Baker McKenzie.

GDPR Survey

Benefits beyond compliance

BearingPoint®

Contents

Foreword

In May 2019, one year after the entry into force and application of the GDPR, Baker McKenzie and BearingPoint launched a survey which aimed to understand the compliance journeys that organizations have gone through so far. After issuing the initial results of the survey in July 2019, we continued to explore the results to further analyze how our clients tackled the GDPR challenge.

About 100 data privacy specialists responded to the questions of our survey, mainly data privacy officers (DPO) across various geographies, sizes of enterprises (small, medium and large) and all key sectors.
Our GDPR survey demonstrated that many of them are still struggling on their way to GDPR compliance.
This can be explained by organizational issues since compliance is a chain of responsibilities where the DPO is a key actor but not the only one (Chapter 1), or difficulties in setting the right priorities in a context where the "compliance project" is just the starting point of continuous compliance (Chapter 2). In this context, respondents identified priorities for 2020 (Chapter 3). Their GDPR compliance journey is a long and challenging one, but they remain globally positive since they have already experienced operational benefits of their GDPR projects (Chapter 4).

Magalie Dansac Le Clerc
Partner, ITC - Data Privacy & Security
Baker McKenzie

Philippe Mannent
Director Risk & Compliance
BearingPoint

1 Compliance is a chain of responsibilities

Compliance is a chain of responsibilities

GDPR main stakeholders

GDPR compliance requires a collective effort from the DPO, who can be compared to a project manager, the data controller and data processors, who are the ones in charge of personal data processing.

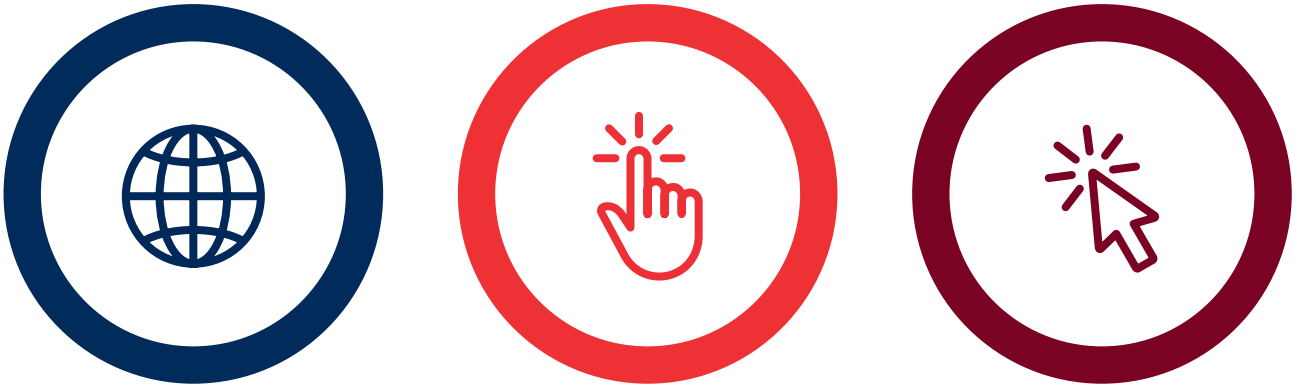
DPO	Data controller	Data processor
▪ a key actor who promotes and manages personal data governance and GDPR compliance ▪ a coordinator between different contributors within the organization ▪ a facilitator and point of contact for the supervisory authority ▪ mandatory for some organizations with significant personal data stakes	Entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. Under the GDPR, controllers are considered as fully responsible for damages caused as a consequence of data processing activities they control (unless the controller proves that it is not in any way responsible for the event giving rise to the damage).	Actor that processes personal data on behalf of the controller by implementing the instructions given by the controller at least with regard to the purpose and the essential elements of the means of the processing. Processors are liable for such damage only: (i) where they have not complied with GDPR obligations that are specifically directed to processors (ii) where they have acted outside or contrary to lawful instructions of the controller (unless they prove that they are not in any way responsible for the event giving rise to the damage)

In a complex environment, where many scenarios can involve controllers and processors with different degrees of autonomy and responsibility, it is more difficult than it seems to determine where each data protection responsibility lies. As an example, if a marketing company, which provides services of promotional advertisement and direct marketing to various companies, enters into a contract with a retail company according to which it provides commercial advertising for the retail company customers, it acts as a data processor. However, if the marketing company decides to use the retail company's customer database for the purposes of promoting products of other companies, it is likely to be considered as a data controller for this processing operation. This example reveals the importance of carefully assessing the roles of each entity in relation to each processing operation in order to efficiently allocate responsibilities, either as a data controller or a data processor depending on the circumstances.

A successful GDPR compliance project is not only about tools and templates, it is also about taking the time and dedicating resources to diving into the reality of the data processing at stake, and allocating responsibilities to the key stakeholders once this initial analysis is complete.

GDPR Compliance main stakeholders

GDPR Compliance



DPO

Specific tasks:

- Raise awareness and deliver training
- Monitor compliance with data protection regulations
- Provide advice and monitor completion of DPIAs

A true GDPR "conductor":

- Inform and advise the controller, the processor and employees who carry out processing, of their obligations

A need for independence:

- The DPO must be independent and avoid conflict of interests. Should be bound by secrecy and confidentiality

A point of contact:

Cooperate with the supervisory authority and act as the point of contact for the authorities and data subjects

Data controller

Specific tasks:

- Give clear instructions to the Data Processors
- Qualify data processing and maintain an up-to-date repository of processings
- Apply internal procedures in terms of data subject rights exercise and data breach management
- Conduct DPIAs in case of high-risk data processing
- Implement remediation action plan (organizational and technical tasks) to secure the data

A compliance "guardian":

- Alert and consult the DPO in case of any project involving major personal data impact, data subject's complaint, etc.
- Control the commitments of data processors, if any, with appropriate contracts, security measures and audits

Data processor

Specific tasks:

- Strictly implement Data Controller's instructions
- Maintain its own repository of processings of all the processing activities conducted within its organization
- Alert the data controller in case of a data breach

The last stage for Data Controller's compliance:

- Make the records available to the supervisory authority upon request
- Help identify potential risks and required mitigation actions to secure data

Source: BearingPoint

Focus on the DPO

The majority of our respondents (78%) have already appointed a DPO, another 11% are in process of nomination and only 11% of the companies surveyed consider that a DPO is not needed for their organizations.

Internalization, externalization or pooling of the DPO function

When appointing a DPO, organizations can choose to appoint an internal delegate, call on an external contractor or pool the DPO function. This decision varies notably according to the size of the company concerned. However, organizations must ensure that the requirements of absence of conflict of interest and independence of the DPO are met.

