noyb

European Center
for Digital Rights

GDPR: a culture of non-compliance?

Numbers of evidence-based enforcement efforts

noyb.eu

Executive Summary

GDPR compliance gap. In May 2018, the General Data Protection Regulation (GDPR) first applied to the processing of personal data in the EU. While it once promised to usher in a new era of stricter data protection through strict enforcement and high fines, the practical experience suggests that the daily practice still lacks behind its political promises. What was missing until today: objective evidence on compliance and evidence-based enforcement and compliance strategies.

Evidence-based compliance efforts. In other areas of the law, extensive sociological, psychological, and practical evidence was generated to develop effective and efficient enforcement and bring law and practice closer together. Such evidence is largely missing when it comes to GDPR compliance. For this reason, *noyb* conducted a survey that is supposed to serve as a starting point for evidence-based compliance approaches. In our survey, we targeted data protection professionals – people who are at the forefront of compliance efforts and have unique knowledge of the internal decision processes of controllers and processors. The aim of this questionnaire was to gain a deeper insight into the organisational drivers that lead to more GDPR compliance, to advance knowledge on the most important internal and external factors, and to derive key takeaways for future effective internal compliance work and enforcement efforts.

74.4% assume relevant violations at an average company. More than 1,000 privacy professionals, largely working as data protection officers (DPOs) or internal compliance departments of large companies, answered our questionnaire. While the survey shows that at least awareness of privacy issues grew during the last five years, most companies still don't comply with the GDPR. 74.4% of the respondents agree with the statement that *"if a data protection authority (DPA) would walk through the door of an average company tomorrow, it would surely find relevant GDPR violations"*. This is an extremely high percentage and indicates that privacy professionals still largely operate in a culture of non-compliance or merely partial compliance. These objective numbers match the experience of *noyb* and continuous anecdotal indications.

Hard to convince internal players. One major reason for this seems to be that DPOs are having a hard time convincing decision-makers within their companies to make the necessary changes in order to achieve GDPR compliance. This is especially the case for sales and marketing departments, where 56% of respondents reported difficulties in convincing them to implement higher compliance. On the contrary, these departments even pressure DPOs to limit GDPR compliance. In addition, 51.3% of respondents reported that non-EEA/EU suppliers are hard to convince of changes to comply with the GDPR – contrary to only 22.3% for EEA/EU suppliers. 38.5% report that senior management is hard to convince of changes, while 32,3% even report pressure from senior management to limit GDPR compliance. While there is a common argument that GDPR compliant products are not in demand, only 12.6% report pressure from business customers to limit GDPR compliance in the interest of business.

Fines, reputational harm and deterrence. When asked about factors that contribute to compliance, the participants responded that fines – especially high fines – are the biggest driver for achieving GDPR compliance within organizations. 63.5% report that the mere fear of fines is a driver for compliance. This isn't only valid for fines against the organisation itself. Instead, DPOs are reporting a clear spillover effect. 51.6% say that if another company gets fined for violating data protection law, it can influence the compliance of their own businesses. 61.5% agree that such a deterring effect exists when it comes to *"high fines"*. In addition, (the risk of) reputational harm is a very influential factor for GDPR compliance.

Soft-law instruments surprisingly inefficient. The least influential in practice, on the other hand, are EDPB and local DPA guidelines. Surprisingly, only 15.7% find EDPB guidelines *"somehow influential"* and only 7.3% find them *"very influential"*. The numbers for local DPA guidelines are only slightly better at 17.7% and 7.9%. This could be due to the fact that the DPOs – in their responses to open questions – considered these guidelines to be very general.

Deterrence stays national. More than seven years after the GDPR had been adopted, privacy professionals hardly take a look across national borders. This is despite the fact that the law was supposed to establish a common European legal framework. Many respondents stated that there are still quite some differences in how the GDPR is interpreted, applied and enforced across the EU. Considering this factor, it seems logical that only 23.0% and 22.8% find DPA or court decisions in other EU jurisdictions influential, versus 48.5% and 45.7% when it comes to decisions in their own jurisdiction. Only the Court of Justice (CJEU) is reported to be about as influential as national decisions at 43.4%.

DPOs call for more enforcement. The answers also provide information on possible solutions. About 70% of the respondents agree that *"we would need more DPA enforcement in order to actually improve user privacy in practice"* and that *"we would need more clear decisions by DPAs and courts to improve compliance"*. Decisions to informally close complaints – currently the most common DPA action in many EEA/EU jurisdictions – are seen as even less influential than social media postings by data subjects. Direct complaints by data subjects are not seen as highly influential, while formal data subject complaints before DPAs are seen as influential by 60% of professionals. The most relevant actions are formal decisions at 58%, orders to comply with the law at 61% and fines at 67.4%.

We hope the objective numbers provided in this report provide a good first basis for DPOs, authorities and decision-makers to focus on efficient and effective work on GDPR compliance!

