1 Starting a compliance program

When you set out to design and implement a data privacy compliance program, you face a number of threshold decisions and preparatory tasks, including the following: 1.01

- Putting a person or team in charge of data privacy law compliance
- Preparing a task list by identifying relevant facts, laws and requirements
- Defining priorities based on business objectives, enforcement risk exposure, and ease of compliance
- Executing the task list
- Working with internal stakeholders and outside advisors

Taking charge

Someone needs to be in charge. If your business is a one-person sole proprietorship, then you are in charge. In larger organizations, there are typically a number of individual candidates or departments that could take charge of data privacy compliance, including lawyers, information technology staff, human resources and internal audit personnel. Each of these groups tend to have different approaches, strengths and limitations. Here are some factors to consider as you look for the right person or team: 1.02

In-house attorneys in corporate legal departments usually take an advisory role and inform others in the organization what applicable laws require, including data privacy laws. Depending on company culture and individual styles, the legal department may advise proactively or upon request. Lawyers are trained to interpret and 1.03

apply laws, including data privacy laws, but not all lawyers are technology-savvy or good project managers.

1.04 Members of the information technology (IT) department are technology savvy, but may not find it easy to understand and apply laws. IT professionals are trained in deploying and maintaining equipment, software and services that other groups (human resources, sales, marketing, production, etc.) use to process personal data. The IT department supports these other groups and provides technology that aids other departments' business objectives. The IT department usually establishes and implements protocols to protect personal data from unauthorized access (by deploying data security measures), but does not typically decide on access privileges for individuals or legal compliance matters.

1.05 Some companies have separate internal audit functions, which are concerned with monitoring and enforcing compliance with laws and internal policies. Such audit departments are focused on verifying that the rule of law or existing compliance programs is adhered to, but audit personnel do not typically define the rules. You lose an extra pair of eyes if you have the same person create and audit a program. Also, when audit personnel conduct investigations, they are at a particularly high risk of violating data privacy laws. Investigators often want to search email boxes, computers and files, interview third parties about suspicious conduct and occasionally intercept live calls and other communications without prior notice to the data subject. Therefore, some companies feel that they would be letting the fox guard the henhouse if they tasked audit staff with designing a privacy compliance program.

1.06 Another option is to select individuals from data user groups within a company, such as human resources or marketing. Companies that develop or sell information technology products consider data privacy not only a compliance challenge, but also a business opportunity. For example, cloud computing service providers and enterprise software and data storage providers increasingly consider data privacy laws in the product development process to ensure that their customers can effectively use the products in compliance with applicable laws (see 'Privacy by design' in Chapter 5). Whether privacy protections are a relevant differentiator for technology providers depends much on the target audience – larger enterprise customers tend to be very focused on compliance features;

whereas consumers and smaller companies may be concerned about some features (*e.g.*, end-to-end encryption for smartphones and online storage) but choose "free" services or convenience over data privacy considerations in other scenarios.

In most larger businesses, the person in charge of data privacy compliance usually comes from any of the above departments or areas of specialization. Larger companies with a great exposure or interest relating to privacy laws may decide to create a new department or office. Smaller companies may find it sufficient to put someone in charge on a part-time basis. If a company has a legal department, attorneys are usually involved in data privacy compliance. Often, legal counsel takes the lead regarding data privacy compliance. But, the ideal candidate for project management does not necessarily have to be a lawyer, particularly if a company views data privacy more as a business opportunity than a mere legal obligation. 1.07

Working with internal stakeholders and outside advisors

Internal stakeholders. To obtain sufficient resources and support from stakeholders within a company, you have to answer the 'Why' question – Why is a data privacy and security program important? For some companies, compliance is a matter of risk management and avoidance of sanctions and liability. Others care additionally about potential reputational risks and opportunities and view privacy compliance as a differentiator. Also, for some companies, data privacy and security compliance is a key condition to selling products and services, for example with data storage or software-as-a-service providers. When you start out implementing a compliance program in a company, it can be very helpful to prepare a brief whitepaper in FAQ format to raise awareness and gain support among key stakeholders within the organization. Additional thoughts regarding the big 'why?'-question can be found in Chapter 5 of this Field Guide, under "Y." 1.08

Outside advisors. Most companies turn to outside counsel for advice on legal requirements beyond their home jurisdiction. Typically, it is too difficult and time-consuming to determine the exact nature and details of formal and substantive compliance obligations in other countries, where laws may be presented in unfamiliar formats and languages. In 1.09

this Field Guide, you will find some pointers on generally applicable privacy law principles and major jurisdictional differences; however, coverage of country-specific details on formal or substantive compliance obligations is outside the scope of this book.

1.10 Many companies experience one particular challenge when working with outside advisors on compliance matters: every subject matter expert (data security consultant, technology vendor, local lawyer in a particular jurisdiction, etc.) is familiar with the risks and possible sanctions in his or her area of expertise and takes these particularly seriously. But, companies tend to have a limited budget and cannot always address all requirements at once and with the same rigor and effort. Companies generally need to prioritize. If you hire coordinated global teams, they may be able to assist with prioritization between the disciplines they are engaged to cover, but even their abilities are limited and they cannot be expected to take all fundamental considerations into account that can make or break a company, *e.g.*, how to ensure operational continuity, sufficient revenue growth and funding, etc. If you hire individual advisors rather than a coordinated team, such individuals are usually not of much help with respect to prioritization and there is a significant risk that the importance of a particular risk or local law requirement is over- or understated in context. Therefore, it can be helpful to ask outside advisors not only about substantive and formal requirements, but also about practical issues, such as whether particular requirements are observed in practice or only honored in breach, whether challenges by regulatory or private plaintiffs are common and what risks and problems other companies have run into in connection with the particular requirement at issue. Answers to such questions could help put things into perspective and help companies prioritize among tasks.