Of those who have appointed a DPO (back in June 2019), the vast majority of them (98%) have appointed an internal DPO, thus choosing to promote knowledge of the internal functioning of the organization and of the sector in which it operates. Opting for an internal DPO also meets the requirement for proximity to colleagues and the company's own practices. This allows the DPO to have better visibility on the processing to be implemented.

Nevertheless, among the organizations who have not appointed a DPO yet, it might well be because they do not have internal resources for such role so they may end up having an external DPO, which may take more time to recruit.

DPO background

The companies interviewed also highlighted the importance of the active role of the DPO. Beyond their initial background, the DPO must primarily be a driving force for compliance, thus requiring excellent diplomacy and communication skills. The DPO's skills are intended to be complemented by other internal expertise.

Questioned about the skills of the DPO, companies responded that the DPOs have:

- transferable skills
- knowledge and understanding of data protection rules, legal and technical skills, which are undeniable assets
- soft skills and an easy to work with communication style to handle all the layers of an organization and manage conflicts

Over half of DPOs (62%) have a legal profile, followed by IT/digital and administrative/HR, which are fields where the most important data processing sits. Among other possible backgrounds, respondents cited finance, as well as a mix of several mentioned above, although it is more common to have only one specialty (Figure 1).

These responses match our own observations:

- DPOs are generally well versed in data protection law.
- DPOs have less experience in IT and security risk than they judge necessary.

The DPO is one single person, but they must not be alone. Being able to rely upon qualified and influential IT resources is key to the success of the GDPR compliance journey.

What is your DPO background?

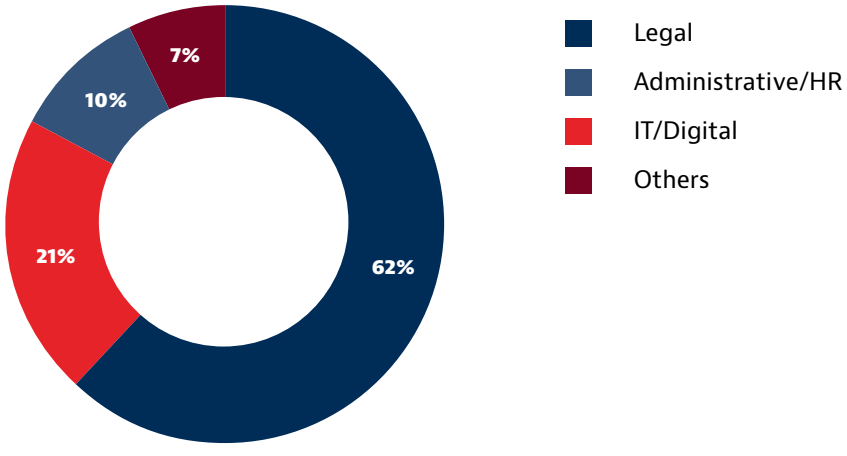


Figure 1.

Respondents comments on their role as a DPO

DPO, financial services company

Which metaphor would you use to explain your role as a DPO?

Depending on the governance maturity within the organization, I would say that the DPO should be a "one-man-band" if the governance is low and should aim to become a "conductor" once the governance is clear and in place.

If you could share one piece of advice with another DPO what would it be?

My main piece of advice would be on the DPO posture: the necessity to be perceived as a business partner and not an obstacle. In order to be well received, a DPO must adopt the right tone, clearly identify the political/strategic issues (power plays in the organization and between third parties) behind operational data protection issues and be flexible by using a risk-management approach to choose their battles. Otherwise, the DPO risks being bypassed.

Who is a DPOs best friend?

A champion/sponsor who knows the organization well and who has some managerial weight to ensure the DPO is not bypassed. The chief information security officer (CISO) can be a good friend because he has the big picture on what is going on within the firm but also brings technical/security expertise complementary to the DPO. An archivist can also be another good friend for the broad vision on information flows and processing within the organization.

What should be in a DPO toolkit?

A DPO toolkit must combine regulatory awareness and data processing tools:

- *Access to websites and other sources (LEGALIS, ECPD, CNIL, court of cassation, etc.) to conduct a regulatory watch and always be aware of latest news and updates*
- *Internal procedures, such as RACI, which recalls roles and responsibilities of actors within the organization; a DPO mission letter to remind the DPO authority and awareness materials (generic and specific by actors)*
- *Clear data processing mapping to have the full picture on data processing conducted within the organization and outside through third-parties*

DPO, service industry

Which metaphor would you use to explain your role as a DPO?

I feel that over the last few years, my role has constantly evolved, depending on the maturity of our people and organization on data privacy challenges and requirements. At first, I was all over the place, reacting to events very much like a fire fighter. A couple of years down the GDPR project, I am growing to be a seasoned data security expert, well-articulated with the business and the IT security guys.

If you could share one piece of advice with another DPO what would it be?

Data is everywhere and data management and protection have many components. So « be everywhere and never alone ». In my case, with a strong legal and regulatory background, I seek support from the CISO and the CIO. Compliance with GDPR is a team effort that cannot be achieved in an ivory tower.

Who is a DPOs best friend?

CISO is absolutely my best friend: while I cover the regulatory aspect of data privacy (including compliance with the GDPR), they secure the technical side of data privacy. And when data breaches occur, our close relationship allows a swift reaction to investigate and inform the individual and the data protection authority.

What should be in a DPO toolkit?

In fact, again, data protection has so many components that a single tool cannot help much. So our DPO toolkit has grown big, including a flurry of training, type of clauses, etc. So, at this stage, I wish I had a GPS or a map to find my way in the toolbox and help the business navigate it more efficiently.

Summary of stakeholders' responsibilities

As a conclusion to this chain of compliance and responsibilities, see below an example of the roles and responsibilities of the main stakeholders and their level of intervention.

- **R** Responsible - is responsible for the completion of the action)
- **A** Accountable - is ultimately accountable for achieving the result expected from the action
- **C** Consulted - is actively contributing to the completion of the action
- **I** Informed - is informed of the progress or completion of the action

	Group DPO	Legal/ Compliance	IT Security	Data Controllers HR	Products & Services (Customer Experience, Marketing...)	IT Dept
Training/ Awareness	A R	I	I	C	I	I
Acountability						
Repository of processings updating	A C	C	C	R	R	R
Data breach management	C	I	A R	R	R	R
Management of sub-processors	C	A	C	R	R	R
Contract Management	C I	A R	C	C R	C R	C
Privacy by Design & Default	A C	I	R	R	R	R
Exercise of rights	A C	C	I	R	R	R
DPIA	A C	I C	R C	R	R	R
Communication						
External - Data Protection Authorities	A R	C	I	C	C	C

Source: BearingPoint

Focus on data processors

Data processors are clearly important stakeholders involved in data processing because of their key role in the actual processing of personal data. Although data processors are directly responsible toward a data subject and must cooperate with data controllers, they are not mentioned within the above RACI since they are not in the front line as much as data controllers (except when such data processors are themselves data controllers of their own data processing).

