Key concepts

Before entering the field, it is helpful for orientation to scope out or recall key concepts and terminology. Acronyms and abbreviations are also summarized at the back of this book.

The field: data protection, privacy and security

The terms 'data privacy' and 'data protection' are often used interchangeably, in particular in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws. Actually, the two terms and legislative concepts have quite different origins and purposes. Here is a simplified overview: 0.14

Data protection: Data protection is about protecting information concerning persons. Immediate focus is not the individual person, but data about a person. By protecting personal data, laws are intended to protect persons (the data subjects) from the effects of automated data processing. When you try to understand or comply with European data protection laws, keep in mind that the default rule is "verboten" (German for: forbidden). Businesses and other organizations are generally prohibited from processing personal data, unless they obtain consent from the data subjects or they find an applicable statutory exemption. European data protection laws are first and foremost intended to restrict and reduce the automated processing of personal data – even if such data is publicly available. My home state, the German State of Hessen, enacted the first data protection law in 1970 due to growing concerns regarding dangers of automated data processing for individual freedoms. Citizens and politicians were concerned that George Orwell's forecast for 1984 could become reality: where 'glass citizens' are observed and controlled by an omniscient 'big brother' – the government. More recently, these concerns were joined by fears regarding 'little brothers,' namely private companies that amass data and databases for commercial purposes, which can then be conveniently (ab)used by governments or criminals. 0.15

Due to these concerns, legislatures decided to regulate automated data processing like other dangerous activities. The Hessian data protection law – and laws of other German states and European countries – established a general prohibition and regulatory regime regarding the processing of personal data. One key feature of European-style data protection laws is a data minimization requirement: companies are prohibited from collecting, using and retaining data, unless they obtain consent or have another compelling reason to process the data. And, companies are required to minimize the amount of data they collect, the instances of processing, the people who have access and the time periods for which they retain data. In practice, many companies in Europe collect and process personal data as much as their competitors in other parts of the world. European data protection laws provide for exemptions and data subjects grant consent to allow this. But, the principal hostility to personal data processing and databases in European data protection laws is important to keep in mind for purposes of understanding and applying European data protection laws. And, this hostility is probably one reason why that European companies do not lead in information-driven economy sectors such as electronic commerce, cloud computing, software-as-a-service and social networking, where much of the innovation and market leaders come from the United States and increasingly also Asia.

0.16 *Data privacy:* The United States and other countries outside of Europe, by contrast, generally allow data processing. Data privacy laws are primarily intended to protect individuals from intrusion into seclusion and interception of confidential communications. Given this focus, individuals are usually not protected, unless they have a reasonable expectation of privacy in a particular situation. Companies can – and frequently do – destroy such expectations of privacy by notifying individuals of the companies' data collection and processing activities, for example, in employee handbooks, website privacy statements and in-store warnings about security cameras. Individuals receive some protection in the sanctity of their homes, but communications and activities outside the home receive little or no protection, *e.g.*, information in public records, assembling in the open, calls on cell phones in public, postings on the Internet or via social networking platforms, etc. Instead of enacting one comprehensive data protection law, the United States has enacted numerous sector- and threat-specific laws on the Federal and State level to address specific concerns narrowly and without too much collateral damage to freedom of information and technological progress.

Data security: More recently, legislatures around the world have started to supplement data privacy laws with sectoral data security laws. These laws aim to protect individuals from specific harm resulting from unauthorized access to personal information, in particular identity theft (*e.g.*, criminals using someone's personal data to acquire or charge credit cards). Examples include data security breach notification laws (California passed the first law in 2003, with most U.S. states and many countries following suit thereafter), detailed prescriptions regarding technical and organizational measures to protect health information in HIPAA and U.S. state laws in California, Massachusetts, Nevada and New York requiring encryption of certain data in certain circumstances. 0.17

Data privacy as umbrella term: In line with common language usage and in the interest of simplicity, this Field Guide will use the term 'data privacy' collectively for data protection, data privacy and data security, except where differentiation matters. 0.18

