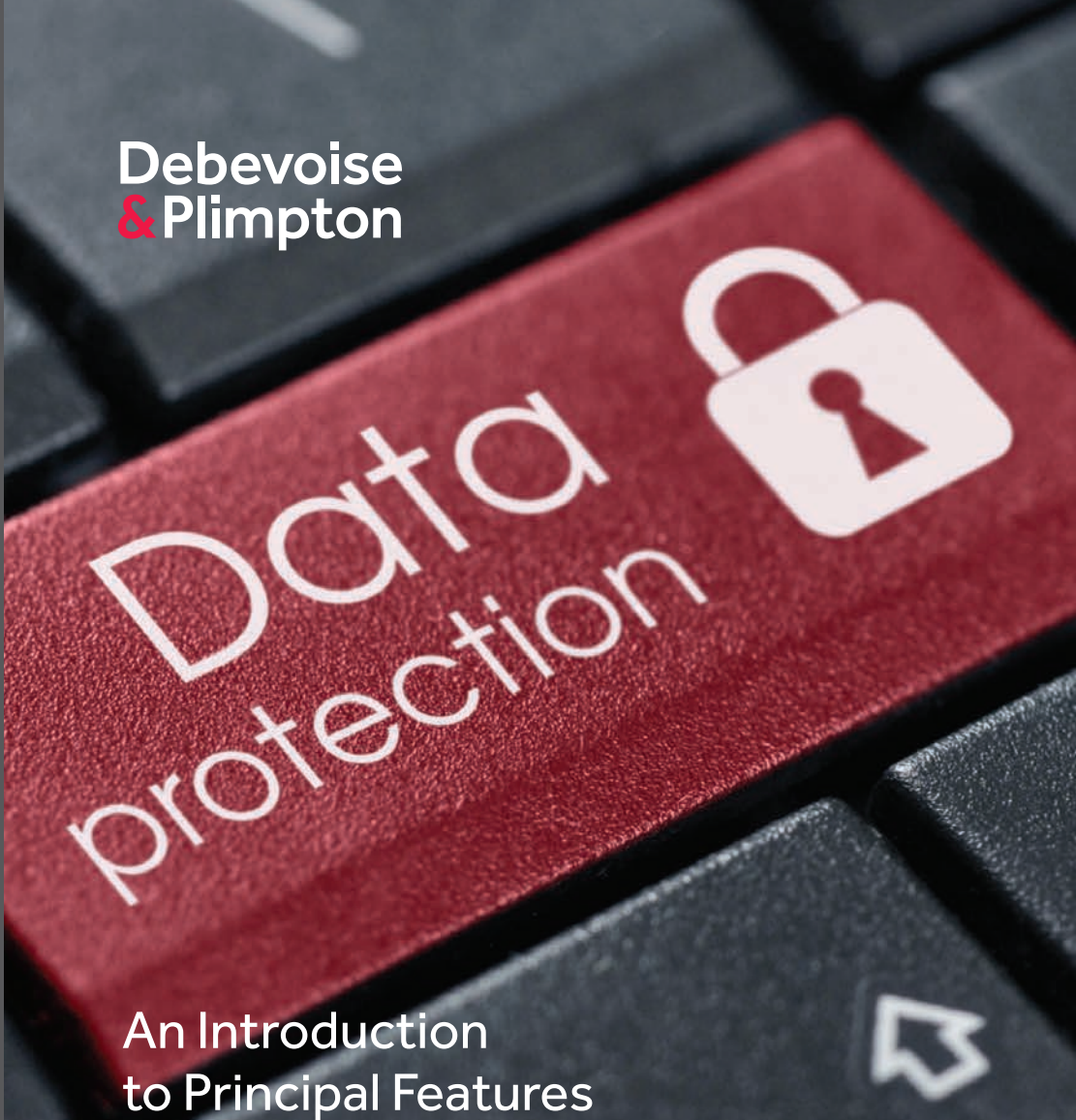
Debevoise & Plimpton



An Introduction to Principal Features and Potential Regulations of Personal Data Protection

Dr. Thomas Schürrle

Debevoise & Plimpton

Data Protection

An Introduction to Principal Features and Potential Regulations of Personal Data Protection

by
Dr. Thomas Schürrle

For permission requests, write to the publisher at the following address: tschuerrle@debevoise.com.

Contents

Foreword

This book addresses members of the management and legal services of business operations. In substance, it describes the conceptual basis of the regulatory control of personal information processing by operations that are out of the relevant person's hands. While technically aspiring to be accurate in terms of legal background and sources, it is *not* meant to be a law book *at all*. The reader will notice the complete absence of legal provisions with relief.

Rather, the following roughly sixty pages will provide a fundamental view on data protection that is necessary and helpful to understand where the blossoming data protection regulations across the globe are conceptually coming from. Supported by stories and examples that illustrate background, need and possibilities, the reader should get into the position to have a sense of what data protection is all about even without having read a single norm or decision. There is obviously no shortage in serious and scientific literature on the subject, some of which are citied at the back of the book to enable further in-depth studies.

The book is also meant to be an introduction to lawyers and managers in jurisdictions that are about to become seriously regulated with a newfangled data protection regulation, such as Brazil.

Although this is not a law book, a good deal of professional work and care went into it to confer a legally accurate picture

of data protection as of the year 2019. And I am forever grateful to the people who helped me in achieving this aim, namely Theresa Neugebauer, Chris Pudelko and Sabrina Pfaff for putting this script together, Nicole Marton of Georgetown University Law Center in D.C. and Ishan Zahoor of the Institute for Law and Finance in Frankfurt for proofreading the English manuscript, and Yasmin Caesar for getting the printing done – and of course my trusted colleague and most critical reader in this field, Dr. Fritz Popp.

September 2019
Thomas Schürrle

Abbreviations

BCR	Binding corporate rules
Big Data	Large industrial data operators
Big Pharma	The same in pharmaceuticals
Blocking statute	A law prohibiting private or public inland investigations in connection with foreign public investigations
Bot	An automated source of electronic communication
Cloud-Act	The Clarifying Lawful Overseas Use of Data Act, enacted by the Consolidated Appropriates Act 2018, PL 115-141, amending the Stored Communications Act of 1986, allowing federal law enforcement to compel U.S.-base technology companies to provide requested data regardless of where they are stored.
DOJ	U.S. Department of Justice
DPIA	Data Protection Impact Assessment, a special review of the adequacy of data safety procedures in connection with particularly data sensitive operations
DPO	Data Protection Officer, a corporate functionary with special powers relating to data protection inside an operation
DTA	Data transfer agreement
ECJ	European Court of Justice

FCPA	Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA")
GDPR	EU General Data Protection Regulation, Official Journal, L119
HIPAA	The Health Insurance Portability and Accountability Act, (1996) Pub. L. 104-191
Privacy Shield	A legal framework for regulating transatlantic personal data exchanges between the EU and the U.S., based on a EU Commission Decision of July 12, 2016, a presidential executive order Enhancing Public Safety and a change in the US Judicial Redress Act, Pub. L. 114-126
Safe Harbour	The predecessor framework to the Privacy Shield, effectively declared inoperative by decision of the ECJ in October 2015 ("*Schrems*")
SEC	Securities and Exchange Commission
Shield-Act	The New York State Stop Hacks and Improve Data Security Act of July 25, 2019, Senate Bill 5575
Subject Access Request	A request for information on one's personal data stored and processed by a data operator under Art. 15 of the GDPR.

Chapter I: Introduction

To gain access to data protection, it is helpful to understand where it comes from.

In 1983, states and communities of the Federal Republic of Germany prepared a population census that would require German citizens to answer a whole set of questions about private issues. The census was to be conducted by public officials on door-to-door visits to citizens, because the government did not trust the accuracy of their own registers.

Nobody thought of any illegality in connection with the planned census, except a small group of people who filed a constitutional complaint with the Federal Supreme Court for Constitutional Matters. Against every expectation, and for the first time in history, the topmost German court established a personal and inalienable right to "informational self-determination," which the court viewed as becoming endangered by data collections of the state aided by modern information technology. The Court reasoned that there is a connection between the state gathering information about people and their behavior as a consequence: If a person cannot know or influence which information about her behavior is stored and kept available, that person will out of precaution adapt her behavior accordingly.

With this argument the court invoked a theory known as "*panoptism*", developed by French philosopher Michel Foucault. It addresses behavioral conformity of the individual

resulting from increasing surveillance and control mechanisms in Western societies in the outgoing 19th century. Such a situation, in the court's view, would not only limit individual freedom but also affect general commonwealth, because the will of the people in a free democratic society depended on the self-determined and cooperative minds of its citizens.

The decision hit the legal world like a thunderclap. Soon after, the German State of Hesse adopted a Data Protection Act. Sweden quickly followed, and before the decade was out, more or less the entirety of the EU member states had adopted data protection laws, and the EU itself issued a corresponding directive providing guidance and standards.

1. HOW IS DATA PROTECTION UNDERSTOOD IN PRINCIPLE AT THE OUTSET?

In summary, data protection is a set of legal regulations that permits the individual to exercise reasonable control over her personal information in a world in which such information is systemically collected, stored, processed and proliferated by not only State-owned, but also private operations, against which the individual would otherwise be defenseless. Ideally, the individual should be in control of where her personal information goes, how long it stays there and what is going to happen with it and for how long.

That is, of course, not the case nor even theoretically possible in the real world. Personal data, broadly defined as information about or linked to an individual, cannot be controlled by the individual itself in the first place. We are constantly visible,

produce audible noises, move around, display our appearance and act in certain ways, all of which being noticed by others. We leave traces everywhere.

2. SO WHAT MARKS THE DIVIDING LINE BETWEEN NORMAL COMMUNICATION OF PERSONAL INFORMATION AND PROFESSIONAL PROCESSING OF DATA THAT REQUIRES LEGAL CONSTRAINTS?