Max Schrems
Honorary Chair of noyb.eu

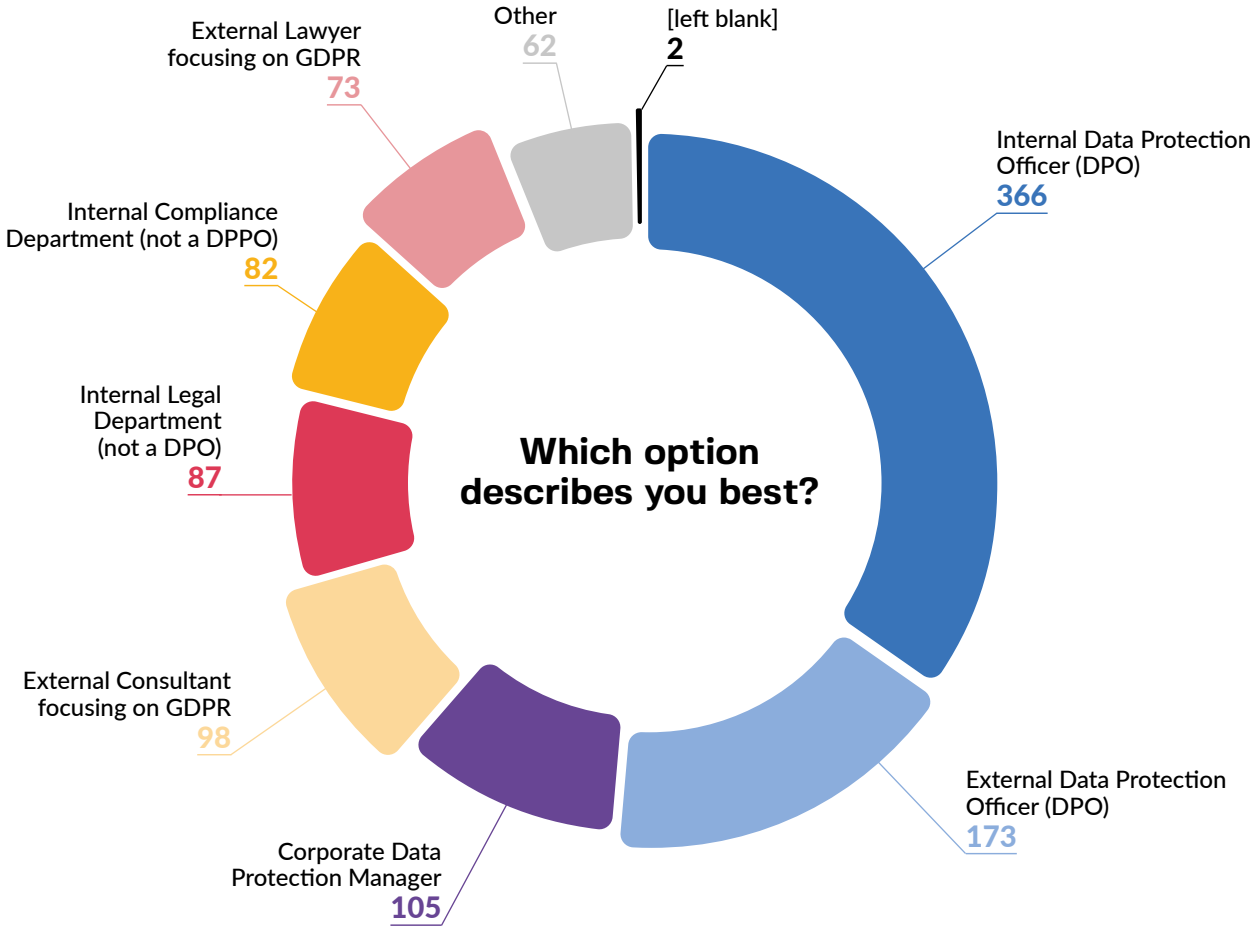
More Details

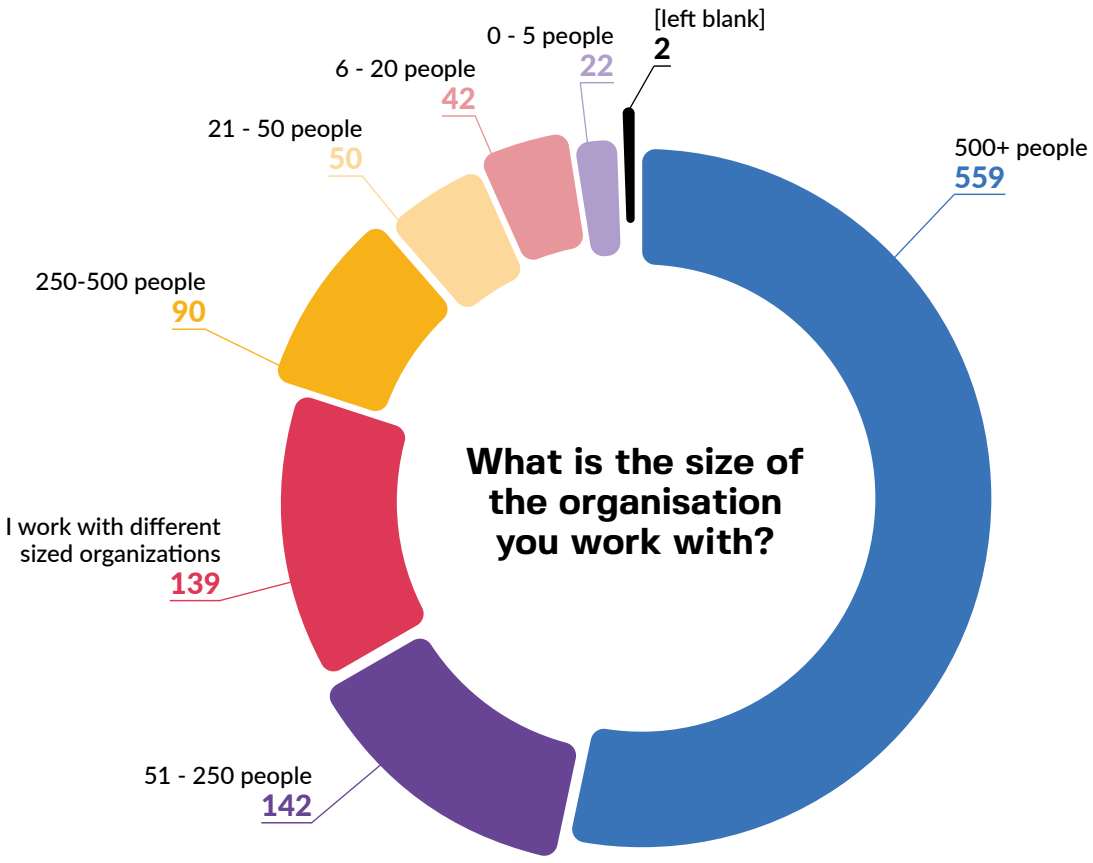
1. Methodology

In November 2023, *noyb* conducted an online survey to gain reliable insight into the practical implementation of the GDPR. The survey included, inter alia, questions about companies' GDPR compliance, about the difficulty of convincing other departments or employees within a company of GDPR compliance, and also questions about the most relevant factors that influence the GDPR compliance. In addition, the survey included questions about the company size, the company being subject to the GDPR and the profession of the respondents.

