeing that the US government had made convincing pledges stating that a strict compliance with privacy regulations would be ensured and the national security agencies would not mass-monitor data indiscriminately.

In fact, however, there are still major hitches, in particular the Presidential Policy Directive 28 allowing the use of mass data monitoring for specific national security purposes such as the fight against terrorism, anti-espionage, preventing the spread of weapons of mass destruction and 'international criminal threats'. Considering those continued data tapping options and the possibility that the new president might extend the authorities' powers, there are clear doubts about how legally robust the findings of the EU Commission may be; in detail:

On July 12, 2016 and with effect of August 01, 2016, the EU Commission has consented to the controversial 'Privacy Shield', with the result that now companies wishing to transfer data between the EU and the US can obtain a certificate stating that they meet the Privacy Shield requirements; they will then be entered into a list of certified companies maintained by the US Department of Commerce. From a legal view, the Privacy agreement is a decision by the EU Commission and as such binding. Therefore, while in force it can be used as a legal basis for the data transfer between EU companies and US data importers and for the transatlantic exchange of data.

From an entrepreneur's perspective, however, the primary goal is to achieve legal certainty, i.e. to establish a sustainable and reliable practice for international data traffic that will enable safe investments. Relying exclusively on Privacy Shield does not seem advisable at present, and considering the mix of risks on the one hand and the interests of the affected companies on the other, it may not be suitable to position the companies for data exchange with the US over the long term in a legally secure way. Without additional safeties – for example in the form of the EU standard contractual clauses ('Model Clauses') and the Binding Corporate Rules (BCR) (which, again, are getting increasingly criticised by privacy activists) – companies should not rely solely on Privacy Shield, for the following reasons:

Simply put, the idea of Privacy Shield is to restrict access by government agencies as much as possible and to establish effective protection measures and oversight mechanisms that protect the rights of EU citizens effectively, respecting their constitutional right to be heard before a court. However, leading EU privacy activists point out that Privacy Shield suffers from the same fundamental shortfalls like 'Safe Harbor' as far is ECJ jurisprudence is concerned. In their view, Privacy Shield may be doomed by the same fate as its predecessor. Indeed, Privacy Shield raises more questions than it answers. Accordingly, numerous companies – heeding the advice of reputable experts – do not intend to rely on the 'shield'. As it is unclear how legally robust the final content of the agreement will ultimately be and due to the increasing criticism by privacy activists, many cloud providers have resorted to moving to regional data centres:

Not only due to the opinion of the influential Article 29 Working Party, Privacy Shield will not be able to provide legal certainty over the long term. The working party only plans to release a final assessment once the EU General Data Protection Regulation (GDPR) has been passed in 2018 (refer to the National and EU legislation section below), since Privacy Shield must also comply with the new (higher) requirements of the EU data protection law.

Also, the history of how Privacy Shield was created is not exactly trust-inspiring. Shortly before the Commission's decision of consent, in the beginning of June 2016 the EU Data Protection Supervisor had rejected the Privacy Shield in its then form, reasoning that it would not stand scrutiny by the ECJ. The main point of controversy was the issue of how the personal data of EU citizens could be protected from mass-surveillance by US government agencies. It was argued that as long as those agencies were allowed to access the content of electronic communication – without valid reason in individual cases – it would automatically be clear that according to relevant case-law regarding 'Safe Harbor', the ECJ would also crush the new agreement, unless the US would simultaneously change their surveillance laws, something the US government has not been prepared to do until today. It only went a tiny step in the EU Commission's direction by ruling that US companies must delete user data once it is no longer fulfilling the purpose for which it had been collected. This, of course, means that US agencies may still access the personal data of EU users, only the amount of data is limited by the industry's obligation to delete specific obsolete data material. Even though under the new agreement any bulk collection of data should only be allowed if it is done "as targeted and focused as possible", such vague legal terms are an open invitation to an opportunistic interpretation of the situation depending on the political agenda of the day.

Also in Germany, leading privacy activists such as Thilo Weichert and consumer protection organisations such as the Federation of German Consumer Organisations (Verbraucherzentrale-Bundesverband - VZBV), the German Data Protection Association (Deutsche Vereinigung für den Datenschutz - DVD) and the Independent Data Protection Centre (Unabhängiges Landeszentrum für den Datenschutz - ULD) of Schleswig-Holstein have opposed the Privacy Shield, regardless of any later amendments that the European Data Protection Supervisor Buttarelli had demanded from the EU Commission.

One of the issues they criticised was that Privacy Shield failed to meet the transparency requirements designed to safeguard the rights of affected users by providing them with information needed to enforce their rights effectively, and that the EU Commission's decision on adequacy finding never carried out a comparative law analysis against European standards. Therefore, they argued, Privacy Shield already failed to meet the requirement for a substantiated explanation of the adequacy finding. Vital basic principles of European privacy law such as the consent principle, the identifying purposes principle and the principle of data minimisation, the right to information and the notification of processing steps were lacking. Also, Privacy Shield disregarded the principle of balancing between the interests of the data processor and the affected individual. Furthermore, the complaints body to be implemented would not act comprehensively for all regulatory areas of Privacy Shield and would not be independent like a court but hierarchically embedded into the US administrative machinery – contrary to the requirements under European law. Accordingly, data protection monitoring would remain inadequate in terms of European standards, and the indiscriminate data access by security and secret service agencies left those affected without rights and subject to controlled data mining. Finally, they argued, the US also did not have any effective legal remedy against violation of basic data protection rights and to ensure that communication is kept confidential. In addition, there was a lack of effective monitoring and control mechanisms, which would be vital to detect and punish any infringements. Another demand is that in the event of impermissible data processing, the rights of affected parties, in particular the right to information and the right to data deletion, needed to be enforced effectively. This meant that the affected individuals always needed to be able to claim damages before European courts, which also was not provided for in this form under Privacy Shield. As a result, they argued, the Commission's decision violated basic European rights and failed to meet the requirements of the EU Data Protection Directive. Therefore, it also entailed an impermissible privileged treatment of the transatlantic data trade in favour of the US. This precedent could encourage other countries that are seen as unsecure 'third countries' in terms of data protection, to demand recognition on the same level, which in turn might lead to a massive lowering of the protection level for data traffic across the outer EU borders. This, in turn, would result in a discrimination of companies in the EU internal market, whose data processing would be subject to the EU GDPR in future. Therefore, (also) organisations like VZBV, DVD and ULD doubt that Privacy Shield will stand before the ECJ in the long run, considering the continued practice of unfounded mass-surveillance by US secret services. After several organisations have already announced legal action, businesses and consumers will have to brace for a situation of legal uncertainty over several years.

Privacy activist Max Schrems, who had won the ECJ judgement declaring 'Safe Harbor' invalid, sees Privacy Shield as equally flawed right from its start. He complained that with the Presidential Policy Directive 28, Privacy Shield provided for no less than 6 exceptions that could be used to allow unfounded mass-surveillance "in exceptional cases". Those were worded so vaguely that they could be applied to "virtually anything". For example, the list of exceptions states the need to "identify and address certain activities by foreign powers" which would equal a license for unfounded mass-surveillance of all non-American data. Also, the protective mechanisms were significantly lower than the requirements established by the ECJ. Therefore, also the EU Commission's approach was misguided, in his opinion. As the ECJ was deriving its 'Safe Harbor' criteria directly from the European primary legislation, i.e. the EU Treaties and the European Charter of Fundamental Rights, which were non-negotiable, the EU Commission had the duty to comply with this primary legislation and not to question it by entering into negotiations with foreign powers such as the US.