The territory: Europe, U.S. and ROW

Most companies are dealing with data privacy issues in more than one jurisdiction, given the global nature of the world economy. But while businesses have to solve global problems, the laws they have to comply with remain territorial. On the Internet, companies can reach more than 190 countries instantaneously – and each country has its own laws. In the United States alone, you are dealing with laws made by 50 states plus federal laws enacted by the U.S. Congress. In Europe, you will find some harmonization due to the EC Data Protection Directive of 1995, which has been implemented in the 31 member states of the European Economic Area (EEA) and closely followed by Argentina, Colombia, Israel, Switzerland, Russia, Uruguay and some candidates for EU membership. 0.19

In May 2018, the new EU General Data Protection Regulation (GDPR) will enter into effect in all EEA Member States with direct and immediate effect on companies within the EEA. Many companies outside the EEA will also be subject to the GDPR, if, for example, they collect personal data via online services from consumers in the EEA or via an establishment in the EEA. The GDPR is the first significant update of EU data protection laws since 1995, provides for draconian fines, and brings many major changes for companies, including the following: 0.20

- Companies must document all data processing activities and compliance efforts to demonstrate how they comply with data protection laws; they must conduct impact assessments for high risk activities and prepare records describing all data processing and compliance measures, including categories of data and data subjects, purposes of processing, recipients, international transfers and suitable safeguards, time limits for erasure, technical and organizational security measures (Art. 30, 35)

- Companies must designate a data protection officer for each of their establishments, subject to exemptions for small and low risk presences and an option that one data protection officer can watch over several companies and offices so long as she is accessible and accountable for each establishment

- Companies outside the EEA must designate a representative within the EEA

- Companies must implement robust data retention and deletion programs to comply with more stringent rules regarding data access, rectification and erasure

- Companies must provide more detailed privacy notices to data subjects, disclosing identity and contact details of the data controller (and representative in the EEA for foreign companies); contact details of the data protection officer; purposes of data processing; legal basis for processing; legitimate interests pursued by the controller or a third party, if that is the basis for justifying the processing; recipients or categories of recipients; in case of international data transfers, the existence or absence of an adequacy decision by the Commission and information on safeguards, including the means by which to obtain a copy of them; and many other details. At the same time, companies are required to present this information in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Art. 12, 13)

- Companies must establish processes to ensure that they can report data security breaches within 72 hours to data protection authorities and data subjects

Besides the GDPR, companies will have to continue complying with national data protection laws. Unlike the Data Protection Directive of

1995, the GDPR applies directly to companies and does not have to be implemented into national law. But, national laws can provide for additional or stricter rules in some respects and will remain effective until affirmatively revoked.

The GDPR is intended to create even greater harmonization in European data protection laws than the Data Protection Directive and it has the potential to achieve this if EEA Member States withdraw their existing national laws in favor of the new GDPR. It is not unlikely, however, that some EEA Member States will keep existing laws around and thus create uncertainties regarding the degree of preemption and harmonization. Another factor adding uncertainty in Europe is the UK's exit from the EU, which could result in the introduction of different privacy laws in one of the most important jurisdictions in Europe by the size of its population and economy.

Given the level of harmonization in Europe, this Field Guide can occasionally refer to general principles of 'European laws'; but this should not obscure the fact that companies have to comply with each individual European country's laws, when applicable, in addition to the GDPR, and possibly also additional laws of states, provinces and other subsections within a European country.