Appointing a privacy officer

1.11 Persons who take charge of designing and implementing data privacy compliance programs sometimes hold the title 'Data Protection Officer' or 'Chief Privacy Officer.' The roles associated with these and similar titles can actually be quite different in nature and you should consider carefully whether your company needs one or the other or both.

1.12 One key reason why multinational businesses have a data protection officer is because they have a presence in Germany. Most multinational businesses consider Germany an important market. Under German

data protection law, companies have been legally required since the 1970s to formally appoint a data protection officer with a watchdog role to supplement supervision by governmental data protection authorities. Germany was the first country to introduce the concept of a data protection officer in an attempt to force self-regulation via a company-appointed guardian of privacy interests.

Some jurisdictions with early data protection laws, including France, opted instead for government notification and approval requirements. Others such as the Netherlands, Norway, Sweden and Switzerland, adopted a middle ground approach These countries give companies the option to appoint a data protection officer in lieu of submitting more substantive filings to data protection authorities. According to the EU General Data Protection Regulation, companies in all EEA Member States must appoint a data protection officer if they engage in particularly sensitive forms of data processing, including systematic monitoring of data subjects or processing of special categories of personal data on a large scale and as a core activity. Affiliated groups of companies can appoint one person as data protection officer for several or all entities if the person is accessible from all locations.

1.13 Some companies model their compliance approach for all jurisdictions where they decide to appoint a local data protection officer after the German rules. This should ensure compliance with the EU General Data Protection Regulation and other countries' rules (as the German requirements tend to be the strictest and most comprehensive), but this is not legally required.

1.14 Many companies also voluntarily appoint data protection officers or privacy compliance liaisons for countries where this is neither required nor incentivized, or even contemplated. In addition, many larger U.S. companies have a Chief Privacy Officer, often as well as compliance officers, internal auditors, specialized legal counsel for data privacy law compliance matters, information security officers and trained privacy professionals. Upon closer review, the purposes, roles and responsibilities of such positions can and often should be quite different. As a reference point in your decision-making process, you could consider the German model for the data protection officer role, or the guidance issued by the Article 29 Working Party around Data Protection Officers and the EU General Data Protection Regulation, and carefully decide which aspects to adopt and not adopt for other specific jurisdictions or a global function.

1.15 *Requirement to appoint a data protection officer under German law.* Under German law, companies typically have to appoint a data protection officer in writing within one month of commencing business. Some exceptions apply, for example, for companies that do not process any sensitive data and have fewer than ten employees.

1.16 • *Qualification requirements.* Candidates must be experienced, knowledgeable or trained regarding data protection legislation, information technology and the company's operations. They must also be reliable and not have conflicts of interests (which typically rules out the appointment of business owners, senior managers and employees with a strong interest in data collection and usage, such as marketing and HR managers). Finally, the company has to enable the data protection officer to perform the statutory obligations; this requires companies to provide information and training and to release internal data protection officers from other work duties (to free up time). Many companies appoint non-managerial employees in their legal, information technology or human resources departments – or contract with external service providers.

1.17 • *External vs. internal candidates.* A company can either appoint an employee or an external service provider. Both options have certain advantages and disadvantages. If a German company appoints an employee, she becomes entitled to even stronger protections against termination than German labor laws afford to all employees. Terminating an external data protection officer tends to be relatively easy by comparison, based on the terms of the applicable services contract. Appointing an employee allows the company to keep all relevant information internal and confidential. Appointing an external candidate means opening the company's systems, processes, security measures and data to someone on the outside. An internal data protection officer tends to be more familiar with actual practices, processes and problems and has better access to information about employee concerns and security weaknesses. External data protection officers may have a better feel for industry standards and more experience and expertise than internal employees who take on the position on a part-time basis. Specialization allows an external data protection officer to focus on the latest developments in data protection law and information technology. Companies also consider the costs and response times: External service providers can be paid on an hourly basis (which can incentivize the data protection officer to be particularly active

and responsive to inquiries and make it difficult for the company to control costs) or with a monthly or annual fixed fee (which occasionally results in lengthy response times and thus delays in project implementations where prior consultations with the data protection officer have to be completed). With respect to internal data protection officers, the company has to consider the impact on the candidate's other contributions in light of the time the role as data protection officer will take up.

- A multinational business could appoint as data protection officer for a German subsidiary an employee of one of its entities outside of Germany or from a different German subsidiary, if it maintains several entities in Germany. Such person could be qualified as an "external" data protection officer for German law purposes to avoid the implications of German labor laws. Some German data protection authorities are skeptical about the appointment of persons who reside outside of Germany and may argue that such persons are not able to adequately perform their statutory obligations. However, German statutory law does not strictly require the appointment of an employee in Germany and companies with headquarters and data centers outside of Germany have good reasons to appoint someone outside of Germany if the person is closer to the companies' regional or global systems. Multinational companies may prefer to have only one person in the role of data protection officer for any jurisdictions where the appointment is required, so that consultations on multinational projects can be conducted efficiently, quickly and without the risk of conflicting opinions and requests. In jurisdictions where the appointment has to be notified to data protection authorities, companies have to be prepared to answer questions and handle resistance to the appointment of a data protection officer who does not reside in the respective country. But, in most cases it is possible to overcome the authorities' hesitations if the company has good operational reasons. The EU General Data Protection Regulation expressly allows groups of affiliated companies to appoint one single data protection officer provided that the data protection officer is easily accessible in every company and office. 1.18

- *Appointment formalities.* Under German law, companies have to appoint data protection officers in writing. Under the EU General Data Protection Regulation, companies have to provide the data protection authority and publish contact details for the data protection 1.19

officer, for example, a dedicated phone number and email address. Companies generally prefer to assign and publish aliases (*e.g.*, data-protectionofficer@company.com) to avoid a need to update privacy notices whenever a data protection officer is replaced. Companies may impose a time-limit on the appointment, so long as the term is not so short that it interferes with the independence of the position. Two to five years seem reasonable. In German companies that have a works council (collective labor representation), the works council has a co-determination right regarding changes to the employment contract that are involved in appointing an employee as internal data protection officer.