Target audience. The survey focused on data protection officers (DPOs) and professionals working in the field of GDPR compliance. Given their legal task to work on controllers' or processors' compliance from within the company, we consider this target audience the most relevant to achieving an accurate, insightful and neutral view on internal decision-making. DPOs regularly engage with all relevant players and are part of the internal decision process in companies, while having a statutory role to ensure compliance.

Potential biases or inconsistencies. We assumed that a relevant number of professionals working in the area may have different views than academics, authorities, or users when it comes to the specific level of compliance that must be achieved. However, given that the survey mainly focuses on identifying factors that lead to decisions in a certain direction, disagreements about the exact level of compliance seemed irrelevant for the purposes of this study. Contrary to this expectation, many responses indicate a very homogenous view as to the current state of compliance in the sector. Responses to open questions did not reveal any elements that were not adequately covered by the questionnaire.

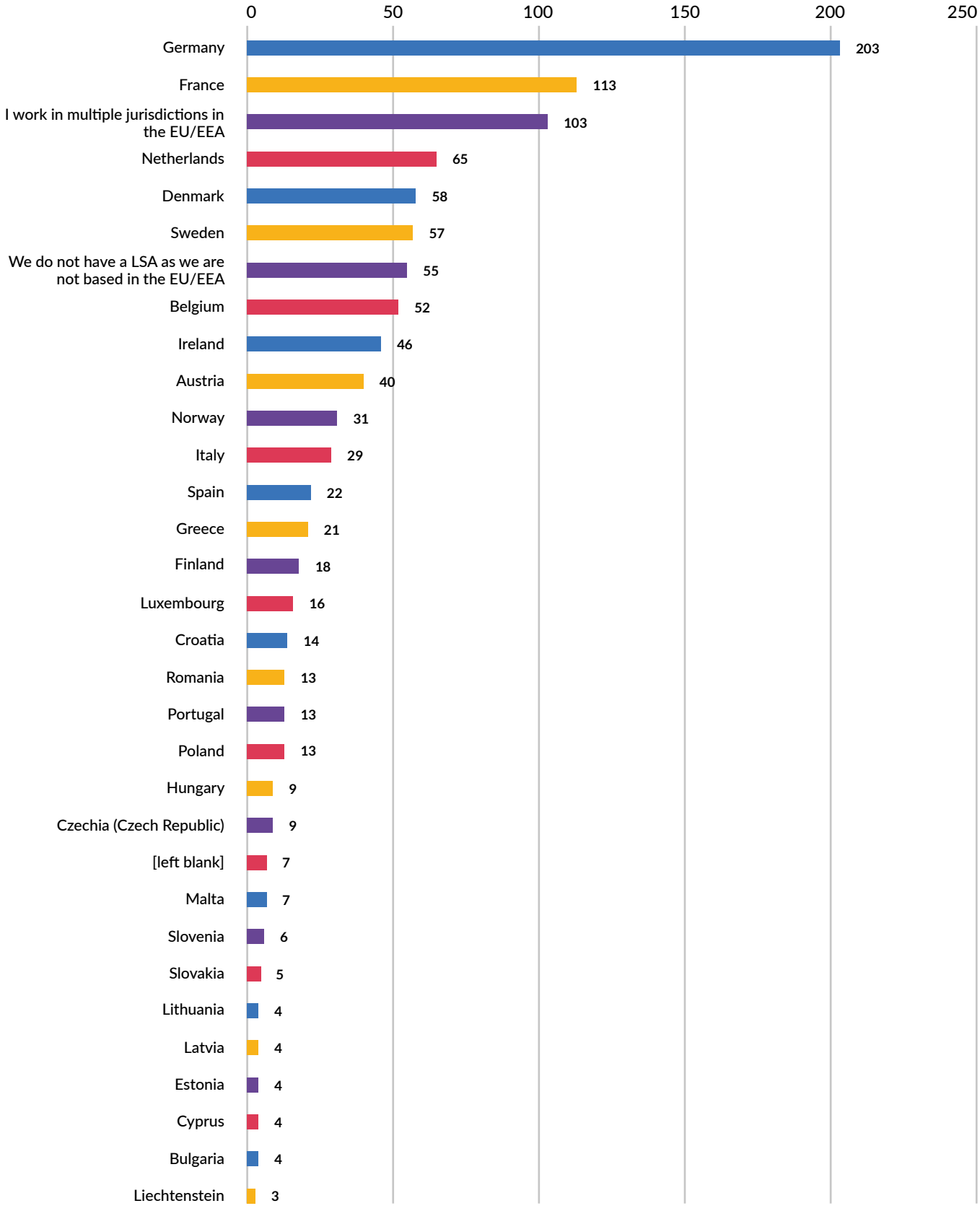

Which option describes you best?
Other 62
[left blank] 2
External Lawyer focusing on GDPR 73
Internal Data Protection Officer (DPO) 366
Internal Compliance Department (not a DPPO) 82
Internal Legal Department (not a DPO) 87
External Consultant focusing on GDPR 98
External Data Protection Officer (DPO) 173
Corporate Data Protection Manager 105


What is the size of the organisation you work with?
[left blank] 2
0 - 5 people 22
6 - 20 people 42
21 - 50 people 50
500+ people 559
250-500 people 90
I work with different sized organizations 139
51 - 250 people 142

Distribution of the survey. We initially shared the survey online, both via *noyb's* social media accounts (for example, on LinkedIn and Twitter/X) and via our weekly newsletter GDPRtoday. GDPRtoday is sent to more than 10,000 subscribers. Traditionally, the followers of these accounts and newsletters have a predominantly corporate background (e.g., data protection officers, lawyers, consultants and alike) with a strong geographic focus on the EU/EEA region. The largest number of participants reached the survey directly or via an unidentified referrer. Of all identified referrers, the largest number of participants came through links on LinkedIn.

