
iapp

# The Top 10 Operational Responses to the EU's General Data Protection Regulation

The IAPP Westin Research Center

www.iapp.org
IAPP - International Association of Privacy Professionals
Distributed by Canon U.S.A., Inc. with permission by IAPP

iapp TOP 10

# The Top 10 Operational Responses to the EU's General Data Protection Regulation

The European Union's General Data Protection Regulation comes into force in May 25, 2018. Even with up to 70 percent of enterprises, globally, predicting they would be ready, according to a study conducted by IAPP in late 2017, thousands of businesses, including many small-to-medium-sized enterprises, are still struggling to digest dozens of provisions of legislative text. Importantly, GDPR compliance is not a discrete point-in-time challenge, but rather an ongoing process that will occupy data professionals in companies all over the world, for many years to come.

There is much to do to build programs compliant with what is undoubtedly history's most comprehensive data protection law. With 99 Articles and more than 170 Recitals, the GDPR challenges even the most experienced data protection and privacy professionals with its sheer size, scope and complexity. Indeed, the top barrier to GDPR compliance according to the IAPP's 2017 study is "complexity of the law."

In 2016, the Westin Research Center published the "Top 10 Operational Impacts of the GDPR." With more than 70,000 downloads in 2017 alone, this series and eventual eBook indicates great interest among professionals in a practical, tactical package of GDPR guidance. But spotting issues and analyzing gaps is just the start of the process. Inevitably, companies need to proceed to the implementation phase and devise practical operational responses. With companies caught up in a flurry of activity to get ready for the GDPR, or in full panic mode as they just prepare to launch their programs, we now offer this companion eBook to the "Top 10 operational impacts," with our new "Top 10 Operational Responses to the GDPR."

These 10 chapters are based on our own research, on crowd-sourced information from our 2017 surveys of IAPP members, and, importantly, on interviews with leading global experts who volunteered from the IAPP's Research Advisory Board. The articles are intended to reflect practical and real-world steps that data protection and privacy professionals are taking to help their companies, employers and clients prepare for the plethora of GDPR data protection obligations.

# Table of Contents

# 1 Data Inventory and Mapping

One can search the GDPR in vain for the terms "data inventory" or "mapping." They simply do not appear in the plain language of the law.

But unquestionably, the first operational response to GDPR, essential to building a program that aims to comply with the law, is a comprehensive exercise of data mapping and inventory. The terms may have slightly different meanings depending on whom you ask, but they involve at least the following:

- Understanding the definition of personal data under the GDPR.
- Determining what personal data is collected and used ("processed" in GDPR-speak) by the organization.
- Finding out where the data is stored, including what third-party systems might house it and where, geographically, the servers are located.
- Mapping where the data goes from point of collection throughout the organization and externally to vendors or other third parties.
- Determining how long the data is retained and in what formats. This includes having a sense of whether the data are "structured" (in relational databases) or "unstructured" (everything else, such as loosely organized systems, including paper files or PDFs, for example).

Without conducting the inventory and mapping exercise, a data protection professional cannot meaningfully build out a program that meets the GDPR's many obligations, including establishing a lawful basis for processing, providing data subjects with transparency and meeting their other data protection rights, knowing when and how to gather and record consent, and the like. It is quite difficult, for example, to prepare a privacy statement or an internal privacy policy without understanding what data is collected, how it is processed, and with whom it is shared.

*Without conducting the inventory and mapping exercise, a data protection professional cannot meaningfully build out a program that meets the GDPR's many obligations.*

Importantly, data inventory is also the first step in complying with obligations to keep records of processing under Article 30. This pivotal provision of GDPR requires companies to maintain detailed records of their processing activities, including the purposes of the processing; a description of the categories of data subjects and of personal data; any recipients with whom personal data are shared, including their geographic location; any cross border data transfers and risk mitigation measures; data retention schedules; data security policies; contact details of a European representative and DPO, where applicable; and more.

## Tools and methods

The best method to conduct data inventory and mapping will depend on an organization's size and complexity, as well as the amount of time allotted to the exercise and the sophistication of the participants.

Many data protection and privacy professionals, perhaps assisted by outside counsel or consultants, begin with a questionnaire. Those with adequate time can engage in an initial discovery exercise to unearth their organization's general personal data life cycles, followed by deeper-dive questionnaires and follow-up interviews, and even workshops.

Ideally, the inventory and processes created to support it allow – eventually, at least – the capacity to identify data location and storage information at the level of an individual data subject: What data do I have on Jane Doe, and where is it located? If Jane wants access to her data, how can I be sure to find it all for her?

Assigning a level of risk to distinct data categories is also important at this stage. After all, the GDPR fundamentally takes a risk-based approach to data protection. Is the information highly sensitive, falling within a "special category" as defined in Article 9? This would require a company to rely on a different legal basis than for regular processing. Would unauthorized access to data create high risks to the rights and freedoms of the data subjects? This would trigger a DPIA or require an individual breach notification.

For many, this information is currently tracked in home grown and adapted tools available through standard enterprise software products. In the IAPP-EY 2017 Governance Report, 45 percent of respondents reported they conduct data inventory and mapping informally, using manual and informal processes including email, interviews and spreadsheets; only 32 percent reported using commercial products developed exclusively for data inventory and mapping.

Over the past few years, a privacy technology industry has exploded in response to the GDPR and other privacy regulatory developments. Dozens of startups have emerged to provide solutions and tools for organizations working on data protection regulatory compliance, accountability, and risk mitigation, as highlighted in the IAPP's annual Privacy Tech Vendor Report.

While less scalable than technological data mapping tools, traditional questionnaires have the benefit of being comprehensive and can be sent to many people within an organization, allowing for a potentially comprehensive and wide-spread investigation. Their risks, however, include the potential for weak or inaccurate responses, and misunderstanding on the part of those completing the questionnaire who make assumptions and do not or cannot get clarification before submitting their answers. The task of answering the questionnaire may be tasked to someone with inadequate knowledge or awareness.

Privacy professionals who are in a rush, then, may not be able to use a questionnaire followed by interviews. Instead, it may be necessary to jump directly to in-person meetings. This may take more personnel time – and at a higher level of management within the organization – but is likely the best way to get useful information about data processing as quickly, accurately, and efficiently as possible in the shortest time.

## Thinking ahead

As the inventory and mapping process is conducted, data protection and privacy professionals should be thinking not only about (a) what types or categories of personal data are being collected, processed and stored, (b) by whom and where they are stored, accessed and processed, but also (c) what the reasons are for the personal data processing. Is it really necessary to have this information and why? Article 5 of the GDPR requires that personal data be processed "lawfully and fairly" and "collected for a specified, explicit and legitimate purpose." Assigning such a basis at the inventory stage expedites compliance with GDPR's core obligations.

Indeed, record keeping under Article 30 is often conflated with inventory and mapping, and although there is no reason they cannot overlap operationally they are not necessarily the same thing. Article 30 does not expressly require the record to demonstrate lawful basis for processing, and yet that is a core GDPR requirement. Best practices counsel in favor of assigning these bases and recording them at the inventory stage.

Our next chapter addresses the various lawful bases under Article 6 and how operationally to select – and appreciate the consequences of – lawful bases options.

*Indeed, record keeping under Article 30 is often conflated with inventory and mapping, and although there is no reason they cannot overlap operationally they are not necessarily the same thing.*

# 2 Establishing Lawful Basis for Processing

Similar to the situation under the 1995 Data Protection Directive, under the GDPR a company may process a data subject's personal data only if there is a "lawful basis" for such processing. Article 5 decrees that personal data shall be "processed lawfully," and Article 6 lays out six different legal bases that satisfy the lawfulness requirement:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Although Article 6 limits the legality of processing to situations where "at least one" of the bases applies, organizations should be cautious about relying on multiple lawful bases for any single processing purpose. The Article 29 Working Party's guidance on consent suggests that "[a]s a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases."

Companies are required to identify a basis for processing at the time of collection, before processing occurs, and per Article 13(1)(3), must furnish the data subject with both the purpose of the processing and its legal basis at the time data is collected.

## What this means in practice

Our interviews with leading privacy professionals suggest that the simplest cases to support will be those where processing is necessary for the performance of a contract, or for the controller's compliance with a legal obligation. In these cases where, for example, an online retailer processes a consumer's address in order to deliver an ordered item (performance of a contract) or a financial institution processes an accountholder's data to comply with anti-money laundering laws (compliance with legal obligation), the existence of a lawful basis is clear cut.

More common — but also more difficult — are situations where processing is undertaken with the consent of the data subject; or processing is necessary for the purposes of the legitimate interests of the controller or of a third party except where such interests are overridden by the privacy interests of the data subject. Guidance documents from the Article 29 Working Party provide examples of both. Examples for legitimate use of consent include a hotel chain's online offer of an opt-in tick-box to a loyalty program, presented to customers who have already made a reservation; or a cable TV network's asking subscribers to consent to the use of their viewing habits in order to present them with personalized content suggestions. An example of reliance on legitimate interests includes a computer store, using only the contact information provided by a customer in the context of a sale, serving that customer with direct regular mail marketing of similar product offerings — accompanied by an easy-to-select choice of online opt-out.

Least common are cases where processing is necessary to protect the vital interests of the data subject or another natural person, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. One example of processing to protect the vital interests of the data subject might be the processing a person's information in order to locate them after a humanitarian disaster. A classic example of processing necessary for the performance of a task carried out in the public interest is a tax authority's collection and processing of an individual's tax return in order to establish and verify the amount of tax to be paid. Recital 46 notes that some processing "may serve" the grounds of both public interest and the vital interest of the data subject, such as processing in order to monitor an epidemic.

Article 9 of the GDPR identifies "special categories of personal data" and sets forth a more limited subset of lawful bases for processing such data. Any data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership," along with "processing genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" is prohibited unless it meets one of the 10 exceptions specified in Article 9(2). Importantly, companies that process "special categories of data" cannot rely on a legimitate interest as a lawful basis for processing such data. However, a restrictive form of consent can be used. Article 9(2)(1) permits processing based on "explicit consent," which requires "an express statement" of approval, a heightened requirement beyond the "clear

affirmative act" necessary to establish consent when processing "regular" personal data. The Working Party suggests that a written statement, signed by the data subject where appropriate, is one means of demonstrating this requirement.

## Unpacking consent and legitimate interests

### Consent

Many organizations start the process of identifying the legal basis for processing by determining which (if any) of their activities require consent. While the tighter requirements of GDPR-compliant consent could be a disincentive for relying on this basis, for some types of processing there's simply no other way. Article 4(11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Conducting properly-resourced data mapping and inventory is a critical first step to identify any instances where consent has not been properly acquired or recorded. Next, companies should determine areas of processing where consent should be sought and identify any processing that currently relies on consent but should cease doing so. Existing databases must be brought into compliance by the May 25 deadline or risk losing their usefulness to organizations until proper consents can be procured.

Clearly, consent is the most talked-about of the six legal bases available under the regulation. According to a 2017 study conducted by the IAPP with TrustArc, obtaining consent ranked third overall among 11 compliance risks, and ranked second among just U.S. respondents. Many businesses rely on consent, often obtained via the ubiquitous "I Agree" button, for the collection, transfer, and processing of personal data. Recitals 32, 42, and 43 of the GDPR give some examples of what constitutes a "freely given, specific, informed and unambiguous" consent, and explicitly warn that "silence, pre-ticked boxes or inactivity" will not qualify.