At the time the German court established data protection as a fundamental right, data processing and storing technically was nothing compared to today. In fact, it was often done by hand, in paper file rooms with mechanical storage systems. As is typical for a fundamental right – data protection was meant to be chiefly directed towards the state, under the notion of an overreaching state control, the key element of a totalitarian statehood perfectly depicted in "1984" by George Orwell and still lingering in the minds of German citizens of both states then. That has changed dramatically over the past three decades with the exponential development of modern computer technology which gives states and private companies alike the tools to process and store data in humongous amounts for ages to come. There is hardly any doubt that such change will continue over the coming decades, looking at the going rate of technical development and growth of online networks.

But what has *not* changed is the fundamental assumption on which humanity and human behavior have always relied, and will mentally and philosophically continue to rely: That memories of any kind linked to a person will not last in

perpetuity, but are generally fleeting, like the proverbial moment. The ability of man and mankind to forget is a fundamental factor in our social interaction, and it is an essential factor to permit change, development and renewed appreciation, of facts, views, of oneself and others as individuals. Human interaction assumes that personal information – as opposed to artifacts that are meant to last, such as inventions, books and works of art (except those by Banksy which destroy themselves) – is not going to be processed and stored for generations to come, and not readily reproduced as evidence of past behavior, views and opinions, with the comported authority of the past.

Yet today, even a momentary contact can suffice for a computer system to collect and store the information forever. In a digital environment with endless storing capabilities and real-time data processing by invisible machines, we leave more permanent footprints per day than was possible in a whole decade in the past. We underestimated in particular the exponential increase of storage capability. We used to think of data storage as being limited in scope, confined to mediums like the old storage tapes, to be seen today only in old movies, spinning inside windowed machines as evidence of *la vie moderne*. We used to feel safe from excessive control by state spies, satellite monitoring and the eyes of our neighbors or bosses, because the information generally available was considered to be too vast and too mundane to be worth or capable of storing. To achieve total control, we used to think, more people would have had to be employed in monitoring others than those actually being subjects to observation. In

today's world, however, data storage mediums of the size of a thumbnail have replaced rows of tape machines. Computer programs are able to monitor and filter all ongoing data communication on Earth and store the findings forever, even if they are completely mundane, irrelevant or boring.

From a philosophical perspective, we want to be able to hide, to escape, to change, to vanish from sight. Except for letters, books, work products or artifacts, in our perception we do not leave lasting footprints in a normal world, and even if we do, the rain of passing time would wash them gradually away. Nothing seemed to be older than yesterday's news. But our perceptions no longer hold true. Our electronic footprints today, in minute detail, will be detectable still in hundreds of years, like petrified footsteps of a dinosaur – but at the touch of a button. We just don't realize it, because we cannot see it.

3. NEVERTHELESS, DON'T WE BENEFIT?

We benefit tremendously from information technology and its increased abilities. An information system that permits immediate access to all sorts of information about various persons or matters is great. Our life enjoyment has vastly expanded. We can be in varying locations and still able to remain electronically involved in life or business somewhere else. Why do data protectionists have a problem with the ability to find an address within nanoseconds? With the instant ability to access street maps, directions, or the duration of walk, and with the ability to know immediately whether the person one is trying to reach is at home, making a phone call

or sitting on her computer doing work online? Why having a problem with information technology if it is helpful and also gets more and more secure for the individual, as they say?

The answer is that the availability of information through virtually instant processing and endless storing capabilities has not been developed from brotherly love but to serve a demand for the processed and stored personal information by others. Data have become a business. The benefits of better access to information notwithstanding, the electronic footprint of a real person left in the process is worth a lot to operations that collect, use and sell profiles of human behavior, demands and needs. Professional information systems generally, not only social networks, have permitted participants to adopt an entire electronic life and personality that knowingly (sometimes even not knowingly, as is the case with Facebook-linked internet pages) participates in discussions, exchanges information with others, and influences opinions. Especially in a technological world of potential or actual fake internet personalities, bots, and machines, either programmed intentionally or hacked in order to influence public opinion, the most valuable thing remaining is the true connection to a real person. Information such as a person's likes, recommendations, purchase behaviors, demands or even just preferences and interests serve as integral bases for trade and industry only as long as there is reliably a natural person behind any such piece of relevant information. Real personal data have become the 20th century oil and their industrial use the 19th century gold rush of today.

4. IF THE ACTUAL LINK OF SOURCED INFORMATION TO AN INDIVIDUAL WOULD BE CUT BEFORE FURTHER PROCESSING, WOULD THAT NOT ALSO MINIMIZE THE NEED FOR REGULATED DATA PROTECTION?

It is correct that data protection does not, and from a regulatory perspective does not have to, apply to anonymized data; it is the link to an individual that triggers data protection and defines personal data as any piece of information linked to a natural person. Separating a name and information permanently avoids the need for data protection. But it is even today virtually impossible to get there.

Technically, there is still no practicable way to achieve true anonymization because it is actually quite difficult: Even without the name being tagged to it, the information made available may already suffice to identify the person or set of persons to which the data belong. It requires intricate mathematical tools to make sure that the information is granular enough to disallow sufficiently going back to the individual where it came from. Anonymization legally, however, requires a full and permanent, irreversible separation of the individual and the information.

Because fully anonymized data are as such not distinguishable from Bot-generated data sets, technology firms need to work hard to find a technique that would enable sufficient anonymization while permitting at least some guarantee that data have really come from an existing natural person. So far, this has been without full success. Technology providers can, legally speaking, only devise an algorithmic replacement of a

regular name by a code or computer address (which data protection connoisseurs call *pseudonymization*). However, this system has not yet developed to the point where names and information cannot, through any process, be restored. Thus, what most people believe is *anonymization* actually isn't.

From the business perspective, an anonymized set of data may only be of sufficient value at the outset if there is an adequate assurance that the data are genuine. To assure trust, one could think of employing an intermediary to issue a more or less independent guarantee that the data came from a person and are not fabricated. This still would not solve the problem, because - again - the anonymization would not be completely irreversible. Moreover, each anonymized data set on a person has a "shelf life" - relevance and reliability degrade quickly. The information business needs a constant supply of new or actualized data, and in reality it does get this information because the information systems technically seek and combine data from an increasingly wide set of sources that a person certain uses without even knowing that somewhere each piece of information is put together.

Here is an example: Already a one-off event combining just one's location of a credit card use, the fact of the card use, the value of a purchase and the personal address (which is the information we leave behind if we do a simple non-cash purchase in the city) tells professional data entrepreneurs a lot of what they need to know to trade this information. And they get this information over and over again, and free of charge on top because we do this business all the time. From repeatedly

getting just this simple set of information, the computer systems of data entrepreneurs get constant free updates (*thank you*) on personal information that permits their systems to learn about one's income, preferences, intellectual background, family status and behaviors, often even more granular. In other words, the information technology is able to easily generate, use and sell a "profile" of a real person.

It is exactly this personal data "profiling" and its use that private individuals cannot effectively control and data protection conceptually seeks to curb.

5. WHAT CAN THE INDIVIDUAL DO?

For a "data subject" (the technical term for a human being whose personal data are at issue) the primary order of the day is to distribute own personal data with care and only to the extent necessary. Data collectors often innocuously ask for a whole variety of information, from private home and mobile phone numbers to the names and addresses of other family members, even the address of a secondary home, not to mention social network memberships. Only those data should be communicated and processed that are necessary for one's immediate business. From the viewpoint of the individual, the only data that are needed for most business transactions are one's name, address, phone number and potentially tax-related information, rarely more. Unnecessary data that are obtained coincidentally but that are not necessary for business performance should therefore not be transferred or be immediately discarded, and should not continue to be stored or

processed. Even if confined to immediate business needs, data obtained in the process still provide a valuable asset for most data entrepreneurs, while admittedly a reduced set of information holds a somewhat reduced value compared to a data set encompassing information available in greater personal detail that tells a better story about someone's life and preferences.

Scarcity of data communication forces the data industry to adapt and restrict not only their own demand for data, but also the amount of data available for other purposes, and thereby the data proliferation generally. In other words, scarcity of data directly leads to a reduction in general data availability. The lesser the amount of data in circulation, the more reduced its usability, especially for profiling purposes. And the less personal information in circulation, the less the vulnerability associated with data processing and the smaller the risk for the individual of data loss or abuse.

6. COULDN'T A SPECIFIC CONSENT REQUIREMENT PROVIDE SUFFICIENT CONTROL BY THE INDIVIDUAL?

While scarcity in information sharing by an individual is definitely helpful to the cause: Making the sourcing and processing of data depending just on the consent of the individual actually isn't.

Contrary to the expectation of many, the consent of the affected individual is in practice the least reliable option and in many cases not an option that protects the individual sufficiently. There is a whole variety of shortcomings: A real

consent deserving the name has to be based on adequate knowledge of the consequences of the sharing of personal data in a given situation. A good consent needs to be "educated". In practice, it is not only factually hard to get the relevant information across to the individual, the incidents for which a consent is requested also have to be identified individually which makes the information for and the obtaining of the consent pretty granular. That opens the door to discussion whether the information provided was ever sufficient. In the real world, the information provided is often crisp because inclusive texting would make the conditions and other material to be read by the individual unwieldy. There are also many situations where the individual and the data user are not on equal terms, such as in employment or patient-doctor situations which raise the issue of inherent use of pressure or abuse of a dependency situation. Another drawback is the fact that most people don't care (although they should) and want to go on with the business, only to wake up and regret this later. Practical and business necessity confines relevant information often to the small-print section (with ensuing insufficient clarity) or causes the industry to oversimplify the processes for which consent is requested. Often the consent requirement is designed as an undifferentiated "all or nothing" – one single consent for all kinds of data use, and sometimes it means for the individual to get no business at all if the consent is not granted.