1.20 • *Duties*. A data protection officer is responsible for monitoring the company's compliance with applicable data protection law and ensuring that it documents its data processing activities. Companies have to consult with the data protection officer regarding their data processing activities and any contemplated changes. The data protection officer shall make recommendations and raise awareness and concerns where appropriate, but does not have to formally approve measures. If the company does not act despite being formally notified of concerns, the data protection officer has the right – and in some cases the obligation – to blow the whistle and notify data protection authorities. The data protection officer operates independently, and is not subject to orders or instructions from management. Day-to-day duties can include assistance with documenting data processing procedures in a register; evaluating and further developing data protection and security policies; suggesting, selecting and implementing technical security measures; drafting forms and contracts appropriate for data protection; selecting employees, service providers and others to be involved in the processing of personal data; monitoring data privacy and security measures and the proper use of data processing programs; handling complaints relating to data protection and violations of law or policies; employee training; and preparing, submitting and maintaining notifications to data protection authorities.

1.21 • *Personal liability*. If you pick an employee as a candidate for data protection officer, you can expect a question regarding personal liability. The short answer is that all employees can be held liable for misconduct and violations of laws and third-party rights. Most candidates, however, are probably as much or more at risk with respect to their other job duties than with respect to the role of

data protection officer. German data protection legislation does not specifically address the personal liability of a data protection officer. Under generally applicable laws, any individual representative of a company can be held accountable for acts or omission of the company if he or she committed the act at issue or had responsibility to avoid the omission. On this basis, a data protection officer can be held accountable for direct involvement in illegal data processing activities (*e.g.*, recording of phone calls without consent or court order). Theoretically, a data protection officer could also be liable for failure to stop illegal activities that were conducted without his or her direct involvement. But, it is relatively rare that employees are charged because of a failure to act.

Mandatory or beneficial appointments in other jurisdictions. If you appoint a data protection officer in accordance with German law also for other countries, you typically satisfy the requirements of the EU General Data Protection Regulation and laws of other jurisdictions that define such a role by national statute, such as France, the Netherlands, Norway, Sweden and Switzerland, except that you may have to notify local authorities of the appointment. Companies tend not to formally appoint data protection officers where local law does not offer any meaningful corresponding exemptions from other requirements. For example, French national law provides for rights and duties of a data protection officer, but does not require or significantly reward the appointment by multinationals. Thus, most companies opt against a formal appointment in France. But, companies operating in the Netherlands, Norway, Sweden, Switzerland and other jurisdictions that reward the appointment by dispensing with other filing requirements tend to opt for the appointment of a data protection officer. Some companies appoint the same person for several or all jurisdictions where a formal appointment is required. This is expressly permitted under the EU General Data Protection Regulation and particularly efficient for companies that use global systems and procedures, which can be monitored best by one person. 1.22

Voluntary, informal appointments. Separate and apart from satisfying formal statutory requirements to appoint a data protection officer, larger organizations especially see operational advantages in establishing a network of local liaisons for data privacy compliance and other compliance efforts in order to have specialized local contacts who can help implement and monitor these legal programs. Also, many companies voluntarily appoint a "global privacy officer" or "Chief Privacy Officer" to demonstrate internally and externally that the company 1.23

takes data privacy compliance seriously. It may also be beneficial to have one point person who takes ownership and responsibility for this topic – which affects many other functions, including IT, HR, physical security, law, finance, and sales.

1.24 For such informal and voluntary appointments and for jurisdictions where the role of data protection officer is not defined by statute (for example, in the United States, except under the federal health data protection law, HIPAA), it is important that the company defines the authority and duties of the privacy officer in a detailed written memo or agreement. In particular, companies need to define expectations as to whether the privacy officer shall advocate primarily for privacy or company interests; provide advice or make decisions; react or be proactive. Similarly, shall the privacy officer coordinate, support, supervise or monitor colleagues in roles with overlapping responsibilities (such as compliance officers, internal auditors, privacy counsel in the legal department and information technology and security staff in the IT, marketing and HR departments)? Companies have to decide and document what the objectives and expectations are: should the Chief Privacy Officer be a coordinator, advocate, advisor and/or guardian of privacy or the company's interests in data and compliance? Each company should find its own way in this respect, and each company should define responsibilities and tasks clearly in writing, so that the appointed individual understands the rights, obligations and expectations of the role. When roles are not clearly defined, a misalignment of expectations could easily result in uncomfortable conflicts. For example, if a global privacy officer at a U.S. company understands her role as independent and public policy-driven as a German data protection officer, she might be quick to notify U.S. authorities of concerns. Or, if a member of the legal department is appointed as 'Chief Privacy Officer' and shifts his approach from acting as legal counsel towards a more executive role, this might undermine attorney-client privilege in certain situations. Companies should consider these and other pros and cons before making voluntary appointments, and then document the role in a detail to increase the chances of achieving the desired benefits and reduce the risk of unwanted consequences and conflicts.