A "written statement, including one given by electronic means, or an oral statement" may suffice. The GDPR also suggests that "ticking a box when visitng an internet website" or "choosing technical settings for information society services" will qualify as conduct that clearly indicates the data subject's acceptance of processing. In its guidance on consent, the Working Party suggests that physical motions such as waving in front of a smart camera, swiping, or turning a phone or tablet in a specific direction could satisfy the requirement for "unambiguous consent," so long as "clear information" is provided to the data subject. Recital 50 warns processors against processing data for purposes other than those disclosed when the data was originally collected. If a company wishes to conduct such additional-purpose processing, it must first obtain a new consent.

Article 7 sets forth additional conditions for valid consent. To rely on consent, companies must be able to demonstrate that data subjects have in fact given it, necessitating an organizational system that

will maintain a record of the required clear affirmative act or express statement (oral or written), depending on the type of data being processed.

Written declarations of consent, if packaged with other matters, must be presented "in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language." This means that a valid consent statement cannot be buried in fine print, written in impenetrable legalese or conflated with other important contract terms. Data subjects also retain a right to withdraw consent at any time, and must be informed of this right before providing consent. Withdrawal of consent must be as easy as giving consent. Finally, the requirement that valid consent must be "freely given" is emphasized; particular scrutiny is warranted for whether "the performance of a contract, including the provision of a service, is conditional on the consent to the processing of personal data that is not necessary for the performance of that contract."

Additionally, to satisfy the requirement that consent be freely given, companies relying on consent must consider the imbalance of power between themselves and data subjects. The Working Party warns that "any element of inappropriate pressure or influence on the data subject … which prevents a data subject from excerising their free will, shall render … consent invalid." For example, a bank that asks for its customers' consent to use their payment details for marketing purposes, but denies banking services or increases fees if consent is not granted, would be exerting inappropriate pressure. The GDPR does not absolutely prohibit offering services conditioned on consent to data processing, but per Recital 43, any consent so provided is presumed invalid, and the Working Party notes that "[valid] cases will be highly exceptional."

In addition to avoiding behaviors prohibited by the GDPR, organizations must meet a number of affirmative obligations to vindicate data subjects' rights when relying on consent. Article 20(1)(1) guarantees data subjects the right to access any data they have provided to a data controller based on consent. Recital 63 adds that access should be provided "easily and at regular intervals" to enable a data subject to verify the lawfulness of processing. Article 20 also guarantees that this data be provided in a "structured, commonly used and machine-readable format," which controllers should consider when designing data storage and categorization tools for the processing of data that will be collected based on consent. Recital 68 clarifies that the requirement of data portability applies to controllers engaging in processing based on consent or pursuant to a contract, but not on other legal grounds, though it does not require all controllers to design mutually interoperable formats.

*Written declarations of consent, if packaged with other matters, must be presented "in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language."*

Article 17 guarantees every data subject the right to "obtain the erasure of personal data concerning him or her without undue delay." This right is specifically implicated when consent is withdrawn by data subjects. Data controllers planning to rely on consent should thus have a workable erasure mechanism in place for cases of withdrawal of consent as part of their plan to cease processing upon a data subject's objection.

Specific operational problem areas include: employment agreements that rely on consent as the basis for the processing, since the requirement that consent be freely given is inherently undermined by the imbalance of power between an employer and an employee; any processing of consumer data based on pre-GDPR data subject consent; any services that obtained consent via pre-ticked boxes or browsewrap; and any processing occurring for multiple purposes. Valid pre-GDPR consent does not guarantee continued validity after May 25, 2018; Recital 171 makes it clear that consent obtained before the GDPR will remain valid only if it satisfies the stricter standards of the Regulation.

## Legitimate interests

Like the 1995 Data Protection Directive, the GDPR permits data processing in furtherance of a company's "legitimate interests pursued by itself or a third party" — with the critical caveat that the "interests or fundamental rights and freedoms of the data subject" cannot be outweighed by the company's interest. Recital 47 gives several examples of such consent-less processing based on legitimate interests, including relationships where the data subject is a client or in the service of the controller. In every case, however, "careful assessment," often referred to as a "balancing test," is required. This process comprises a two-step analysis: First, a company must present an interest that is legitimate; second, processing in furtherance of that interest must satisfy a balancing test between the controller's legitimate interest and data subjects' privacy rights.

In its guidance on legitimate interests, the Working Party states that "any interest can be considered legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws." Next, a company must determine if its "interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data." This test is not an easy "either-or" proposition; it is a complex assessment that must take in to account four broad factors: the controller's legitimate interest; the impact on the data subject; the provisional balance between the two; and additional safeguards applied by the controller to prevent any undue impact on the data subjects.

As a lawful basis for processing, legitimate interest, like consent, triggers complex compliance considerations. Article 13(1)(4) and Article 14(2)(2) of the GDPR require an organization to specifically identify its legitimate interests to a data subject. Importantly, under GDPR Article 18(1)(4), companies that choose to rely on legitimate interest grounds must create a mechanism to restrict processing for a data subject who chooses to challenge a controller's application of the balancing test. Both Article 21(1)and Recital 69 guarantee data subjects a mechanism to object to processing based on legitimate interests.

Ultimately, to chart the waters of the fact-specific balancing test, companies will have to look to a history of enforcement actions by supervisory authorities. In the meantime, they can rely on the example legitimate interests given by the Commission and the Article 29 Working Party in their advice. The Working Party's 2014 guidance on legitimate interests, while issued under the 1995 Directive, can nevertheless provide useful examples of how this test might be applied in different situations.

### In the workplace:

Establishing a company-wide internal employee contact database with the name, business address, telephone number, and email address of all employees, to enable employees to reach their colleagues, could be justified under a legitimate interests test, so long as "appropriate measures," such as the adequate consultation of employee's representatives and institution of effective security policies, are taken.

Compliance with a foreign legal obligation, such as a whistle-blowing scheme required by the United States' 2002 Sarbanes-Oxley Act, qualify as legimate interests. Non-EU legal obligations do not authorize processing based on a "legal obligation" under Article 6(c). If such programs include appropriate safeguards, the legitimate interest of the company in complying with its foreign legal obligations will justify data processing.

In contrast, electronic monitoring of employee internet, email or telephone use, particularly if accompanied by video surveillance, will likely fail the balancing test without the institution of substantial additional safeguards to protect employee privacy interests. The nature of employement in any given context would also be critical to this type of processing.

Despite furthering an employer's legitimate interest of ensuring compliance with non-smoking rules, a company's use of hidden cameras to identify employees and visitors who smoke in unauthorized places would likely fail the balancing test as a disproportionate invasion of individuals' privacy rights, when other less intrusive solutions are available.

### Processing consumer personal data:

Companies clearly have a legitimate interest in collecting information about their customers' preferences in order to "better personalize their offers and ultimately offer products and services that better meet the needs and desires of customers." Some types of marketing can be conducted pursuant to this interest, such as direct physical or electronic mailing with an effective opt-out. However, according to the Working Party, the combination of "vast amounts of data about [customers] from different sources" used to build "complex profiles of customers' personalities and preferences" is likely "a significant intrusion into the privacy of the customer" that will be overridden by the interests and rights of the data subject.

The Working Party engaged with one scenario in particular detail: a fictitious interaction between a pizza chain and a customer. It explained that the restaurant, pursuant to its legitimate interest of increasing sales, could directly mail coupons to the address provided by a past delivery customer,

> *Companies clearly have a legitimate interest in collecting information about their customers' preferences in order to "better personalize their offers and ultimately offer products and services that better meet the needs and desires of customers."*

so long as it provided an easy-to-use opt-out. However, if that company's processing of customer information for marketing purposes were expanded to include years of the customer's purchases, as well as her purchases at a grocery store owned by the chain's parent company, her browsing history captured via cookies placed by the store's website, and location data from her mobile device, the outcome of the balancing test would swing away from the company to the individual.

Similarly, an internet company that provides a variety of online services including a search engine, video sharing, and social networking, which adopts a privacy policy enabling it to combine all personal information collected through different channels from each user for the identified interest of "providing the best possible quality of service" would likely fail the balancing test. This is due to the fact that the users cannot control or object to specific combinations of data and that the level of information potentially collected creates an imbalance of power between the company and its users.

Given that a controller's legitimate interests must be specified at the time of collection, repurposing data is hard to justify under this basis. Per Recital 69, controllers always bear the burden of satisfying the balancing test. Under GDPR Article 40, controllers should consult their trade associations or similar industry groups, since they are authorized to prepare codes of conduct to define controllers' legitimate interests in specific situations.

Usefully, the Working Party identified certain measures that may help "tip the balance to ensure that … processing can be based on the [legitimate interest of the controller]," including:

- A workable and accessible mechanism to ensure data subjects an unconditional opt-out from processing.
- Strict limits on how much data is collected.
- Immediate deletion of data after use (for example, an app scanning users' contacts solely to determine which ones had already consented to the app's processing of their information).
- Use of anonymization techniques.
- Aggregation of data.
- Privacy-enhancing technologies, privacy by design, and data protection impact assessments.

- Technical and organizational safeguards to ensure that data cannot be used to take decisions or actions with respect to individuals.

- Data portability and related measures.

- Pseudonymization and encryption of data.

## Order of operations

As with any organizational response to the GDPR, the first step is the adoption of an effective data mapping and inventory strategy. Once a company maps its personal data processing, it should carefully document a lawful basis for each processing purpose. Of the six lawful bases permitted under the GDPR, consent and legitimate interest are not the most commonly used, but are the source of the greatest amount of uncertainty. Nevertheless, there are pre-enforcement steps companies can take to minimize processing risks.

Pre-GDPR consent-based processing should be reviewed to ensure that the underlying consent remains effective. If necessary, new consent should be sought. If any "special category" processing was identified, the company must solicit "explicit" consent. Under the GDPR, in all instances of consent-based processing, companies should ensure the availaibility of withdrawal mechanisms.

For processing based on a company's legitimate interest, the required balancing test should be reviewed and documented. The fact-specific nature of this legal basis highlights the importance of good recordkeeping. In line with the Working Party's guidance, data use and privacy policies should be evaluated for potential opportunities to add "balance tipping" mechanisms.

# 3 Building and Maintaining a Data Governance System

While data mapping and inventory, and establishing a lawful basis for processing, are logically the first two steps on the road to GDPR compliance, these activities require coordination among many people throughout the organization to be performed by at least one person who is both knowledgeable about the GDPR and capable of project management. Whether that person's title is DPO or not will depend on additional analysis of the relevant GDPR provisions.

Organizations may engage a consulting firm for data mapping and inventory assistance, and may seek legal counsel for help understanding which lawful basis applies to each processing activity. Indeed, companies can outsource even some privacy leadership functions in the form of an external DPO. But many organizations either do the work entirely in-house with their own privacy staff or take a blended approach, with in-house privacy professionals who draw on assistance from outside experts where necessary.

Regardless, projects as important as building GDPR-compliant systems and processes do not happen without leadership.

According to the 2017 IAPP-EY Privacy Governance Report, legal training is the most common background for a privacy lead. The most common corporate rank for a privacy leader is "manager," although many are more senior with a title of "director," "associate general counsel," or even — 7 percent of the time — "Chief Privacy Officer." According to the report, moreover, three out of 10 organizations have promoted their privacy leader within the organization due to GDPR compliance concerns. Privacy leaders also earn, on average, nearly U.S. $130,000 annually, and as much as $170,000 for those whose title is chief privacy officer.

## The DPO

Although not all privacy leaders serve in the role of DPO, most professionals with DPO responsibilities — 74 percent — serve as their employer's privacy lead.