The relationship between different stakeholders and the lack of communication which may arise from these different actors in the data processing chain emphasizes the need to put in place a governance structure, by implementing notably efficient reporting lines.

The question to have in mind, however, is how to implement such governance and under which conditions. Indeed such governance would work only if sufficient means and resources are allocated, and the DPO, which is at the heart of the process, might well need to be a team, not only one person, to bear the varied tasks and responsibility.

2 GDPR compliance is still a work in progress and may always be so

GDPR compliance is still a work in progress and may always be so!

Compliance with the regulation is actually a continuous journey rather than a goal that can ever be achieved.

Indeed the laws and regulations the organization operates under, its ambitions and creativity for launching new data processing, the maturity of its business environment, its geographic span and the sensitivity of data subjects and data protection authorities are constantly evolving. Hence the data protection organization and systems have to adapt constantly to this changing environment.

It is indeed of the essence of this regulation that companies (or public organizations or associations) be led to implement a dynamic and risk-based data protection framework, which such companies must adapt to their evolving context and environment.

> "I wish I had realized at the beginning that there is no end, the work is always ongoing. That is an important message to manage expectations."
>
> **Respondent**

The pursuit of "run mode"

Rather than a depressing insight, it should be seen as a pragmatic and realistic perspective that hardly more than half of DPOs considered that their organizations can claim to be in "run mode" regarding the GDPR one year after its entry into application, with a widely spread data protection culture, operational discipline and well-oiled processes on data management. Today, if the proportion of organizations in run mode must be slightly higher, one must take into account the time and energy spent by DPOs and data privacy teams on dealing with the day to day challenges raised by the GDPR, such as the management of data subject access rights, and the conduct of privacy impact assessments, since their businesses continue and rely on them for GDPR compliance, even if the compliance project is not completed

'Run mode' means when the internal procedures have been implemented and the status of the GDPR compliance project is considered finalized and is being maintained. Indeed, the ultimate goal should be to be in run mode and to maintain compliance, not to be compliant, at the end of the compliance project.

Only 54% of respondents consider themselves in run mode or run mode with marginal remediation actions (Figure 2) although 82% of respondents had started their compliance journey before 2018 (Figure 3).

How would you define your current GDPR compliance status within your organization?

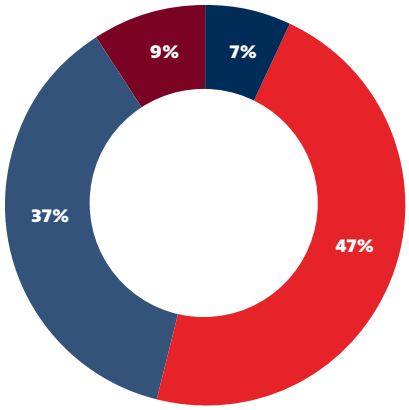


Figure 2.

- Run mode with marginal remediation actions
- Run mode
- Beginning of run mode with significant readiness actions
- Project mode

When did your company kick off its first GDPR project?

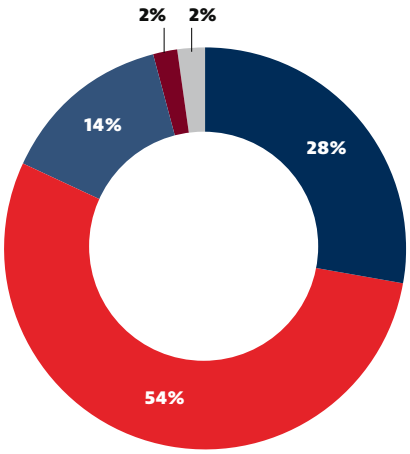


Figure 3.

- 2016
- 2017
- 2018
- 2019
- We haven't started yet

While considering themselves in run mode or run mode with marginal remediation, in fact, organizations are only mid-way on structuring items such as "setting the data protection governance," "implementation of technical security measures," "completing the data processing register" or "managing data breaches" (Figure 4).

This shows that the concept of run mode varies significantly across organizations and that GDPR compliance project is a long work-in-progress journey.

What is the status of your GDPR projects?