Finally, with his statement the European Data Protection Supervisor Buttarelli concurs with the numerous critics by forecasting that the agreement in its current form would not stand scrutiny by a court, as it lacked protection from surveillance by the state and an effective monitoring of US agencies, in particular by the lacking implementation of legal remedy mechanisms for affected individuals. Therefore, Buttarelli had requested the EU Commission – while negotiations were still ongoing – to find a permanent and sustainable solution with the USA.

The good news is: as Privacy Shield came into effect, we are currently experiencing a factual grace period, shown by the fact that even though the data protection agencies impose fines for continuing data exchange with the US based on the previous 'Safe Harbor' agreement, they are currently not sanctioning those who prefer to make use of the alternative option of the EU standard contractual clauses in view of the principle of good faith, with the effect that those companies only favouring Privacy Shield may at present claim such good faith, until Privacy Shield may eventually be found as failing to comply with European law by the ECJ, as many fear. However, it is doubtful that such a (yet another) knock-out decision by the ECJ is still far away and that Privacy Shield would take away pressure from businesses for now, winning them time. To the contrary, the signs are becoming increasingly gloomy as far as the various data exchange options are concerned. Now the data protection agencies have already started to suspend the approval of data exchange contracts on the basis of Binding Corporate Rules (read more under Model Clauses and BCR below). And even the first legally viable alternative to 'Safe Harbor' (and now Privacy Shield) – the EU standard contractual clauses ('Model Clauses') – have in the meanwhile come under court scrutiny when the Irish Data Protection Commissioner brought the question whether they comply with EU law in terms of data protection before the ECJ, as was announced on May 25, 2016. This is an indication that the Irish privacy protectors do not believe that Privacy Shield can be legally implemented, instead focusing on the Model Clauses as an alternative solution.

MODEL CLAUSES AND BCR

Therefore, it seems doubtful whether the EU standard contractual clauses (Model Clauses) or the Binding Corporate Rules (which also require approval by the authorities) can be used as a sustainable, legally secure alternative for commissioned data processing. As no suitable successor had been in sight, many companies had switched to the standard contractual clauses for the same data exchange practice, even though the protection of European data in the US had not factually and legally improved. As a result, not only the successor agreement Privacy Shield but also this currently preferred alternative solution in threatened to be knocked out.

The Art. 29 Data Protection Working Party has already announced that they intended to critically scrutinise those alternative company practices against the background of ECJ jurisprudence. To be compliant, the data importer would need to guarantee to the European data exporter that according to his knowledge he is not subject to any laws that would prevent him from adhering to the data exporter's instructions and from meeting his contractual obligations. However, it is precisely this contractual obligation that US contract partners are unable to meet, considering the legislation in the US. After all, just like with Safe Harbor, also with the EU standard contractual clauses it cannot be excluded that US agencies may access personal data coming from Europe. There are no recognisable reasons that those clauses would provide any efficient protection from access by US agencies. Instead, the US legislators should rather drastically restrict the access options of their government agencies and secret services, which they are not prepared to do. This was eventually also the reason why the Irish Data Protection Commissioner has submitted the EU standard contract documents for verification before the competent Irish court. It is seen as certain that within those proceedings, the issue whether the standard contracts are valid will be submitted to the ECJ and decided within the following 12 to 24 months.

In view of this background, according to reputable privacy activists, the European data exporter – considering the supervisory authorities' right to prohibit or suspend transmissions to the US via administrative decree – can only avoid contract violations of an EU standard contract by the US partner by making use of his contractual right to terminate the standard contract with the US data importer.

Also, according to a position paper of the individual German data protection authorities of the federal and regional governments (Data Protection Conference), in light of the ECJ ruling, it is questionable whether data transfers to the US on the basis of the other used instruments, in particular the BCR, are permissible. After the data protection authorities have until further notice stopped issuing new permits for data transmissions to the US on the basis of such company agreements or data export contracts, the affected companies are therefore required to restructure their data transfer procedures promptly. Accordingly, companies wishing to export data to the US or other 'unsecure third countries' in terms of the data protection laws should consult the decision of the Data Protection Conference from March 27, 2014 regarding the "safeguarding of human rights in electronic communication" and the orientation guide "Cloud Computing" from October 09, 2014 for guidance.

Consent in terms of data protection law (as a last basis for legitimation) is no serious option within automated business processes for data exchange with the US. Such express and individual consent can only be a sound basis under narrowly defined conditions. As a basic principle, however, such data transfer may not occur on a repeated or routine basis and in bulk. Therefore, when exporting employee data or when data of third parties is affected at the same time, consent can only in extreme exceptional cases be a reliable basis for data transfer to the US.

INTERIM FINDINGS REGARDING EU/US DATA EXCHANGE

Data transfer to the US can no longer be based on 'Safe Harbor'. Where data protection authorities become aware of this, they will prohibit such practice and issue a fine. A certification under Privacy Shield, on the other side, still enjoys the protection of good faith in the correctness of the related EU Commission ruling until further notice. Although the admissibility of data transfers to the US based on the EU standard contractual clauses and BCR has in the meanwhile also been questioned, until the Article 29 Working Party issues statements to the contrary it can be presumed that data transfers on this basis will not be sanctioned by the German authorities. Yet, the national authorities will scrutinise data transfers to the US autonomously and independent from any Commission decisions. New permits for data transfers to the US based on BCR or data export contracts should not be granted at present.

Until a legally sound successor agreement has been found, the legal uncertainty continues. Any transmission on the basis of 'Safe Harbor' may lead to fines of several hundred thousand Euro[18]. Also the regional data protection authorities, who handle the situation differently from region to region, cannot be expected to provide legal certainty. The good news is that Privacy Shield will offer companies a 'grace period' until further notice, as supervisory measures and actions limit themselves to sending hearing questionnaires to companies regarding their data protection practices. Regardless of this, however, the industry is left with the additional risk that competitors, data protection authorities, affected parties or associations – encouraged by the new right to bring collective action – may make their life difficult with formal warnings, injunctive relief and actions for injunction against unlawful handling of personal data.

COMMISSIONED DATA PROCESSING

All this makes a data protection-compliant outsourcing of personal data processing to global clouds virtually impossible, unless in the exceptional case of a permissible 'commissioned data processing' (CDP) involving a controller and a processor. In terms of European law, CDP is only permissible if this is permitted by a law or if governed by a written contract. If the latter applies and there is no such contract, this constitutes an infringement against the controller's obligation to document the relevant responsibilities in writing, which may lead to sanctions. The processor must be selected carefully according to criteria such as reliability, performance, its state of the art technical-organisational security measures, etc. The selection includes in particular monitoring of the technical-organisational measures prior to the start of any data processing and then regularly during CDP. The corresponding contract must meet specific minimum requirements. It must in particular stipulate that the processor himself and those people reporting to him and having access to personal data may only process such data as instructed by the controller. Nevertheless, the controller must still be legally and factually able to intervene in the processor's decisions regarding the means of processing; so the overall responsibility is still with him. This means that the controller must monitor all processors effectively to ensure that their decisions are in line with his instructions, the CDP contract and data protection law. If a processor fails to adhere to the specified restrictions on how the data may be used, the processor 'mutates' to become a controller himself, who is responsible for the processing and would then act unlawfully. The original controller, for his part, would have to answer for why and how the processor could have infringed on his contractual order. In such case, the Article 29 Data Protection Working Party tends to assume that there is a joint legal responsibility (also in terms of liability), as this provides the best possible protection of the interests of affected individuals. An important consequence of such joint responsibility is then the joint and several liability for damages. An additional aspect is that although the EU Data Protection Directive in principle regards the controller as liable, but – apart from the above-mentioned exceptions – this does not prevent the national data protection legislations from also holding the processor liable in certain cases.