7. IF CONSENT ISN'T ADEQUATE: WHAT NEEDS TO BE DONE CONCEPTUALLY TO PROTECT THE INDIVIDUAL?

The European style answer is simple, although not the only one possible: To make sure that less personal data are in circulation. The inhibition of data proliferation is conceptually the underlying basis of what is technically called "data minimization". Similarly, personal data should not be forever in circulation unless in exceptional circumstances. From the inception, this has been a strong pillar of data protection in the EU and its member states. It is also this feature that principally separates data protection in the EU from cyber- or privacy laws in the United States, where, for good reasons, the freedom of information, the flow and the availability of information for everybody takes preference. U.S. data entrepreneurs have traditionally much greater freedom in handling personal information but face strict – and increasingly stricter - consequences in the case of accidental data loss or data breaches. The current basic concept prevailing in the U.S. prefers data safety over limitation of the flow of information which the U.S. Federal Constitution considers a fundamental right of the individual.

Data safety is in fact a core concern with data processing everywhere. Regulatory concepts needs to safeguard and monitor data processing by data entrepreneurs and provide sanctions to disincentive intentional or negligent exposure of the individual's data to unwanted access, alienation or loss.

Last but not least, persons sourcing and processing other people's data need to be held responsible for what they are

doing with appropriate restrictions and sanctions protecting the rights and freedoms of the individual.

Taking all these considerations, data protection as a concept rests principally on five pillars: safety, necessity, accountability, finality and enforceability. Those will be the subjects of the next five chapters.

Chapter II: Data Safety

The willingness of a person to share data with a professional data handler (a "controller," if the handler has discretion, or a "processor," if he is strictly bound by instructions) depends chiefly on the assumption that the data transferred or otherwise acquired will be held in safe custody. First and foremost, the transferor of personal data does not want the data to become lost in any way, through deliberate erasure, accidental deletion or otherwise. But data safety encompasses, upon closer inspection, several additional elements.

A transfer of personal data to a data handler today is normally done not just for storage purposes but also because the parties to a data transfer share a common goal for the subsequent processing of the data. Data processing is done for a purpose. So as a first step to achieve data safety it needs to be assured that the data processor sticks to the purpose for which the data were acquired and avoids unpermitted deviations from the purpose. Modern data protection regulations state this as one of the fundamental rules, to make sure that data do not get lost. By the same token and equally importantly, the transfer of data is done on the premise that the data not be lost, altered or alienated in any way by virtue of the process and the technology applied.

1. THE CHALLENGES OF INDUSTRIAL DATA PROCESSING

From this starting point, since long a fundamental element of data protection, data safety has evolved considerably in

keeping up with the challenges of a data industry that today collects, stores and analyzes data at an advanced level, involving large amounts of personal data that are acquired often without the individual actually knowing or realizing that her personal data have been collected. Over the past decades, the absolute volume of collected data has increased manifold as a result of automated processes for the digitalization and the migration of data relating to the social behaviors of data subjects.

Smartphones, tablet computers and other easy-access devices with increasingly widespread internet connectivity are capable of handling, generating and transferring data of a considerable variety and with near-instant velocity. The newly formed data industry operating on a grand scale, called "Big Data" similar to Big Pharma, has increased its ubiquitous presence and broadened its business model by using automated processes using processors with state-of-the-art - speed and storage capabilities of ever-increasing capacity to collect large amounts of different types of data produced in near-real time from multiple and diverse sources. The information technology that permitted the rise of this whole new industry has completely changed the lives of individuals and businesses more than ever in the history of industrialization. The business opportunities in the data industry compare easily to those in the oil industry of the 20th century, but with a much more profitable business foundation: Unlike oil, personal data are sourced and provided more or less free of charge, immediately, directly, constantly and in a format that is being continuously updated through the data originator's repetitive interactions with others and by

using essentially the same data set. With virtually no collection cost, the economic gains from data processing on a grand scale are so much greater than those from the oil industry of the prior century that the enterprises providing the networks and those providing the technology for storing and processing are now among the most valuable industries on the stock market. It is the vastness of the data business that makes the data safety aspects of it a dire and, but for the noise of political discussions, invisible consequence.

2. THE DARK SIDE OF THE FORCE

Alongside Big Data, however, shadow industries and players thriving on cybercrime have likewise developed and prospered. Computer attacks and hacks have blossomed on the back of the same technological advancements of processing technologies. While stealing oil once proved to be virtually impossible as a business, stealing personal data has developed into an extremely valuable enterprise. Personality theft, breaches into secure data vaults with the aim to make direct money or bitcoin transfers, and outright extortion with ransomware attacks have become the daily concerns of data operations and law enforcement alike.

Computerized data crimes have in many cases completely overrun the data industry, and it is for this reason that data safety has become quite a different concept from its original manifestation as the protection of people's data on the basis of an agreement or understanding. Data safety today is a vital necessity of the entire data business already for systemic

reasons – modern societies cannot afford major data breaches and criminal attacks on systems that have become so essential for the operation of any business that a prevalence of criminal behavior would create a substantial systemic risk for the entire society. In addition, today's technology advancements permit data acquisitions without the data subjects knowledge on a much greater scale – without a regulation, these data remain without protection from a legal perspective.

This has led to two legal consequences.

3. LEGAL CONSEQUENCES

For one, lawmakers had to devise public agencies charged with ensuring that cyber attacks or other security breaches relating to personal data are defended against with the latest technology, and responsible for safeguarding the functioning of information systems that provide essential services to a community. Many countries have installed special agencies since.

Secondly, today's data protection laws had to increase measurably the responsibility by requiring controllers and processors to implement appropriate and effective safe-processing measures and to demonstrate effective compliance of processing activities with appropriate technology standards. Modern data protection laws require the data handler to define, evaluate and assume the risk of data loss or alienation through objective assessments, and to identify practices to mitigate that risk. The canon of requirements is long:

Controllers and processors have to implement appropriate technical and organizational measures that ensure a level of security which is commensurate with the relevant risk identified, and to use pseudonymization and encryption of personal data where possible and appropriate, to make sure that the technology used assures ongoing confidentiality and integrity, to enable a quick restoration of lost or breached data and to regularly test and evaluate the effectiveness of technical and organizational measures.

Already at the outset of a data business but even more so on an ongoing basis, a sober evaluation of the relevant risks and the degree of possible exposure has to take place, to make sure that technical measures to be established are appropriate in relation to the established risks.

4. CONTROL AND SUPERVISION

Measures to be implemented by controllers and processors to ensure data safety are theoretically subject to varying degrees of public agency control and review. Of course, no agency can perform a sensible review on an everyday basis – the means to perform a daily supervision are simply not available or would be fully automated through computers, which would rather defeat the purpose of human control at some point. It is for this reason that regulations generally avoid permanent ongoing inspection or control, except in limited criminal cases. But that doesn't mean that supervisory agencies in charge of data protection may not review the safety measures that were established at operational level: Not only are supervisory

agencies authorized to inspect companies at any time upon demand which is regularly expected for critical industries, data handlers have also to be aware that any complaint by a data subject or any occasion of a data breach will most likely cause the supervisory agencies to conduct a detailed review – and discussion - of whether the standard safety applications were sufficient.

A good example of a situation invoking trouble is the decision of a data handling operation to run the business through server vendors that are for cost reasons located in jurisdictions away from the one of the data handler, often in locations that do not have appropriate safety standards comparable to those that are required at the seat of the data operator. An internet company operating out of Germany should not have its data server provided by a vendor hailing from a place that has a good reputation for originating cyber attacks in bulk (this is not made up, it happens). It would of course not only look bad in the eyes of the data supervisory agency upon inspection and cause protracted reviews. It would also shift the burden of proof to the data handler, to show that everything had been done to provide adequate data safety in view of the additional risk. Besides, in case of a data breach, such a situation would often lead to a significant reputational damage and loss of business even if the vendor was actually not at fault and actually employed appropriate safety standards.

5. BUT IS IT ENOUGH?

Given that many data breaches keep occurring on an everyday basis, also the law enforcement had to step up its powers and defenses considerably in order to cope with the disturbingly increasing number of cybercrimes. Yet, it is probably fair to say that even the speediest law enforcement only works retroactively and provides in practice little to no deterrence of cyber crime. Even well thought-through safety systems and tight restrictions on data processing are not, and will not be, sufficient to avoid the accidental or deliberate loss or change of personal data through unwanted access or disclosure. Without wanting to borderline on fatalism: personal data simply will get lost or changed, and although data safety is a necessary goal to be achieved and maintained on a technical level, a data protection concept would need to think of alternative measures to protect personal data against alienation or alteration.

As discussed in the Introduction, a natural step in the direction of data safety is to curb the availability of personal data within the system, which in data safety terms translates into restrictions on onward transfers of personal data, inside as well as beyond the outer limits of a data processing operation, except where an onward transfer is necessary and data safety is reasonably assured by the applicable standards of data protection and the technology used by the transferor and the transferee. This concept that EU style data protection laws call the necessity or "data minimization" concept principally requires an established process to make sure that a decision whether, how, where and to which extent data should be

transferred is only taken after serious consideration whether the reasons for an onward transfer are strong enough to justify a transfer against the assumed concerns of the individual to keep the data where they were delivered to, and behind lock and key.

Data minimization as another conceptual key element of data protection will be discussed in the next chapter.

Chapter III: Necessity

Minimization of data proliferation is one of the core concepts in European-style data protection. The lesser the amount of data in circulation, the lesser the risk of accidental or intentional data loss or abuse. The individual wants to keep her data where they are supposed to be and that they do not start wandering on and about without restraint or control. Sounds good. But how regulate data minimization in a society that thrives on interaction and communication?