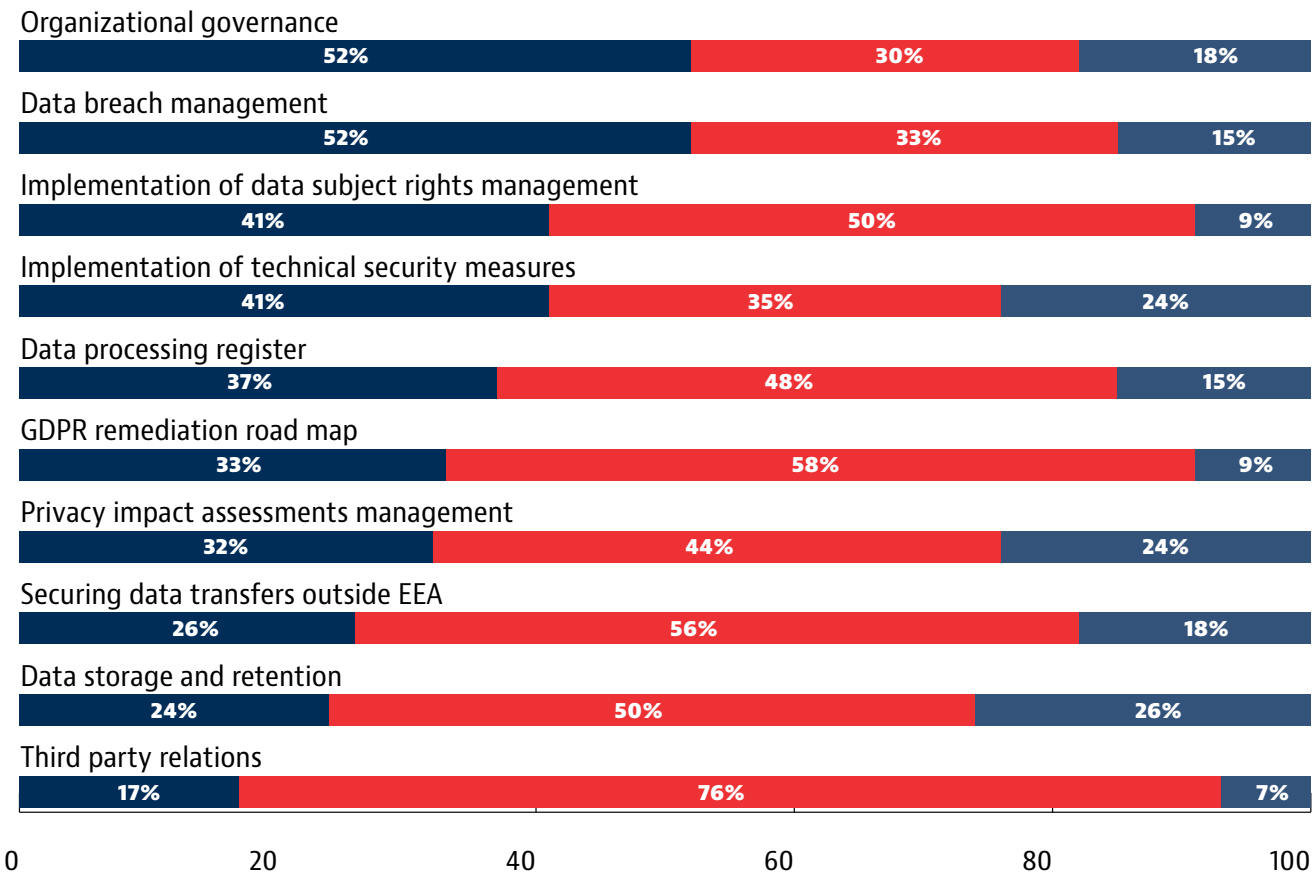


Figure 4.

What is generally considered as "finalized" by the respondents?:

Organizational governance, with 52% of respondents considering this work stream completed.

- This can be explained by the need to appoint compliance teams at the beginning of the projects, but some respondents specified that the new reporting lines were still difficult to follow.

Data breach management is also considered completed by 52% of the respondents.

- The new obligation to report data breaches, the increasing awareness of cybersecurity risks, and the frightening consequences of any breach have motivated the companies to work on this stream as a priority.

What is generally considered as "in progress" by the respondents?:

Third party management (i.e., the management of external data processors or business partners): 76% of respondents are still working on this work stream, with only 17% of respondents considering this work stream completed.

- This is not surprising given the complexity in controlling the different stakeholders that are involved inside and outside an organization.
- Third-party management is not limited to contract updates but also implies operational alignment and true collaboration in managing data breaches or data subject requests.
- Business negotiations and strategies can also influence the fact that such work stream takes a lot of time to be finalized.

Securing data transfers outside the EEA: 56% of respondents are still in progress on this work stream, and 18% of respondents have not yet started this data transfer compliance project.

- This is not surprising given the multiple data flows that may arise from a global company (i.e. internal data flows to other subsidiaries/parent company; data flows to data processors, suppliers, business partners…)
- The constant evolution of the geopolitical environment emphasizes the need to secure data transfers by different means (e.g., instability of Privacy Shield, Brexit, etc.).

The **data processing register**, considered in progress by 48% of the respondents.

- This work stream is a true backbone of the overall compliance organization as it describes:
  - the list/category of data processed
  - the lawful basis and purpose that influence the data retention horizon
  - the data location and the related security measures
  - the main departments processing data
  - the extent of use of an external data processor and business partners
- Completing this work stream requires broader mobilization across the organization (see section 'Chain of responsibilities'), i.e., operations, legal, IT, procurement, and third parties.
- Promoting a common definition of what data processing is (i.e., granularity; criteria to assess; template) is a challenge when simultaneous projects have kicked off in the organization, although concepts have been gradually clarified and guidelines provided by the data protection authorities and the EDPB (https://edpb.europa.eu/) since 2016. Equally, setting workflows that ensure a reliable inventory needs to strike the right balance between an as-comprehensive-as-possible documentation of data processing and the quality of the collected information.

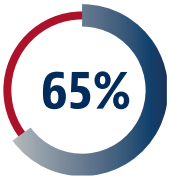
What is generally considered as "not started" by the respondents?:

Implementation of security measures: 24% of respondents have not yet started this work stream on security measures, despite most of the recent sanctions in France by the CNIL being imposed because of a breach to the security obligations of the data controller.

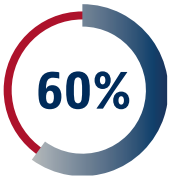
Data archiving and deletion: 50% are working on it and 26% still have not started this work stream.

- Many organizations find it difficult to develop data retention policies. A large number of them have not got their head around this topic and "keeping the data just in case" seems to have been the wide spread data retention strategy — although not allowed even before GDPR came into effect!
- Defining the data retention rules is not easy. They result from crossing the industry regulations and legal requirements of several countries, data protection authority or court decisions, industry usual practices and the specific needs and interpretations of the organization, depending on the lawful base and purpose of the data processing.
- Last but not least, enforcing the data retention in systems bumps into technical issues such as:
  - "Have we got the initial recording date of the data?"
  - "How can the data be easily retrieved and segregated from the data to be kept?"
  - "Is the data still needed for other data processing?"
  - "What strategy should we adopt at the end of the retention period: deletion or anonymization?"

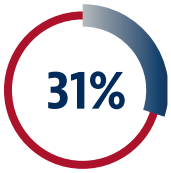
Struggling with capturing the right level of attention



of respondents struggled to implement GDPR due to lack of resources.



of respondents had difficulty establishing their level of risk.



of respondents acknow ledge that their organization originally saw GDPR as solely an IT issue.

Defining the desired compliance level is a classic challenge for organizations: if non-compliance is never an option, best-in-class full compliance is scarcely targeted either.

Beyond the risk of being fined up to 2%, or even 4%, of the global turnover, there is a consensus that other risks should be considered, such as reputational (i.e., loss of trust in providing one's data to an organization) and operational (i.e., inability to perform certain data processing; worsening of the user experience).