Since, as discussed above, 'Safe Harbor' can no longer be claimed as legitimation but the use of US clouds constitutes a data transfer to an unsecure third country, according to the Article 29 Working Party any such data transmission would additionally require an agreement on the CDP with the above-mentioned contents to ensure fulfilment of the carefully considered necessity and proportionality requirements. This, however, would impose virtually insurmountable obstacles for data processing within the US clouds to be permissible.

LEGAL RISKS

Flexibility and cost benefits notwithstanding, outsourcing of data storage to external data centres (including cloud platforms) entails a host of new risks to which previous generations of electronic information and communications management processes were not subject. This affects the security, confidentiality, integrity, and availability of business-critical data from the cradle (generation of that data), through the life cycle (editing, transfer), to the grave (archiving/deletion). Business-critical data encompasses personal and taxation-related data, trade secrets (e.g. R&D data), customer data, personnel data, etc. For personal and taxation-related data, heavy fines can be levied for each individual access denial or illegal overseas data storage event.

External data centres can unleash novel income streams and deliver major cost savings, but a detailed (and transparent) spec is needed, and companies thinking of going down this route need to carefully examine whether the specific solution can be implemented so that it is technically secure and legally watertight. From a judicial point of view, it is taken as a given that business-critical and evidentiary documents will be retained within the business. Under German law, when this is not done, it can be deemed failure to meet the obligation to provide evidence and be enough to tip the scales of justice against the offending party. Businesses must be in a position to deliver up digital documents in an orderly manner or expect to face appropriate sanctions. It is not uncommon for such documents to prove key in resolving a legal dispute, either by providing proper evidence for the plaintiff's or by undermining the counterparty's position.

A fully auditable document management system able to deliver legally admissible evidence is particularly important for businesses with US or UK operations, where stipulations on digital evidence were added to civil procedure rules in 2006 and 2010 respectively. (The new rules were also accom-panied by the introduction of new sanctions for breaches of confidentiality and new data protection obligations.)

In the face of global competition and rising risks from data loss and data theft (and a thriving black market in stolen data), businesses are finding protecting and accessing their intellectual property increasingly difficult. As a result, IT and legal departments now work closely together to compile and implement new policies and utilise technical and organisational security measures to protect business processes. Issues at stake when data is lost or stolen include reputational damage, lost orders and consequential financial losses. But serious data protection breaches can also give rise to major sanctions – in Germany this includes fines of up to €300k per case. Breaches of German Tax Code regulations on external tax auditing and data access can entail fines of up to €250k per breach, as can improper outsourcing of electronic bookkeeping to a non-domestic service provider. Tax legislators have taken into account the need of international businesses for efficient cross-border labour arrangements by allowing taxable entities to have their bookkeeping carried out electronically in another EU member state (as long as defined conditions are met). They have, however, balanced this with heavy sanctions where outsourcing, whether domestic or international, fails to comply with relevant legal requirements.

Whilst the consequences of failures to protect personal, tax, or business critical data can be serious, breaches of data retention obligations can attract more severe (and even criminal) sanctions. For example, should a company lose or be unable to locate financial data, and, as a result, be unable to provide a proper account of its finances, the company and its institutions may find themselves liable for the consequences. Likewise where the security of trade secrets is compromised. The German Appeals Court has extended the duty of care owed by boards of directors and compliance officers by requiring them to ensure that employees do not perform criminal acts when acting for the company. That duty also extends to ensuring that criminal acts are not committed from within the company[19]. This applies to compliance officers, to posts such as IT security officers and potentially also to data protection officers.

To ensure that it is admissible as evidence in civil courts, archiving of business email must be fully compliant with all legal requirements, be well organised, and permit access at all times. This provides businesses with strategic legal certainty in the event of legal disputes with contractual partners, works councils, individual members of staff, third parties, the tax office, etc. Financially, the major risk is liability for failures of IT risk management. Non-availability of evidential data or of business-critical systems can result in significant losses. Management's personal liability notwithstanding, this can, as noted above, have wide-ranging consequences, from potentially invalidating shareholders' formal approval of the board's activities, to sackings and removal of the CEO's authority.

Information and communication management systems are a cornerstone of this risk control process. One of their key tasks is to guarantee the operational continuity of the IT infrastructure and provide protection from attacks on that infrastructure. At stake are the security, confidentiality, integrity, and availability of business-critical information such as emails, development documentation, trade secrets, other highly sensitive documents (such as health data), evidential data, etc. In practice, businesses are often slow to deliver on these requirements. Problems (such as the loss or inadvertent release of key data) arising as a result of organisational failures can have wide-ranging consequences. Culpability may be laid at the door of senior management, those responsible for such failures could be saddled with liability and they could also invalidate the company's insurance cover. (See also "Consequences of inadequate information management".)

NATIONAL AND EU LEGISLATION

There are a range of domestic and international regulations concerning the protection and security of personal, tax-related and other business critical data (and in particular data relating to intellectual property). In Germany, these regulations are set out in a variety of specific laws, but in particular in the Federal Data Protection Act. Under Section 9 of this Act, all organisations which process, collect, or make use of personal data are obliged to have technical and organisational security measures in place to meet the Act's requirements. This requirement is specified in more detail in the Annex to Section 9, clause 1, which states that measures must be taken "to ensure that personal data is protected from accidental destruction or loss (availability control)." This means, among other things, having a backup concept which ensures that data is not lost if it is accidentally deleted or destroyed.

Other countries impose similar, in some cases more exacting, requirements. All US businesses and audit firms, as well as foreign businesses and audit firms listed on a US stock exchange, are subject to the 2002 Sarbanes-Oxley Act, which lays out strict rules on the retention, modification, and destruction of documents and data. Safeguarding finance and business data are key factors in meeting these requirements. The extra-territorial effect of this act has meant that most countries now have corre-sponding domestic regulations, for example Directive 2006/43/EC of the European Parliament and of the Council. In addition to numerous other IT regulatory requirements, banks are required by the Basel II and III accords to, at all times, preserve the confidentiality of data, maintain data integrity and availability, and to have backup plans for their systems.

At the European level, this issue is set to be addressed by the planned General Data Protection Regulation (GDPR). In contrast to EU Directives (in this case in particular Data Protection Directive 95/46/EC), EU regulations enter into force immediately, meaning that the GDPR will not need to be separately transposed into national law by EU member states, but will come into effect immediately and will have priority over national regulations. The objective is to do away with the need to deal with multiple data protection instruments for cross-border transactions. By enshrining the legislation in a regulation, the EU has ensured that it will not be implemented differently in individual member states. This would appear to be essential if the regulations are to be effective, as experience suggests that businesses could otherwise migrate to those countries which offer the lowest level of protection.