This Field Guide is intended to provide you with guidance for all territories and help you identify globally recurring themes and pitfalls to watch out for. For illustrative purposes, you will see examples mostly from Europe and the United States. Europe and the U.S. have had data privacy laws, litigation and regulatory proceedings for the longest time and so they are the most charted territories with respect to many issues. Also, Europe and the U.S. lend themselves well to illustrations because they are frequently on the opposing end of the spectrum of regulatory approaches: Europe tends to be more protective/paternalistic with respect to individuals and leans towards imposing heavy regulatory burdens on companies, including requirements to obtain prior approvals, submit filings and comply with various formal requirements. The United States on the other hand has consciously passed on European-style omnibus data protection legislation and instead enacted sector-specific, narrowly framed laws, providing for a private right of action, in response to concrete threats to particular aspects of individual privacy. Once you have familiarized yourself with the U.S. and European position on a particular question, you can often navigate other countries (charmingly referred to as "ROW" for "Rest Of World") by grouping 0.21

them closer to the U.S. or European position. This is particularly effective when you have to implement global systems or processes and your organization or technology can accommodate only a limited number of options.

Please keep in mind that you are looking at approximation and high-level themes when the Field Guide refers to European or U.S. laws for orientation purposes. Some states within and outside the U.S. and EEA have different laws or interpretations of laws, many countries do not have any specific laws yet and there is little harmonization in other continents and regions (*e.g.*, Asia-Pac, Latin America, Middle East and Africa).

The species: personal data, PII and sensitive data

0.22 When you encounter terms like 'personal data' and 'personally identifiable information' in laws or contracts, you must check the applicable definitions to determine the impact of a particular provision. When you draft a website privacy statement, notice or contract clause, you can either assume a very broad range of application or include an express, limiting definition yourself.

0.23 *Personal data:* For the purposes of European data protection laws, personal data is any information that relates to an identifiable human individual. For example, a person's name, photo, address or birth date would be considered 'personal data.' It is not necessary that the data by itself allows identification of the data subject. It is sufficient that the data relates in a meaningful manner to an individual person who could be identified.

0.24 For example, a company phone number that can be answered by a number of persons does not constitute 'personal data,' but an individual extension that is permanently allocated to an individual person does. Also, a general company phone number can become part of 'personal data' in combination with other information, such as the time of a particular call whose participants can be determined. An Internet Protocol (IP) address of a router or other device can constitute personal data if it relates to an individual user (*e.g.*, single person household). But, an IP address does not constitute personal data if it relates to a large business without a reasonable connection to an individual person. The question whether IP addresses and phone numbers

constitute personal data has been hotly debated for years by academics and even legal practitioners, but if you take a close look, it often does not matter to a company: If some of the data that your company processes can be linked to an individual, then you have to either treat all of the data as personal data or differentiate and separate. But, differentiation is usually impractical or too expensive to implement. For example, if you implement cookie technology to analyze website visitor conduct and you log IP addresses in the process, you will inevitably gather some IP addresses that can be linked to an individual and for compliance purposes, it does not matter whether the large majority of IP addresses could be excluded from the scope of data privacy laws.

Data can cease to qualify as 'personal data' if it is redacted or aggregated 0.25
in a manner that destroys the connection to an individual. Encryption and partial redaction do not do the trick, as long as someone holds the key and could re-identify the data subject. Thus, for the most part, you still have to treat encrypted data as 'personal data' under data protection laws. On the other hand, true aggregation can remove data from the scope of data protection laws. For example, if you take information on video rental habits of a thousand randomly selected individuals, and you merge the information to create statistical information about less than all one thousand individuals, the resulting aggregate data (*e.g.*, 20% of video renters watch less than 20 hours a month) is no longer 'personal data' (while the raw data on individual habits continues to be personal data). Theoretically, you could also redact data relating to an individual by removing names and all identifiers from a profile. But, this is harder than one would think in practice. If the redacted data sets retain any information that allows the reversal of the redaction process (*e.g.*, an address, birth date/place, etc.), then the data will typically continue to qualify as 'personal data' under European data protection laws. Reversible redaction is also referred to as "pseudonymization." It does not remove data from the scope of European data protection laws, but is recognized as a legitimate data security measure and an effort to protect the privacy of the individual.