Sanctions: snapshot of the highest sanctions

Austria

Data protection authority: Datenschutzbehörde (DSB)

Highest sanctions:

EUR 18 million against the Austria's leading logistics and postal services provider for insufficient legal basis for data processing (23 October 2019)

EUR 50,000 against a company in the medical sector for non-compliance with information obligations and for non-compliance with the obligation to appoint a DPO (12 August 2019)

Belgium

Data protection authority: Autorité de Protection des données (APD)

Highest sanctions:

EUR 15,000 against a website providing legal information for non-compliance with information and transparency obligations (17 December 2019)

EUR 10,000 against an electronic identity card merchant for non-compliance with general data processing principles (17 September 2019)

France

Data protection authority: Commission Nationale de l'Informatique et des Libertés (CNIL)

Highest sanctions:

EUR 50 million against a US-based multinational tech giant for the absence of transparency and consent rules violation (21 January 2019)

EUR 500,000 against a French construction company for infringements in relation to the use of call centers for its cold-calling marketing campaigns (21 November 2019)

Germany

Data protection authority: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)

Highest sanctions:

EUR 14.5 million against a German property company for non-compliance with general data processing principles such as data minimization and storage limitation (30 October 2019)

EUR 9.55 million against a Telecoms provider for insufficient technical and organizational measures in order to prevent data breach (9 December 2019)

Italy

Data protection authority: Garante

Highest sanctions:

EUR 8.5 million against a subsidiary of an Italian multinational oil and gas company for unlawful processing of personal data in the context of telemarketing and telesales activities (17 January 2020)

EUR 3 million against a subsidiary of an Italian multinational oil and gas company for unlawful processing of personal data due to the conclusion of unsolicited contracts for the supply of electricity and gas under "market economy" conditions (17 January 2020)

Netherlands

Data protection authority: Autoriteit Persoonsgegevens (AP)

Highest sanctions:

EUR 900,000 against a Dutch employee insurance service provider for insufficient technical and organizational measures to ensure information security in relation to the online employer portal (31 October 2019)

EUR 460,000 against one of the largest general hospitals in the Netherlands for insufficient technical and organizational measures to ensure information security in relation to patient records (18 June 2019)

Portugal

Data protection authority: Comissão Nacional de Proteção de Dados (CNPD)

Highest sanctions:

EUR 400,000 against a public hospital for insufficient technical and organizational measures to ensure information security (17 July 2018)

EUR 20,000 against X (unknown) for denial of the right to access recorded phone calls by the data subject (5 February 2019)

Romania

Data protection authority: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)

Highest sanctions:

EUR 150,000 against one of the leading multinational banking groups for insufficient technical and organizational measures to ensure information security (9 October 2019)

EUR 130,000 against one of the leading European banks for failure to implement appropriate technical and organizational measures resulting in the online disclosure of the personal data of 337,042 data subjects (27 June 2019)

Spain

Data protection authority: Agencia Española de Protección de Datos (AEPD)

Highest sanctions:

EUR 250,000 against the Professional Football League for inadequate information of application users and inability to manage consent withdrawal (11 June 2019)

EUR 75,000 against the Spanish subsidiary of one of the world's leading wind energy producers for processing personal data without obtaining prior consent from the data subjects (7 January 2020)

United Kingdom

Data protection authority: Information Commissioner (ICO)

Highest sanction:

EUR 320,000 against a pharmaceutical supplier for the failure to protect around 500,000 documents containing personal data from the elements resulting in water damage to the documents (20 December 2019)

Formal notices (proposed fines):

EUR 204.6 million against a global airline company for inadequate security standards resulting in a data breach (1.5% VAT 2017) (8 July 2019)

EUR 110,390,200 against an international hotel group for insufficient technical and organizational measures to ensure the prevention of data breaches (9 July 2019)

The typology of breaches and companies sanctioned shows that GDPR compliance should be a concern for everyone. Unsurprisingly, the US-based multinational tech giant was the first company sanctioned under the GDPR era for EUR 50 million. However, even small companies are impacted. For instance, CNIL in France sanctioned a small translation company with less than 20 employees; it was not profitable yet but was fined for EUR 20,000 (2% VAT in 2017) for excessive video surveillance. The common trait to all these sanctions is that they have been proportionate to the size of the company. However, it is still very difficult to anticipate and estimate the amount of the fines that may be imposed by the data protection authorities across Europe, who are not always transparent on their rationale behind the calculation of sanctions. This said, a new trend may emerge, following the example of Germany, where the Conference of German Data Protection Authorities (Datenschutzkonferenz) has recently published (in October 2019) some guidelines suggesting a calculation system for administrative fines under the GDPR, which gives more visibility to companies as to what to expect as sanctions.

The shift of sanction magnitudes is clear, but the chances to be controlled are still considered limited, rightly or wrongly. And indeed, the number of sanctions (public notifications or penalties) have not sky-rocketed (in France, for instance, the CNIL only published nine sanctions over 2019, in comparison to 12 in 2018 and 14 in 2017) and it has kept a rather stable headcount (from 195 FTE (full time equivalent) in 2016, to 199 in 2018 and 208 in 2019), but the number of controls is increasing.

Considering that compliance with GDPR is a continuous journey (with no set compliance picture) and that case-law and EDPB guidelines are gradually emerging, organizations struggle in assessing their compliance status and in defining the level of resources they want to dedicate to their compliance projects.

60% of the respondents to the survey struggle with assessing their risk of non-compliance, with slightly lower shares in financial services (44%), telecom-media-entertainment (50%) and industrial-manufacturing-transportation (55%).

Efforts (both financial and non-financial) put into GDPR compliance projects vary significantly from one organization to another: some project teams consist of the DPO with the support of a handful of people (often including the IT security officer), whereas others run compliance programs mobilizing tens of people including lawyers, consultants and compliance management solution providers.

Unsurprisingly, the greater the difficulty to assess the level of risk, the greater the challenge to mobilize resources: only 44% of financial services respondents say they experience difficulty, while they are 50% in telecom-media-entertainment and 73% in industrial-manufacturing-transportation.

This diversity of approach is a natural consequence of the regulation that has promoted a pragmatic risk-based principle to drive the compliance efforts of the organizations.

Often raising awareness on the stakes of data protection over the compliance projects, resources can be gradually increased. Conversely, sharply cutting efforts after the first phase of the project can be a pitfall that puts the continuous compliance journey at risk.

Investing in GDPR

When asked about the investment in GDPR solutions, almost 40% of the companies surveyed had not invested yet, and among the remaining 60%, two thirds have chosen an in-house solution rather than a market one (Figure 5).

Data processing recording is by far the predominant feature of GDPR solutions (Figure 6).

Even if the investment in a solution is not a guarantee of compliance, and for small organizations may not be necessary, it can still provide various direct and collateral benefits.

Have you invested in GDPR solution?

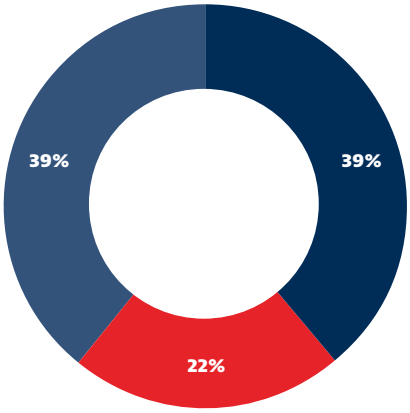


Figure 5.