Received data. Between November 16th and December 4th, we received 2,173 responses in total. The data was reviewed for inconsistencies or manipulative answers. No inconsistencies were found. From the total number of responses, participants answering less than 75% of all questions and participants working in companies that are not subject to the GDPR were excluded from the analysis. This led to a total of 1,048 respondents for the following analysis. As planned, the responses were provided overwhelmingly by external or internal DPOs, data protection managers and consultants from the EEA/EU. The geographic distribution of responses deviates from the distribution of the EEA/EU population. Some jurisdictions are overrepresented (e.g., Ireland, Denmark and Germany) and others are underrepresented (e.g., Italy, Spain and Poland). Some divergence is likely based on the higher number of controllers in some jurisdictions (e.g., Ireland). Overall, the geographic distribution did not seem to have influenced the outcomes on a European level. Given the typical controllers that employ a DPO, it is not surprising that the majority of responses were provided by professionals working in organisations with 500 or more employees. This led to a situation where the respondents are not representative of the overall number of controllers, which largely consist of small and medium enterprises. At the same time, large enterprises are especially relevant when it comes to large-scale non-compliance that affects large numbers of data subjects.

Which jurisdiction is your main GDPR regulator (LSA) based in? If you don't have an LSA, in which jurisdiction do you work the most?



2. Compliance per Chapter of the GDPR

While questions on the following pages concern the overall compliance with the GDPR, we initially asked participants to grade compliance per chapter of the GDPR.

Data transfer rules seem to be violated most often at 68.4%. Surprisingly, participants mentioned documentation and organisational obligations to be the second most problematic area at 65.7%, while data subject rights are reported as the least problematic at a combined 38.7% of respondents that felt *"some still have problems"* or *"most still do not comply"*.

Core principles of the GDPR (Article 5-11 GDPR) More than half of the respondents (50.1%) said that most companies still have problems complying with the core principles of the GDPR (Article 5-11 GDPR). These include principles such as purpose limitation or data mininisation in Article 5 and the need to have a legal basis for processing under Articles 6 to 10. These numbers clearly illustrate how GDPR compliance by companies is still different from compliance with other laws and regulations.

Information obligations and data subject rights (Article 13-22 GDPR) A surprising 57.8% and 58.9% of respondents think that most companies comply with the GDPR's *"core"* information obligations and *"core"* data subject rights. These responses differ from the actual experiences of data subjects.[1] *noyb* has filed a number of complaints with several data protection authorities, dealing specifically with controllers' lack of compliance with data subject rights.[2] These issues are also regularly the most common reasons for complaints. The numbers may be more consistent with data subjects' experiences if compliance with *"core rules"* would be defined as, for example, simply providing some form of a privacy policy or access to core elements of personal data.

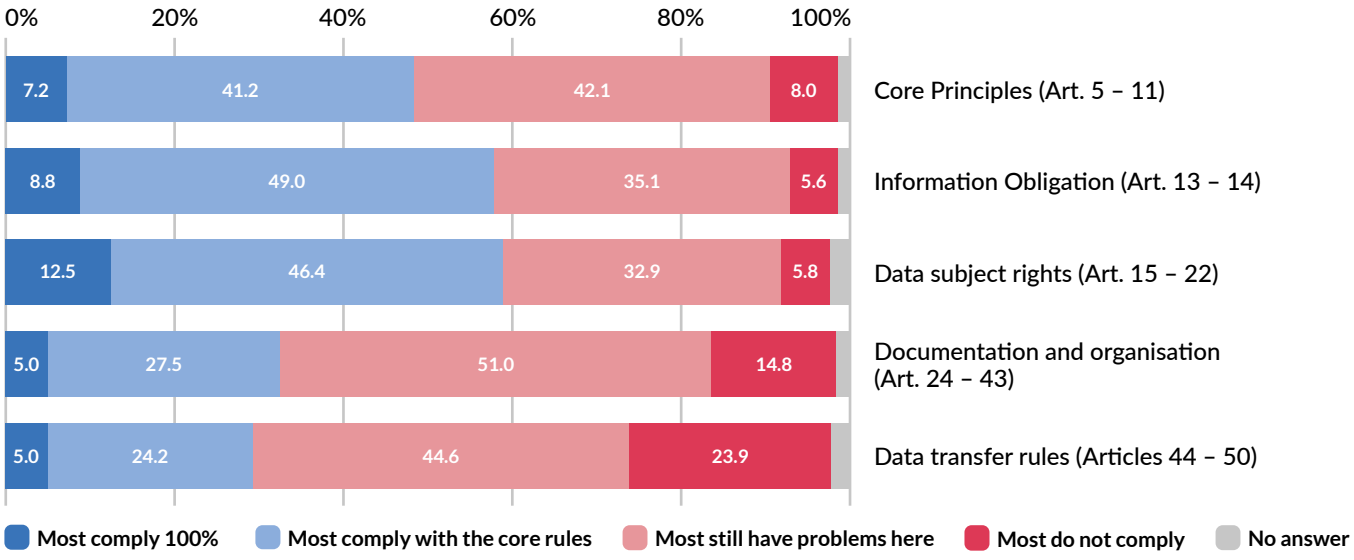
Documentation and organisational obligations and data transfer rules (Article 24-50 GDPR) On the other hand, the responses show that roughly two-thirds of the respondents think that most companies are still struggling to comply with the documentation and organisational obligations (Art. 24-43 GDPR) and data transfer rules (Art. 44-50 GDPR). Only 5% of respondents said that companies comply with these obligations 100% of the time. We would expect that survey participants largely work on these GDPR requirements and may focus their attention on these elements, which could lead to a certain bias in comparison with other elements.