Article 37 of the GDPR requires certain organizations to appoint a DPO. Much has already been written about the DPO role, and the IAPP's Resource Center has a DPO toolkit, job description, and other information to help organizations and their DPO understand and manage the position. According

*Projects as important as building GDPR-compliant systems and processes do not happen without leadership.*

to IAPP research, this mandatory role will lead to the creation of at least 75,000 new DPO appointments globally.

In short, an organization must designate a DPO when one of the following is true:

- It is a public authority or body.
- It conducts regular and systematic monitoring of data subjects on a large scale.
- Its core activities consist of processing on a large scale of special categories of data or of personal data relating to criminal cases.
- It is required to do so by member state law.

The DPO must be knowledgeable with the GDPR and able to guide the organization's GDPR compliance. At the same time, the DPO is to serve as a point of contact for data subjects, ever vigilant to their rights and interests, and able to cooperate with data protection authorities during investigations of consumer complaints or on routine compliance matters. DPOs must be consulted, for example, in the event of a suspected data breach, or when conducting a data protection impact assessment, the subject of the next installment in this series.

Because of the high public visibility of the DPO role, many organizations may decide to appoint one even if they can make the argument that their processing activities don't fall under the scope of Article 37. The Article 29 Working Party has encouraged erring on the side of appointing a DPO when in doubt. Whereas data mapping, privacy risk assessments, recordkeeping, and the like are entirely internal processes of which consumers and regulators may never be made aware, a DPO's appointment may visibly demonstrate that a company is aware of and seeking to comply with the GDPR especially if that information is shared with consumers through privacy statements and otherwise in consumer communications.

That said, because the term "DPO" has legal significance triggering obligations and responsibilities under the GDPR, some argue that the term should not be used casually to refer to any privacy leader but instead only to the person who is fulfilling the unique statutory role of the DPO. This may be someone within the organization who is consulted only at specific times as set forth in the GDPR. Alternatively, the role could be outsourced to a firm that specializes in DPO fulfillment.

*Because of the high public visibility of the DPO role, many organizations may decide to appoint one even if they can make the argument that their processing activities don't fall under the scope of Article 37.*

## Privacy policies

Each year, privacy professionals report that their number one activity is drafting internal privacy policies and procedures. The Privacy or Data Protection Policies set forth the organization's intentions and practices regarding the processing of personal data. They should not to be confused with the public-facing Privacy Notice or Privacy Statement that typically lives on an organization's website for transparency purposes.

Many organizations create an overarching general privacy policy and use other documents to drill down into specific processes and procedures, such as those concerning the data of employees collected in an investigation, as these may differ from one department to the next. If the organization already has a privacy policy in place, it's best to start with it and revise it for GDPR compliance rather than begin again from scratch.

Examples of general internal privacy policies are hard to come by because they are often considered proprietary, but some have been posted online and can provide a place to start.

An example of an outline for a GDPR-focused privacy policy may look something like this:

- **Purpose or Privacy Mission Statement.** This is a broad-based statement of commitment to data protection and privacy principles by the organization.

- **Definitions.** Some key words to be used in the document require definition, especially if they have legal significance. Examples include: personal data, data subject, data processing, data processor and data controller, third parties and vendors, consent, profiling, special categories of data, and anonymization. Other terms may be applicable to different organizations depending on the scope of their data processing activities.

- **Responsibilities/Accountability.** Here is the place to make it clear where responsibility lies within the organization (e.g., privacy lead, DPO, chief executives, staff). This may also be a good place to prominently place the DPO's and/or privacy leader's contact information.

- **Principles for Processing Data.** Many policies use the Fair Information Practice principles, restated in the GDPR, to organize and explain internal organizational data protection and privacy policies.

- **Reliable, Lawful and Fair Data Processing.** Here is where lawful bases may be broadly described for different data processing activities, tracking against the data inventory and map. For example, data processing to fulfill contractual relationships, data processing pursuant to legitimate interests. consent-based processing, processing to satisfy a legal obligation, and the general category of direct marketing may be appropriate headings.

- **Transferring Data to Non-EU Countries:** This section can serve as a place to list the organization's plans for complying with Chapter V of the GDPR.

- **Data Retention:**The GDPR makes explicit that personal data should be stored no longer than necessary, unless maintained for historical, archival, research, or statistical purposes. For each processing activity and lawful basis of processing, then, a retention plan must be in place. This will likely require detail beyond the scope of the broad-based privacy policy, but reference to a detailed data retention policy and to the storage limitation principle is appropriate in a privacy policy.

- **Data Subjects' Rights:** These rights will help define data protection processing within an organization and understanding them will help employees comply with the GDPR. By outlining them in the policy, moreover, a privacy leader can help focus attention during training on these core rights: information access, rectification and supplementation, objection to processing, data erasure, objection to profiling, restriction of processing, and data portability

- **Confidentiality and Access Controls:** Akin to but slightly separate from technical security measures are principles of maintaining confidentiality of not only personal data but also other corporate information. This section encourages the organization to establish and maintain access controls to limit those within the organization who can access, modify, process, and transfer personal and confidential information.

- **Security:** Separate written security and incident response plans are crucial, but because security is a feature of privacy, it's important to mention that physical, technical and administrative security are core operational values. Here is one place to alert employees to the Chief Information Security Officer or equivalent role.

- **Data Incidents:** The privacy policy may also mention what to do in the event of a privacy incident, including a reminder to inform and consult the DPO, and should also point to the company's incident response plan for additional information.

- **Key Contacts (e.g., privacy leader, DPO, CISO, etc.).** This information should appear prominently in the policy.

Of course, this high-level explanation of privacy's importance to an organization does not necessarily tell employees precisely what to do in all situations. Accordingly, more detailed guidelines may be required depending on the type of data the organization processes and the size and complexity of the organization.

Once a policy is in place, training can begin, since training to the law is not nearly as effective as training to an organizational policy.

## Training

The GDPR rather subtly requires training. Under Article 39, the DPO is obliged to monitor the organization's compliance with the GDPR, including keeping track of "awareness-raising and training of staff involved in processing operations."

Training and awareness-raising is an age-old responsibility of privacy professionals, especially privacy leadership. Nonetheless, only in last year's Privacy Governance Report did privacy professionals for the first time cite investing in training as their number one tactic for GDPR compliance. In a separate study, they listed training staff on data protection and privacy as the top mitigation tool for 10 out of 11 perceived GDPR-compliance risks.

Engaging staff at least annually in privacy training can help reduce the risk of data breach, enhance consumer trust through more overt attention to privacy company-wide, increase the likelihood that new data processing activities — including the use of new technical tools — are brought to the DPO's attention in a timely manner for risk assessment and record keeping, and enhance the potential for privacy by design and default in new products, services, and systems.

For many privacy professionals, translating the GDPR into human-readable language is a tall order — especially for U.S. privacy professionals, who cited the law's complexity as the top reason for not complying by the May 25 deadline. A good privacy policy can launch training off on the right foot, however, and, regardless of friction, training employees to understand the vocabulary and main requirements of the GDPR is a task that must be accomplished as part of any compliance program.

# 4 Data Protection Impact Assessments and Data Protection by Design and by Default

The GDPR takes a risk-based approach to data protection. Under the regulation, data controllers' and data processors' responsibilities are calibrated to the likelihood and severity of the risks of data-processing operations. Recital 76 suggests that risks should be assessed in an "objective" manner "by which it is established whether data processing operations involve a risk or a high risk." Where initial risk analysis flags a potential high risk to individuals' privacy rights, it triggers a formal DPIA obligation under the GDPR.

Organizations should not only conduct risk assessments on a regular basis, but also each time they commence new personal data processing activities or implement new data processing tools. GDPR Recital 75 suggests risk "may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage..."

Initial risk assessments are appropriate before embarking on a more formal data protection impact assessment. This is because DPIAs are not required in all instances. Moreover, calling everything a DPIA may trigger unwarranted regulatory compliance obligations and dilute the operational significance of a meaningful DPIA.

The distinction between DPIAs, privacy impact assessments (PIAs), and risk assessments is not clear cut. Considering the complexity of the data processing operations and also the concept of risk itself, it's understandable that people in the industry often lump all three together. Here, we use the term "risk assessment" to refer to the initial analysis of the data processing operations to determine the level of risk, and whether a DPIA should even be conducted.

## How to conduct data processing risk assessments

Risk assessments can be conducted in a variety of ways, with manual paper processing, spreadsheets, email and in-person meetings, as well as with tools developed for such activities. They typically involve a standard set of questions designed to identify high risks to the rights and freedoms of data subjects.

*Initial risk assessments are appropriate before embarking on a more formal data protection impact assessment.*

As recommended by the U.K.'s Information Commissioner's Office, questions that should be asked prior to conducting a DPIA include:

- Does the program involve the collection of new information about individuals?
- Does the program require individuals to provide information about themselves?
- Does the program involve making decisions or taking actions that can have a significant impact on individuals?

For each risk identified (e.g., illegitimate access, loss of personal data, repurposing, data-based discrimination, etc.), a company should take account of the threat source and estimate the risk's likelihood and severity. While there is no standard framework for conducting such an analysis, CNIL's Methodology for Privacy Risk Management and NIST's Risk Management Framework are two useful sources for guidance in assessing privacy and data protection risks.

Other risk analysis frameworks, such as the Future of Privacy Forum's analysis of potential harms from automated decision-making, apply to certain organizational processes or operational concerns.

If the program involves new technology that could be perceived as invasive (e.g., biometrics or facial recognition), collects the kinds of information that can raise privacy concerns (e.g., health or criminal records), or contacts individuals in a way that they may find privacy-intrusive, a DPIA is likely called for.

## When are DPIAs required?

After May 25, 2018, DPIAs will become mandatory under Article 35 of the GDPR for organizations that engage in data processing that is "likely to result in a high risk to the rights and freedoms of natural persons."

The GDPR provides a non-exhaustive list of conditions that trigger a mandatory requirement to conduct a DPIA. For example, a DPIA will be required if data processing activities involve a "systematic and extensive evaluation of personal aspects" based on automated processing, the processing of large-scale sensitive data, or the "systematic monitoring of a publicly accessible area on a large scale." Conversely, there are several circumstances where an organization is not obligated to conduct a DPIA. When the processing has already been authorized or has a legal basis in EU or Member State law, a DPIA is not required. Processing that is not likely to result in a high risk also does not trigger the DPIA requirement.

The Article 29 Working Party offers several rules of thumb that can serve as useful guidance for determining when data-processing activities meet the "high risk" standard. Namely, an organization should consider a DPIA if it engages in any of the following data processing activities:

- Profiling, evaluating, or scoring data subjects (e.g., for predictive purposes).
- Automated-decision making.
- Systematic monitoring.
- Processing sensitive data or data of a highly personal nature.
- Large-scale data processing.
- Matching or combining data sets.
- Processing data concerning vulnerable data subjects.
- Innovative uses or applications of new technological or organizational solutions to personal data.

## How to conduct a DPIA

Organizations that have undertaken an initial risk assessment will typically have already satisfied the first task of a full-scale DPIA, which is to systematically evaluate the organization's data-processing operations and their purposes. The results of the initial risk assessments as well as data-inventory and data-mapping processes can serve as a point of departure for a DPIA. If not already documented, any legitimate interests pursued by the processing should also be determined at this stage.

The GDPR does not provide a definition of the DPIA process, but it states that it should contain at least "a systematic description" of "the purposes" and an "assessment of necessity and proportionality" of envisaged data processing activities, as well as "assessment of the risks to the rights and freedoms of data subjects" and "measures envisaged to address the risks."