The GDPR is in force since May 25, 2016 and will become applicable law after a two-year transitional period. Therefore, all data processing documents and processes will have to be adjusted to the new regulation by May 25, 2018. In the member states, the GDPR replaces the previously applicable EU Data Protection Directive 95/46/EC from 1995 and the national data protection laws enacted in its implementation. It comprises 99 articles, 173 recitals and numerous flexibility clauses that will be defined by the national legislators and then will have to be observed by businesses and authorities.

From a competition perspective, the GDPR ensures that when it comes to data protection the same rules apply to all companies that offer goods or services on the European market. Additionally, it also applies to all areas of public administration.

The GDPR applies to all businesses and organisations which collect, process, or store personal data. Personal data is defined as all information pertaining to a natural person, irrespective of whether this data relates to their private or professional lives. This includes for example names, photographs, email addresses, bank details, postings on social media, medical information, and IP addresses. (There may be an exception for employee data which is subject to regulation by individual member states – this remains to be clarified.)

This means that the GDPR will affect all businesses which carry on their business from within the EU, have business relationships with businesses or organisations based in the EU, or which collect, process, or store data or have data collected, processed, or stored on their behalf in EU member states. It will apply where the company responsible for data processing (the "controller") or the processor processes data as part of the activities of a subsidiary located in the EU or where the "data subjects" are based in the EU and data processing is used to offer goods or services to (or observe the behaviour of) people domiciled or resident in the EU. The regulation will therefore also apply to processors which are not based in the EU. This is allowable, as countries – including the EU community of states – are permitted under international law to legislate in areas with there is a genuine link to their sovereign territory. The fact that this requirement is tied to the data subjects being resident in the EU means that this requirement is legally uncontroversial as far as processors are concerned. This is even clearer in the case of processors based in the EU which process data outside the EU. (To what extent EU data protection standards can actually be enforced in practice is admittedly another question.) The GDPR will therefore also have significant consequences for non-European businesses with operations within the EU, since the connecting factor is business or trading activities within EU member states.

An Ipswitch survey of 316 European businesses and organisations found that 56% of participants were unable to say exactly what the GDPR would mean for their business. 52% admitted that they were not yet prepared for implementation of the regulations, and 35% did not know whether their IT policies and processes would meet the regulation's requirements. 81% of IT managers were completely unaware of the regulation. Around a quarter of businesses were intending to review and tighten up their IT security policies. The survey also revealed that hardly any businesses had given consideration to whether their cloud service provider was adequately prepared for the changes the regulations will bring[20]. This was despite the fact that 79% of the businesses surveyed work with cloud service providers, that they would be held to have full legal liability should their cloud provider fail to adhere to security standards and be fully liable for any errors made in carrying out data processing on their behalf. (For more detail on this, see "Trends in case law".)

The parts of the GDPR which deal with data security are in large part based on the domestic regula-tions set out in Germany's Federal Data Protection Act. As far as data security is concerned, the regulation follows the maxims 'privacy by design'[21] and 'privacy by default'. Taking into account the current state-of-the-art and implementation costs, the controller must, both when specifying the systems to be used for processing and at the time of processing, utilise technical and organisational security measures and procedures which ensure that data processing is carried out in accordance with the regulations and that the rights of data subjects are safeguarded. This means that the controller must specify appropriate internal strategies. The procedures must in particular ensure that data is not made available to an indeterminate number of natural persons. The European Commission has wide-ranging authority in these matters and can set out requirements for these measures and procedures – particularly requirements for data protection by design and privacy-friendly default settings for specific industries or specific products and services – and can specify technical standards.

The principle of data protection by design requires that data protection be embedded in the entire lifecycle of a technology – from the design stage, through deployment and use, to decommissioning. That includes responsibility for products and services used by the controller or processor. This means that risks need to be identified and measures for mitigating these risks developed even before a technology is deployed. These measures need to ensure an adequate level of security dependent on the risks involved in processing and the nature of the personal data to be protected. In specifying technical standards and organisational measures for ensuring security of processing, technological neutrality, interoperability, and innovation should be promoted, and, where appropriate, cooperation with third countries should be encouraged.

Technical and organisational measures for data security should always be based on a risk analysis. As in the corporate governance field, where effective risk management (including an internal system for auditing this risk management and appropriate documentation) is a statutory obligation, this risk analysis must be documented. This applies equally to IT security measures identified in the course of risk management processes and in particular to business-critical IT-related risks relating to data loss or failure to preserve the confidentiality of data or trade secrets. These measures must take into account the state-of-the-art "for specific sectors and in specific data processing situations" and developments in technology. Early stage and regular target-performance comparisons including risk analysis and a data protection/data security impact assessment are therefore strongly recommended.

Any security breaches must be documented by the controller, with this documentation to include a description of all factors relevant to the breach, its effects, and remedial action taken. The documenta-tion must be sufficient to enable the supervisory authority to verify compliance with the regulation. All parties involved have a duty to ensure that processing is carried out securely. That means both the controller and the processor and – within a group of companies for example – both or all companies which process data covered by the regulation for each other, for third parties or in common.

As with Section 109a of Germany's Telecommunications Act, the regulation provides for data breach notifications, particularly in the case of security leaks. As with the German Telecommunications Act, businesses must notify the supervisory authority and those affected by the breach (the "data subject"). The regulation provides for exceptions where it can be shown that suitable technical security precautions have been taken. After examining the adverse effects, the supervisory authority can require the business responsible for a breach to notify the data subjects. Notification is not required if the business can demonstrate to the supervisory authority that appropriate technological protection measures had been taken, and that these measures had been applied to the data affected by the breach. (These technological protection measures should in particular include encrypting the data for all persons who are not authorised to access it.) There is therefore a counter-exception to the notification requirement where a business can demonstrate to the satisfaction of the supervisory authority that appropriate technological protection measures had been taken, and that these measures had been specifically applied to the data affected by the breach. Irrespective of this counter-exception, the supervisory authority retains the option of requiring the controller to notify the data subjects.

It is disquieting to see that the GDPR does not explicitly preclude data transfers for disclosure purposes ordered by an authority in a third country. Instead it allows for exceptions to be made where there are "important grounds of public interest". Given the risk that privacy standards will be watered down, this kind of deliberate loophole in privacy rules may lead to a preference for jurisdictions such as Iceland, where information disclosure on the grounds of the public interest of third countries (and their intelligence services) is explicitly forbidden. This applies in particular to secret court orders (see 'An Icelandic data haven – the Switzerland of bits?' in Part 2).

The range of sanctions detailed in the GDPR provides for an initial warning for first, non-intentional breaches of the regulation and fines of up to €250,000 or, for companies, up to 0.5% of their annual worldwide turnover, for even minor acts of non-compliance. The regulation cites as an example omissions in the procedures and arrangements required to allow data subjects to exercise their rights. For serious failures of compliance with the regulation, such as infringements of the 'right to erasure', the regulation provides for fines of up to €500,000 or up to 1% of a business' annual worldwide turnover. The most serious failures of compliance can attract fines of up to €1 million or up to 2% of annual worldwide turnover, with serious failures including processing personal data without sufficient legal basis, without adequate security measures or without meeting relevant notification obligations. Unlike the original version, however, the latest version no longer includes the option of (in addition to any fines) removing any financial advantage obtained as a result of breaches of data protection law, as provided for in the German Data Protection Act.