PII – Personally identifiable information: In stark contrast to the broad 0.26
concept of 'personal data' under European laws, many other countries use slightly different terms and define them much more narrowly. For example, the California Civil Code uses the term 'personally identifiable information' in many statutory sections and defines the term narrowly and differently each time, depending on each section's context and purpose. Other California laws, as well as federal law and the laws

of other states, use different definitions. Often only particularly sensitive types of information are covered (*e.g.*, credit card numbers, social security numbers, etc.).

0.27 *Sensitive data:* Most jurisdictions and laws apply higher standards to certain categories of personal data. Reasons and covered categories vary from jurisdiction to jurisdiction. For example, laws in the United States protect social security numbers and credit card information in particular because consumers are exposed to high identity theft risks due to relatively lax authentication procedures by banks and merchants. Identity theft is less of a concern in Europe, but under European laws, companies generally have to observe special restrictions regarding personal information relating to:

- political opinions,
- trade union membership,
- medical or health conditions (*e.g.*, employee sick days, prescriptions, clinical trial data – even if stored by impersonal IDs without patient names),
- racial or ethnic origin (*e.g.*, place of birth, photos showing skin color),
- religious or philosophical beliefs (*e.g.*, German church tax status in payroll systems),
- information relating to sexual orientation (*e.g.*, marital status in jurisdictions that do not recognize same sex marriages), and
- certain types of criminal records.

0.28 Some limited exceptions apply in Europe, particularly for collection and local processing of sensitive data by employers as required by law. Companies need to obtain express consent, however, before transferring any sensitive data outside the European Economic Area (see Chapter 2).

0.29 International conflicts between national laws are possible. For example, a company might be required to produce certain sensitive data in U.S. litigation or government investigations, which the company is

prohibited from sharing under European laws. But, upon closer review, you can avoid many apparent conflicts. For example, U.S. export control compliance programs can require collection of certain information on citizenship and residency of foreign workers with access to controlled U.S. technology, but information on racial or ethnic origin (which would constitute 'sensitive personal data' under European laws) is usually not required.

Laws in the United States and other jurisdictions also differentiate between various categories of personal data with respect to particular scenarios. There are hardly any common themes beyond what common sense would suggest, so companies must survey their data collection practices in each relevant jurisdiction separately. 0.30

Activities encountered: transfers and other forms of processing

European data protection laws regulate any processing of personal data and define the term 'processing' very broadly to include any activity relating to personal data. Processing includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure and destruction, whether by manual or automated means. Even as you are redacting personal data – making it anonymous – you are processing the personal data under European laws and you trigger the same general prohibitions and data minimization requirements. 0.31

Under U.S. and other countries' laws, however, data privacy laws tend to pertain to particular activities. In most jurisdictions, people and data privacy laws tend to be particularly sensitive with respect to one form of processing: data transfers. A transfer occurs when one company sends data to another company or country via email, mail or otherwise, but also if someone in the other company or country can remotely access data via the Internet or other technologies. Thus, if a company posts an employee directory for all employees worldwide to access, that constitutes a data transfer to all jurisdictions where such data is available. If you post information on the Internet, you transfer such information everywhere. Therefore, a 'transfer' in the broadest sense of the word occurs every time you allow someone else to access data – regardless of the technical means or commercial context. 0.32

0.33 Conceptually, however, an important distinction applies with respect to transfers within an organization and its circle of service providers (*i.e.*, data processors, which often include the parent company providing IT infrastructure-as-a-service as well as unaffiliated providers of payroll processing, Internet access and physical security services). Companies do not typically have to explain details regarding data sharing with data processors in privacy notices or government filings and data subjects typically do not have a choice in this respect. To be on the safe side, you should draw the net wide and consider restrictions under data privacy laws each time you make data available to someone else. But, you should also keep in mind that transfers to mere data processors are often less restricted than transfers to data controllers, *i.e.*, those who use data for their own purposes. The rationale for this is that what matters to the data subject is that the company he or she entrusts with personal data stays responsible and that any individuals who act for this company comply with all of the company's privacy promises and applicable law – regardless of the employment status of such individuals. Companies are legal fictions that do not themselves act except through employees, individual independent contractors and employees of corporate service providers. Which individuals a company chooses to process personal data – its own employees, individual independent contractors, employees of corporate contractors or subcontractors – does not usually affect the data subject's privacy interests. Therefore, companies are usually permitted to share personal data with individual and corporate service providers (*i.e.*, data processors) without notice to or consent from data subjects, so long as they execute a written data processing agreement that clearly documents the limited discretion of the service provider regarding data usage.