- No investment
- Yes, in market solution
- Yes, in in-house solution

What GDPR issues the implemented solutions address

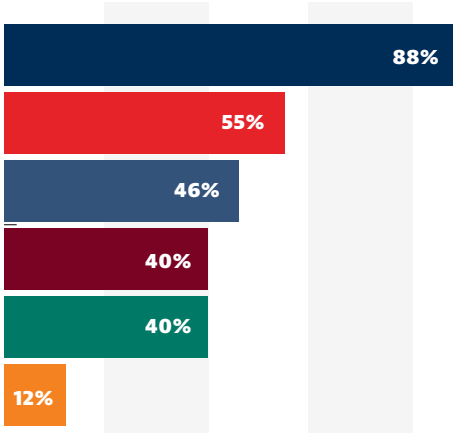


Figure 6.

- Record of data processing activities
- Data breach management
- Access management system
- Data subjects exercise rights
- Consent
- Others

Collateral benefits

Automation: automated processing through a solution is more robust than a manual process, especially on topics such as consent or cookies management.

Workflow effectiveness: given stakeholders multiplicity, the use of workflows can rationalize and optimize process efficiency but also formalize clear roles and responsibilities with associated profiles and tasks attributed to actors.

Monitoring reinforcement & information sharing: solutions provide the most up to date information about the progress of the remediation actions underway or the alerts on projects at the DPO's finger tips; data protection being a true organization-wide topic, solutions facilitate the sharing of information across the organization (upwards, downwards and across departments) to have swift mobilization of all relevant stakeholders in case of a data subject exercising their rights or an inspection from the data protection authority.

Traceability and documentation: with the shift of paradigm regarding the demonstration of compliance (from the authority having to demonstrate non-compliance to the organization having to demonstrate their compliance), traceability and documentation become crucial —all the more when organizations need to explain, for instance, how they have set they priorities (risk-based approach), how long they think they need to retain data or how data processing is rightfully based on legitimate interest.

3 Top GDPR Priorities from now on

Top GDPR Priorities from now on

While most of the GDPR projects started in 2017, the next priorities identified by respondents relate to GDPR internal procedures.

The **preparation and rolling out of procedures** is the cornerstone of every GDPR compliance project, and it is not surprising that, even though it started long ago, it remains the top priority for 2020 (Figure 7).

Review of contracts is a short distance behind, and it reminds us that companies must first verify that they can use a complete register of data processing which clearly reflects the allocation of roles and qualifications between controllers and processors to do so.

Review of consent and information notices is also among the top three priorities, and it seems wise given the current trend of increasing protection of the rights of data subjects in a world where digital solutions help to "follow" them everywhere.

What are the three main GDPR priorities in your company for the coming year?

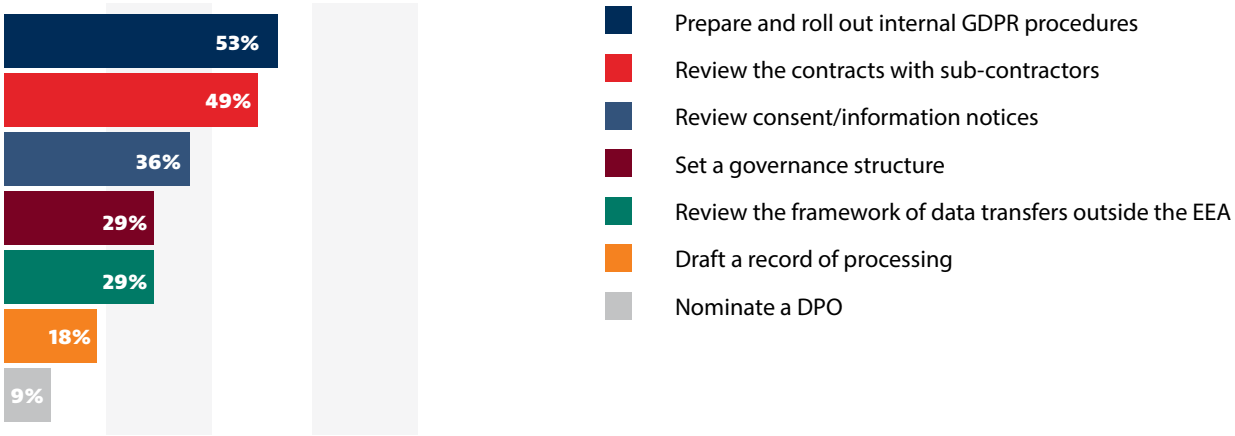


Figure 7.

TOP 1 PRIORITY: Prepare and roll out internal procedures

Preparation and roll-out of internal procedures is identified as the first priority by respondents. GDPR principles require transparency and accountability. In order to meet these requirements, effective operational processes are needed, such as drafting and implementing a data retention policy, an IT security policy, a Privacy by Design and Privacy by Default procedure, a data subject rights procedure and a data breach management procedure. While all of these internal procedures are necessary to comply fully with the data controller's accountability duty, we notice that among these procedures, companies have prioritized completion of data subject rights and data breach management procedures. Indeed these two expose the organization to interactions with the data subjects and thus are more "visible" from the outside.

Key procedures prioritized by data controllers

Data subject rights exercise: data subject can be internal, such as employees, but also external, such as clients. Both can have different motivations, from the need for information to a potential conflict of interest, to exercise their rights.

✓ Best practices recommended are:

- Use of an application form to "standardize" the exercise of rights format
- Funneling of the inflow of data subject requests into a single channel and centralization of the process to ensure more efficiency and avoid loss of information
- Acknowledgement of the receipt of the data subject request through an automated mail
- Use of a solution to automate the process and ensure its completeness
- Identification of third parties and transmission of data subject requests to ensure completeness of the process
- Reporting and control in respect of the 30 day respond delay

Data breach management: a data breach can be both internal and external, technical or operational, through the communication of personal data to a wrong recipient. The analysis/qualification of the breach is required to decide if notification of the supervisory authority and/or data subject is needed.

✓ Best practices recommended are:

- Integration of data breach management to "incident management" process to ensure coherence and synergies
- Data breach analysis and qualification phase should involve DPO and data controller to have a collective assessment of risks and mitigation plan
- Process should be defined as a crisis management one to respect the 72 hour notification period if needed
- Report on each data breach in a learning experience perspective and ensure lessons are learned

TOP 2 PRIORITY: Review the contracts with subcontractors

It may be the case that an organization that contracted a cloud service provider to store and analyze its data, prior to the entry into force of the GDPR, made sure to impose security obligations on its contractual partner with regards to the data the latter processes on its behalf. Under the GDPR, the security obligations imposed on the cloud service provider will not be sufficient to ensure that data is processed in full compliance with the new data protection requirements.