100% compliance out of reach for most? Across all areas of the GDPR, only 7.7% of respondents said that, in their experience, *"most"* controllers comply 100% with any chapter of the GDPR. Compared to most other areas of law (tax, copyright or labor law), this is an alarming sign. Overall, the results indicate that it still seems to be largely "accepted" that companies violate even the core principles of data protection laws. The results clearly show a *laissez-faire* approach.

[1] Average numbers in noyb projects e.g. see more than half of controllers not responding to access requests under Article 15 GDPR and less than 10% providing a full response within the maximum deadline of one month.

[2] https://noyb.eu/en/project/right-rectification-art-16-gdpr

In your experience, how would you assess the compliance of most companies (your own and others) with the following parts of the GDPR?



Comments by Participants

"There's an improvement in awareness, but most profit-making businesses see [the GDPR] as something that restricts business."
– Internal Compliance Manager

"The GDPR's main principles are still not fully understood and followed by most controllers. This will not change as long as the authorities (especially the DPC) allow the big players to build their business models on intransparent processing of personal data of European data subjects."
– Corporate Data Protection Manager from Germany

3. Interplay between DPOs and Other Players

The ability of DPOs to carry out their duties is, among other things, influenced by how easy it is to convince management, other departments and external suppliers of the necessary changes to achieve GDPR compliance. Another important factor is the protection against undue influence by other players. The results clearly show that, in general, DPOs are having a hard time doing their job.

GDPR compliance is a hard sell to management and marketing. An analysis of the responses shows that management oftentimes is more of an obstacle than an ally when it comes to making the necessary changes to bring a company into compliance with the GDPR. Overall, top management seems to be slightly easier to convince of GDPR compliance than middle-management. Nevertheless, 38.5% of the respondents find it difficult to convince top management of necessary changes to comply with GDPR.

European suppliers only "net positive" group. The only group that is predominantly *"easy"* or *"somehow easy"* to convince of GDPR compliance are EEA/EU suppliers. It seems that, at least within Europe, the GDPR's approach of requiring a compliant supply chain is practical and provides GDPR compliant products.

Non-European suppliers are a major headache. The exact opposite can be seen when professionals have to deal with non-EEA/EU suppliers. 51.3% report that it is *"somehow hard"* or *"hard"* to convince non-EEA/EU suppliers of necessary changes to their products. We would expect that the issue of data transfers plays into this assessment, but also that overall market dynamics (like large *de facto* monopolies) are a source of frustration for many privacy professionals.

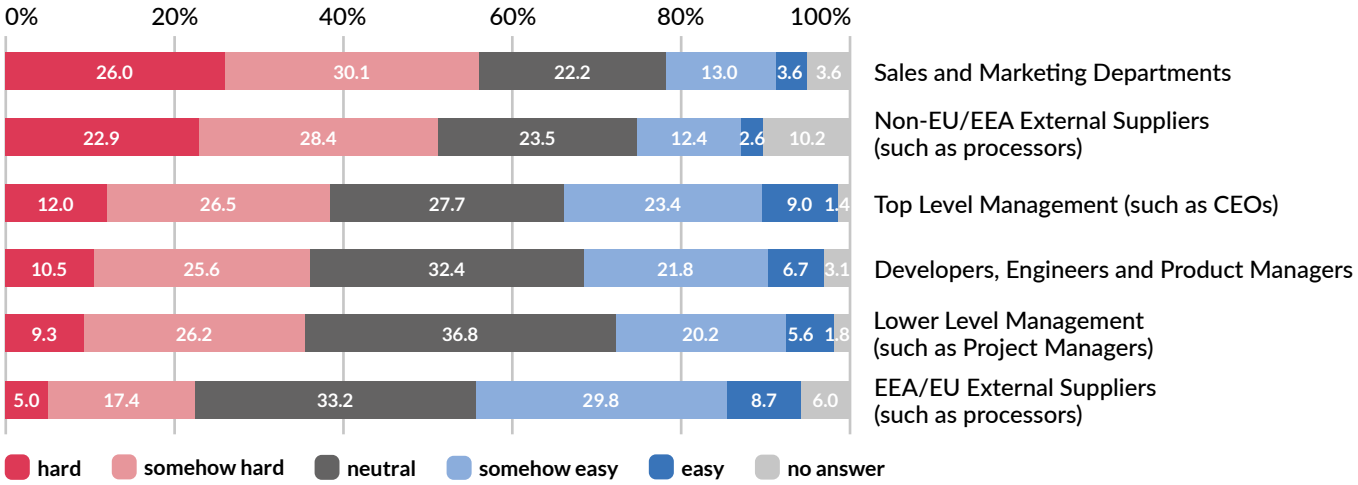
Sales and marketing hardest to convince. Reasoning with the sales and marketing department seems to be even harder: 56% of respondents said that it is hard to convince them of necessary changes in the interest of improved compliance.

DPOs report active "pressure" to limit GDPR compliance. A lot of respondents also experienced pressure to limit GDPR compliance in the interest of business. For example, almost a third of DPOs said that they experience pressure from management/CEOs to limit compliance. The survey also showed that it's not only hard to convince sales and marketing of necessary changes, but 46.9% of respondents said that they experience pressure from Sales and Marketing Departments, of which 19.0% can be considered serious pressure.