TRENDS IN CASE LAW

Recent case law underlines the point that, in an era of digital data processing, IT security systems which provide effective protection for business data are anything but an optional extra. The German Appeals Court (Bundesgerichtshof, Germany's highest civil court of appeal) considers securing communications to be a legal duty and has ruled that internal business information must not be transmitted by unsecured email. The court found that a business which transmits such data over the internet despite being aware of the potential risk could be guilty of revealing trade secrets[22] (a criminal act under German law). A key, legally mandated component of IT risk management systems is the maintenance of efficient, rapid continuity management systems (disaster recovery and business continuity). This includes rapid restoration of systems following failure or data loss. Having an appropriate, up-to-date emergency plan is likewise, therefore, an essential component of effective corporate governance. Its resilience should be tested at regular intervals by means of stringent 'live' tests[23]. A recovery management system able to model disaster scenarios (broken down according to the importance of the data to the business) is essential. Key systems such as ERP systems need to be able to be reloaded with the most recent data possible, preferably same-day data. Less time-critical data, such as data required for internal or external audits or as evidential documentation for legal proceedings, should be available within one or maximum two weeks.

Modern backup systems should be used to mitigate against data loss or hacking attacks. They should be checked regularly to ensure they are functioning correctly, and modified to deal with changing threat scenarios as required. Backup systems must also meet data protection requirements. The role of management is therefore to take effective technical and organisational IT security measures, in particular by employing backup strategies, fully auditable archiving systems, and IT policies, to protect business critical and personal data from loss and unplanned disclosure.

Where outsourcing (e.g. to international cloud structures or domestic data centres) has not been properly thought through and has not been made fully secure, liability (in some circumstances personal liability) remains with the business doing the outsourcing and its management team, and does not pass to the business to which the service has been outsourced. It is also important to note that the usual burden of proof is reversed in this case, so that in the event of a dispute, it is up to the responsible board member to prove that they have exercised proper care in performing their executive role.

Specifically in the case of backup management, case law has established that regular, reliable, gapless data backup routines are part of the general duty of care. External specialists, such as IT businesses contracted to provide maintenance or support, or data centre providers which undertake commissioned data processing for a business, can be expected to provide such a service without requiring specific instruction to that effect. Companies are not therefore subject to additional auditing or notification obligations with respect to external providers providing services in this area.

Under the specific regulations of the German Data Protection Act on availability controls, businesses must ensure that personal data is protected against destruction or loss. The list of essential measures includes use of a modern backup system and regular checks that the system is sound, appropriate, and functions as it should. These checks must also be properly documented.

Case law suggests that implementing and monitoring reliable security routines for live systems, archive systems, and backups is essential. Data backup routines which fail to backup business data daily and all data weekly are, according to case law, inadequate[24]. Delegating these tasks to a specialist provider does not absolve a company from its responsibility for protecting and securing its data and systems. This can even apply where an external IT service provider is responsible for an incident of data loss, should the company which contracted out the services be deemed to have some degree of joint responsibility for the data loss due to an inadequate disaster recovery and backup strategy. The extent of the company's responsibility may be up to 100%, i.e. it may be found to be fully liable[25]. In some cases, the courts have taken the view that backing up business data daily and performing a full backup weekly are essential requirements[26]. Even if responsibility for loss of business-critical data lies with staff from an external IT specialist, the company itself still retains sole culpability for the data loss and any resulting financial losses. The German labour courts have ruled that data security is a legally protected interest which takes priority over the country's robust employee representation rights. Technical security measures called for include frequent backups, a fully auditable archiving process, firewalls, filtering and monitoring systems, encryption of sensitive data, and continuity management systems which guarantee that systems and data can be restored in the event of failure. Required organisational security measures range from IT and data protection policies to appropriate staff training.

In summary, and in the light of recent legislation ranging from new SEC rules to the Sarbanes-Oxley Act and Basel III, case law is increasingly imposing a general duty to employ effective, up-to-date IT security systems. A general trend is discernable of courts requiring companies to submit legally admissible data to the court even where that data was archived or backed up long ago in large external or overseas storage facilities, making access very difficult. This requirement is deemed to be independent of force majeure or any failing on the part of a third party. This will generally require the use of up-to-date IT systems which meet exacting evidentiary standards.

CONSEQUENCES OF INADEQUATE INFORMATION MANAGEMENT

Having discussed direct liability risks, we now turn to the question of how businesses can mitigate this liability or obtain compensation for losses arising from these risks.

One issue here is insurance cover. Since businesses with IT coverage or directors' and officers' insurance are obliged to notify their insurance company of any IT compliance failures (as they represent an increase in the insured risk), omissions in IT risk management can strip a company of its insurance cover. Failure to operate an appropriate, state-of-the-art IT infrastructure or to incorporate that infrastructure into the company's overall risk management system could be adjudged to represent gross negligence. In the event of a legal dispute, this could invalidate the company's insurance, or serve as grounds for rejecting a claim against a third party's insurer. In the worst-case scenario, where IT compliance failures have facilitated, been partially responsible for, or increased the magnitude of losses, they may stop a company from pursuing claims for compensation for those losses entirely[27].

In the light of the huge rise in IT-related incidents, such as sabotage and espionage, the insurance industry has recognised the new threat landscape in which businesses now operate, and has developed novel 'cyber-risk' products to plug gaps in the coverage offered by existing products. This is in recognition of the fact that theft or inadvertent publication of confidential data and IT infrastructure failures can easily lead to significant reputational damage, which can be far more damaging than any tangible losses. This is especially true where major failures in data protection are made public.

German data protection legislation can require companies which lose or divulge sensitive data to do three things: inform the relevant supervisory body, notify the person affected by the data protection breach, and notify the public of the breach by means of half-page advertisements in two national newspapers. (Sensitive data covered by the legislation ranges from bank details and customer or staff- related data to correspondence with customers, staff, public authorities, auditors, lawyers, etc.) Companies are, however, exempt from the requirement to notify potential victims and the Federal Commissioner for Data Protection and Freedom of Information if they employed an appropriate security concept and encrypted storage. Here again, it is evident that higher IT security standards can prevent consequential reputational damage.

MITIGATING MANAGEMENT LIABILITY WITH IT COMPLIANCE

The term IT security is usually taken to refer to the security, integrity, confidentiality, and availability of business-critical data. Companies have a variety of legal obligations in areas ranging from secure receipt and transmission of electronic information (email, bookings, orders) to storage and protection of customer and staff-related data. On top of these general requirements, Germany's Control and Transparency of Business Correspondence Act ('KonTraG') requires private companies to operate an effective risk management system. This is universally understood to include monitoring and early warning systems, and appropriate contingencies for disaster recovery and business continuity. The boards of public companies and larger limited companies have a duty to implement adequate IT security measures, especially for business-critical systems and data. They are also assumed to be culpable in the event of losses. Of particular note is the fact that KonTraG makes the boards (German companies have a bicameral board system) personally liable for making good losses caused by IT mismanagement. The act also reverses the normal burden of proof so that the onus is on board members to show that they have fulfilled their obligations properly – the law assumes that they are guilty until proven innocent. Management board members are therefore personally liable and the supervisory board is obliged to pursue claims for compensation against them.