1. THINK LAW

The concept, as simple as it appears, needs to translate, from a regulatory point of view, into several aspects of a potential regulation. First, lawmakers will seek to stipulate a requirement for data operators to process data only to the extent necessary for the purpose the personal data have been sourced for. As important as this first step is: There is not too much hope, though, that just that would lead to much effect. It is true that the lawmaking bodies in the EU since long implemented this as a fundamental rule, a general "necessity principle". In reality, however, lawmakers need to take - and did take – a big step further: Most EU-style data protection laws today prohibit any use of personal data generally unless specific exemptions permit the use. In other words, other people's data should not be use at all unless one can find a rule in the book that expressly permits the activity.

From a lawyer's point of view, this kind of regulation is about the strongest wrench in the legal toolbox of administrative law, and it is actually under debate among scholars whether such a strict approach really serves the purpose and the regulations actually deserve such a strict reading. The acquisition, use and transfer of data are standard activities that occur continuously as a matter of everyday life. Trying to curb interaction and communication between people is not a good idea, especially if one starts with a total prohibition and projects the necessary features of data processing into an exception. As a consequence, data protection laws need to be interpreted in line with what German law calls "practical concordance", in other words to align the real purpose of data protection, the protection of the individual against a machinery that would otherwise be left unguarded, with the freedom of information as a fundamental basis of a society of free individuals. Thus, the law would have to make it very clear in which circumstances the handling of data is permitted, to give safety to data handlers and information businesses.

To cope with legal reality, most laws applying EU style data protection provide for quite long sets of permissions, in EU law called "derogations", that allow the sourcing and processing of data. Most of these permission regulations usually provide a standard minimum set such as consent of the data subject, overriding interest on the part of the data handler, necessity for defenses in court, permitting responses to public authority requests and legal requirements, and so on.

That is, in a modern legal concept, only the first step. The second relates to the onward transfer of personal data to someone else which typically requires a separate set of authorizations and in addition special precautions and safeguards. The reason for this separate set of regulations for transfers indeed is the importance of onward transfer restrictions in view of data safety and control mentioned above. Some of these features will be discussed further below.

Before addressing the obligations of data handlers imposed by law, the preliminary question that comes to mind is whether the data subject itself should be restricted in providing personal data in the first place - or accept the consequences.

2. IS IT OUR OWN FAULT?

Although it is obviously prudent for all of us to make sure that only those personal data are being put into circulation that are necessary to conduct normal life and regular business transactions, there is actually no legal obligation to do so. As surprising as it may appear: An obligation to take (better) care of one's own data is not necessarily farfetched. Insurances, for instance, may require such care in order to curb the insured risk, and there is also generally a good reason to provide such a regulation in the public interest. Although data protection as a legal regulation has existed for decades, and while at least in Germany individuals are generally trembling with fear that their information may become accessible to a public, it is surprising how little people care about the vast amounts of personal data they confer.

On the other hand, it is in today's reality no longer the individual's fault if too many personal data are transferred and we ultimately get exposed to exponential data proliferation for unknown purposes: Take employers, for instance, in particular international employers which habitually seek to obtain a lot more data from an employee than are really necessary to conduct the employment relationship. Requests for unnecessary personal data are often clad in concerns for security, internal team building or marketing needs. Taken under a magnifying glass, a true need for all the information is often not there and the collection process completely lacks a necessity test. There is no question that certain information may indeed be important and that serious reasons do require those data to be available, but there is also no need to ask for personal mobile phone or home phone numbers, secondary home addresses, parental addresses, names and so forth. Also many internet businesses seem to have an insatiable need for information that they do not really require but request nonetheless with a view to further business in the future – and some to actually sell the information on to online marketing firms.

3. CARPE DATA, PROCESSOR!

As a consequence, the minimization of personal data processing has to happen at the receiver, *i.e.* the processor/controller-level. Data protection regulations, therefore, require controllers and processors to minimize the amount of data that they process, even if the individual has transferred more data than are actually necessary to conduct

the transaction or to fulfill the purpose of the communication between the individual and the data controller/processor. A public regulation in furtherance of data minimization addresses the data handling of each relevant controller/processor by requiring that the processing of personal data must be limited to what is necessary in relation to the purposes for which the data are processed.

Another reason why a regulation should require data minimization from the data handler rather than the individual is that data handlers have, as already mentioned, a tendency to source and process more data as part of their data processing systems than are necessary to conduct the business or communication at hand. The professional data industry not only seeks more data to have a better picture of the person whose data are processed but also to provide crosslinks through and a greater usability of the set of data on the individual for a variety of purposes and industries (not to mention some that abuse such spillover data for a different business). The broader the set of data available on a person and the more actualized, the higher its value on the market for personal data. So even if the individual provides more data than are actually necessary, data protection regulations will limit the processing by data handlers to what is strictly the necessary to fulfill the agreed purpose for which the data needed to be sourced. Since the potential scope and duration of data processing cannot be predetermined, most data protection lawmakers have articulated the minimization principle in a general, overarching obligation on the part of data handlers to minimize data processing.

4. DON'T YOU DARE - TO SHARE!

The other principal tool for minimization is a limitation on proliferation of personal data. Data protection not only targets the sourcing and processing, but also – and separately – the onward transfer of personal data to others. To this aim, regulations of an onward transfer require, for each time of transfer a further set of permissions and safeguards to be fulfilled, on top of the ones in place for data collection and processing. An onward transfer from one data handler to the next, therefore, will not only require a special reason (the consequence of the data minimization principle) for the onward transfer, but also further special safeguards to make sure data are not getting lost or changed in the process. This holds true in particular if the onward transfer is aimed at a jurisdiction that is not recognized as having the same legal standards of data protection as the transferor's jurisdiction. In this situation, the transferor is required to apply further, additional safeguards to make sure that the recipient party will observe the data protection standards of the transferor jurisdiction.

This is easier said than done. The transferor jurisdiction has basically two options. One is to make a transfer of personal data to a different jurisdiction depending on a prior recognition of the recipient jurisdiction's legal data protection standards by the transferring jurisdiction. This isn't achieved by the stroke of a feather and consequently there are only few cases where this has been made. The other is to make the transfer dependent on the certain agreements between the parties to

confer the transferor's data protection obligations on to the data recipient.

The first option would require that jurisdictions would have to match each other's protection standards pretty well. At the moment, the EU has recognized only a handful of foreign jurisdictions as being equivalent in data protection terms. Countries like Switzerland, Argentina and Japan (Japan recently acceded to similar data protection standards) are examples. But not belonging to that circle of jurisdictions is biggest single market on the globe (besides EU/Japan), the U.S., even though some of its states and certain business areas have already strict data protection standards, for example hospitals and medical providers in connection with patient data under the U.S. HIPAA, the stricter data protection applying in the State of California or the latest change in New York State law relating to data breaches and reporting requirements. Because the U.S. generally do not provide an adequate data protection standard in the view of the EU, the EU and the U.S. have agreed on certain minimum standards (called the "Privacy Shield"), and as the regulations currently stand, it is sufficient that U.S. personal data recipients from the EU self-certify their compliance with the Privacy Shield requirements to the U.S. Federal Trade Commission which monitors also data protection compliance. It is a fairly limited, kind of minimum standard approach, and it remains yet to be seen whether the European Court of Justice (ECJ) will accept the Privacy Shield agreed between the U.S. and the EU as sufficient in EU data protection terms on U.S. premises. A case currently pending with the Court is expected to shed more

light on the issue by early 2020. Suffice to say that the EU/U.S. data protection bridge currently in place does not look too stable.

As an alternative, data protection regulations may also allow data transfers if agreements between parties of an onward data transfer create a contract that ensures that the data protection obligations of the transferor jurisdiction are observed by the transferee in the processing and a possible and necessary onward transfer. EU-style lawmakers have over the years devised a number of ways accomplishing this goal, in particular such as legally binding corporate rules that apply sufficient protection standards throughout a group of companies ("BCR") and data transfer agreements ("DTAs") to regulate the way data handlers process and transfer information, based on standard data protection clauses adopted by the EU Commission (or an EU supervisory authority with approval of the Commission). There are further options to regulate compliance by data recipients, such as agreed codes of conduct and other forms of binding and enforceable commitments on the part of the receiving data handler. Their common denominator is that the data transferor entity in the sourcing (home) jurisdiction assures by contractual commitment that EU data protection rules are observed at the receiving end.

Today, DTAs on the basis of EU-approved standard clauses are probably the most common tool to regulate data transfer used in daily transatlantic practice. They come, however, with strings attached: The standard contractual clauses provided by

the Commission may not be departed from. If they are, then individual approvals from the competent data protection authority are required. Obtaining such approval takes time and usually defeats the purpose of an easy transfer. Further, the expected amount, reason for and kind of processing must be accurately described, and the recipient actually has to know and apply EU data protection law. Finally, data transfer agreements "mean business" in that the transferor may not just sign a data transfer agreement and then forget about what the transferee recipient does with the personal data. Data transfer agreements, according to the standard EU provisions, require the transferor to monitor the recipient data handler's behavior through visits, recurring reports, checks on procedures and immediate reporting in case of data breaches or other attacks on the integrity of the data protection at the receiver. And to take action, if there are signs that the recipient is not or no longer compliant.

But what if the receiver notices access attempts or breaches into the data base by public authorities, such as national security agencies? Should this be immediately reported to the "foreign" data transferor, thereby compromising the interest of the national security agency? Or rather remain silent and breach the DTA as a good citizen? These issues have come up in connection with the discussion on the EU/U.S. Privacy Shield at the time it was conceived. They are also sparking similar discussion in relation to all forms of regulation that permit data transfers, such as Binding Corporate Rules. It suffices to say that a data transfer arrangement, even if following a pre-approved set of clauses, does not and cannot

solve data protection problems arising from data transfer forever. There is simply too much change in the relevant technical environment. To assign responsibility to a data recipient cannot be permanent and will not help in any situation. Consequently, European data protection agencies have so far not taken a firm position on this issue, as they wait for the decision of the ECJ mentioned above by the beginning of 2020.