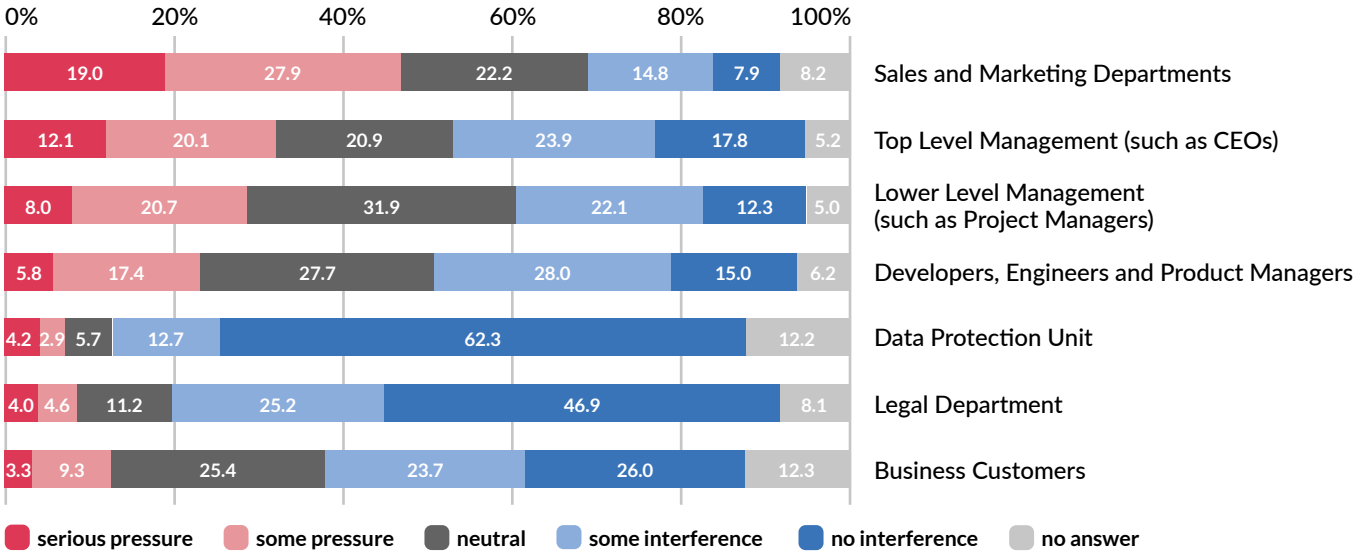
Little B2B pressure. Legal department backs compliance. Interestingly, business customers do not seem to pressure DPOs into limiting GDPR compliance within their company all too much. This may be an indication that products that comply with the GDPR are not rejected by B2B customers. Legal departments hardly exert pressure. There also seems to be almost no pressure within data protection units.

Recent EDPB report about the role of DPOs supports findings. The findings of this survey are in line with a recent EDPB report on the role of Data Protection Officers. Similar to this report, it shows the need for changes within organizations to make sure that DPOs can properly do their job. The EDPB report also highlights the fact that in some organisations, the DPOs aren't really independent.

How easy do you find it to convince the following players of necessary changes to achieve GDPR compliance?



From where did you experience pressure to limit GDPR compliance in the interest of business?



Comments by Participants

"GDPR principles require a strong data protection team in order to meet all the necessary requirements. In practice, this is not the case. Data protection is usually covered by an understaffed team, which cannot carry out all necessary tasks. I believe this problem needs more attention."
– DPO from Slovenia

"The law is complex and a lot of controllers/processors do window dressing. Management wants to use the data to make money and only wants to have to do the bare minimum to comply with the laws and regulations. Marketing departments and IT just want to do their thing and bypass privacy advice as much as possible. Even after providing training for 5 years, people still do not know how the law works as it is a complicated piece of legislation. Basically, it feels like fighting a tidal wave and loosing."
– DPO from the Netherlands

4. Internal Drivers for Autonomous Compliance

Our survey included several questions dealing with the biggest drivers for improving GDPR compliance. The questions were split into internal drivers for autonomous compliance, which mean stand-alone reasons for companies to comply with the GDPR, excluding any external action against the company by an authority, data subject or anyone else. The respondents were asked to rate 14 factors related to autonomous compliance.

Most influential internal factors for autonomous compliance

The results of the DPO survey show that possible fines and other sanctions and the possible loss of reputation are considered to be the biggest drivers for compliance:

– About two-thirds of respondents considered possible fines or loss of reputation somehow or very influential. Only 6.5% and 5.4% of respondents considered fines and the possible loss of reputation not influential at all.

– 57.9% of the respondents also said that compliance demands by suppliers and customers are influential.

– In addition, 50.4% said that the general company culture and company ethics lead to autonomous compliance.