The observed: data controllers, processors

0.34 European data protection laws differentiate between 'data controllers' – who use data for their own purposes and at their own discretion – and 'data processors' – who process data only on behalf of a data controller as a service provider. Data controllers are the ones who are primarily obligated to comply with data protection and privacy laws. Data processors are obligated to comply with instructions from the data controller, keep data secure and refrain from using data for any purposes other than as instructed by the data controller. Data processors are also referred to as 'agents' or service providers in many laws and privacy statements. A company can qualify as data controller with respect to some activities (*e.g.*, processing of employee and customer relationship

information) and as a data processor with respect to other activities (*e.g.*, assisting its subsidiaries with payroll processing and customers with respect to computer maintenance).

Service providers that gain physical custody and technical access, but that are not allowed or expected ever to access data under any circumstances, refer to themselves as 'data handlers' or 'mere conduits' in order to excuse themselves from any direct obligations under data privacy laws. Some types of providers have a compelling case, for example telecommunications companies that are not allowed or expected to know whether their systems are used to communicate health or other information. Also, colocation providers (companies that rent secure cages to companies to host servers) and more traditional landlords usually have some physical access rights to computer systems, but very limited or no rights to access data (sometimes in the context of disaster recovery or Internet access and troubleshooting arrangements). Legislatures rarely acknowledge exemptions from data privacy laws for data handlers or mere conduits. Customers tend to insist on commitments from their service providers just in case these qualify as data processors, business associates or the like, in order to protect themselves from challenges regarding their own data privacy compliance efforts. 0.35

The game wardens: data protection authorities, officers

European countries have established independent public authorities responsible for enforcing national data protection laws. Their representatives formed an EU-wide institution that was called "Article 29 Working Party" under Art. 29 of the Data Protection Directive of 1995 and is called "European Data Protection Board" according to Art. 68 of the EU General Data Protection Regulation. This institution has been issuing guidance to companies and legislatures and publicizing views of national data protection authorities. Such guidelines and views are quite relevant to companies, given that the data protection authorities are tasked with enforcing data privacy laws against companies. In many European countries and some non-European countries, companies have to notify the local data protection authority before they start processing personal data. In some countries, companies have to obtain prior approval from the data protection authorities before they engage in certain kinds of data processing activities, *e.g.*, international transfers of personal data outside the EEA. 0.36

0.37 In most European jurisdictions and a few other jurisdictions, companies must (or may, as an alternative to notifying data protection authorities) appoint a data protection officer, either an employee or external service provider, who is tasked with monitoring whether the company complies with applicable data protection laws. Such data protection officers are not government officials, but they are required to cooperate with the local data protection authority and report serious offenses. Similarly, government agencies in Europe and elsewhere (including the NSA since February 2014) have appointed data protection officers whose task is to monitor the particular government agency's own compliance efforts. Whether in government agencies or private sector organizations – the role of the data protection officer is focused inwards to monitor compliance by their own organizations. This distinguishes data protection officers from data protection authorities whose task is to monitor compliance by other organizations.

0.38 In the United States and other countries that have not established data protection authorities, data privacy laws are enforced by consumer protection agencies (*e.g.*, the U.S. Federal Trade Commission) and general law enforcement authorities (including State Attorneys General), but prior notifications or approvals regarding automated data processing is not typically required outside Europe.