5. THE STATE: A HUNGRY BIG BROTHER

A typical but often unseen mass-access to personal data is caused by the data hunger of the state itself. To remember: This is how data protection started in the first place, as a fundamental right against the ever-nosy administration. There are two tools that are meant to actually curb the sourcing, processing and onward transferring by an European state: first, the state is operating under a separate set of similar data protection laws like the private data industry, and in fact the overarching legality requirement of a public administration makes the observation of data protection rules and its exemptions supposedly even stricter. Secondly, many states operate with communication barriers between various agencies to curb proliferation of information unless provided for in a special procedure and with a special permission. The typical example is the information of a criminal activity rising in the hands of a public prosecutor office which should only be communicated to the border services if there is a search warrant in place. Not every state has those barriers.

In addition, states have usually strictly defined rights to collect other people's information, first and foremost in law enforcement, but also in connection with supervisory responsibilities over regulated industries. Both kinds of public state involvement confer rights to collect information, and those rights are widely recognized also across state borders: Many states cooperate with each other, and many of the Western states have mutual legal assistance treaties in place that provide for the sharing of information in cases of law enforcement. This is, however, not always the only rule that states follow. The United States, for instance, reserve the right to issue information requests against U.S.-based companies including their foreign subsidiaries, and hold the addressee company responsible for failure to submit the information that is supposed to be sourced outside of the U.S. In recent years, data demands from the U.S. in relation to subsidiary operations of U.S. firms abroad have increased significantly and the resistance against them by several data industries operating abroad resulted in the U.S. "Cloud-Act" that permits U.S. law enforcement to request from U.S. enterprises the release of data that have been sourced or transferred outside of the United States. Conversely, EU and other's regulations do not recognize such information request in the absence of an applicable mutual legal assistance treaty between the countries and prohibit the submission of the requested data, thereby creating a stalemate situation. European law has made this very clear with the introduction of the GDPR, and several states, such as France and Switzerland have laws in place that prohibit other states from directly or indirectly investigating unless by using a mutual legal assistance treaty.

6. DIVIDE ET IMPERA: ANONYMIZE AND PROCESS?

Because data safety and data protection are still limited even where data processing is justified or a transfer is governed by a data transfer arrangement, the idea has been proposed to increase data safety standards in connection with data processing and transfers by separating personal data from the affected data subject. This process, if done completely and irreversibly, is called anonymization, as already discussed briefly in the Introduction. Its advantage is that a set of data, once permanently and irreversibly separated from the data subject, no longer qualifies as "personal data" and is not subject to data protection regulations, so it may be freely sourced, processed and transferred – data protection simply does not apply any more.

But it does have a number of key disadvantages that make it rather unusable as a tool for data processing. Because anonymization – even if fully achieved technically, see the discussion in the Introduction – needs to be permanent and irreversible, the processor of anonymized data can no longer go back to the data subject for actualization purposes, to re-install the data set or to verify authenticity. An anonymized data set may already by itself provide less significant information, because much of it has to be anonymized or even deleted to assure anonymity, such as credit card information, addresses, time and location – this kind of information often permits to track back the information to the real person, thereby defeating the anonymization. Conversely, the absence of a tool or source permitting reinstallation of the full personal

data set makes anonymization for transfer or processing purposes unusable in practice.

The data and information industry has tried hard to solve those problems by providing a part- or part-time-anonymization. However, from a legal point of view, partly-anonymized data which at some point permit retracing or – installation of the data set, do not qualify as anonymized data. The legal term describing a situation where data can be traced back to the data subject is "pseudonymization", which means that the name has been simply replaced by a symbol and the symbol can be used to uncover the true data subject at a later stage.

This does not mean that pseudonymization is a bad thing. In fact, data protection regulators do prefer companies active in the data handling industry to apply pseudonymization where possible. From a minimization perspective, it is still better to have pseudonymized data rather than original, readily readable personal data.

7. AGAIN: CONSENT?

Last but not least, data protection regulators may also choose to permit the onward transfer of personal data with the consent of the data subject. This measure was actually preferred in some jurisdictions prior to the release of the European General Data Protection Regulation. A legal derogation on the basis of a consent, however, is no longer the gold standard and has in most jurisdictions been abolished as a

standard tool unless it is assured that the individual is granting the consent specifically for the concrete business, fully educated and expressly. Especially in labor relations or other situations where the individual is not at liberty to take a consent decision, the value of a consent is limited and for serious reliance purposes actually too limited. It is often easier and more appropriate to resort to the general derogations like predominant interest, legal defense or other necessity requirements.

Individual member state regulations in the EU permit the sourcing of data in labor relations only with a sufficient legal foundation. German law, for instance, permits data sourcing from an employee's business device if the employer has a documentable criminal suspicion or if a special agreement exists between management and the employee representation. In practice, these kinds of restrictions have been found more helpful than a consent requirement to make sure that personal data derived from sensitive situations do not end up, in one way or another, in different jurisdictions where they could lead to sanctions and other unwanted measures against the affected individual.

Chapter IV: Accountability

Because the control of personal data and their processing is such a pervasive and everyday-life affair, accountability is another major pillar on which proper data protection rests. It is not only important, but also extremely difficult to provide, conceptually as well as legally.

Conceptually, data protection accountability means that data handlers have to act responsibly in sourcing, processing, transferring and deleting other people's data. As shown before, the main aim is to make sure that data handlers have a system in place that assures not only data safety, but also that data are not proliferated, i.e. transferred outside of the operation unless in exceptional circumstances that are kept under control. In addition, it requires data handlers to process data responsibly, in simple terms: to know what they are doing, considering the technology used, processes applied and safety procedures established.

The key factor of accountability is that it is supposed to fully operate at the data handler level and that it is in principle not depending on the constant involvement of supervising authorities.

1. DON'T COUNT ON THE STATE!

The supervising authorities, in the early days until a few years back, consisted of few, notoriously understaffed authorities. Some countries' data protection offices turned out to be

complete failures, in terms of any effective supervision. In many countries, like in Germany, state data protection authorities consisted of three to five people, sometimes even only one official, with just a few assistants located in a remote location or tucked away invisibly in an unimportant-looking government building. It took the *author* once 15 minutes of scrambling to find the Austrian data protection commissioner inside the maze of the Vienna *Hofburg* – today, she heads the European Data Protection Board. Responsibility for personal data was quasi unenforceable, seen from the perspective of public authorities. Again, the EU Court of Justice brought the fundamental change, this time forcing the Irish data protection commissioner to exert control over Facebook's uninhibited data transfers back to the U.S. and – to make matters worse – at the same time ripping apart the cozy EU/U.S. Safe-Harbour arrangement which had served as a shaky basis for data transfers into the U.S. for many years *sans critique*.

2. LA CENERENTOLA OF CORPORATE LIFE

Early data protection, effectively, almost entirely relied on the willingness of data handlers and their advisors to develop and maintain processes that ascertained data protection. There was a little to none accountability in everyday data processing, in fact, in people's mindsets data protection as a responsibility was for a long time largely ignored or overruled. During the first decades of data protection, corporate in-house bodies in charge of data protection were virtually not there, inoperative or understaffed. Persons in charge of data protection inside an

operation had quite a difficult life when objecting to business measures affecting personal data of customers, employees or third party contacts.

3. WHAT BROUGHT THE CHANGE

Long time before the ECJ's *Safe Harbour* judgment, the change was brought on with the advent of cross border transactions and corporate investigations across the Atlantic. In particular the U.S. government had, as a result of the Lockheed scandal, enacted strict prohibitions on foreign bribery. One of the essential features of the new foreign corruption law (the Foreign Corrupt Practices Act of 1977, "FCPA") was its extra-territorial reach by design. Enforcement was strengthened considerably when President Bill Clinton authorized the Securities and Exchange Commission (SEC) in Washington D.C. to also enforce the FCPA against U.S.-listed corporations, which included listed European companies and their subsidiaries abroad. As a result, European companies with stock listed on any U.S. exchange found themselves and their subsidiaries exposed to investigations from the U.S. Department of Justice (DOJ) and the SEC. To carry out these investigations, the U.S. requested huge amounts of information, including personal data, from European companies.

At the time when such investigations were first beginning, European data protection laws, which varied to some extent among the individual member states of the EU, provided only limited and untested grounds for the transfer of personal data

to a non-EU jurisdiction. Only few exceptions permitted derogations from the principal wholesale prohibition to transfer personal data to a jurisdiction like the U.S. that would not have the same data protection standard prevailing in the EU. Most EU member states did provide a derogation for a data transfer in response to a legal proceeding, but the derogation was arguably to be construed narrowly, which led a number of advisors and supervisory agencies to believe that no personal data could be submitted in response to U.S. government requests for information in investigations, unless – through legal assistance treaties – local law enforcement or prosecutors got involved through information requests from the U.S. authority as part of an official legal assistance request. Some companies unwilling to risk the wrath of the U.S. government, however, devised methods to transfer information to the U.S. government by submitting personal data under agreed processes and arrangements with the U.S. authorities which assured acceptable standards of data protection for the submitted information. Opening up a documented path for responsible data transfers was a huge novelty for the U.S. government as well as European data protection authorities and practitioners alike. Conversely, it opened the eyes of European companies for the restrictions of data protection that had been dormant for a long time.

As a consequence of early cases like the *Siemens* investigation starting in 2006 by German and U.S. prosecutors, internal corporate investigations with the aim of reporting findings including the personal data of involved subjects to foreign authorities became more and more prevalent. The resistance of

local governments against seemingly "U.S.-controlled" investigations in Europe, however, grew in tandem – until today, as the recent discussion on the reach of the French blocking statute shows, a law that is meant to limit a data transfer to processes permitted by legal assistance treaties. One result was that some member states also added restrictions on the sourcing of employee data in connection with investigations, recognizing that employee data need to be specially protected. This led to another jump in accountability because the compliance with data protection was now assured through the involvement of labor relations parties, namely works councils where local laws provide for them like in Germany. Today, the data protection aspects of internal investigations are the biggest stumbling block and require almost always the advice of experts and advisors specializing in the data protection aspects of an investigation as well.