DPIAs are intended as a tool companies can use to manage risks to data subjects. Data controllers should "seek the views of data subjects or their representatives on the intended processing," as well as consult with their data protection officers while conducting the DPIAs. It is also crucial to take into account the different risks that are unique to various stages of the information lifecycle, from collection to retention and dissemination.

DPIAs can and should be conducted with the involvement of both internal and external actors. The Irish Data Protection Commissioner (DPC) suggests that people with deep knowledge and expertise on the

relevant operational projects should lead the DPIA. For organizations with insufficient experience and knowledge and for projects likely to involve high levels of risk for a large number of people, the Irish DPC also recommends the use of an external DPIA specialist. Moreover, it emphasizes the importance of "a wide internal consultation" to receive feedback from people that are involved in the processing operations, such as developers, engineers, and public relations teams, to better communicate with external stakeholders regarding the results of the DPIAs.

Some data protection professionals also rely on technological tools to assist them in the DPIA process. For example, both Avepoint and OneTrust offer PIA and DPIA automation tools for IAPP members that can be used to tailor the questions asked to a particular business, flag risks, and generate metrics and reports.

Once data risks are discovered and documented, an organization conducting a DPIA should proceed to determine and implement measures to address those risks. In general, risk treatment includes various measures, such as: deciding to not proceed with an activity that gives rise to the risk; removing the source of the risk; changing the likelihood and/or consequences of the risk; avoiding the risk; accepting the risk; or sharing the risk with another party or parties (such as through contracting or financing). However, some risk-mitigation measures create new risks themselves, so it is important to be cognizant of these as well. For example, creating a third-party relationship to address a risk (e.g., contracting with an identity provider for authentication services) can increase risk for an organization if the third-party fails to or inadequately performs the functions it was contracted for, mismanages data, or does not comply with relevant laws and regulations.

Since every organization's data-processing operation is unique, no two DPIAs will look exactly alike. Thus, specific measures that should be taken to mitigate risks identified in a DPIA will depend not only on the threats identified, but also on the data protection program and nature of the organization itself. Specific security and privacy controls include access control, awareness and training, and having a contingency plan in case an adverse event were to occur. Encrypting data, keeping personal data to a minimum, and de-identifying data are also examples of concrete actions a data controller or processor can take to mitigate risks. Communicating and sharing information about the results of risk analysis both with decision-makers and appropriate personnel are also important steps that can serve to mitigate an organization's exposure to risk.

As Recital 84 states, if a data controller cannot mitigate the risks of processing using appropriate measures, it must consult with the supervisory authority before proceeding with the processing operation. To assist in this, it is important to develop a working relationship and a channel of communication with your DPA discussed in Chapter 10.

*Since every organization's data-processing operation is unique, no two DPIAs will look exactly alike.*

As between data controllers and processors, the ultimate responsibility to ensure DPIAs are carried out properly falls on the data controller. As the Article 29 Working Party explains, however, while the controller is ultimately accountable, "the processor should assist the controller in carrying out the DPIA and provide any necessary information." Moreover, for the purposes of a DPIA, Article 35 states that compliance with approved codes of conduct by data processors "shall be taken into due account in assessing the impact of the processing operations performed by such … processors."

In sum, to be effective and GDPR-compliant, companies should bake DPIAs into a process of continuous assessment. Post GDPR, controllers will have to continuously and rigorously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons."

## Data protection by design and by default

In addition to the requirements on data controllers to conduct DPIAs, the GDPR also legally obliges data controllers to implement "data protection by design and by default." Article 25 lays out these obligations, defining it as "appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, … and to integrate the necessary safeguards into the processing." The measures should adhere to the principle of purpose limitation by ensuring that only the personal data necessary for each specific purpose of the processing are processed "by default." The amount of data collected, the extent of the data processing operations, and the period of storage and accessibility are fundamental considerations in data protection by default.

Although the terms "data protection by design" and "data protection by default" overlap and are often used interchangeably, there are differences between them. Ruth Boardman explains what data protection by default is by using social media settings as an example. As Facebook users know, a post can be shared with all of one's friends (and the friends of anyone tagged), a specific group of friends, or made publicly available for all people on and off Facebook to see. Data protection by default would mean that the system is preconfigured to the most privacy-friendly setting (e.g., posts would be shared with specific friends only) unless the data subject voluntarily or actively chooses to change it. Essentially, data protection by default builds a data processing operation so that "[n]o action is required on the part of the individual to protect their privacy – it is built into the system, by default."

A common approach in practice is that, just as data processing risks assessments and DPIAs flow from processes such as data inventory and data mapping, data protection by design builds upon the results of such risk assessments and DPIAs. Indeed, data protection by design should be "hinged on the privacy risks," especially those that DPIAs help to identify.

> *In the end, doing privacy by design well requires knowledge of both the business and the privacy program.*

At the same time, however, data protection by design is not about simply applying patches or fixes to the privacy risks that have been identified. As Jason Cronk puts it in an IAPP white paper, "The bare essence of privacy by design is that the original design should consider privacy, not be a hodgepodge of miscellaneous solutions 'bolted on.'" Data protection by design is better conceived as a holistic or strategic approach to design, rather a laundry list of operational responses to privacy threats, and it requires promoting privacy and data protection "from the start." Indeed, instead of trying to implement every control imaginable, organizations should create data protection by design programs "as a fit-for-purpose implementation."

In the end, doing privacy by design well requires knowledge of both the business and the privacy program. The current program's maturity, the industry, what types of personal information the organization is collecting, and their risk levels should be taken into account. Moreover, data protection by design should consider not only the privacy environment (including legislative, regulatory, industry, and jurisdictional privacy requirements), but also the organization's culture. For large organizations, keeping internal audit in the loop is also essential. They will often have the information, or be able to do the fact-finding, to help privacy professionals leverage the available resources.

# 5 Data-Retention and Record-Keeping Policies and Systems

For data retention policies and procedures, we have good news and bad news.

The good news is that the GDPR's requirements on data retention are, for a change, not complicated or difficult to understand. Indeed, the EU Data Protection Directive and the privacy laws of other countries such as Canada's PIPEDA have long required that data not be retained or processed longer than the minimum necessary. The GDPR's data retention requirements merely implement the use limitation principle of the traditional Fair Information Practices: Keep personal data only so long as necessary to fulfill the original basis for collecting and processing it — and no longer.

The bad news is that actually following through on this requirement and deleting personal data is one of the most difficult tasks an organization may attempt and many organizations are already woefully out of compliance with current privacy laws. After all, it is human nature to hoard and save in case something may be useful, valuable, or necessary later. Information — especially the personal data of former customers who may become future customers — is inherently valuable to an organization. Moreover, what are the chances of getting caught? Enforcement actions are rarely brought merely on an organization's excessive data retention practices; that is, unless they are discovered following a security breach.

The GDPR commands that these hoarding instincts be overcome.

Article 5 sets forth the general principles applicable to personal data processing and commands, under 5(1)(e), that personal data "be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." Logically, prolonged storage is permitted if the data is anonymized and thus no longer "permits identification" of a data subject.

Noncompliance with Article 5 triggers potential administrative fines up to 20,000,000 Euro or four percent of global annual turnover.

Organizations that have failed to routinely purge personal data that is no longer being processed for its original purpose will struggle mightily to meet the Article 5 retention restrictions by the

*The GDPR commands that these hoarding instincts be overcome.*

May 25 GDPR implementation deadline. Wholesale data destruction efforts might compromise systems if data is kept in an unstructured format and even structured data can be difficult to delete. Many commercial customer relations management (often called CRM) systems are not set up to allow for complete destruction of records, requiring that fields be written over with anonymizing text rather than deleted altogether. This is incredibly time consuming and for many organizations will require additional headcount — or at least overtime — to complete data erasure by the deadline. Indeed, for commercial CRMs – like Salesforce, for example – format changes (a classic opportunity for privacy by design) may be required in the future to help controller clients more easily meet data destruction requirements under the GDPR.

Until then, organizations will be in triage mode. This requires identifying which personal data will present the greatest risk to the data subject if kept beyond its processing shelf life, and by extension will be of greatest risk to the organization should its unlawful retention be discovered. Here, the organization's data mapping and inventory efforts will pay off, as data should already have been risk-rated in that process.

It's also crucial to refer to the lawful basis assigned to the original processing because that will help determine whether processing is still being pursued on that basis, or whether such basis has expired. Although Article 5(1)(e)'s data retention language references the expiration of the "purposes for which personal data are processed," and Article 6 discusses the lawfulness of processing generally, it is logical to connect the processing "purpose" to its "basis" as those terms are often cross-referenced in Article 6 (e.g. "the purpose of the processing shall be determined in that legal basis," or "the processing is necessary for the purposes of the legitimate interests of the controller").

The organization's privacy lead must also implement a data retention policy (or amend the existing one) along with its cousin, a data destruction policy, to provide guidance around when and how data is to be deleted and/or destroyed (i.e. when data processing purposes expire for each category of personal data). These policies may be combined, but at a minimum should be referenced in the Article 30 data processing records, discussed below. Such policies will be meaningless, however, unless the highest levels of management are consulted and convinced to support them. The privacy lead or team may draft such polices, but many people within the organization are likely to be involved in complying with them, from the information technology team to customer relations staff. Reliable tools for easing this process — personal data search and discovery, for example — are presently difficult to find and many organizations will have to tediously and manually track down records that are ripe for destruction or anonymization.

The GDPR allows for secondary data processing and for longer data retention in the following circumstances: (a) for archiving purposes in the public interest; and (b) for scientific or historical research purposes or statistical purposes. If retention is for these purposes, it must still be accompanied by "appropriate technical and organisational measures" to safeguard the data subjects' rights and freedoms. Psuedonymization is one such safeguard.

## Article 30 record-keeping requirements

Article 30 of the GDPR requires controllers, processors, and their representatives (where applicable) to maintain records of their data processing activities.

For organizations facing data protection laws for the first time, the Article 30 requirements are new and can seem daunting. Organizations operating under their member state's implementation of the EU Data Protection Directive, however, will find Article 30's requirements familiar territory because they mimic many of the Directive's notice and filing responsibilities. Under the U.K.'s Data Protection Act, for example, organizations processing personal data must register— or "notify" — with the Information Commissioner's Office. The Belgian data protection authority has similar obligations, setting forth a list of required notification information similar to Article 30's requirements. Indeed, Belgium's DPA recently published guidelines for Article 30 compliance suggesting notification compliance should be leveraged for Article 30 record-keeping compliance.

The GDPR lifts the Directive's notification obligations but requires that records kept under Article 30 shall be available to supervisory authorities upon their request.

Much of the information Article 30 requires should have been gathered during the data mapping and inventory process. Indeed, it is possible to combine the efforts, although Article 30 records do not necessarily cover all the requirements a proper mapping and inventory exercise will require. For example, Article 30 mandates that controllers keep records of processing activities along with:

- The name and contact information of the controller, joint controller, the representative where applicable, and the data protection officer.
- The purposes of the processing.
- A description of the categories of data subjects and categories of personal data.
- Categories of recipients to whom the data are or will be disclosed including those in third countries.
- Information on transfers to third countries or international organizations and documentation of suitable safeguards for the transfer. Retention or erasure time limits for categories of data.
- A description of the Article 32(1) technical and organization security measures deployed.