1.25 • Determine where you have to appoint a data protection officer under local law and to satisfy legal requirements (consider internal vs. external, in-country vs. regional or global appointments).

- Determine how your company can best achieve and maintain compliance in jurisdictions where you are not legally required to appoint a data protection officer, and whether your company would benefit from the voluntary appointment of a Chief Privacy Officer and local liaisons; if yes, carefully document the job description, authority and duties, and consider relations to similar or overlapping functions, such as corporate legal counsel, information security, human resources and marketing managers. 1.26

Preparing a task list

Once you have put someone in charge, it is time to prepare a list of tasks and keep track of implementation status and priorities. Creating and monitoring such lists helps prioritization, planning (budgets, achievements), management of complex situations (*e.g.*, involving several jurisdictions and different types of databases) and transitioning projects from one employee to another. On a task list, you can keep tabs on formal compliance requirements (*e.g.*, notices, filings, appointment of privacy officer, data transfer agreements) and substantive tasks (*e.g.*, implement access controls, deploy encryption technologies, replace vendors, etc.). 1.27

For example, a U.S. company that has incorporated a few foreign subsidiaries may have the following items on its initial task list – perhaps supplemented by columns for status, action items and business owners: 1.28

	Data privacy law compliance task	Purpose
1.	Designate role and prepare appointment documentation for global data privacy officer; appoint local data protection officers where required, *e.g.,* for German subsidiary	Manage risks, satisfy compliance obligations
2.	Assess where government filings (notifications, application for approvals) are required, prepare and submit	Satisfy local compliance obligations
3.	Take inventory of databases and data flows	Compile facts for notices, agreements, filings; satisfy record keeping requirements
4.	Prepare and implement intra-group data transfer agreements based on EU Standard Contractual Clauses and/or other measures to legitimize international data transfers (including EU-U.S. Privacy Shield registration, Binding Corporate Rules, Cross-Border Privacy Rules and Codes of Conduct)	Overcome legal instructions on international data transfers

	Data privacy law compliance task	Purpose
5.	Review, revise and/or translate privacy policies and notices directed at consumers and individual representatives of corporate customers and business partners; determine how best to obtain and document consent	Satisfy notice requirements
6.	Review or prepare notices directed at employees with respect to processing of employee data, including: ● Global human resources information system (HRIS) ● Monitoring tools *(e.g.,* anti-spam, anti-virus, web surfing protection, data loss prevention, firewalls) and investigations ● Whistleblower hotline ● Payroll, benefits, stock options	Satisfy notice requirements
7.	Review or prepare standard templates for data sharing/ processing in agreements with business partners such as vendors, customers, intermediaries (resellers, sales reps for advertising services) ● Template data transfer contracts (intra-group and third party) and/or intra-group policy(ies) ● Review/prepare data processor contracts and policies	Satisfy data security obligations, protect data as an asset, mitigate against risks from unauthorized disclosure/ hacks, etc.
8.	Review or develop internal protocols and processes regarding access to data, data retention, information security, incident response and response to disclosure requests from law enforcement, regulators, private litigants, etc.	Satisfy compliance obligations; protect consumer/employee privacy
9.	Direct Marketing: Implement global or jurisdiction-specific protocols for opt-in/opt-out processes	Satisfy local compliance obligations
10.	Routine training, audits	Manage risks, satisfy compliance obligations

1.29 To define tasks for your company, you have to determine what data you have, what laws apply, what the laws require and how your company can best satisfy the requirements (where the law gives you options or if resource limitations force prioritization). You could prepare a task list for your company as you read through the remainder of the Field Guide, where typical requirements and tasks are introduced.

1.30 Finding and analyzing all applicable laws and requirements can feel like a Sisyphean task if you work for a large organization or any business with an international scope: by the time you have taken

an inventory of existing databases, usage patterns, transfer flows and applicable laws, the company has probably swapped out a few systems, acquired and spun off businesses, entered new jurisdictions, and found new opportunities to commercialize data, while several new data privacy laws have been enacted. Given the rapid pace at which data privacy laws and information technology move, it is usually most effective to design and implement the data privacy compliance program in phases. Focus first on high-risk requirements and low-hanging fruit in both the design and implementation phase. Start with implementation of high priority tasks while you still refine the design of the program. Compile a list of known compliance requirements that your organization and your peers and competitors already try to satisfy, or that are actively enforced. When you identify compliance gaps in high-risk areas, take action immediately. After that, add tasks to the list and turn to prioritization. Companies that start out by trying to develop a complete inventory of applicable legal requirements often find the challenge overwhelming and become paralyzed. 'Perfect' can become the enemy of 'good'.

As you prepare your task list, note the following considerations: 1.31

Take inventory of your data. At the outset, consider what personal data your business uses. At a minimum, you should prepare a brief summary with basic information on your key databases, including data categories (*i.e.*, data fields populated), primary purposes (*e.g.*, HRIS, CRM, email exchange server), geographical location of servers and who has access (*e.g.*, employees, departments and third party vendors). If you have international operations, you will also need to know names, addresses and headcount of all your legal entities and branches. 1.32

If you are working for a small or medium-sized company, it should not take you more than a few hours to prepare such an initial summary: you can go to the IT department, open the various software interfaces for the databases and copy basic information from screen shots; the legal department should have a list of subsidiaries and the human resources department should know headcount. This is enough to get started.