This development did not come without some surprising negative side effects: Corporate wrongdoers started to abuse the limiting effects of data protection to prohibit the discovery of criminal activity. Some even avoided deliberately the use of own computers and email correspondence altogether, leaving those to their assistants and their computers, with the deliberate aim to disable data searches of computers because of employee personal data protection rules (which require a founded suspicion of criminal activity for a permissible search). Defense counsel of potential wrongdoers invoked data protection laws to avoid interviews of their clients on unpleasant issues and to suppress or stall the reporting of information generated from any interviews that could damage

the position of their clients. Complaints to data protection officers have mounted since – not only by the good guys.

In any event: At the end of the day, data protection had become a significant factor in corporate information flows. And it strengthened the function of a special corporate officer in charge of data protection.

4. BE NICE TO YOUR DPO

With the increased sensibility for data protection maintenance inside a business operation, the data protection officer (DPO) whose function was already provided by many data protection laws but effectively subsisted in hibernation until then, became relevant, powerful and visible. Data protection laws had identified already very soon the need for a special corporate officer who would have to be involved in sensitive data protection issues inside a business operation, and the position of the data protection officer, although with locally much differing results, was required not only to have a special education in data protection matters but also hold a position in which he or she could form an effective opposition to the management. Thus, the management could neither ignore nor direct the data protection officer in her views. Today, virtually all businesses have the data protection officer firmly established. The ultimate decision and responsibility resting with the management, the legality requirement for the business operation under most laws requires the management to act lawfully and to consider the advice of the data protection officer.

5. A KICK FOR THE FUTURE

In spite of an increasing awareness and accountability in special situations of corporate management, data protection in terms of data safety, minimization and accountability long remained inadequate in many other respects of modern technology and its fast development. For over 20 years, data protection laws continuously ignored increasing concerns and risks associated with the exponentially growing proliferation of personal data in connection with machine-run day-to-day activities, such as phone calls and electronic communication with mobile devices, travelling records, credit card payments records or other footprints left in a person's "electronic" life and interaction. In particular, the risks associated with the vast amount of data being generated through the "Internet of Things", data exchanges conducted by machines with little to no human involvement, was for a long time not addressed by the EU. EU lawmaking bodies finally began to recognize the lack of effective data protection and accountability in modern data processing and after a long fight with considerable push of lobbyists passed the European General Data Protection Regulation ("GDPR"), entering into force in May 2018, principally taking the German data protection model as a standard and amending it to reflect a more efficient approach to data protection for modern society as a whole.

6. THE EU GDPR: TODAY'S GOLD STANDARD?

The GDPR's greatest advancement is certainly the considerably increased level of accountability that it requires. So let's take a closer look.

First, the GDPR recognized that the ultimate goal of data protection, as already envisaged by the 1983-decision of the German Federal Constitutional Court, is to keep the individual in control of its personal data. Therefore, the GDPR accountability approach relies chiefly on the individual by granting the data subject a number of enforceable rights, in particular to

- access processed own information in a formal procedure with strict time limits, a "Subject Access Request";
- obtain similarly information about data that have been circulated by others;
- obtain a clear picture of how own data are processed and what will happen with them;
- correct incorrect data stored/processed; and
- erase data that are false or no longer being circulated, needed or current (the "right to be forgotten", to be discussed later in more detail).

In addition, EU regulations grant the individual the right to data portability and to be notified about the rectification or erasure of personal data or restrictions of processing. Modern data protection standards also oblige data handlers to certify that they know exactly where they keep specific personal data, what it is being used for, how and by whom it is being processed, and last but not least where the data will ultimately end up. All these details are commanded to be put down in writing and to be kept ready for inspection by authorities. Data processors do not have to report these details on a constant or recurring basis, because that would create too great a burden

for the authorities. But as soon as the authorities have a reason to inspect the company and its data processing procedures and internal safety measures, for instance because a breach has occurred that required reporting, they will also inspect the data operator with a keen eye for proper recordkeeping and observance of processing requirements. In practice this often leads to results that are not only embarrassing for the data controller/processor but also lead to costly efforts to rectify the omissions under the watchful eye of the data protection authority - and the *Damocles' sword* of a possible hefty fine which may amount to up to 4% of the yearly revenues under the GDPR.

Both the internal organizational obligations and the long canon of rights granted to the individual data subject provide a very effective tool to ensure that professional data handlers observe data protection requirements. The combination of the two in fact avoids mishandling of personal data in the first place, so that the power of data protection authorities to issue fines is in daily practice much less critical, contrary to the expectation of most U.S. firms that are involved in European data processing.

The EU regulations have also strengthened considerably the role and position of the data protection officer which is now uniformly required already for relatively small operations handling other people's data. Like before, the data protection officer has a quasi-independent position in the corporate operation vis-à-vis the management and cannot be so easily replaced by someone else.

EU data protection regulations also require a special view of the impact and risks of business operations to personal data basis in special situations when mass data processing and transferring is likely to be involved. Data handlers need to assure that all necessary precautions are upgraded and in place before operations on personal data begin that carry a special risk of rights impairments for the data subjects. This process is called "data protection impact assessment" (better known in the short form DPIA) and is expected to provide a very effective tool to safeguard data subjects' rights in critical situations.

By today, data protection accountability has reached a much higher level compared to where it was only a few years ago. Other states' laws, such as Japan, Argentina and the Mercosur states, have followed or are about to follow the guidance of EU law and provide the same or similar levels of accountability going forward.

What is important to keep in mind before moving on: The data protection laws, at least of EU standard, will *not* be enforced chiefly by authorities. Yes, there will be supervision and the authorities can jump in at any time, but they do not have to: In most states, other sets of regulations, often internal and provided by labor, corporate and consumer protection laws, for instance, will provide the grounds for enforcement by state but also many non-state players, at least the affected individual, and no company that processes personal data in the course of its business can afford to have constant legal arguments, proceedings and complaints galore.

Chapter V: The Right to be Forgotten

While European lawmakers, and similarly other countries such as Argentina, Switzerland, and Japan recognize the rights of the individual for information, participation, and control as the primary tools to enforce data protection and assure accountability, one individual right stands out like a light tower: The claim against public media for de-referencing, better known as the right to be forgotten.

1. AGAIN THE ECJ: THE *COSTEJA*-CASE

The right to be forgotten, as a concept, has been discussed since the early 2000s and is based on the expectation that a processing and storing of personal data needs to be finite, in line with the actuality of the data. It has taken some years of discussion before it was actually put into practice, again by a landmark decision of a court, this time the European Court of Justice. In the famous *Costeja*-judgment, the Court decided on May 13, 2014 that the right to be forgotten is a human right. Although the court did not explicitly grant such a right, it derived the fundamental protection aspects of it from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, i.e. the respect for the private and family life and the protection of personal data. Mario Costeja González, a Spanish national, had claimed from Google Spain that the links to certain public announcements on him be removed. Google Spain refused, and so did Google Inc. in California. The court eventually cut through the defenses that Google's operation was not based in the EU in any relevant way: It observed that

Google Spain was a subsidiary of Google Inc. and, therefore, an EU establishment within the meaning of then existing EU regulations, and rejected Google's argument that its Spanish subsidiary would only promote and sell advertising space. The Court took the view that Google Inc. and Google Spain should be treated as a single economic unit because they interacted and supported each other in furtherance of Google's principal mission. On the right to be forgotten itself, the Court held that the processing of data which are inadequate, irrelevant or excessive (and not merely inaccurate) is incompatible with EU regulations, and the information as well as the links in the list of Google Results must be erased. The decision commanded a balancing of the right to privacy and data protection in European law with the legitimate interest of the public to access such information, and also opined that it does not necessarily mandate that information is instantly removed upon request. The Court's decision also makes a distinction between public personalities and private individuals. Stressing the ubiquity of internet search engines profiling individuals in modern society in a permanent manner, the Court eventually found that the data subjects' rights must be able to overrule the economic interest of the operator of a search engine and also the interest of the general public in finding that information on it.

2. THE HISTORY

The notion of a right to be forgotten in the legal discussion is derived from numerous preexisting ideas that were discussed across several European countries, including England,

Germany and Spain but also Argentina, India, South Korea and the United States. In the United Kingdom, for instance, there has been a longstanding view that after a certain period of time criminal convictions should no longer be regarded when obtaining insurance or seeking employment. Similarly, France values since long *le droit á l'oubli* and recognized it in 2010 officially in law.

3. CRITIQUE

This does not mean that a right to be forgotten was always readily accepted. In fact, the views on its justification differ greatly between the United States and the EU countries. In the United States, transparency, the right of free speech according to the First Amendment, and the general "right to know" have typically been favored over the deletion of truthfully published information on individuals. While courts in the U.S. do recognize the right to happiness which includes a freedom from unnecessary attacks on character, social standing or reputation, they have also held that a person cannot ignore the status and information relating to it, in particular if the person is a celebrity, so that there are limits to the right to control one's life and facts about oneself. More recently, however, contributors to the discussion in the U.S. noted that many privacy protections that Americans believe they enjoy – even some guaranteed by law – have, in fact, been eroded or even obliterated by technological advances. And it is indeed the exposure of the individual to ever-recollecting electronic brains that has changed the views of many. In previous times, people with a "personality" rather sought to be remembered by

the generations to come, politicians, soldiers, artists, scientists: It was completely natural to aspire to become "famous" and to be remembered for generations to come. What changed the views, was obviously the realization that reminiscence today is no longer tied to important publications or works generally but available on any person and at the touch of a button – through access to an electronic system that will not forget unless the information is positively deleted or destroyed. To require search engines and online services to remove information from circulation and availability that is inaccurate, irrelevant, excessive or no longer material to current public debate or discourse is only a natural consequence from the possibility that continuing accessibility of information on a normal person can cause real harm to it.