Originally, only public companies were required to set up a risk management system. The legislative rationale behind KonTraG has, however, resulted in its effects spilling over to other company types and it has come to be subsumed into the general duty of care to which all commercial and public sector organisations are subject. Boards of larger groups, holding companies, etc. are expected to fulfil their risk management obligations in respect of all companies within the group, holding company, etc. Since risks entered into by subsidiary companies can also imperil the parent company, the legal form of the subsidiary is irrelevant. As a result of this ripple effect, the obligation to undertake effective risk management following the model set out by KonTraG is no longer limited to private companies. By extension, public sector organisations are also substantially bound by these obligations.

SUMMARY

What all of the regulations and legal obligations described above have in common is that their effects also extend to secure dissemination and storage of information. All deal with sensitive information and the availability of that information in a specific form for a specific period of time. Companies are liable if they fail to ensure that sensitive data is stored securely and in full compliance with applicable legislation, and that the confidentiality, integrity, and availability of this data is maintained at all times. They could also be liable should they fail to have in place suitable systems for protecting and, in an emergency, restoring this data. Risk management needs to be 'integrated'. It should not be limited to technical security measures, but needs to be firmly rooted in a company's internal legal and organisational processes. Backing up and archiving business data is now standard practice. Integrating these activities into the company's everyday business processes such that they are fully auditable and in full compliance with all applicable legal regulations is the responsibility of senior management. The choice of system and the complexity of its implementation need to reflect the value of the information it seeks to protect.

PART 2: EXPORTING DATA TO INTERNATIONAL CLOUD PLATFORMS – ICELAND

Within the EU and the European Economic Area (EEA), users and data centre operators involved in cross-border data transfers to external data centres benefit from a legal privilege known as 'commissioned data processing'. This means that the usual requirement when carrying out cross-border data transfers to check that the country in which the data processor is located "ensures an adequate level of protection" no longer applies. Companies wishing to take advantage of this arrangement must, however, undertake a reliability audit of the processor and of its technical and organisational security measures, and the data processor must provide appropriate security guarantees.

Although the European Commission has explicitly determined that Iceland affords an appropriate level of data protection, this does not automatically mean that data processors located in Iceland can legally be commissioned to process data. They are still external third parties and data may only be transferred to them if a series of very strict and restrictive conditions have been met.

AN ICELANDIC DATA HAVEN – THE SWITZERLAND OF BITS?

Under German data protection legislation, non-EU EEA states (Iceland, Liechtenstein, and Norway) are now afforded the same treatment as EU member states. The EEA Agreement obliges them to implement EU Directive 95/46/EU, aka. the Data Protection Directive, which forms the basis for their inclusion within the European digital single market. The aim is to create a European Economic Area which guarantees free movement of goods, services, capital and labour in the same way as the EU's single market. Since this involves extensive cross-border data transfers, the EU's Data Protection Directive is a key component of the EEA's regulatory framework. This will be equally true of the EU General Data Protection Regulation (GDPR) once it comes into force, but in the case of Iceland with the notable difference that disclosure of data to third parties and compliance with transfer requests from foreign states and organisations is prohibited entirely (see part 1 above, "Legislation").

The general trend towards globally harmonised data processing and data transfer rules is particularly noticeable in Iceland. In 2010, the Icelandic parliament instructed the government in Reykjavik to construct the legal framework needed to turn Iceland into a 'data haven' – "the Switzerland of bits", as a popular phrase had it. In 2011, the government passed the first of 13 pieces of media legislation collectively known as the Icelandic Modern Media Initiative (IMMI). The initiative also involved new regulations on data security, without which it would be impossible to guarantee effective data protection. In particular, the regulations were concerned with data security at large data centres and for distributed storage and processing of large volumes of data (cloud computing, 'cloud-sourcing').

The intention was to create a jurisdiction which combines extremely liberal press freedom and freedom of expression legislation and extremely strict data protection legislation to create a highly advanced national data protection framework. The initiative represents an attempt to take the best aspects of media legislation from a number of different countries.

Iceland guarantees the basic right to privacy of communication. This right can only be suspended by a directive from a court or other state institution if there is specific evidence of a crime punishable by a custodial sentence of at least 8 years. A second exception allows access to communications data where a court rules that the public interest is of greater importance than the basic rights of the individual. In Iceland, foreign intelligence agencies are unable to eavesdrop on communications for the simple reason that the main undersea data cables linking Iceland with North America and the European mainland are publically owned, rather than being owned or controlled by US or UK companies and thus subject to surveillance by these countries. Iceland's domestic cable network is state owned, and the state's controlling influence ensures that foreign organisations are unable to access undersea cables.

On the legal side, this means that disclosure of information for legal reasons is ruled out entirely. Put simply, the law enables users conducting operations on servers located in Iceland to enjoy the full protection of the IMMI. This presupposes secure communications and a technical infrastructure that is secure from third party interference. That shuts out conventional internet service providers. On the technical side, in addition to the measures employed by the Icelandic state detailed above, the onus will be on Icelandic data centre operators to employ systems which protect sensitive data from outside attack.

One of the key aims of the legislation is to eliminate the risk of information being misused by foreign intelligence services. The US Patriot Act, the subject of strident criticism in Germany, has been a key vehicle for such misuse. It allows US intelligence and investigation services to access cloud data stored by US companies even where it is hosted outside the US. All that matters is that the provider is based in the US. The act also provides for gag orders to prevent target companies from finding out that their data has been accessed. Most cloud providers, including the market leaders, come under US jurisdiction, either because they are US companies or because they regularly do business in the US.

Not least in the light of the publication of various 'national security letters' (NSLs) to US companies and secret court orders (SCOs) issued by US courts requiring companies to disclose data hosted on servers located in or processed by subsidiaries in Europe, the focus of the IMMI in 2015 has been on data protection and data security. A policy document submitted to the Icelandic legislative process notes that encryption is the most effective means of ensuring an appropriate level of security for data and communications. In particular Icelandic law will not permit backdoors in, the imposition of other governmental controls on, or impediments to the development and distribution of encryption software. There is also a need to explicitly ensure that, under Icelandic law, companies cannot be compelled by an NSL or SCO to hand over personal data (for example through the use of the US Patriot Act, discussed above). The intention behind the IMMI is therefore to place legislation before the Icelandic parliament which anchors these objectives in law and which will also act as a model for legislatures in other countries. Under Icelandic law, secretly exporting data to a third country would be outlawed, as would state-sanctioned industrial espionage such as that which, recent revelations suggest, has been carried out by the NSA with the unwitting complicity of the BND[28].

Even before the IMMI, in 2001, under its obligation under the EEA Agreement to implement EU Directive 95/46/EU, Iceland enacted new data protection legislation inspired by the Norwegian model. The legislation aimed to enable rapid, simple access to data via a series of interlinked regulations. (The EU's Data Protection Directive was already a model for international data protection legislation, a fact that was underlined by the passage of new data protection legislation in April and May 2000 in Iceland and Norway respectively.) The Icelandic regulations are directly comparable with data protection legislation in EU member states and member states therefore need to treat them in the same way as domestic legislation.