If your company is subject to the EU General Data Protection Regulation, you have to maintain more formal and detailed records of data processing activities, including 1.33

- names and contact details of your company or companies, their representatives in the EEA and their data protection officer, if any
- purposes of the data processing
- categories of data and data subjects
- categories of recipients to whom you disclose data, including data processors (and customers, if your company acts as a data processor)
- international transfers and specific safeguards
- time limits for erasure
- technical and organizational security measures

1.34 Larger companies sometimes conduct more elaborate assessments and audits of databases and data flows, often with the help – and sometimes at the initiative – of outside advisors. This can be beneficial and even necessary to get a solid grip on the status of data privacy law compliance in complex multinational organizations. However, such exercises can also take a long time, use a lot of resources and produce reports with overwhelming details that do not directly translate into improvements of the organization's compliance status. Consider starting with a high level inventory unless you are fairly sure that your company is past the initial compliance phase and you can stomach a full-blown data flow mapping exercise.

1.35 *Define your objective and priorities*. Companies have different objectives with respect to data privacy compliance per se or specific legal requirements. Some companies view data privacy compliance like any other legal requirement: they want to do only what is legally required (or as much as is commonly done in their industry and market segment). Other companies – particularly companies with information technology products or services – view data privacy as a potential competitive differentiator; consequently, they want to do whatever their customers expect or desire, and perhaps more than the competition. Also, with respect to particular aspects of data processing and compliance, the objectives vary. For example, some companies depend heavily on direct marketing and may want to collect and use personal data to the maximum extent in each jurisdiction, whatever the costs may

be, whereas other companies would be content to find and comply with the strictest requirement worldwide and implement a uniform compliance protocol in the interest of uniformity and cost savings. It is important to define and communicate these objectives efficiently to ensure that appropriate priorities are established.

Find the best approach for your company. Based on an initial assessment of applicable requirements and your objectives, you can select an approach that suits your organization and situation: 1.36

- Proactive or reactive? It is usually less risky, easier and cheaper to take proactive steps to avoid a problem than to cope with a lawsuit, investigation or negative press campaign. At the same time, only a small fraction of potential problems materialize. If cost containment is a key driver and your organization views privacy compliance as just another legal obligation, you may consider a risk-benefit analysis and the 80–20 rule (Pareto Principle). A relatively smaller percentage of potential problems (perhaps 20% in some cases) is responsible for the vast majority of adverse impacts (perhaps 80% in some cases – but the numbers are randomly picked). Conversely, companies can perhaps cover 80% of their problems with 20% of the budget it would take to address all problems. To address the remaining 20% of problems, which may not even be the most serious problems, the company would have to expend 80% of the total potential budget. Based on these insights, companies first try to find and rectify those problems that are most likely to result in major issues or require the least amount of effort and resources to fix. 1.37

- Some problems (*e.g.*, outdated website privacy statements) are easier and cheaper to fix than other problems (*e.g.*, a lack of budget for encryption technology or replacing a legacy system that does not allow differentiated access controls). Companies on a budget may find it easier to start with 'low-hanging fruit.' Most companies can quickly assess what their main competitors are doing by reviewing their website privacy statements and processing notices, determine whether particular steps are legally required, and then follow suit based on precedents. This approach does by no means guarantee full compliance, but it can help a company catch up to an industry standard relatively quickly and with modest resources. 1.38

- If your company is or wants to become an industry leader, you have to consider a more comprehensive assessment of legal requirements 1.39

and business needs. You can poll stakeholders in various departments (including legal, HR, IT, sales, product management, procurement, etc.) to prepare a list of company-specific priorities, subscribe to legal and trade publications and conferences to obtain a broader picture of the compliance landscape, follow guidance from government authorities , possibly even proactively seek guidance from authorities, and monitor enforcement and litigation cases.

1.40 • In terms of following guidance from government authorities, it is important to determine how much your business is exposed to action from governments. A regulated entity (*e.g.*, a bank or telecommunications service provider) usually has to take its regulator's views seriously whether based on laws or not because it depends on the goodwill of its regulator in many respects. Entities that are neither regulated nor sell primarily to regulated entities, however, are freer to take their own positions and views; such entities will typically ask not only what the views of a particular government entity are, but also if and how such views are enforced. This is particularly important with respect to gauging the relevance of official guidance from government authorities abroad. European data protection authorities, for example, have taken relatively extreme positions on various topics over many years without any enforcement activities that could have resulted in "reality checks" in court. A company that readily follows the official guidance at the expense of missing out on business opportunities may regret doing so if the guidance is not followed in practice or at some point challenged and invalidated in courts of law.

1.41 • Keep in mind that a company may find different approaches appropriate for a particular jurisdiction or part of its business. For example, a company with a large employee population and a hostile works council in Germany would seem well-advised to be particularly proactive with respect to data privacy of German employees, whereas other jurisdictions may present less of a priority. Or, a company with a particularly sensitive information technology product (*e.g.*, a repository of online medical records) may go out of its way to achieve or surpass compliance requirements with respect to its products, but it may decide that following industry standards will suffice with respect to employee privacy. Employee privacy compliance may be even less of a concern for a company that is still managed and operated largely by a group of founders who have a significant financial stake in the company and hence a relatively strong interest in minimizing compliance costs and efforts.

Identify legal and other requirements. As you identify legal require- 1.42
ments for purposes of designing and updating a data privacy compliance program, you will find thousands of laws around the world that address data privacy in one way or another. Even very large and compliance-oriented companies struggle with keeping up to date. Smaller organizations have to establish priorities and a system to ensure that they are capable of complying with key requirements – even if they may not be able to identify each and every law in detail.