Missing from these required records is an assignment of the lawful basis for processing for each category of personal data and many other GDPR requirements. Thus, relying exclusively on Article 30 recordkeeping requirements may leave an organization without a documented picture of GDPR compliance.

The ICO, for example, recommends that so long as an organization is creating documentation under Article 30, it might also consider adding fields in the records for not only lawful basis, but also records of consent, contracts with processors, data protection impact assessment reports, location of personal data, and even references to security incidents or data breaches. The ICO has developed templates for data controllers and data processors that contain these additional optional fields and that can double as Article 30 reports. The IAPP 2017 Privacy Tech Vendor report also describes commercial tools available to assist companies with Article 30 compliance.

Because Article 30 reports are subject to a regulator's review upon demand, keeping too much information in one place may not be advisable in all cases. It may depend, as well, on who has control over the Article 30 records. A crowd-sourced document such a shared file that many people throughout the organization can update may have the benefit of capturing new data processing activities quickly and efficiently, but it may also contribute to record-keeping errors or misinformation. A field for "data breach" as recommended by the ICO could have legal consequences, so care should be taken in completing that field. Thus, a data inventory and mapping tool, or even a comprehensive record of data processing activities, lawful basis assignment, and security incident tracking may best be controlled by a trained privacy leader or team, and may not be the same document as the Article 30 report. Each organization must decide this for itself.

## Article 30's SME exemption

The final version of the GDPR has few carve-outs for companies with fewer than 250 employees — the consummate "small- and medium-sized enterprises," or SMEs. For the most part SMEs must comply with the GDPR just as large organizations do.

Article 30 offers the one explicit exception. Under subsection 5, controllers and processors "employing fewer than 250 persons" are not obliged to keep records unless their processing:

- Is likely to result in a risk to the rights and freedoms of data subjects.
- Is not occasional.
- Includes special categories of personal data under Article 9(1) or criminal conviction and offences data under Article 10.

For those SMEs hoping to simply ignore Article 30, a note of caution: Any SME already feeling obliged to comply with the GDPR is likely processing data more than "occasionally." Moreover, DPAs such as the Belgian Privacy Commissioner advise keeping records anyway, if not obliged by Article 30.

# 6 Transparency and Privacy Notices

Perhaps the most common privacy practice followed globally is the familiar "notice and choice" paradigm, which typically involves a statement on an organization's website explaining its data processing and security practices and the opportunity (in theory) for consumers to avoid those practices. "Choice" has involved, at least, the opportunity not to share data with the organization by not doing business there. Notice is sometimes accompanied by an opt-in option, though opt-outs are also common.

The GDPR term for "notice" is transparency, and it is a central theme of the Regulation. Part of the core principle of accountability set forth in Article 5 is the requirement that "personal data [be] processed in a transparent manner in relation to the data subject." As set forth in Recital 60, transparency allows data subjects to be informed of the existence and purpose of any processing activity involving their data. Transparency is also about engendering trust in the processes that affect data subjects "by enabling them to understand, and if necessary, challenge those processes."

## Required disclosures

Articles 13 and 14 of the GDPR and associated guidance from the European Commission give the specific information that must be disclosed to data subjects and the required time of disclosure. Which article applies depends on how the data controller comes to possess the personal data. If from the data subject directly, then Article 13 applies. But if the controller receives personal data from a third party – say, by purchasing a list of potential leads or by sponsoring an event and getting the attendees' names from the event host – Article 14 spells out how and when disclosures should be made.

Taken together, however, the types of information that must be disclosed are similar in both articles. Controllers will need to have a privacy notice — discussed below — that is prominently visible on their websites and available by link in commercial email communications with data subjects. Those communicating with data subjects whose contact information was provided by others may also want to place the information in the body of the first email communication, but

*The GDPR term for "notice" is transparency, and it is a central theme of the Regulation.*

at a minimum should include a link to their website's privacy notice. Finally, much of the information required to be disclosed is similar to what will be needed if a data subject exercises a right of data access, so the transparency disclosure may be used in a variety of different places and contexts.

When data is obtained directly from a data subject, Article 13 requires that disclosure occur "at the time when personal data are obtained" and include:

- The identity and contact details of the controller and, where applicable, the controller's representative, as well as the contact details of the controller's data protection officer.
- The intended purposes and legal basis of the processing. This information should already be available from the data mapping and inventory exercise conducted early in the GDPR compliance process, but should be explained in plain and unambiguous language in the privacy notice.
- If applicable, the legitimate interests pursued by the controller or by a third party. This reflects the lawful basis analysis the organization has conducted pursuant to Article 6.
- Data mapping and inventory as well as Article 30 record keeping efforts will inform the following required transparency disclosures:
  - The recipients or categories of recipients of the personal data.
  - Any transfers of personal data to a third country or international organization and the existence or absence of an adequacy decision for such a transfer, or reliance on Articles 46 or 47, or Article 49(1), as well as references to the appropriate or suitable safeguards.
  - The period for which the data will be stored or the criteria used to determine that period.
- A description of the existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing and the right to data portability.
- If the processing is based on consent, an explanation of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- A description of the right to lodge a complaint with a supervisory authority.
- Whether the provision of personal data is required by statute or contract, or is a requirement necessary to enter a contract, whether the data subject is obliged to provide the personal data, and the possible consequences of failure to provide such data.

- The existence of any automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If a controller intends to process already-collected personal data for a purpose different than the one disclosed when the data was collected, it must inform the data subject of the new purpose, and provide any relevant further information, prior to the new processing.

Under Article 13, controllers are exempted from disclosure requirements only "where and insofar as the data subject already has the information." Companies that wish to make use of this exemption should take care — the Article 29 Working Party notes that controllers must document what information a data subject has, how and when it was received, and that no changes have occurred that would put it out of date. Such documentation could be a feature of comprehensive Article 30 record keeping.

When data is obtained from a source other than the data subject, Article 14 requires that controllers meet the same disclosure requirements described in Article 13, and additionally disclose: (a) the categories of personal data concerned in the processing; and (b) the source from which the personal data originated, including whether it came from publicly accessible sources. This must be done "within a reasonable period after obtaining the personal data, but at the latest within one month," except when the controller communicates directly with the data subject or passes along the information to yet another third party, in which case disclosure must occur right away.

Controllers subject to Article 14 have more exceptions from disclosure than those subject to Article 13, although the Working Party cautions that the exceptions should be interpreted narrowly. Exceptions include the data subject's prior possession of the information; impossibility of or disproportionate effort in disclosure (such as when personal data is acquired for scientific or historical research purposes or statistical purposes), in which case a publicly available privacy notice should suffice; when member state law provides otherwise; or where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or member state law, including a statutory obligation of secrecy.

For example, historical researchers who have obtained a large dataset collected 50 years ago, which has not been updated since, and does not contain any contact details for data subjects, might qualify for the "disproportionality" exception. A professional secrecy exemption might apply when a bank does not inform an account holder that the bank has passed data to a financial law enforcement authority, in compliance with an anti-money laundering statute making such a "tip-off" a crime. Even in the latter scenario, to comport with transparency principles, the bank should provide "general information" to all new customers that their data may be processed for anti-money-laundering purposes.

## Crafting a GDPR-compliant privacy notice

Pursuant to Article 12(1), as well as Recital 39 and Recital 58, privacy notices should be concise, transparent, intelligible, easily accessible, and easy to understand, using "clear and plain language, and where appropriate, visualization." If the processing relates to a child, the disclosure should be easily understandable by the child.

The WP29 suggests that compliance with the intelligibility requirement should be regularly checked to ensure that "the information/communication is still tailored to the actual audience" and that user panels could provide an effective mechanism for doing so. "Hall tests" or live user trials should be conducted and documented in advance of processing "going live." The WP29 cautions against the use of overly complex sentence and language structures, and warns organizations not to phrase policies in "abstract or ambivalent terms, or leave room for different interpretations," particularly regarding the purposes of and legal basis for the processing of personal data. Organizations are specifically encouraged to avoid using the passive voice or indeterminate qualifiers like "may," "might," "some," "often," and "possible." Guidance on creating specific and informed consent may be useful in the broader transparency context, particularly in regard to the intelligibility requirement.

Notices can be presented to data subjects in written form, orally, or in an electronic format, where appropriate. Web-based privacy notices should be clearly visible on each page of the website under a commonly used term such as "Privacy Notice" or "Data Protection Notice." A website's layout and format must not be manipulated to make privacy disclosures more difficult to find — for example, altering the size or color of a privacy policy's hyperlink to make it more challenging to locate will violate the requirement of accessibility.

For the collection of personal data via apps, the Working Party advises that transparency requirements should be met in the online store prior to download, and after installation "should never be more than two taps away." As a general rule, this means menu functionality should include a "Privacy" or "Data Protection" option that links to the relevant policy.

The WP29 recommends the use of "layered" privacy notices in the online context, which should allow the data subject to navigate to whichever part of the privacy statement they wish to access without being required to scroll through large amounts of text. An effective layered notice is not simply a group of nested webpages — the design and layout of the first layer "should be such that the data subject has a clear overview of the information available to them" and need only expand sections for greater detail. Organizations should take care to avoid providing conflicting information within different layers of a policy. Microsoft's privacy statement is a good example of a layered privacy notice.

The U.K. Information Commissioner's Office also provides guidance on how to effectively structure a privacy notice. The ICO reiterates the points that privacy notices should include the identity of the controller, the intended use of the personal data being collected, and the identity of any parties with

whom the data will be shared. It's also wise to prominently identify and provide contact information for the organization's DPO (or whoever handles subject access requests if you don't have a DPO).

## Alternatives to layered notices

The WP29 suggests several methods of providing transparency information in lieu of or in addition to a layered privacy notice. These include "just-in-time" push notices, or "pull" notices such as permission management interfaces and "learn more" tutorial options. A "just-in-time" notice will provide specific privacy information when it is most relevant to the data subject — for example, during an online purchase a pop-up next to a field requesting the purchaser's telephone number might explain that the information is only being collected concerning contact related to the purchase and will only be disclosed to the relevant delivery service.

For organizations supplying services that span multiple devices, a "privacy dashboard" that allows data subjects to access and control the use of their personal data in multiple contexts may be appropriate.

Transparency must always be based on the circumstances of the data collection and processing; although the WP29's position favors electronic privacy notices for data controllers with a digital or online presence, other formats of disclosure may sometimes be required. Alternatives may include hard copy notices with written explanations or notices included in leaflets, infographics or flowcharts for contracts concluded via post; oral explanations provided via telephone either by a real person or automated system that includes options to access more detailed information; icons, voice alerts, QR codes, SMS messages, or written information included on IoT devices; or visible, real-world signage or newspaper and media notices for real-world recording by CCTV or drone.

Special requirements attach to any processing that qualifies as automated decision-making under Article 22(1). The Working Party has issued guidance that addresses this situation. Broadly, organizations utilizing automated decision-making are obligated to inform data subjects that it is occurring, and "find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision." The Working Party suggests that disclosures should focus on "real, tangible examples of the type of possible effects" of the automated processing. For instance, if a data subject's age would put them in a specific category for marketing materials, the organization should explain that providing their age will expose them to specific and targeted marketing materials.

Although Recital 60 allows for the use of standardized icons as part of an organization's transparency disclosures, the use of such icons "should not simply replace information necessary for the exercise of a data subject's rights." Icons that are presented electronically should be machine-readable, although the use of icons may be appropriate in other contexts. Examples might include physical paperwork, the exterior of IoT devices or device packaging, or public notices concerning Wi-Fi tracing or CCTV recording. Any use of icons for transparency purposes is dependent on forthcoming decisions by the European Commission standardizing their meaning and permissible use.