Icelandic data protection law is applicable for the public and private entities responsible for the processing, for the processors and regarding the processing of personal data (1) if the processing is done on behalf of a responsible entity that is based in Iceland, if the processing is done within the EEA, in an EFTA country or in a country or at a place that is officially rated as secure by the data protection authority; (2) if the responsible entity, which is based in a country outside the EEA or EFTA, uses equipment and facilities located in Iceland for the processing; and if (3) data regarding the financial capacity and creditworthiness of legal entities are processed with equipment situated in Iceland, even if the responsible entity is not based in Iceland. Responsible entities processing personal data by means of electronic technology are obliged to inform the data protection authority in good time before processing starts.

Cross-border data transmissions are permissible if the transmission meets the general requirements for cross-border data transmissions to countries with an adequate data protection level. It is recognised that the following countries provide an adequate protection level for personal data: EU, EEA and EFTA member states, Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Faroe Islands, Andorra, Israel and Uruguay. The responsible entities may assess at their own discretion whether personal data is being adequately protected after its transmission out of the EEA. The data protection authority may approve transmission to a country without an adequate level of protection, in particular if the entity responsible for processing has provided sufficient guarantees that this data is protected. In the case of cross-border data transmissions into a country rated as secure or on the basis of individual exceptions (e.g. consent, contract fulfilment, vital public interest etc.), the data protection agency merely needs to be informed. Any other cross-border data transmissions, including transmissions on the basis of standard contractual clauses ('Model Clauses'), must be submitted beforehand for approval. In practice, Binding Corporate Rules / BCR may need to be put in place to prove that personal data is protected even after its transmission out of the EEA.

Responsible entities are obliged to comply with the general data protection regulations. They are responsible for implementing and updating risk analysis procedures and for implementing security measures meeting the laws, regulations and instructions of the authorities. The data protection authority has issued instructions recommending the use of encryption, among other things. The responsible entities must document the process that was used as a basis for security guidelines, risk analyses and security measures to be implemented. Upon enquiry, the data protection authority must be granted access to such information.

The responsible entities are entitled to appoint processors if (1) it is ensured that the relevant processor will protect the data, and (2) they are entitled to audit the processor. The responsible entities are obliged to enter into a written contract with the processor, stipulating in particular that the processor may only act upon instruction by the responsible entity and that any processing done by the processor must comply with Icelandic data protection law.

Where the processing of personal data by a responsible entity or processor infringes against any provisions of the Icelandic data protection law or against any instructions by the data protection authority, the responsible entity shall indemnify the affected party for any financial loss incurred as a result of such infringement. The data protection authority may order the processing of personal data to stop, the deletion of personal data, prohibit any further use of the data or instruct the responsible entity to implement measures ensuring that the processing is legitimate. Any violations of the provisions of the Icelandic data protection law and the regulations enacted on its basis will be punished by fines or three years imprisonment, unless other laws require heavier sanctions. The same sanctions will be imposed for failure to comply with official instructions by authorities. When an offence is committed by a legal entity within its activities, this legal entity can be fined according to the provisions of the penal code.

Transfers of data to Iceland are therefore legally privileged, since the outcome of such transfers is broadly the same as transferring data to domestic recipients. Legally and technically, data transfers to Iceland are no different to domestic data transfers. It is not necessary to check whether Iceland offers an acceptable level of data protection. It does not require use of the European Commission's standard contractual clauses for the transfer of personal data to processors established in third countries or of the EU's 'binding corporate rules' (which provide an appropriate level of protection for data transfers within a multinational company). It does not require any specific certification or other undertakings, in particular adherence to the US Department of Commerce's 'safe harbor' principles. Such transfers are treated in the same way as domestic transfers and do not have to be covered by a specific 'permissive rule'. This is thus categorized as cross-border commissioned data processing under section 11 of Germany's Federal Data Protection Act. This is the default case where data is transferred from Germany to another EU/EEA state and also applies where a domestic business which is a subsidiary or branch of a foreign company transfers data to its head office located in another EU/EEA state. It should also be noted that automated transferral of staff data requires the consent of the works council. It is advisable to ensure that either contractual clauses or BCRs are used to make internal works agreements legally binding.

COMMISSIONED DATA PROCESSING

Strict rules on data protection and security also apply in the case of commissioned data processing. These are directed in the first instance at the data controller, but are in turn passed on to the processor. The processor must, for example, ensure that customer data is properly compartment¬alised and warrant the use of specific methods to separate such data. If encryption is used, it must offer an adequate level of security – taking into account expected future technological advances – and must not be able to be compromised by other customers or the operator itself. The operator therefore needs to have in place properly documented data protection and data security management systems, a general IT security management system, and an incident management system. Since the reliability of the operator and the systems employed by it are key criteria for restricting liability in the event of losses, when selecting an operator, due priority should be given to transparency and external auditing by an independent auditor.

Although Iceland enjoys the privilege of being an EEA member, so that the free flow of data is broadly permissible, some spadework is still required.

TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES

Having determined that an operator offers an appropriate level of data protection does not absolve the 'controller' (see below) from having to think about technical and organisational security measures for ensuring secure data transfer. Commissioned data processing contracts need to include mechanisms for protecting those affected by the contract (in particular staff and customers).

The applicable jurisdiction for such data transfers is always that of the state in which the controller is domiciled. The controller is responsible for ensuring compliance with data protection legislation. Under the EU's Data Protection Directive, the "controller" is the body which "alone or jointly with others determines the purposes and means of the processing of personal data." The "processor" is the body working "on behalf of controllers". The "purpose" here is 'why' the data is being processed, the "means" is 'how' it is being processed. The decisive factor is which body actually has the authority to decide these issues. In the case of cross-border data transfers, German data protection authorities determine who the controller is by asking "Who initiates the data transfer?".

In the case of commissioned data processing, to ensure that the processor really does process the data only as instructed by the controller, there are a number of areas which the processing contract needs to cover. Section 11 of Germany's Federal Data Protection Act sets out a list of ten points which must be contractually regulated for such processing to take place. This is in contrast to the EU's Data Protection Directive, which merely requires a written contract. A further peculiarity of the German system is that transfers of data from a controller in Germany to a processer located in the EU or EEA is not considered to be a data transfer (Übermittlung) in the legal sense of the word, since the actions of the processor are ascribed to the controller. They do not have to be covered by a specific 'permis¬sive rule'.

Data processing agreements must be written agreements and must set out permitted locations for data processing and the controller's rights with respect to auditing the processor and any subprocessors. In the case of subprocessors, auditing may be carried out by the processor and does not necessarily have to be carried out directly by the controller. The processor must tell the controller about any subprocessing arrangements and inform them of all locations in which data is stored or processed. Controllers also need to include a clause stipulating that data will be deleted free of charge or transferred back to the controller at the controller's discretion (in particular once the processing is finished) and to ensure that technical and organisational security measures put in place by the operator are checked before processing commences and at regular intervals thereafter. Official legal opinion is that the customer is not obliged to undertake on-site checks directly and that the reliability of an operator can be verified by means of transparent audits by appropriate certification service providers. Customers should, however, ensure that the right to undertake an on-site audit is included in the contract.