What are data privacy laws? Despite different histories and public 1.43
policy motivations, there are common themes that help categorize and identify laws that are relevant to data privacy compliance programs. Data privacy laws in the narrow sense are typically concerned with personal data (*i.e.*, data relating to individual human persons as opposed to legal entities) and place conditions or restrictions on the collection, use, transfer and retention of personal data. These laws are of primary concern for the designing and maintaining of data privacy compliance programs. There are a lot of them, but you can narrow the realm of relevant laws down by applying subject matter and jurisdictional filters:

Which laws apply to you? Subject matter limitations. Some data pro- 1.44
tection laws apply directly only to certain types of entities.

- For example, European data protection laws do not typically 1.45
apply to data processing by national security agencies or private individuals in the course of a purely personal or household activity (*e.g.*, what someone posts about friends on Facebook). Healthcare-related data privacy laws in the United States (HIPAA) apply only to certain 'covered entities' and their 'business associates,' such as medical doctors, health insurers and certain service providers. Some laws relating to financial or telecommunications data apply only to banks or telecommunications providers respectively. Anti-spam laws tend to focus on for-profit, commercial enterprises and contain exceptions for political and non-profit organizations.

- Also, if your business is – or could be – typically acting as a data 1.46
processor on behalf of other entities, then your compliance obligations may be much more limited and not extend far beyond following instructions from the data controller and keeping data secure from unauthorized access.

1.47 Even if a certain law does not apply to your business, it may nevertheless be relevant if it applies to your business partners or clients. Most businesses, though, are able to remove a significant number of laws from consideration based on subject matter limitations.

1.48 *Which laws apply to you? International applicability*. There are more than 190 countries in the world and within each country, there may be several different jurisdictions (*e.g.*, 50 states in the U.S.). Companies usually take a hard look at which jurisdictions they primarily have to consider.

1.49 • Under customary international law, every sovereign country is free to legislate whatever it is interested in. There is no 'world constitution' or treaty that effectively draws limits on what countries can cover in their national laws.

1.50 • Typically, countries apply their data privacy laws to companies that are incorporated or registered in such country or that deploy employees or equipment on such countries' territory. Some countries go further and also apply their data privacy laws to companies abroad if: such companies collect data remotely via targeted websites (as indicated by country-specific URLs, languages, localized content, local phone numbers, etc.), business partners are located in the jurisdictions concerned, or even just on the basis that the foreign company collects data on residents of the legislating countries. Internet service providers, multinational enterprises and many other companies with more or less direct business connections to other countries find upon closer review that many countries' privacy laws apply to some of their data processing activities. But, there are also many companies with a domestic focus that can rule out most countries' laws (*e.g.*, local banks, hospitals and construction companies).

1.51 • European Union law sets some limitations on the ability of EU member states to apply their national data privacy laws extraterritorially (*i.e.*, outside their own country) to make it easier for EEA-based companies to do business everywhere in the EEA Common Market. An EEA-based data controller has to comply only with the laws of the EEA member state where it maintains a branch or other significant, physical presence, even if it collects data from other EEA member states (over the Internet or otherwise). This privilege is not available to companies outside the EEA. Therefore, a U.S.-based e-commerce company with customers throughout

the EEA may have to comply with the laws of numerous different EEA Member States. If it incorporates a subsidiary, however, in, say, Ireland (low corporate income tax rate) or Luxembourg (low value-added tax rate), to become the sole contracting party and data controller for all European customers, then the new subsidiary would have to comply only with the data protection laws of the one jurisdiction where it is incorporated. After the EU General Data Protection Regulation takes effect in May 2018 and further harmonizes data privacy law in the EEA, companies may become less concerned with national laws, but some differences will remain and location planning will still be necessary. Companies in the United States may be able to invoke similar protections under the U.S. Constitution's 'Commerce Clause' against state laws that discriminate against, or unduly burden, interstate commerce. Such jurisdictional privileges provide some companies with a planning opportunity to actively influence which laws apply to them.

- If you apply the above considerations and end up with a shortlist of jurisdictions that is still too long, you can prioritize further by identifying the countries where you need to be particularly concerned about enforcement. Concerns tend to be greater regarding countries where you have a subsidiary, employees, key assets, or key customers, or where regulators are particularly active. Aside from business concerns, you should also consider where compliance is particularly easy (*e.g.*, no language hurdles, similar legal system to your home jurisdiction). Based on such practical considerations, most companies can come up with a manageable shortlist of priority jurisdictions. 1.52

Data privacy by region – an overview for orientation purposes. Before you turn to an analysis of national data privacy laws, it may be helpful to take a brief look at different regional legislative approaches for orientation. 1.53

- In Europe, data protection laws are worded very broadly and apply to most kinds of private and public sector data processing activities. Some jurisdictions (including Austria, Italy and Switzerland) even rope in information relating to legal entities as 'personal data.' The basic premise in most European countries is that the processing of personal data is prohibited, except with valid consent from the data subject or based on another, statutory exception. Such exceptions may be available, for example, if a company needs to process 1.54

personal data to perform a contract with the data subject, to comply with a statutory duty, to protect vital interests of the data subject, to perform a task carried out in the public interest, or to pursue its legitimate interests, except where such interests are overridden by the privacy interests of the data subject. This last exception, also known as the "legitimate interest exception," requires companies to balance their own interests with those of data subjects. European data protection authorities had taken restrictive views on this exception in the past, but more recently acknowledged the "legitimate interest exception" as a justification of equal standing and not a matter of only "last resort," a development that may foster convergence and interoperability with U.S.-style data privacy law focused on protecting reasonable expectations of privacy. Still, consent and notice requirements are relatively stringent, international transfers of personal data outside the European Economic Area are restricted and many jurisdictions require government notifications, appointment of data protection officers and other formal steps. Due to broad and undifferentiated prohibitions, companies and regulators have taken interpretative liberties in the past. Also, private lawsuits are relatively uncommon. This has resulted in lax enforcement and uncertainties in many countries.