# 7 Accommodating Data Subjects' Rights

Accommodating data subjects' rights can be one of most nuanced and challenging areas of GDPR implementation. Indeed, as the IAPP-EY Annual Privacy Governance Report 2017 demonstrated, data portability, the right to be forgotten, and gathering explicit consent are perceived as the most difficult issues for privacy professionals. One suggested way of tackling these issues is not to consider them as separate workstreams, but to think of them as the same question asked in different ways.

Generally speaking, data subjects can request access to a copy of their personal data and to a variety of other information, such as the purpose of processing, categories of data that are processed, information on the parties to which their personal data have been disclosed (specifically, recipients in third countries), and retention periods. In addition, responses to these requests need to be given within a short time frame. Data subjects have the right to request rectification of inaccurate personal information "without undue delay," or to have incomplete personal information completed. Similarly, the right to be forgotten gives data subjects the right to request the erasure of their personal data "without undue delay" under certain circumstances (e.g., when the personal data is no longer necessary for the collection purposes, when consent is withdrawn, or when the processing is unlawful).

In addition to having systems for deletion in place, organizations also need to be capable of halting processing activities, as individuals can also ask to restrict the processing under certain circumstances, including when the accuracy of the data is contested, the processing is no longer necessary, or when the subject objects to it. Organizations also need to create communication channels where they can inform recipients about erasure or rectification of data unless such a task can be proved to be impossible. Individuals can also request their data be transferred to another controller and object to data processing under certain circumstances.

Individuals' rights, their application, and limitations to them are crafted in detail under the GDPR. To be able to actually respond to data subjects' rights in practice, the Irish Data Protection Commissioner (DPC) suggests asking the following questions as part of an organization's GDPR readiness checklist:

- Is there a documented policy or procedure to address Data Subject Access Requests (now commonly referred to as DSARs)?
- Is your organization able to respond to DSARs within one month?
- Are there procedures in place to provide personal data to data subjects in a structured, commonly used, and machine-readable format?
- Where applicable, are there mechanisms in place to allow personal data to be deleted or rectified?

*Individuals' rights, their application, and limitations to them are crafted in detail under the GDPR.*

- Are there mechanisms in place to stop the processing of personal data when a data subject seeks to restrict the processing?
- Are individuals informed about their right to object to certain types of processing?
- Are there mechanisms in place to stop the processing of personal data when individuals object to it?

## Building upon established systems

The first step to creating a data subject response system is to find out what is already in place. Does the organization have procedures for channeling customer questions to people who have the ability to validate the customer's identity and respond meaningfully to the request? Is there a pattern and practice of involving the data protection officer in the chain of communication? How are records of requests and responses currently kept, including records of how long it takes to respond?

Data subjects need a way to exercise their rights — either independently through an automated system or by contacting the organization directly. Making this process transparent and easy is key not only to good customer relations and to fulfilling the organization's transparency obligations, but to ensuring that data subjects feel comfortable bringing their complaints directly to the organization and not, at least at first, to the regulator.

## Automation

Some organizations maintain customer information in accounts specific to the customer and to which the customer may have access, perhaps via a user name and password. Such systems can empower data subjects to maintain the accuracy of their own records, and possibly even gain access to at least some of their personal data the organization processes. Indeed, Recital 63 encourages controllers, where possible, to provide "remote access to a secure system" that allows direct access to the data subject's personal data. Such subject access processes must be built with database management and programming staff and without compromising security.

The simplicity suggested by Recital 63 belies a fundamental dilemma controllers face, however. Indeed, one of the major issues confronting data controllers is the extremely broad definition of personal data. For data mapping and inventory exercises, as well as for lawful basis assignment and the like, many

categories and types of personal data may be identified and steps taken to segregate direct identifiers from indirect ones. But even indirect identifiers may fall under the scope of a general data access requests. In their guidance on data portability, the Article 29 Working Party states that, in addition to the data that is "actively and knowingly provided by the data subject," observed data provided by the data subject by virtue of the use of the service or device (e.g., search history, location data, and "raw data" tracked by a wearable technology) may fall under data "provided by the data subject" and be covered by the right to access and portability.

Recital 63 provides that, when the controller processes a large quantity of information concerning a data subject, the controller may request that the data subject "specify the information or processing activities to which the request relates." Most data subjects will seek only the most basic, directly identifying, profile information, which may be more easily automated. And Recital 64 clearly counsels against keeping data subject to routine destruction merely to respond to a potential access request. Still, for many controllers, the potential scope of "personal data" responsive to subject access requests will be very broad indeed and practical solutions for minimizing operational headaches are elusive.

## People, process and technology

Article 37(4) provides that data subjects should be able to contact an organization's DPO for "all issues related to processing of their data and to the exercise of their rights." Accordingly, the ideal first point of contact for data subjects is the DPO, which should be clearly stated in privacy notices and other data subject communications.

Because the DPO is not likely to also have the job of inputting, correcting, or deleting data, and indeed should be free from conflicts of interest in that regard, the DPO will need to develop a system for working with others to evaluate and respond to data subjects. This system must record the time of the response, the unit or the person that responded to the request, as well as an explanation of the response. While this might be carried out in manual processes at the beginning through spreadsheets — depending on the extent and the frequency of the data subject requests — technological tools or more sophisticated solutions may be used. Currently, most organizations manually manage processing involving data subjects' rights, but there are also tools in the market for these tasks. Currently, these technologies do not yet seem to have been significantly incorporated into businesses practices, but this may vary depending on the maturity of the market and organizational needs.

There is nothing like receiving a data subject request to focus the mind on the problem. But for those organizations anticipating such requests, a good strategy is to prepare standard templates with answers to questions that most people are likely to ask — such as types of data collected about them, collection methods, and retention policies. This information should already be readily available to data subjects in publicly accessible privacy notices, but placing it at the hands of customer service personnel is also key.

> *Costs and response times can be minimized if databases containing personal data are searchable and as accurate as possible.*

Importantly, as much as building new systems and responding to requests costs an organization time and money, responses to DSARs should be free of charge — or for a "reasonable fee" if the request is excessive — and without delay. In case an organization does not accept the DSAR, they need to provide reasons for it and inform the data subject that they have a right to complain about it to their local data protection authority.

Costs and response times can be minimized if databases containing personal data are searchable and as accurate as possible. Strictly adhering to data destruction policies can also ease the burden of responding to DSARs and other requests, including rights of erasure. The GDPR is clear that data should not be retained merely in anticipation of data subject requests. In some places, the system might not be set up well due to either data being spread across multiple systems or data not being recorded correctly. Organizations should regularly audit their systems to ensure data collection and retention procedures are clear and enforced.

## Portability

Data subjects have a right to receive their personal data that they have provided to the data controller "in a structured, commonly used and machine-readable format" when the data is processed by "automated means." In addition, they can request data controllers to transmit their personal data to another controller "when technically feasible." While the GDPR does not oblige data controllers to "adopt or maintain" "technically compatible" systems, they are "encouraged to develop interoperable formats that enable data portability." The Article 29 Working Party suggests paying "special attention" "to the format of the transmitted data, so as to guarantee that the data can be re-used, with little effort, by the data subject or another data controller."

Organizations, therefore, need to ensure that the applications and systems that house the data can port personal data easily. The Article 29 Working Party recommends data controllers begin to develop the means by which data portability requests will be answered, such as through download tools or application programming interfaces. Most data controllers may prefer the use of an "automated tool that allows extraction of relevant data" when large and complex data sets are involved, as this can minimize privacy risk.

These tasks may not, however, be as straightforward as organizations wish, especially those that have unstructured data. Organizations need a deployable and easy-to-use tool that can help them to mine unstructured data. This seems to be an area where organizations are in most need of automated solutions, as right now they are mainly relying on manual processes.

## Erasure

The GDPR provides that data subjects have the right to request erasure of their personal data from the controller on certain conditions, such as when:

- "[T]he personal data are no longer necessary" for the original purposes of data collection or processing.
- The data subject withdraws the consent which was the basis of data processing, and when "there is no other legal ground for the processing."
- The data subject objects to data processing and "… no overriding legitimate grounds for the processing" exists.
- "The personal data have been unlawfully processed."
- The erasure is necessary to comply with the Union or member state law.
- The personal data was collected in relation to services referred in "conditions applicable to child's consent," such as if the data subject gave his or her consent as a child but was unaware of the risks.

Moreover, to strengthen this right in the "online environment," data controllers that have made the personal data public and are required to erase the data have to take reasonable steps to inform controllers who "are processing such personal data to erase any links to, or copies or replications of those personal data," in light of "available technology and cost of implementation."

The scope and practical application of the right to be forgotten and the right to erasure, however, have been the subject of heated debate, and these rights are not absolute. Obligations on data controllers to erase personal data and inform third parties do not apply "to the extent that processing is necessary" for various reasons, including:

- Exercising freedom of expression and freedom of information.
- Complying with Union or member state law.
- Performing a task for the "public interest…in the area of public health" or "for archiving purposes…scientific or historical research purposes," or "in the exercise of official authority vested in the controller."
- Establishing, exercising, or defending legal claims.

Practically speaking, moreover, organizations may find that maintaining a data subject's contact information is necessary to prevent communicating with the data subject in the event they request not to be contacted.

Where GDPR deletion requirements conflict with EU member state archiving requirements, organizations should set up a schedule for archiving per document and per data set, which would include a maximum period of storage or the length for which the data can be only held for that purpose.

## Authentication

Finally, most privacy professionals are concerned with making sure the request is legitimate and comes from the actual data subject. There are several reasonable steps data controllers can take to authenticate individuals, requiring users to provide "something one knows (e.g. passwords or passphrases), something one has (e.g. a security token) and something one is (e.g. biometric information)."

Decision-making around accommodating data subjects rights is not a single-person activity. Rather, it is a team-driven effort involving people who know the business, lawyers and privacy professionals that know the extent of the law and legal requirements, employees from human resources that deal with a variety of information, and IT teams that have the relevant knowledge about data systems, processes and data transfers.

## Collaboration

To ease the challenges associated with configuring systems to accommodate data subjects' rights, it is critical to be aware of the systems and processes in place as well as constantly work to find ways to address weaknesses. Most importantly, it is essential to strengthen communication with people from different departments and work together to understand the expectations of data subjects, while focusing on the most-likely scenarios.

*Practically speaking, moreover, organizations may find that maintaining a data subject's contact information is necessary to prevent communicating with the data subject in the event they request not to be contacted.*

# 8 Data Breach Response

Security incidents are common. Perhaps someone leaves a secure door unlocked or a sensitive paper file exposed on their desk. Whether a security incident rises to the level of a "data breach," however, is a legal question.

Under the GDPR, "data breach" is much broader term than under U.S. state data breach laws, for example.

Article 4(12) defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access, personal data transmitted, stored or otherwise processed." Many U.S. security breach laws define "personally identifiable information" as first and last name plus an account number or password, such that fraud or identity theft is possible. But "personal data" is very broadly defined in Article 4 of the GDPR as "any information relating to an identified or identifiable natural person."

Organizations seeking to minimize data breach risk under any law should consider three general steps: planning to detect and contain an incident; steps for breach response (including notification if necessary); and cyber insurance.

## Breach preparation

As with all processing activity, the first step in effective preparation is understanding what data the organization has through data mapping and inventory. Multiple GDPR provisions evaluate controller responses to breach events based on the type of data compromised, so controllers must have an accurate picture of their own data. Indeed, as discussed below, data subject notification turns on an evaluation of risks to data subjects' rights and freedoms, requiring knowledge of not just data categories but specific data elements as well.