Controllers have a strict legal duty to exercise due care in selecting a data processor. A cursory examination of data security is not sufficient. Controllers need to ensure that data is available and that its confidentiality and integrity are maintained at all times, but they also need to ensure that the processor complies with all of the technical and organisational security measures set out in Annex 1 to section 9 of the Federal Data Protection Act (aka. the '8 commandments of data security'29). Appropriate certification from industry bodies such as the VOI and ULD (the latter through its EuroPrise certification scheme) enables data centre operators in the EU and EEA to demonstrate proper compliance with legal regulations simply and transparently (Cloud "Made in Europe").

SUMMARY

Before outsourcing data services, companies need to be extremely thorough in ensuring that the security, integrity, confidentiality, and availability of personal, business-critical, and tax-related data will be preserved. Non-compliance can lead to fines, and failure to provide evidential documentation where required can result in major financial and non-financial losses and reputational damage. In an era of outsourcing of services and data, good IT management is an essential component of a secure, insurable business strategy. Once a business has chosen to go down this route, it needs to identify a data haven which both complies with relevant legal requirements and meets technical and organisational security needs. Data transfers to Iceland meet these requirements, and the process is no more complicated than a domestic data transfer. Checking the reliability of the data centre provider is still, however, essential.

AUTHOR: DR. JUR. JENS BÜCKING

The author is a lawyer, specialising in IT law. He is also a founding member of the e/s/b Rechtsanwälte legal practice (http://www.kanzlei.de), author of books on IT law, visiting lecturer at Stuttgart Technical University and associate professor at ENU in Kerkrade, The Netherlands.

Dr. Bücking advises businesses and public sector organisations on IT projects. He provides support with staff training and with drawing up employment and work-related contracts in the IT and user spheres.

Disclaimer

This document is intended as a general guide. It is not a substitute for definitive legal advice from a specialised lawyer. Please be aware that, although care has been taken in assembling this document, no guarantee is given and no liability is accepted for its accuracy. For data protection-related issues, all businesses are advised to obtain individual legal advice prior to implementation.

SPONSOR: VERNE GLOBAL

This paper was sponsored by Verne Global, an innovative developer of energy efficient data centre campuses located in Keflavik, Iceland. We offer our clients scalable and secure data centre solutions that combine unparalleled cost savings and renewable energy to meet the business demands of a data driven economy. Discover how companies like BMW Group, VW, and Earlham Institute are lowering their operational costs and going green with their data at www.verneglobal.com.

[1] META Group, 2003. [2] National Archives and Records, 2012. [3] British Ministry of Economic Affairs, 2012. [4] London Chamber of Commerce research, 2012; the Institute for Business and Home Safety (IBHS) also found that around 25% of businesses which suffer a severe data disaster are unable to continue their operations. [5] Gartner, 2013. [6] Spiegel Online, June 30, 2013. [7] According to research published on Spiegel Online on April 23, 2015, the US National Security Agency has been spying on targets in Western Europe and Germany with the knowledge of the German intelligence agency (BND) for years. In 2008, the agency became aware that the NSA was submitting requests which were outside the scope of joint agreements on combating global terrorism negotiated between Germany and the USA in 2002. The NSA was found to be looking for information on organisations such as defence contractors EADS and Eurocopter and French government agencies. The BND did not, however, take the opportunity to carry out a systematic examination of "NSA search parameters". [8] In conjunction with Aris Umfrageforschung, in January and February 2015, Bitkom Research surveyed a total of 1,074 businesses employing at least 10 people. The interviews were carried out with management level staff responsible for business security (CEOs and corporate security, IT security, risk management or finance managers). The survey is representative of the business sector as a whole. [9] This is according to European Commissioner for Home Affairs Cecilia Malmström, announcing the creation of the new European Cybercrime Centre on March 28, 2013. [10] German Ministry for Economic Affairs, 2013. [11] CA-Technologies, 2014. [12] National Archives & Records Administration, 2013. [13] The Cost of Lost Data, David. M. Smith). [14] Boston Computing Networks study, 2014. [15] Data loss prevention: keeping your sensitive data out of the public domain, Ernst & Young, 2011. [16] Wake Up Call: You Aren't Ready For A Disaster, Forrester Research, Inc. [17] ECJ ruling dated October 06, 2015 (C-362/14). [18] The transmission of personal data to the US without a legal basis was held to be punishable by a fine according to section 43 para. 2 cl. 1 of Germany's Federal Data Protection Act (BDSG) (note: and can thereafter be punished by a fine of up to 300,000 € for any further incident). The ULD will verify whether instructions towards non-official entities must be made, on the basis of which data transmissions to the US must be suspended or prohibited. Furthermore, they will verify whether non-official entities had committed offences by transmitting data to a third country without an adequate level of data protection. [19] German Appeals Court ruling dated July 17, 2009, 5th criminal division 394/08. [20] Source: http://www.searchsecurity.de/meinung/Ist-Ihr-Unternehmen-bereit-fuer-die-EU-Datenschutz-Grundverordnung. [21] Cf. Ann Cavoukian's 7 principles: 1. Proactive, not reactive; 2. Privacy as the default setting; 3. Privacy embedded into design; 4. Full functionality; 5. End-to-end security, full lifecycle protection; 6. Visibility and transparency; 7. Respect for user privacy (in part already incorporated into the current German Federal Data Protection Act; source: www.privacybydesign.ca). On the issue of privacy by default, similar objectives are set out at various points in the Act, e.g. opt-ins, data reduction, limitation of use to specific purposes, list of technical and organisational security measures, etc. Separate default settings may be required for products on EU markets (e.g. smartphones, software, cars, etc.). [22] German Appeals Court ruling dated February 26, 2013, ref: KVZ 57/12. [23] Forrester Research, 2012. [24] OLG Hamm, op. cit. OLG Karlsruhe, NJW RR 1997, 554; OLG Cologne, NJW RR 1994, 1262. [25] See previous footnote. [26] Cf. OLG Hamm, op. cit. [27] OLG Hamm, op. cit. (100% co-responsibility – effectively sole liability for an inadequate data backup strategy). [28] See footnote 7, above. [29] Annex to section 9, first sentence of the Federal Data Protection Act: Where personal data are processed or used in automated form, the internal organization of authorities or enterprises is to be such that it meets the specific requirements of data protection. In particular, measures suited to the type of personal data or categories of data to be protected shall be taken. 1. to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control), 2. to prevent data processing systems from being used without authorisation (access control), 3. to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control), 4. to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control), 5. to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control), 6. to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control), 7. to ensure that personal data are protected against accidental destruction or loss (availability control), 8. to ensure that data collected for different purposes can be processed separately. One specific measure required under clause 2, points 2 to 4, is the use of a state-of-the-art encryption procedure.

* Author: Dr. jur. Jens Bücking. The author is a lawyer, specialising in IT law. He is also a founding member of the e/s/b Rechtsanwälte legal practice (http://www.kanzlei.de), author of books on IT law, visiting lecturer at Stuttgart Technical University and associate professor at ENU in Kerkrade, The Netherlands.Dr. Bücking advises businesses and public sector organisations on IT projects. He provides support with staff training and with drawing up employment and work-related contracts in the IT and user spheres.