4. IT'S THE (WRITTEN) LAW NOW

While legislative movements in the U.S. so far have not taken big strides in the direction of a right to be forgotten, the European data protection regulation (GDPR) enacted on 25 May 2018 now provides detailed recognition and regulation of the right to be forgotten and to erasure, by permitting an individual to whom the data appertains to claim from the controller the erasure of personal data relating to it and the abstention from further dissemination of such data. This holds true especially in relation to personal data which are made available by the data subject while he or she was a child or where the data are no longer necessary for the purpose they were collected for, the subject withdraws consent, the storage period has expired, the data subject objects to the processing of

personal data or the processing of data does not comply with regulations. The European Union and its data protection regulation is expected to exert strong influence on many other states such as the Mercosur-states, and its regulations on the right to be forgotten are a step forward towards its global recognition as a right.

5. BUT NOT WITHOUT LIMITS

In practice, however, the right remains quite difficult to apply. It is and will continue to be a challenge to reconcile the right to erasure of personal data with the rules governing freedom of expression, in particular considering the fact that these regulations on deletion of information directly oppose freedom of speech, and the menacing effect of the right to deletion allows on the one hand more autonomy and control of the individual over a machined world but also reduces the amount of information that may become necessary to be removed at some stage. Many share the view that journalistic work must not be touched and is to be protected. Yet, the anticipation of a regulation applied strictly may force search engines to take down, under the GDPR and the *Costeja* precedent, news too early or to produce neutral or biased information results upon searches which could compromise the integrity of the internet based information in general.

Although the interest of the public in publication and access to information is a valid concern in the balancing approach, the Courts may tend to give support to the view that the basic fundament of societal interaction is the right of individuals not

to be harmed unless by a strongly overriding interest. In this sense, data protection authorities and courts are expected to rather enforce the deletion of unnecessary, outdated or otherwise unnecessarily harmful information as a matter of necessity.

Another hotly debated element of the *Costeja*-decision was its international reach and the question whether search engines would need to take down references to a person around the globe in order to satisfy EU requirements. The ECJ just clarified (C-507/17 *Google/CNIL*) that an operator is not required to carry out the de-referencing on all search engines around the globe - although the Court still requires that internet users need to be discouraged to conduct searches from the EU into foreign data bases, which likely doesn't make it all that much easier for the operator to comply.

Chapter VI: Data Breach – When Data Protection Goes Dead Serious

Before considering actual or potential measures against or in case of data breaches, consideration should be given to where data breaches actually come from in practice and how often they occur. A data breach, in the German and French language "*Panne*" (the same term is used for a flat tire), encompasses a huge variety of unpermitted access to a data processing system, involving a breach of security leading to a destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

1. IT HAPPENS A MILLION TIMES

To get a sense of the magnitude and frequency of breaches, one should consider a situation, where someone leaves a personal device such as an iPhone inadvertently in a taxi (which happens monthly to some). Many of us do not secure access to such a device with anything more than four easily memorable digits or characters – a home game for professional engines that figure out passwords. By the same token, a data breach can also occur through professional hackers entering a data processing system with tools that are widely available even for amateurs, and once they are "in", all sorts of things may happen: Sometimes hackers just enter "to look around", but in many cases to make money: by placing viruses, Trojans and other malware such as random ware which threatens to destroy the system unless a certain amount of bitcoins is paid to a bitcoin account on the Internet. Internet crime has

become so vast that 500 attacks on a system are no longer considered being worth raising eyebrows. Interesting targets for attacks can at least count on about 20,000 attacks – per day.

It is for this reason that data protection primarily starts with the data safety of machine processing, as discussed in chapter II. But what happens – or is supposed to happen – if a data breach occurs and the data safety is no longer there?

2. IT'S UNAVOIDABLE

The obvious answer is to avoid such a breach in the first place. But personal data need to be accessed because just storing them away without any further access defeats the purpose why personal data are being processed. So a data breach is, philosophically speaking, inherent in data processing. It simply cannot be avoided.

For this reason, data protection will aim conceptually not only at requiring high safety standards, but once the breach has happened at mitigating the consequences of a data breach by establishing obligations on data controllers and processors what to do post facto in case of a breach. Looking at the developments across the globe, the U.S. in particular, it seems that the data breach laws tend to provide, with increasing strictness, the requirement for immediate reactions on the part of the operator, and extend the reach of those requirements beyond the limits of the jurisdiction, to cope with the internationalism of the data operation industry generally. (A

typical example is the recent data breach law development in the State of New York, the *Shield*-Act.)

3. SUFFER AND MITIGATE

Conceptually, the first and foremost consequence of a breach should be the information of the data subject whose personal data are affected by the breach. Unless it can be assured that nothing really happened or will happen from an unauthorized access to or an inadvertent opening in the data security system, the controller should inform the data subject about the breach and the likely consequences. They should also advise the data subject on what to do to avoid further unpermitted access and in particular to reduce exposure. On the other hand, while many such incidents pose a risk of identity theft or other serious consequences, in many cases there is no lasting damage or even exposure, the breach of security is remedied before the information is actually accessed by an attacker, or the hacker is interested in something else, not in the personal data the system contains. In such a case, alarming a data subject is creating unnecessary ado while actually nothing can or should be done in the situation.

As a consequence, data protection laws have to strike a balance between the necessity to inform the data subject immediately and the consequences this may have for the data subject's reaction, in particular its willingness to continue having its data stored with the attacked controller/processor, and the interest of the processor to maintain the business and to correct the attack or its consequences quickly, before any

further damage is done. European data protection law takes a dual approach to this conflict, in requiring the data controller and processor to inform both the data subject as well as the data protection authority, but with different degrees of necessity. A notification of a personal data breach to the data protection authority is always required unless the personal data breach is unlikely to result in a risk which the data handler has to prove. By contrast, the communication of a personal data breach to the data subject is only required if the data breach is likely to result in a high risk which is the case if financial (removal of funds from bank accounts) or personal trouble (breach of very personal information such as specially protected data). The information of the data subject is not considered necessary if the controller has implemented measures avoiding any further damage, has taken subsequent measures insuring that the high risk no longer exists or would involve disproportionate efforts in which case the information needs to be made public.

4. BE QUICK ABOUT IT

The regulations are normally very detailed about the time frame in which a data breach needs to be reported which is undue delay in case of the data subject and usually a day up to three days in case of the notification obligation towards the authorities. Some states, although very few, require an immediate reaction. In sum, no time must be wasted and the data handler has to get active fast which in turn requires that the relevant procedures are already in place that have been pre-

established and tested, usually with the help of outside advisors, for effectiveness.

5. TO INFORM, OR NOT TO INFORM – THAT IS THE QUESTION

Since a good deal of business is depending on the right decision, also in terms of business reputation, most data controllers and processors undertake great efforts in reviewing whether a filing/reporting is really necessary, to the authorities or the data subject. This holds true in particular if it is not clear whether a data breach has actually occurred or where it occurred. A typical headache case in this respect is the problem of "credential stuffing". In this situation, the breach has actually occurred elsewhere, but enabled a perpetrator to obtain large sets of passwords and names which the perpetrator then sets out to machine-play on various organizations' access systems where an access by using name and passwords can be expected, such as banks and insurances. Since the breach has not occurred at the bank or insurance itself but is only a consequence of a breach that occurred elsewhere, often a lost portable device or a set of passwords and names gained through a Trojan download, the question arises whether the bank or insurance needs to notify the data subject or the authority in case it notices that a potential perpetrator is running attempts to get access. It is not clear in every jurisdiction whether such a case would require a notification by the formal terms of the law, but it is probably good advice to give the customers at least a wink about what is happening, to allow them to change passwords and to monitor

their accounts' information for potential unauthorized access or activities, such as withdrawals.

6. MIND FURTHER CONSEQUENCES!

The notification requirement to the authorities and or the data subject does not only confer embarrassment and mitigation work on the part of the data handler. It also comports a number of unexpected further consequences that are likely to produce considerable economic damage: A notification of the data subjects may very well cause many to ask for a status report of stored and processed data on the basis of permitted subject access requests (see above in Chapter IV), one of the fundamental control rights that individuals have in relation to controllers and processors. Large data operations may suddenly be faced with thousands of subject access requests by email or telephone that can only be mastered if operations are in place that can handle those requests. Since the request needs to be answered usually within a relatively short time frame, violations or other shortcomings will certainly be reported by the data subjects to the data protection authorities which in turn causes the authority (which may be working on the breach case already) to use the opportunity to enforce the subject access requests by appropriate means which compounds to the problem.

In addition, the data protection authorities will not only address the data processing operations ability to respond to the data breach and to provide appropriate measures to avoid further damage into mitigated damages that already occurred.

They will also use the opportunity to review existing standard procedures, safety measures, and internal documentation in line with accountability requirements. It can prove extraordinarily embarrassing for a professional data handling operation not to be able to show proper records of existing processes, involved processors or outside server operations. In addition, also the relationships to outside service providers or servers located in foreign countries will come under scrutiny, along with the data transfer arrangements.

7. TAKE COVER

Last but not least the problem arises that while there is a notification and reporting obligation vis-à-vis the data protection authorities, there is also a criminal liability for data processors and controllers for mishandling data or for not complying with data processing obligations under existing data protections laws. Reporting obligations run counter to the rights of the participants to remain silent and not to burden themselves. As a consequence, both sets of provisions need to be closely checked, and often the end result is to do only the legally required reporting but refrain from the dealing with more intricate information requests issued by data protection authorities in the course of their investigations. Needless to say that such a tightrope walk requires the full concentration of the management which should be prepared to spend the time already before a breach occurs.