Although not the subject of this post, avoiding a breach in the first place through effective data security is obviously a crucial breach preparation task. The GDPR requires controllers and processors to implement appropriate technical and operational security measures, proportionate to the risk facing the rights and freedoms of data subjects. Technical security measures like pseudonymization and encryption of data are encouraged, but may not be fully sufficient for compliance; Article 32 also requires controllers to put in place appropriate "organizational measures" as well. These measures include a breach response plan, ideally one drafted in collaboration with the information security team, the privacy leader, risk management, compliance personnel, firm management, and perhaps also public relations and communications staff as well.

A good response plan will dictate who must be notified within a company once a potential breach has been discovered or reported. Potentially serious events should be brought to the attention of a company's legal representatives and senior management so that a unified response can be coordinated. Companies should also ensure that breach response plans include a strategy for dealing with any breaches reported by a processor, if applicable. And a short list of which regulators might need to be notified within Article 33's 72-hour breach notification period will aid in compliance should the crisis occur (more about this below).

Some forensic and security capabilities may be managed in-house, but for some organizations – and for some security incidents – outsourcing investigation of the situation may be required. Engaging outside legal counsel to oversee the investigation may provide legal privilege for some components of the investigation, so part of breach preparation is engaging qualified counsel who can assist when needed.

Some experts suggest separating personnel responsible for an organization's security from those tasked with forensic investigations, so that any incident requiring a forensic analysis is approached with unbiased eyes. In larger organizations, this may mean the establishment of a separate, full-time data forensics team, while smaller organizations may wish to identify outside data forensics providers ahead of time to call on in the event of a security incident.

For companies that lack the resources to conduct a proper forensic investigation internally or those that choose an outside vendor, the breach response plan should identify in advance the vendors that will conduct an appropriate investigation, including outside legal counsel. Cyber liability and data breach insurance policies often include networks of professionals that can help organizations with IT forensics, public relations, and other crisis management needs if companies' internal resources are lacking.

Training to prepare for a breach is also crucial. Many data security professionals suggest conducting table-top breach simulations with both relevant IT personnel and C-suite level management as an invaluable tool for preparing the relevant personnel when personal data is compromised. After all, 72 hours for notification is a tight window indeed.

## Breach response and notification

When a security incident is discovered or reported, the DPO should be notified right away. Key first steps are to contain the incident, initiate an investigation of its scope and origins, and ultimately decide if it qualifies as a "breach." Here is another place where effective privacy governance (including training) pays off; all employees should be aware of what constitutes a reportable security concern and should know whom to contact upon discovery. Containing the incident to prevent additional misuse of personal data should be a top priority and this is facilitated by rapid communication to the proper personnel.

If a security incident qualifies as a breach under the GDPR, an organization may be required to notify the relevant supervisory authority and affected data subjects.

As a baseline rule, Recital 85 and Article 33(1) provide that a personal data breach must be reported to the relevant supervisory authority "without undue delay," meaning "where feasible" not later than 72 hours after the controller has become aware of it. Processors are only required to notify controllers "without undue delay" upon discovering a breach.

Recital 87 indicates the determination of whether a notification was "without undue delay" is a fact-based inquiry "taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject." As mentioned above, good breach preparation will include identifying the relevant supervisory authority for each jurisdiction in which the organization operates, as well as the "lead" authority to be contacted in any cross-border incident. It may also help to prepare draft notifications for each to provide a quick basis for the creation of any necessary future notification. Qualified outside counsel will likely also be helpful in meeting these compliance deadlines with the proper notification procedure.

The Regulation requires that controllers' notification to supervisory authorities include several specific pieces of information:

- The nature of the personal data breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records.
- The data protection officer's contact information, or other contact point.
- The likely consequences of the breach.
- A description of how the controller proposes to address the breach, including mitigation efforts.

Controllers are only exempted from reporting to the supervisory authority if they can show that the breach "is unlikely to result in a risk to the rights and freedoms of natural persons." If for any reason notification cannot be achieved in 72 hours, "the reasons for the delay must accompany the notification." Whether or not the supervisory authority is notified, controllers must still document any personal data breaches, recording "the facts relating to … the breach, its effects and the remedial action taken," as authorities may audit such records for compliance with the Regulation.

*For many privacy professionals, the 72-hour window for notification is the most challenging part of the GDPR's data breach requirements.*

For many privacy professionals, the 72-hour window for notification is the most challenging part of the GDPR's data breach requirements. This window begins to close when a company becomes "aware" of a breach, which the Article 29 Working Party's guidance on data breaches (analyzed in more detail here) clarifies to mean when the controller has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." This determination is a fact-based inquiry, and the WP29 gives several examples of situations sufficient to show "awareness," ranging from a controller discovering the loss of a USB containing unencrypted personal data (which creates a breach of availability, even if the controller is unable to confirm that unauthorized persons gained access to the data contained) to the more straightforward example of a cybercriminal demanding a ransom after hacking a controller's systems. The WP29 does note that controllers, upon learning of a potential breach, are permitted a "short period of investigation" to determine whether or not a breach has actually occurred, during which time the controller does not qualify as "aware."

The narrowness of this window is extended only by the limitations of "feasibility," which many data security professionals are hesitant to interpret broadly. As a result, some experts suggest that older breach response plans should be updated to include involving counsel at the earliest stages of the investigative process, to assist security personnel in making the fact-based determinations that will affect whether a notification is required.

Recital 86 and Article 34 further require organizations to inform data subjects of a breach when "that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person." The communication "should describe the nature of the personal data breach as well as offer recommendations [to] mitigate potential adverse effects." A breach notification to a data subject must:

- Include the data protection officer's contact information, or other contact point.
- Explain the likely consequences of the personal data breach.
- Describe how the controller proposes to address the breach, including mitigation efforts.

Communication to a data subject must also be in "clear and plain language," discussed further in our analysis of the GDPR's transparency requirement. Controllers are excepted from notifying data subjects if able to show any of the following:

- The controller has implemented appropriate technical and organizational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Annex B of the Article 29 Working Party guidance on data breaches offers examples of security incidents to help companies chart if notification to supervisory authorities, data subjects, or both is required. Controllers should also note that supervisory authorities retain the power to independently decide to inform data subjects of a breach, even if the company has determined that one of the exceptions applies.

Finally, it is important to recognize that, per Recital 73, Member State law may impose additional specific data breach response requirements beyond those in the Regulation—so companies may be subject to further requirements beyond those described above depending on their specific jurisdiction. Under Article 40, industry associations or other similar bodies may also create codes of conduct for specific market sectors that set forth additional responsibilities for personal data breach notifications.

## Insurance

For organizations with large potential liability, data breach insurance is a critical part of effective breach preparation. Most standard corporate liability insurance policies will not cover data breach exposure, and for data-heavy companies, the combined costs of appropriate forensic investigation, breach notification, legal advice, and potential remuneration to data subjects can be burdensome. Indeed, a 2016 PwC report estimated that the market for cyberinsurance will climb to $7.5 billion in annual premiums by 2020.

Additionally, cyber insurance policies often provide companies with access to "crisis networks" of data forensics experts, outside counsel, specialist PR services, and other high-cost capabilities that may not exist in-house. Coverage comes in different flavors, including data breach liability, computer and network security liability, media liability, and identity theft. With the explosion of connected devices, moreover, comes new opportunities for mishaps and thus new liability policies to cover them.

Because of the range of potential pitfalls that may occur to personal data, and thus create liability for organizations, cyber policies should be reviewed carefully for coverage of the organization's most likely data risks.

# 9 Vetting and Contracting with Processors

The GDPR did not invent vendor management responsibilities. Organizations have long had procurement programs scrutinizing vendor selection on a variety of bases, from financial solvency, to service-level commitments, and beyond. Health-related privacy laws in the U.S., for instance, require business associate agreements for sending personal health information to third parties. And for information privacy and security personnel, the infamous Target data breach underscored the risk of giving third parties access credentials to secure systems housing personal data, raising risk awareness to the highest levels of management.

The GDPR takes vendor selection and agreements to a new level, however. To prepare for this, organizations should:

- Ensure that privacy professionals are notified and brought in to the discussion early for any new program or acquisition that involves sharing personal data with a third party.
- Determine whether the organization in any given transaction is serving as the controller, joint controller, or processor.
- Have the right agreements in place to comply with Articles 27 or 28 of the GDPR as appropriate, as well as Article 46 as necessary.

## Get involved before the deal closes

It's difficult to overstate the importance of having privacy and security professionals involved in vendor selection as early as possible. The best time to insist upon privacy by design in a new system, certain contractual privacy and security assurances, or favorable allocation of liability, is when considering whether to buy; after the purchase order and license agreements have been signed and payments made, the buyer has little leverage to seek technical or legal accommodations. Accordingly, privacy leaders must insist that no contracts be signed with vendors who will have access to personal data unless they have been consulted.

In many cases, the processor's sales staff will not be equipped to provide all the privacy and security answers to the privacy team's questions. Privacy professionals must, therefore, insist

*It's difficult to overstate the importance of having privacy and security professionals involved in vendor selection as early as possible.*

on tracking down and engaging with the vendor's equivalent of their counterpart, if any. The vendor's failure to have a privacy professional available — or a referral exclusively to the security team — might be a red flag that it isn't prepared to safeguard personal data or meet other GDPR compliance concerns.

Engaging a processor may require a risk assessment, perhaps even a data protection impact assessment, depending on the nature of the transaction and the personal data involved. These must be documented and added to any Article 30 records along with the appropriate contracts, as discussed below.

Because a crucial component of maintaining data privacy is security, the security team will also be involved in vetting potential vendors. In most situations, visiting the data processor's facilities to conduct a personal security audit is impractical. Instead, the controller's security professionals will need to confer with the processor's appropriate counterparts. As well, many controllers and processors rely on security audits and certifications as proxy signals for "technical and organizational" safeguards. According to a 2017 IAPP study, the top security credentials privacy professionals seek from vendors is ISO 27001 certification, followed by SOC 2 Privacy, and PCI compliance.

Although these tools have yet to be fully developed, moreover, the codes of conduct and certifications defined and anticipated in GDPR Section 5 (Articles 40 and 42, specifically) may one day help also controllers in processor vetting and selection.

## What role today: Controller or processor?

One of the most determinative distinctions under the GDPR is that between controllers and processors. Controllers bear the brunt of the regulatory burden, including having to legitimize data processing and respond to individual complaints, while processors have it easier. Organizations widely and routinely engage third parties for cloud-based data storage and processing solutions, to assist with shipping or billing processes efficiently, to enhance marketing efforts, and the like. The GDPR defines these third parties as "processors" in Article 4 as a "natural or legal person, public authority, or body, which processes personal data on behalf of the controller." Amazon Web Services, for example, is a prototypical processor. So are, typically, the customer relations management company Salesforce, the human capital management firm Workday, and myriad other software-as-a-service (SaaS) companies supporting organizations globally.

An organization is a "controller" if it "alone or jointly with others determines the purposes and means of the processing of personal data." The GDPR places the bulk of responsibility and liability upon controllers. Nearly all companies — even classic processors — are controllers at some point, at least regarding their employees' data.