Reviewing the contracts with subcontractors should be a top priority for companies since the GDPR imposes broader contractual requirements with respect to data processing agreements between controllers and processors, compared to those imposed by the previous Directive 95/46/EC. Before the entry into force of the GDPR, contractual requirements pertained mainly to ensuring the security of personal data, while now they are designed to guarantee that processors comply with all GDPR requirements applicable to the processing carried out on behalf of controllers. In addition to the general obligation for controllers to execute a contract with any entity processing data on their behalf, the GDPR imposes the inclusion of specific contractual terms in any contract entered into between controllers and processors such as, inter alia, the obligation for the processor to assist the controller in ensuring compliance with its GDPR requirements (Article 28 of the GDPR).

Moreover, reviewing the contracts entered into with processors may become necessary to take into account the strict allocation of responsibilities between controllers and processors set out by the GDPR. Under the GDPR, the respective responsibilities for complying with regulatory obligations between the controller and the processor are set expressly by the regulation (as explained above in the section titled "Compliance is a chain of responsibilities"). In that regard, it is important to note that the determination of the responsibility of each entity in the processing is essential insofar as, whenever a controller or a processor is liable for infringement of a GDPR requirement, they are each held jointly and severally liable, and may both be subject to administrative sanctions including fines.

Finally, it is wise to put this review in priority two since in France CNIL announced in 2019 that its strategy of controls for the next months will focus on "the sharing of responsibilities between controllers and processors," especially through the control of the existence and concrete implementation of the contract between them.

TOP 3 PRIORITY: Review consent/information notices

As the example of the fine issued in January 2019 against the US-based multinational tech giant by the CNIL suggests, a multinational technology company must now find innovative ways to provide the required information to data subjects, including the use of new tools such as granular notices or dashboards, to allow for full compliance with the new stringent requirements set out by the GDPR.

With the entry into force of the GDPR, more stringent rules apply to the information notices that controllers are required to provide to data subjects regarding the processing of personal data they carry out, making it necessary to review existing information notices to ensure compliance.

- **More information:** Articles 13 and 14 of the GDPR set out a more extensive list of specific information that must be provided to data subjects such as, inter alia, the identity of the controller, the purposes of processing, the recipients of the personal data, the transfers of data to third countries, the retention periods and the rights of data subject.
- **More transparency:** In addition, controllers have a general transparency obligation in drafting information notices which imposes the providing of information in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12 of the GDPR). In that regard, a poor practice example would be to use insufficiently determined expressions such as "We may use your personal data to…."

Under the transparency requirement, there is an emphasis on providing clear and complete but also concise information. Thus, controllers are required to adopt innovative approaches for providing the relevant information, adapted to the context of the data processing. The European Data Protection Board (EDPB) insists on following a layered approach, typically in a digital environment, consisting of providing data subjects with a short notice containing key information (such as the identity of the controller and the way personal data is used) with links to more detailed information.

4 GDPR brings operational benefits too

GDPR brings operational benefits too

Around three-quarters (71%) of survey respondents stated that they have achieved operational benefits as a result of implementing GDPR compliance. These benefits were realized through the activities necessary to move toward compliance.

Raising data culture within the organization

"Data is the new oil!" Indeed it flows everywhere within the organization, but data culture and the awareness of the value and obligations to handle the data with due care and consideration is not that widespread. GDPR awareness training and information turns out to be a great means to educate people on data.

Being a true organization-wide topic, with data flowing from one department to another or being shared between several departments, training brings together people from front and back office, core business and support functions, breaking organizational siloes.

Clarifying ownership, relevance of data processing and breaking the data processing black boxes

Data tends to be everybody's interest but nobody's responsibility: the data processing inventory exercise allows us to clarify the ownership of the data processing.

Beyond the regulatory requirement, this inventory provides valuable insights on:

- pools of unused data, forcing the organization to see whether it is worth keeping it
- the purpose of the data processing: what is the business need fulfilled by this data
- the end-to-end data processing, with data controllers understanding the ins and outs of data processing that they mechanically performed, with the involvement of IT architects exposing the actual data flows (behind the screen)
- the actual level of protection the most valuable data have

Questioning & optimization of business practices

Far from being a mere compliance exercise, the GDPR project actually questions many business practices:

- Why are we sending the full employee report (with phone numbers and relatives) for an event organizer, when only the headcounts, special dietary information and children are needed?
- Why are we storing client details endlessly when we have never had a situation of litigation beyond the warranty period?
- Why generic accounts set up to face the system failure when it went live years ago still exist and are used?

Data cleansing and IT architecture

- System/application mappings tend to be done punctually when IT architecture projects occurs, but they are not maintained over time: GDPR forces companies to maintain an up-to-date list of where personal data is located, which is very useful information for data architects.
- Eliciting multiple data sources also raises the question of the "right" data: reducing conflicting data sources and making the data more reliable increases the amount of quality data that can feed algorithms and the quality/relevance of their outputs.
- For efficient data deletion and data subject right enforcements, the organizations have to reconsider redundant/fragmented data storage. They also need to refine the way they can trace data and allow data processing: for instance, beyond the retention period, the data of a given individual should be deleted or anonymized.

Besides the operational benefits, it should be mentioned that, from a legal standpoint, implementing GDPR does not enable only compliance with data protection regulations, it brings other legal benefits such as restructuring the contracts' templates architecture and centralizing all legal issues arising from data processing implemented by different business units.

5 Conclusion

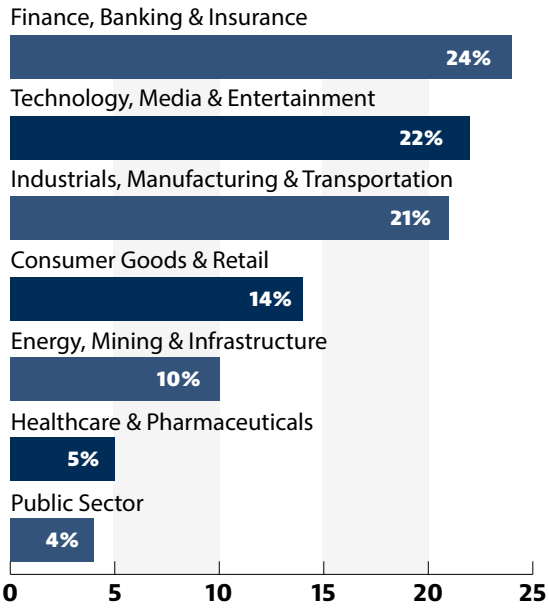
GDPR compliance is a continuous journey that can be eased with clear governance and a collective mobilization around the DPO, but also through operational procedures and the use of a solution if needed. However, to be able to do that, resources, budget and strong sponsorship are required. So even if sanctions have been low for now, it is not only the threat of them that should motivate compliance but the ability to nurture a data culture, clarify data governance and improve its management, security standards and process effectiveness.