8. BE PREPARED

Because any data breach with reporting consequences will lead to a full review of the data protection processes and procedures, data controllers and processors are well advised to establish and test incident response plans ahead of time with the help of outside service providers, to make sure that all processes and procedures are prepared to deal with a data breach situation. This includes simple things such as a list of telephone numbers of people to call, pre-prepared filings with authorities and law enforcement to go after a potential perpetrator with all appropriate means, and to set up a response team that can jump into action.

Summary, Myths and Errors

Many readers, the *author* included, made it a habit to start reading a book from the back and seeking to grasp the essence without reading the bulky middle part. To those who share this habit and landed immediately here, welcome!

Now what is data protection all about?

Data protection is a set of obligations that assure a certain degree of control of an individual over the sourcing, processing, transferring and deletion of its personal data, defined as any piece of information linked to a natural person. The fundamental means by which data protection is assured encompasses several requirements and rules, which are in shorthand:

- to keep data safe and inaccessible to others,
- to source and use them only if and to the extent permitted,
- to transfer them onwards only if and to the extent permitted,
- to give the data subject access to the processes applied,
- and to delete the information when it is no longer useful, or false,

while assuring that a normal, day-to-day exchange of information in the course of our lives and businesses and the necessary flow of information to permitted constituencies, including state administration and law enforcement, remain possible.

There are number of myths and errors in circulation about data protection, in particular in areas where data protection does not exist as a concept or isn't yet known as an own term. Therefore, here is what data protection is *not*:

- a barrier to share information in everyday life situations: the apartment building administration can still display the names of its canons, the bakery does not have to avoid calling a customer by his or her name, businesses may send advertisements to individuals (whether businesses may use email or calls to contact an individual is not a question of data protection but of e-commerce regulations)
- a prohibition of asking questions to employees about their conduct of business and to search their business email accounts (what is prohibited is sniffing around without any special purpose, such as running permanent email checks or the use of cameras in dressing areas)
- a prohibition of transferring data to someone else (this just requires a special permission and additional safeguards that are relatively easily obtainable)
- a prohibition to transfer data to other countries that do not have the same data protection level such as the United States (there are sufficient permissions in place that allow such a transfer in response to proper investigation request by public authorities or courts but again no pervasive, sweeping information requests without necessity)
- a prohibition to use data that have been acquired for a certain purpose for any other purpose (such a use is possible if the new use is independently permissible and the individual is informed about it)

- a deliberately used tool to inhibit big data businesses (the opposite is true – data protection regulations assure the same set of legal framework for everyone, thereby creating reliability for an entire industry on standards)
- an effective information barrier for news, education and research results and discussion (the opposite is true).

Data protection has become a vital necessity for all individuals on the globe. Some may not be interested or do not care whether their information is widespread and available to everyone. The key issue is that personal data are "assets" with a surprising value to professional operators. In addition, personal data become part of machine-only exchanges which would be completely out of control in the absence of data protection regulations. Last but not least, technical processing and storage capabilities have reached a level that makes total surveillance, profiling and remembrance of every electronically storable footprint we leave possible and outside of our control – unless data protection rules provide individuals with the appropriate shield. And although we all want to be famous for our achievements and remembered by generations to come: We certainly do not want every aspect of our lives, private or public, to be remembered in detail forever. There are too many things in life that we prefer not to revisit.

It will not be long, and most of the globe will be covered by data protection regulations in one form or other. Whether they take the shape of EU data protection, as the most advanced and being followed by many states, such as Japan, Argentina or Brasil remains to be seen. Also the data privacy

laws in the U.S. become stricter and more protective every year – as is apparent from the recent *Shield* – Act of the State of New York which in many ways fundamentally changed the regulatory concept of data safety.

What started back in 1983 as a simple fundamental law defense against a nosy state census has developed into one of the most important regulations in the 21st century and an integral part of our protection as individuals.

List of International Literature on Data Protection

ALLEN, DARCY W. E. / BERG, ALASTAIR / BERG, CHRIS / MARKEY-TOWLER, BRENDAN / POTTS, JASON (2019): *Some economic consequences of the GDPR*. In: Economics Bulletin, 39(2), pp. 785-797.

BHAIMIA, SAHAR (2018): *The General Data Protection Regulation: The Next Generation of EU Data Protection*. In: Legal Information Management, 18(1), pp. 21-28.

BRIMBLECOMBE, FIONA / PHILLIPSON, GAVIN (2018): *Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression*. In: Canadian Journal of Comparative and Contemporary Law, 4(1), pp. 1-66.

BUCKBEE, MICHAEL (2018): *GDPR Requirements in Plain English*. In: Inside Out Security Blog, online source: https://www.varonis.com/blog/gdpr-requirements-list-in-plain-english/, last access: 09/19/2019.

DOE, SUSAN (2018): *Practical Privacy: Report from the GDPR World*. In: Legal Information Management, 18(2), pp. 76-79.

FEILER, LUKAS / FORGÓ, NIKOLAUS / WEIGL, MICHAELA: *The EU General Data Protection Regulation (GDPR): A Commentary*. Globe Law and Business, Woking, Surrey, 2018.

GRAEF, INGE / HUSOVEC, MARTIN / PURTOVA, NADEZHDA (2018): *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*. In: German Law Journal, 19(6), pp. 1359-1398.

INFORMATION COMMISSIONER'S OFFICE: *Guide to the General Data Protection Regulation (GDPR)*. Online source: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, last access: 09/19/2019.

KUNER, CHRISTOPHER / SVANTESSON, DAN JERKER B. / CATE, FRED H. / LYNSKEY, ORLA / MILLARD, CHRISTOPHER (2016): *The Language of Data Privacy Law (and How It Differs from Reality)*. In: International Data Privacy Law, 6(4), pp. 259-260.

MOHAN, JAYASHREE / WASSERMAN, MELISSA / CHIDAM-BARAM, VIJAY (2019): *Analyzing GDPR Compliance Through the Lens of Privacy Policy*. In: ArXiv, online source: https://arxiv.org/pdf/1906.12038, last access: 09/20/2019.

MURRAY, ANDREW D.: *Data transfers between the EU and UK post Brexit?* In: International Data Privacy Law, 7(3), pp. 149-164.

SCHILDHAUS, AARON (2018): *EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices*. In: International Law News, 46(2), pp. 11-14.

SELBST, ANDREW D. / POWLES JULIA (2017): *Meaningful information and the right to explanation*, In: International Data Privacy Law, 7(4), pp. 233-242.

SHAH, AASHAKA / BANAKAR, VINAY / SHASTRI, SUPREETH / WASSERMAN, MELISSA / CHIDAMBARAM, VIJAY (2019): *Analyzing the Impact of GDPR on Storage Systems*. In: ArXiv, online source: https://arxiv.org/pdf/1903.04880, last access: 09/20/2019.

SUPREETH, SHASTRI / WASSERMAN, MELISSA / CHIDAM-BARAM, VIJAY (2019): *The Seven Sins of Personal-Data Processing Systems under GDPR*. In: ArXiv, online source: https://arxiv.org/pdf/1903.09305, last access: 09/20/2019.

WACHTER, SANDRA / MITTELSTADT, BRENT / FLORIDI, LU-CIANO (2017): *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. In: International Data Privacy Law, 7(2), pp. 76-99.

WONG, BENJAMIN (2019): *Delimiting the concept of personal data after the GDPR*. In: Legal Studies, 39(3), 517-532.

ZARSKY, TAL (2017): *Incompatible: The GDPR in the Age of Big Data*. In: Seton Hall Law Review, 47(4/2017), pp. 995-1020.

Laws

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU). In: BGBl. I 2017, p. 2097.

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. In: JORF n°0141, 06/21/2018.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data. In: Official Journal, L119, p. 1.

The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA").

Decisions

BVerfG, Urt. v. 13.4.1983 – 1BvR 209/83, 1 BvR 269/83 – *Volkszählung*, NJW 1983, 1307.

Case 131/12 *Google Spain SL, Google Inc. v AEPD and Mario Costeja González* (2014), ECR I-000.

Case 362/14 *Maximillian Schrems v Data Protection* (2015), ECLI: EU:C:2015:627.

Case 507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (2019), ECLI :EU :C :2019 :772

* * *

About the Author

DR. THOMAS SCHÜRRLE

Dr. Thomas Schürrle, LL.M. (Michigan) is a lecturer at the Institute for Law and Finance at the Johann Wolfgang Goethe University in Frankfurt and Managing Partner of the Frankfurt office of Debevoise & Plimpton LLP.

He graduated and received his PhD in Law from Ruprecht-Karls University in Heidelberg and earned an LL.M. degree from the University of Michigan Law School.

Since 1985 Dr. Schürrle is admitted as Rechtsanwalt in Germany and as a member of the New York State Bar since 1988.

Dr. Schürrle led several international corporate defense cases and related investigations. He has significant experience in compliance with regulatory requirements for industrial, trading and banking clients, in particular data protection. Over nearly three decades, he assisted European clients in managing cross-border data transfer issues associated with complex multinational litigation and corporate investigations.

Debevoise & Plimpton

919 Third Avenue
New York, NY 10022
+1 212 909 6000

801 Pennsylvania Avenue N.W.
Washington, D.C. 20004
+1 202 383 8000

65 Gresham Street
London
EC2V 7NQ
+44 20 7786 9000

4 place de l'Opéra
75002 Paris
+33 1 40 73 12 12

Taunustor 1 (TaunusTurm)
60310 Frankfurt am Main
+49 69 2097 5000

Business Center Mokhovaya
Ulitsa Vozdvizhenka, 4/7
Stroyeniye 2
Moscow, 125009
+7 495 956 3858

21/F AIA Central
1 Connaught Road Central
Hong Kong
+852 2160 9800

13/F, Tower 1
Jing'an Kerry Centre
1515 Nanjing Road West
Shanghai 200040
+86 21 5047 1800

Shin Marunouchi Bldg. 11F
1-5-1 Marunouchi, Chiyoda-ku
Tokyo 100-6511
+81 3 4570 6680

www.debevoise.com