Yet even controllers can sometimes serve as processors. Consider, for example, a university that produces an online course in leadership. When it offers the course itself to students, who enroll directly through the university, it is a data controller. But if the university allows businesses to "white label" the

course and offer it internally to their executives, while the college continues hosting the course on its own servers, it may become a processor to the extent the system collects personal data. Depending on the circumstances — if, say, the university grants some form of certification or other acknowledgment to the companies' executives — it may instead be a "joint controller."

These distinctions matter because they govern the type of agreements — if any — that may need to be in place, and the terms GDPR requires in those agreements.

## Data protection agreements

Article 29 explicitly prevents processors from processing personal data except on the controller's instructions. Article 28 provides details on documenting these instructions by written agreement.

Indeed, Article 28 has become such a significant compliance responsibility — forcing itself into daily business transactions — that if it is not printed out and taped to the wall of most privacy professionals, or marked with a dog-eared page, it probably should be.

Specifically, Article 28 requires that controllers "shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." Processors are also restricted by Article 28 from engaging subprocessors without the controller's "prior specific or general written authorization." In the case of general written authorization, the controller must have notice of and an opportunity to object to additional or replacement subprocessors.

Article 28 also requires controllers to enter into a "contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller." The contract must contain the following elements:

- The subject matter, duration, nature, and purposes of the processing.
- The controller's documented instructions governing the processing.
- The type of personal data processed along with categories of data subjects.
- The controller's rights and obligations, and the processor's promises to assist with ensuring the controller's compliance (in particular regarding information security and breach response, as well as respecting and responding to data subject rights).
- Processor obligations to implement technical and organization security measures, to commit employees and contractors to confidentiality, to delete or return all personal data to the controller at the relationship's conclusion, to submit to audits and otherwise provide information necessary to demonstrate compliance with Article 28, and to bind all subprocessor to the GDPR requirements as well.

Already, agreements embodying these terms are flying between controllers and processors, some of them entered — as is ideal — at the beginning of the relationships, but many following on as addenda to earlier-entered agreements. These data protection agreements or addenda contain some commonalities, but also reflect the different bargaining power of the respective parties. For example, Salesforce has produced and published on its website a pre-signed data protection addendum for its customers to download, sign, and store in their record keeping systems. These agreements, for most Salesforce enterprise customers, are not negotiable.

Smaller SaaS providers — particularly if just catching up to GDPR's processor obligations, and especially if approached during the sales cycle rather than after the deal is signed — may yet be open to negotiating the terms of a data protection agreement and to allowing controllers more favorable treatment. Consider, for instance, the controller's right to restrict the use of subprocessors. Under Article 28(2), controllers may require prior specific written authorization for each proposed subprocessor. Processors with leverage, however, may require controllers to agree to prior general written authorization, updating them with any newly engaged subprocessors only by adding names to a list on a website, and perhaps allowing the controller to opt-in to an automated updating email.

Article 28(7) and (8) provide that the European Commission and supervisory authorities may adopt standard contractual clauses for controller-processor and processor-subprocessor agreements.

## Data transfers outside the EU

Article 28 agreements must also address any transfers of personal data outside of the EU. Although the Regulation does not discourage businesses from seeking the most effective and efficient solutions to their information management needs, regardless of geography, it does require that care be taken to safeguard the personal data internationally.

In general, personal data can be transferred to a third country only if certain conductions are met by both the controller and processor. These conditions include that the third country has achieved an "adequacy" designation under Article 45, or that the controller or processor has taken upon themselves to provide "appropriate safeguards" under Article 46.

Among the appropriate safeguards are binding corporate rules (further described in Article 47), approved codes of conduct or certification mechanisms, or "standard data protection clauses" adopted by the Commission or by a supervisory authority (and approved by the Commission). Contractual clauses

*Although the Regulation does not discourage businesses from seeking the most effective and efficient solutions to their information management needs, regardless of geography, it does require that care be taken to safeguard the personal data internationally.*

between controllers and processors may also suffice, under Article 46(3), subject to the authorization from the competent supervisory authority. One example is the AWS data protection addendum, which has Article 29 Working party approval.

While awaiting standard data protection clauses under the GDPR, controllers and processors continue to use the model clauses published by the European Commission pursuant to the Data Protection Directive, even as the adequacy of this mechanism is challenged in European courts. Accordingly, appended to many data protection agreements or addenda are additional contractual terms often named "Standard Contractual Clauses" with annexes setting describing the data exporter and importer, the particular data processing activities involved, and the appropriate security measures employed to safeguard the data.

# 10 Communicating with Supervisory Authorities

Knowing which DPA is the "lead" supervisory authority is the first step in establishing healthy lines of communication with that DPA. For data processors or controllers that carry out cross-border processing of personal data, or processing that "substantially affects or is likely to substantially affect data subjects in more than one Member State," this is a critical task. The lead supervisory authority has the "primary responsibility for dealing with the cross-border data processing activity" and, additionally, engages in investigations that may involve other relevant supervisory authorities.

For organizations with a main establishment in the European Union, the DPA in that country will act as the lead supervisory authority. Identifying the country of main establishment requires determining the "central administration" of the organization in the EU, which is the place "where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented." Recital 36 states that the main establishment of a controller in the Union "should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements."

For organizations active in various member states, determining the main establishment may be more challenging. The Article 29 Working Party's guidelines on the lead supervisory authority may assist. Notably, the data controller's designation of its main establishment can be challenged by the concerned supervisory authority.

For organizations that do not have an establishment in the EU, however, there may be no single lead supervisory authority, and they must anticipate interacting with several. As the Working Party explains, "controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative."

## EU Representative

Data controllers not established in the Union must appoint an EU representative, someone "nearby" who is "available to both the local DPA and data subjects," and who "speaks their language and understands their customs and expectations." This representative is tasked with both passing messages to the data controllers and communicating back to data subjects and DPAs based on the instructions of the controller.

A sticking point for law and consulting firms rushing to serve in the representative role is the potential liability they may face. Article 27(4) provides that the representative "shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities or data subjects, on all issues relating to processing, for the purposes

> *Data controllers who fail to comply with the 72-hour notification period must provide reasons for the delay.*

of ensuring compliance with this Regulation." The Article further notes that "the designation of such representative does not affect the responsibility and liability of the controller or the processor under this Regulation." Nonetheless, Recital 80 explicitly states: "The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor."

Because companies may be subject to up to €20,000,000 in fines (or up to 4 percent of global revenues) for wrongdoing, the risks for prospective representatives is formidable. Consequently, finding a representative is shaping up as a challenge for controllers established outside the EU.

## What to communicate to the DPA and when

Before creating a system for communicating with the DPA, privacy professionals should become aware of their legal obligations regarding what to communicate and when to do so. For example, the GDPR requires data controllers to document data processing activities, notify DPAs about personal data breaches and consult with them prior to undertaking certain processing operations.

## Making data processing records available

Article 30 anticipates that data processing record keeping will include cooperating with DPAs, and requires controllers, processors, and their representatives to make these records available to DPAs upon request. Although this replaces the obligation to "notify" (or file") records with DPAs under the EU Data Protection Directive, organizations should anticipate cooperating with DPAs during investigations of complaints and should therefore prepare data processing records with an assumption that they will not be confidential. The task of cooperating with the DPA will likely fall to the data protection officer or privacy lead, bringing in the EU representative as appropriate.

### Notifying the DPA about a personal data breach

Under the GDPR, data controllers have to notify the competent DPA about a data breach "without undue delay and, where feasible, not later than 72 hours after having become aware" of the breach, unless it "is unlikely to result in a risk to the rights and freedoms of natural person." Data controllers who fail to comply with the 72-hour notification period must provide reasons for the delay.

As discussed in the eighth installment in this series, the content of the data breach notification should include at least the following information:

- Information about the breach (containing a description of its nature, approximate number and types of individuals affected by it, and the types of information compromised).
- Information about the organization (the name and contact information for the Data Protection Officer or another person who can provide necessary information).
- Information about the likely consequences of the breach.
- An explanation of measures to mitigate the potential adverse effects (taken or planned ones).

Data controllers must therefore document personal data breaches when they occur, including information about "the facts relating to the personal data breach, its effects and the remedial action taken" to "enable the supervisory authority to verify compliance" with the GDPR. Documenting a data breach or potential data breach is particularly important because, as the Article 29 Working Party suggests, even if no notification is initially required, "this may change over time and the risk would have to be re-evaluated." Moreover, the Working Party clarifies that "[t]here is no penalty for reporting an incident that ultimately transpires not to be breach."

## Consulting with a DPA Following a DPIA

Depending on the results of their DPIAs, data controllers may also need to communicate with their DPA. If a DPIA suggests that the data processing would bring "a high risk in the absence of measures taken by the controller to mitigate the risk," then the data controller should consult the DPA prior to undertaking the data processing.

During the consultation, the data controller should provide following information to the DPA:

- The "respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings."
- "The purposes and means of the intended processing."
- "The measures and safeguards provided to protect the rights and freedoms of data subjects."
- The DPO's contact information and any further information requested by the DPA.
- Evidence that the DPIA was carried out in accordance with the GDPR.

> *As the Article 29 Working Party guidelines on BCRs state, "Any substantial changes to the BCRs or to the list of BCR members shall be reported once a year to the competent Supervisory Authority with a brief explanation of the reasons justifying the update."*

Data controllers should also make sure to check whether their member state laws require consultation with the relevant DPA for data processing activities related to performing a task "in the public interest, including processing in relation to social protection and public health."

## Communicating results of verification and changes to BCRs

The GDPR explicitly recognizes binding corporate rules (more commonly referred to as "BCRs") as appropriate mechanism for data transfers, and sets forth the details regarding their use. At a minimum, BCRs must include mechanisms "for ensuring the verification of compliance" with them, such as "data protection audits and methods for ensuring corrective action."

Importantly, the results of these verification procedures "should be available upon request to the competent supervisory authority." Thus, data controllers should devise a plan for communicating the results of the verification of compliance to their DPA. In their BCRs, data controllers must also specify "the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority." A mechanism must also be in place to communicate to the DPA "any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules."

As the Article 29 Working Party guidelines on BCRs state, "Any substantial changes to the BCRs or to the list of BCR members shall be reported once a year to the competent Supervisory Authority with a brief explanation of the reasons justifying the update." Modifications that may affect the BCRs or the level of protection they offer must also be "promptly communicated" to the relevant DPA.

## Certification

Under the GDPR, controllers that are certified by a data protection certification body must, where applicable, be able to provide, "the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure." Certification mechanisms, including data protection seals and marks, are potential tools for demonstrating GDPR compliance "at-a-glance" including for transferring data to controllers in jurisdictions that do not have "adequacy" designations. Although many organizations eagerly await the development of accredited certification bodies, they are currently engaged in a waiting game for both A29 Working Party guidance as well as entrepreneurial programs to seize the role.

## How to communicate with a DPA

Many privacy professionals have already established working relations with their DPAs, especially if they have notified them of data processing or worked with them on approving BCRs. Regarding communication mode, some privacy professionals may choose to communicate with their DPA through email, or even with DPA employees over the phone anonymously or without revealing a client's identity.

Attending events where DPAs often gather — such as an IAPP conference or the ICDPPC annual conference — is another way to meet a member state DPA and create a relationship. For indeed, relationships matter. In the absence of clear rules and guidance on how many of the GDPR's provisions should be interpreted, building strong relationships with DPAs is becoming increasingly important. Communicating with DPAs is not only an issue of GDPR compliance, but it is also one of the factors affecting decisions about administrative fines in individual cases. Organizations that lack their own channels of communication with DPAs should engage outside counsel who have established and maintained mutually respectful relationships with their member state DPA.