- Things may change in Europe after the EU General Data Protection Regulation takes effect in May 2018. This Regulation constitutes the first significant update of EU data privacy laws since 1995 and it applies directly to companies and individuals (without a need for implementation into national law). Data protection authorities will be able to levy much higher administrative fines of up to the greater of €20m or 4% of annual worldwide sales. Companies face stricter requirements regarding privacy impact assessments, data minimization, deletion and security breach reporting (within 72 hours). The basic default principle under the Regulation remains "verboten": companies must not process personal data unless they can claim an exception from the general prohibition.

1.55 • In the United States, on the other hand, the basic premise is that the processing of personal data is permissible. There are no specific data protection authorities or government filing requirements. Generally applicable privacy laws impose restrictions only where data subjects have a reasonable expectation of privacy (meaning an actual expectation that society considers reasonable). For the most part, companies can destroy such expectations relatively easily by

issuing notices informing data subjects of data processing practices. When broad, omnibus data protection laws in Europe were passed in the 1970s, legislatures in the United States decided to take a different approach and legislate only around serious problems. Consequently, legislatures passed laws with specific types of risks and abuses in focus. The United States now has myriad specifically scoped data privacy laws at the federal level and in the 50 states. If and when such laws apply, the restrictions and liabilities for violations can be surprisingly harsh, particularly for European companies entering the U.S. market expecting no significant privacy laws. For example, the California Song-Beverly Credit Card Act of 1971 prohibits retailers from collecting contact and other information from credit card holders, except as necessary to process the credit card transaction. This prohibition applies absolutely, even if cardholders consent in writing to the data collection and subjects merchants to significant liability and exposure to class action lawsuits. Yet the California law places no particular restrictions on information collected from cash-paying customers. As another example of a very strict but narrowly crafted law, the U.S. Congress enacted the Federal Video Privacy Protection Act in 1988 in reaction to publicity around the videotape rental history of a candidate for judicial office to prohibit disclosure of videotape rental information; but, this statute does not apply to book or video game rentals. U.S. federal law on health information privacy (HIPAA) restricts health data collection and usage by 'covered entities' and their 'business associates,' as well as providers of certain 'protected health records,' but not by anyone else; as a result, various online services providers are exempt from the law even though they may collect extremely sensitive health information from consumers over the Internet. Similarly, the Gramm–Leach–Bliley Act (GLB) applies directly only to financial service providers and not to most of the FinTech companies. In addition to U.S. federal privacy laws, companies have to assess state laws and find that California, for example, has enacted many stringent and detailed privacy laws that close perceived gaps in federal privacy laws.

- Consequently, companies have to carefully assess whether their contemplated activities are covered by a sector-specific federal or state law in the United States. If so, companies may find much more rigid restrictions and exposure to liability than under European laws. But, it is also possible that the contemplated activity falls outside the scope of any specific laws (based on the company's original

plan or conscious changes in light of the legal situation), and as a result, the company only has to post an appropriate notice and ensure compliance with such notice. As in Europe, violations of U.S. laws can be sanctioned by government authorities (including the Federal Trade Commission and State Attorneys General). On the other hand, in the United States, private lawsuits play a much greater practical role, given the possibility of class action lawsuits, punitive damages, civil jury trials and contingency fees for lawyers (who can pocket attorneys fees and a significant portion of damages awards while plaintiffs do not incur much financial risk if they engage lawyers on a contingency fee basis).

1.56 • Other countries have often modeled their laws more or less after the European templates (*e.g.*, Argentina, Colombia, Israel, Russia and Uruguay) or have pursued a hybrid approach – with some elements of the European legislation but more differentiated or lenient consent and notice requirements and less stringent administrative duties (*e.g.*, Australia, Canada, India, Japan and Mexico).

1.57 *What other laws and requirements need to be considered?* Besides data privacy laws in the narrow sense, companies have to consider a variety of other requirements for purposes of designating data privacy compliance programs, including the following:

- statutory obligations under employment, consumer protection and unfair competition laws, as well as constitutional safeguards, which are applied directly to companies in some jurisdictions,
- contractual obligations (for example, regarding data security standards, breach notifications and incorporation of privacy statements by reference in contract terms),
- promises extended previously to data subjects in privacy policies and notices, and
- customer expectations and other business needs (what data do you need, for how long, for what purposes?).

1.58 *Identify applicable substantive compliance requirements.* Substantive compliance requirements vary significantly in jurisdictions with European-style data protection laws versus the rest of the world. However, there are also a couple of requirements that apply globally.

Abide by policies, notices, and contracts. One universal requirement is: Do what you say – comply with the limitations you assume in notices, policies, website privacy statements and contracts. If a company remains silent on its data processing practices, then this requirement does not have much significance. But, in more and more jurisdictions and industries, companies are forced to issue statements and notices, either as a matter of law, industry practices or technical requirements (*e.g.*, many mobile app stores require developers to post privacy statements). In the United States, for example, the Federal Trade Commission urged Internet companies early on based on unfair competition law theories to publish website privacy statements, and much of the early enforcement focused on failures to comply with promises in semi-voluntarily issued privacy statements. If companies fail to comply with their own notices, policies and statements, they can be sanctioned in most cases under various legal theories, including unfair competition laws and tort law (misrepresentation). Therefore, companies have to focus on keeping their notices, privacy statements, contracts and other privacy-related communications accurate and up to date – either by adapting their communications or their practices. 1.59