Least influential internal factors for autonomous compliance

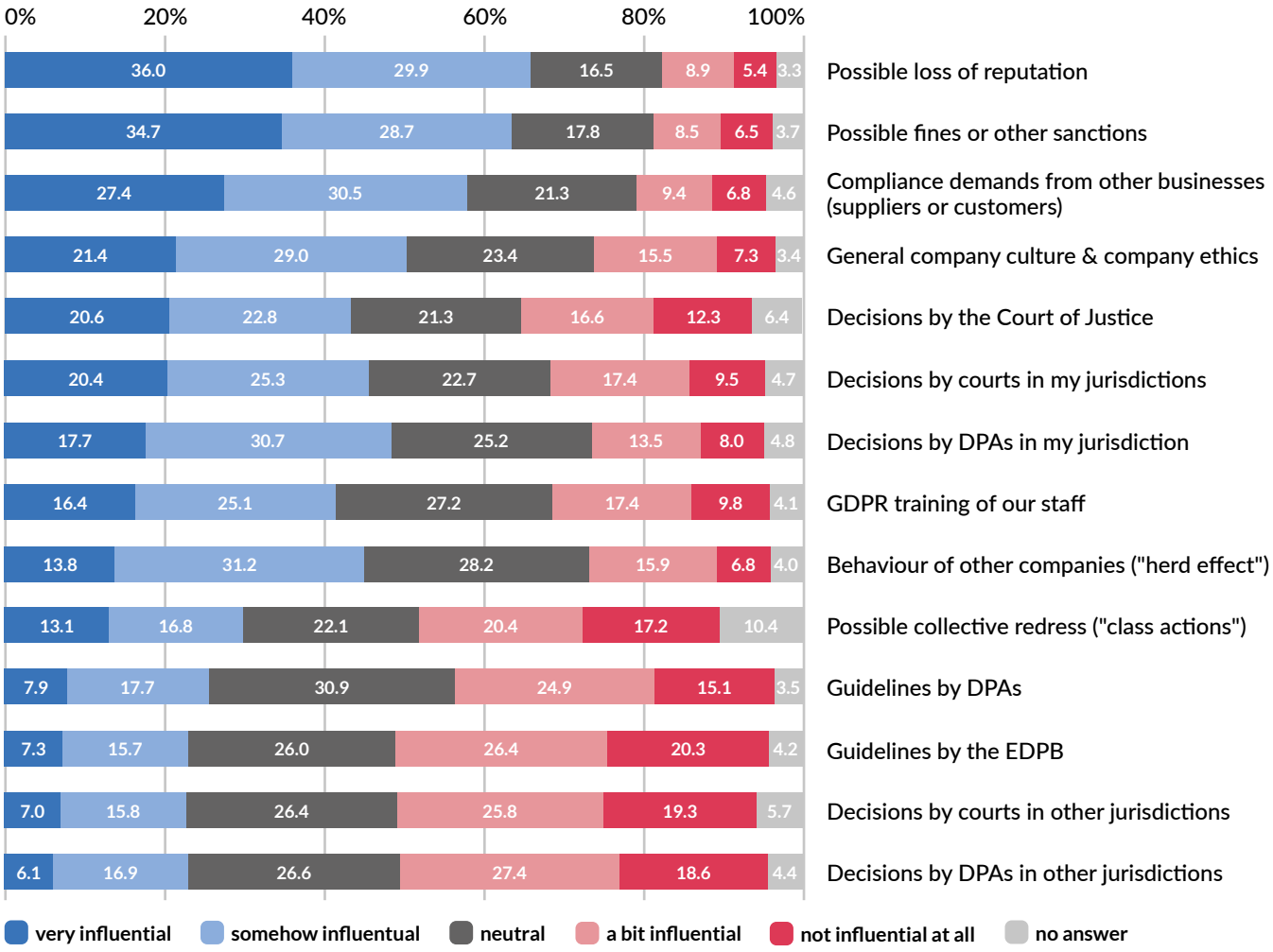
The analysis shows that the following factors were found to be not very influential or not influential at all:

– Surprisingly, EDPB guidelines were found to be the least influential factor: 46.8% of respondents considered these guidelines not influential. Considering the fact that the establishment of such guidelines is the main focus of the EDPB and that they are endorsed by all DPAs, this result is remarkable. According to the respondents, the guidelines are too general, making them inapplicable in practice. However, it seems unclear if guidelines are still avoiding concrete positions on matters relevant for controllers and processors or if there is a lack of ability to apply abstract law and guidelines to concrete situations.

– DPOs also seem to focus on their own jurisdiction, meaning that decisions by DPAs or courts in other countries aren't considered as influential: 46% of respondents stated that decisions by DPAs in other countries are not influential, while 45% considered court decisions in other jurisdictions as not influential. The respondents said that there are still relevant differences in the interpretation, application and enforcement of the GDPR between EU member states, despite it being a European law.

– Last but not least, possible collective redress is not (yet) considered to be an influential internal driver for autonomous compliance. The reason for this could be that there haven't been many class actions in the area of data protection yet.

Even before issues are raised externally (e.g. by a data subject or regulator), which factors are the biggest drivers for decision makers in your organisation to opt for more compliance?



Comments by Participants

"The biggest motivators for change are the media and large GDPR fines."
– DPO from Croatia

"Unfortunately, we are greatly dependent on our DPAs and how they choose to enforce the GDPR. The EDPB helps a lot with their proactive approach, as well as the ECJ with more clarity about some issues, but most organizations will rely and only look up the local DPA's work, which means that the end results may vary. [...]."
– DPO from Croatia

5. External Drivers for Autonomous Compliance

The survey also included questions about external drivers for autonomous compliance. By that, we mean external events that influence the GDPR compliance of companies without there being any direct external action against them. External events that can indirectly trigger actions within a company that lead to improved compliance are especially relevant for compliance through deterrence. The respondents were asked to rate 11 factors from not influential at all; a bit influential; neutral; somehow influential; to very influential.

Most influential factors

The survey results clearly show that fines – especially large fines – and reputational damages are, again, considered to be the most influential external drivers for autonomous compliance:

– 61.5% of respondents considered DPA decisions that include "high fines" against other organisations as influential. This compares to 51.6% who said that DPA decisions against other organisations that include just any fine are influential. The amount of any fine therefore increases the general deterrence by about 10%.

– 52.1% of respondents considered reputational harm to other organisations as influential.

– Furthermore, 46% said that court decisions against other companies that lead to reputational harm are influencing their own company's compliance.