Methodology

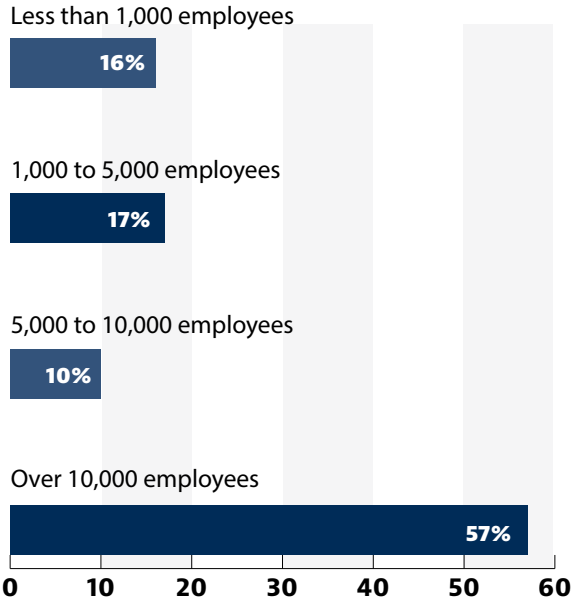
The GDPR survey is based on the results of an online survey of data privacy specialists, mainly data privacy officers, across various geographies, sizes of enterprises and all key sectors.

Respondents' profiles

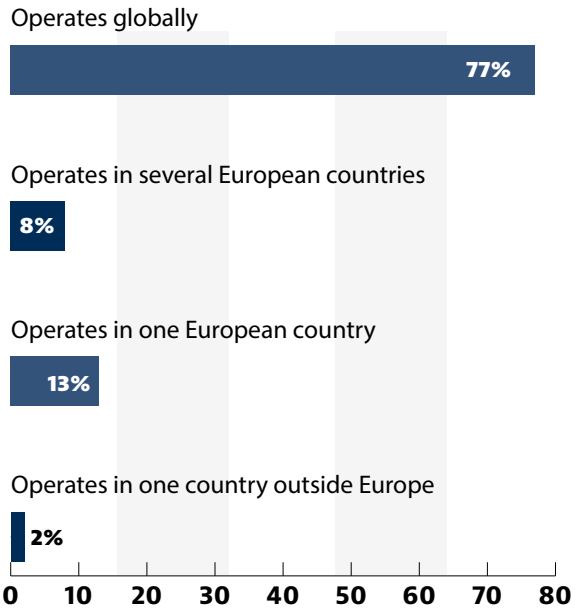
Company Sector



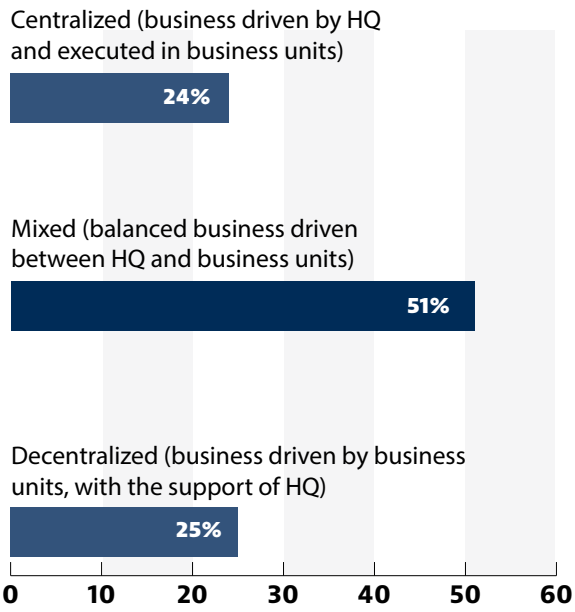
Number Of Employees



Company Geographic Structure



Company Operational Structure



About Baker McKenzie

Baker McKenzie: An international and market-leading Data Privacy & Security practice

Baker McKenzie's world-renowned Data Privacy & Security practice focuses on providing advisory, risk management and transactional support to our clients. We understand the interplay between privacy requirements in multiple practices, industries and jurisdictions. Our experience and agile cross-border coordination enable us to seamlessly advise clients at every stage. With an understanding of business and operational realities, we provide balanced and effective advice to guide clients through the complex regulatory landscape and partner to devise practical solutions that are scalable and customized to their objectives, budget and resources. Ranked Band 1 in Data Protection by Chambers Global since 2008.

To contact a member of our Global Data Privacy & Security Leadership Team, **please click here.**
Please direct any questions or feedback about this publication to:

Magalie Dansac Le Clerc
Partner, ITC - Data Privacy & Security
Baker McKenzie
Paris, France
+33 1 44 17 59 82
Magalie.dansacleclerc@bakermckenzie.com

Alexandra Coti
Senior Associate, ITC - Data Privacy & Security
Baker McKenzie
Paris, France
+33 1 44 17 59 44
Alexandra.coti@bakermckenzie.com

About BearingPoint

BearingPoint: Management consulting in data privacy

BearingPoint is an independent management and technology consultancy with European roots and a global reach, with more than 12,000 people and supports clients in over 78 countries, engaging with them to achieve measurable and sustainable success. Since 2016, across Europe, more than 150 practitioners have supported private and public companies, government agencies, central and local governments in shaping effective and sustainable responses to the greater obligations set by the GDPR. Coordinated via the GDPR Center of Excellence, these consultants are addressing a broad range of operational challenges: from setting up the compliance programme and governance; to designing and implementing GDPR specific processes (e.g. data subject rights; data processor relationship). Our teams also engage in upstreaming data protection technical and organisational measures (e.g. access management, IT security measures) and revisiting data management and usage with the business lines and support function (e.g. customer relationship, marketing, human resources, IT and digital, security).

To contact a member of our Data Privacy & Security Team, **please click here.**
Please direct any questions or feedback about this publication to:

Philippe Mannent
Director Risk & Compliance
BearingPoint
Paris, France
+33 1 58 86 31 01
Philippe.mannent@bearingpoint.com

Aïcha Benabdeljalil
Manager Risk & Compliance
BearingPoint
Paris, France
+33 6 24 39 41 48
Aicha.benabdeljalil@bearingpoint.com

Yaël Gozlan
Bank & Insurance Partner
BearingPoint
Paris, France
+33 6 21 01 0171
Yael-stephanie.gozlan@bearingpoint.com

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 70 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instil confidence in our clients.

bakermckenzie.com

Baker McKenzie.