Data security. Companies have to maintain reasonable security measures to keep confidential data protected against unauthorized access and dissemination. Security requirements follow also from trade secret laws and confidentiality agreements and extend beyond personal data, but the reach of trade secret laws ends once the secret is disseminated. Data protection laws also require reasonable security measures and can apply even to personal data that has become public. Therefore, the typical definitional carve-outs in confidentiality clauses (independently developed information, information in the public domain, compelled disclosures, etc.) may not be used in the data protection law context. Companies have to confirm compliance with data protection law requirements separately and in addition to compliance with trade secret laws and contractual confidentiality obligations. 1.60

Companies around the world have been obligated for decades to keep personal data secure under statutes and contracts. In the past most laws and contract clauses simply set forth a general reasonableness standard and did not prescribe specific safeguards. More recently, after California enacted the world's first data security breach notification law in 2002 and companies started reporting security breaches en masse, more and more jurisdictions have passed data security breach notification laws and lawmakers around the world have started prescribing 1.61

very specific technical and organizational measures intended to ensure that companies take more comprehensive steps to prevent security breaches and protect the data and privacy of consumers, employees and other individuals.

1.62 The extent to which companies collect, store, manipulate, transfer, and otherwise process personal data depends on their business needs and legal obligations to collect and retain information. All businesses process some personal data. At a minimum, they handle the contact information of their own employees, customers and business partners. Most businesses also process more sensitive data, such as payroll information, consumer purchase histories, data from credit card transactions, and other financial and medical data. So, as part of implementing a data privacy compliance program, you need to assess the specific requirements on your business regarding data security and develop an information security program that is appropriate for your company, considering specific legal requirements per jurisdiction, your risk profile and tolerance, as well as contractual and practical necessities.

1.63 Successful data security programs typically involve the following parameters:

- methods for keeping track of where data is stored and secured and for what purposes and how long it is needed (records of data processing activities),
- physical and technical protection for premises, networks and devices (including encryption, firewalls, strong authentication, passwords, etc.),
- organizational access controls within the organization ('need to know'-based restrictions),
- employee training,
- secure deletion of data that is no longer needed (*e.g.*, on discarded devices, paper),
- ongoing monitoring plus random audits and investigations into data security,
- prudent vendor selection, management, monitoring and contracting,

- a plan to address data security breaches individually and proactive changes to avoid recurrence, and

- proactive privacy impact and security-by-design assessments before any major changes to data processing activities, including the implementation of new products, processes and data use cases.

1.64 As a first step, you should determine whether your company has written policies or unwritten processes addressing these points and representatives in charge of assuring compliance. As a second step, you could prepare a written summary of the existing measures and then assess whether the existing measures meet legal requirements (under laws and contracts) and adequately address risks threatening your company. Next, you could consider validation of your security program by outside advisors to confirm alignment with industry practices. In that regard, it is important to reach a clear understanding and agreement with the outside advisor on objectives and deliverables. Some companies experience frustration because they hire data security consultants who deploy an infinite number of scans and tests but are not willing to advise when enough is enough or issue an opinion regarding the adequacy of the company's security efforts.

1.65 *Additional substantive data privacy compliance requirements.* Under European data protection laws, companies have to satisfy a number of additional substantive data protection law compliance requirements:

- minimizing data processing and retention,

- maintaining data integrity by updating, correcting or deleting data,

- granting access to data subjects on request, and

- seeking consent or other justifications.

1.66 These requirements apply in most European countries, but may not apply outside of Europe. Many countries have consciously opted against data minimization requirements because they constitute a particularly severe restraint on innovation, economic liberties and freedom of information.

1.67 *Identify applicable formal compliance requirements.* A number of data privacy compliance requirements are 'formal' in the sense that you

need to generate certain notices, government filings or other paperwork. Such formal compliance obligations do not directly require you to change your data processing activities. But, if you are not substantively in compliance, then you are usually unable to issue appropriate notices, government filings, etc., because you would just be notifying everyone that you are not in compliance. Thus, substantive compliance logically comes first. Practically, however, it is often most efficient to start working on formal compliance tasks because this work will help identify substantive compliance requirements and gaps. Also, most companies find it comparatively easy to achieve formal compliance and see a particularly high risk associated with failing to comply with formal requirements, as such failures are especially easy to prove by government investigators, private plaintiffs and other potential adversaries. The question 'Did you make the required filing or not?' tends to be more black and white than, for example, 'Is a three year data retention time period appropriate for employee records after termination?'

1.68 You have to research applicable details on a country-by-country basis outside the scope of this Field Guide (see the section on Resources at the end of the book). But, for orientation purposes, you can expect that formal requirements typically include the following:

- appointment of a data protection officer,
- preparing records of data processing activities,
- documentation of data security measures,
- concluding appropriate data transfer agreements with affiliates, service providers and other business partners,
- issuing notices to data subjects or obtaining their consent,
- submitting notifications to data protection authorities or seeking their approvals, and
- consulting with works councils, labor unions or other employee representative bodies, if any.

Executing tasks

Once you have prepared a list of concrete tasks to achieve compliance with data protection laws, you should start executing them, perhaps first on low-hanging fruit and tasks that help mitigate major risks. Many companies find it helpful to start preparing the required notices to data subjects because in the process they naturally go over the status quo and can then best address gaps and other issues. An important practical point is: don't get overwhelmed. It is better to close some compliance gaps than none; and even though many tasks are interconnected, it is often possible to complete tasks in some areas without prejudice to others (*e.g.*, address employee data privacy and security before or after tackling consumer data privacy, and approach compliance for some priority jurisdictions before turning to others). 1.69