Average factors

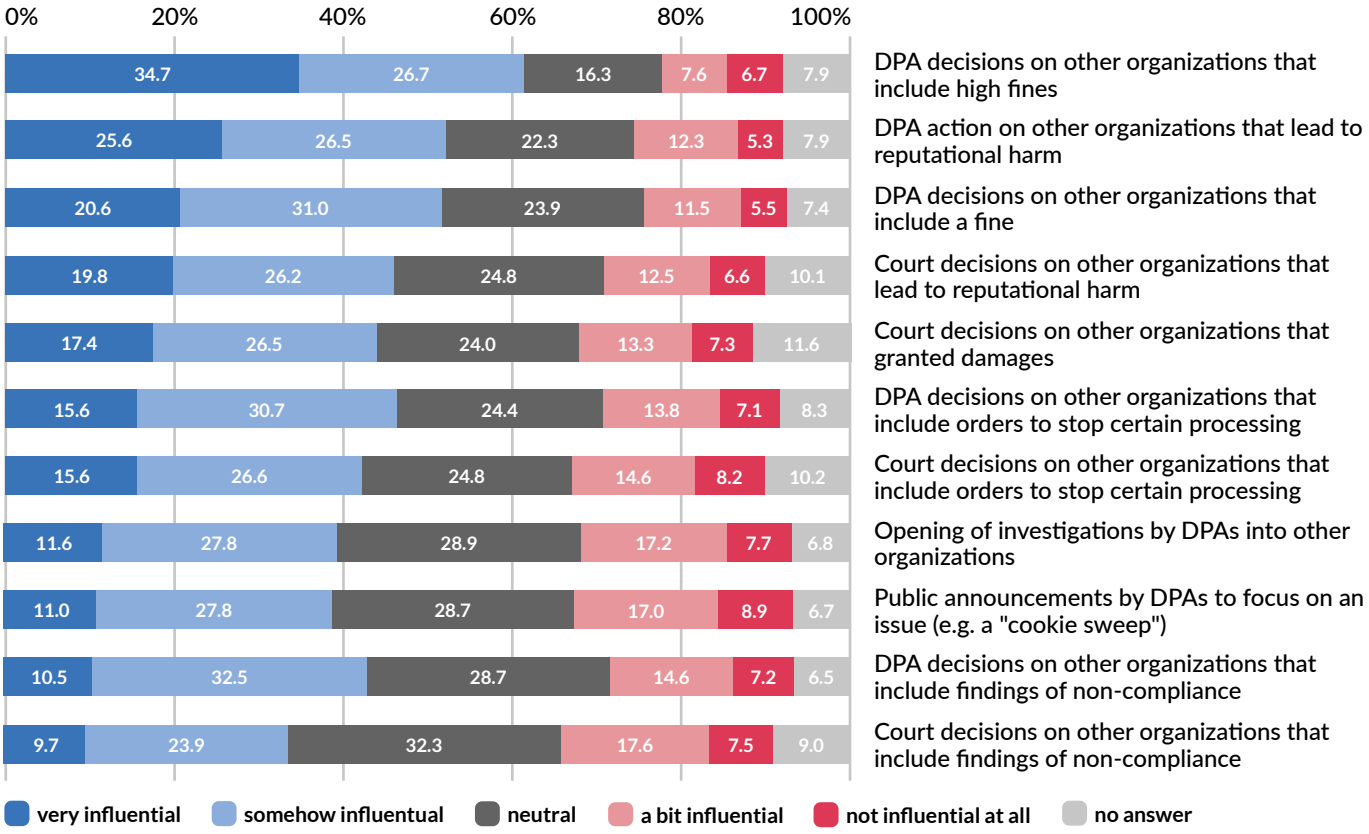
– Public announcements to focus on a topic, such as "cookie sweeps" or the opening of investigations into other organisations, are not seen as highly influential but still show an overall positive influence. In our experience, we saw strong evidence for such approaches working.[3]

Least influential factors

– According to the respondents, the least influential external drivers for autonomous compliance are court or DPA decisions against other organisations that merely include a finding of non-compliance (declaratory judgements). Only 33.6% consider such decisions as influential.

[3] When the CNIL announced enforcement against deceptive cookie banners, we could see a significant drop in non-compliant French websites during our cookie banner project

Even before any issues are raised externally (e.g. by a data subject or regulator), which types of enforcement actions against others are the biggest drivers for decision makers in your organization to opt for more compliance?



Comments by Participants

"The GPDR is essentially good. It just needs more enforcement and court action, both so that we get more clarifying CJEU jurisprudence, and so that organisations run a greater risk of losing money over violating the GDPR."
– Internal Compliance Department employee from Sweden

"Without fines or bad press it's hard to get people truly involved."
– Internal Legal Department employee from France

"There is a lack of enforcement, more enforcement is needed. Without it, the GDPR is a toothless tiger."
– DPO from Germany

6. Enforcement and Reactive Compliance

Besides general deterrence, law enforcement usually requires individual direct action. Respondents were therefore asked which direct external actions are most influential for a company's decision to improve GDPR compliance. The survey distinguished between 12 factors that had to be rated from not influential at all; a bit influential; neutral; somehow influential; to very influential.

Most influential

According to the respondents, the following external actions by an authority are most influential:

– 67.4% of respondents said that DPA decisions against their company, including a fine, are the most influential external factor leading to improved compliance. This would be in line with Article 83(1) GDPR, which requires *"effective, proportionate and dissuasive"* penalties.

– Also, 61% of respondents said that DPA decisions against their company, including an order to comply, were influencing compliance. In practice, an order to e.g., stop a profitable form of data processing may have even higher financial implications than a mere fine.

– According to 60% of respondents, data subject complaints with a DPA against their company are influential, while only 39.3% think that raising an issue directly with the company has a relevant influence.

Least influential

The following direct external actions issued by an authority were found to be the least influential:

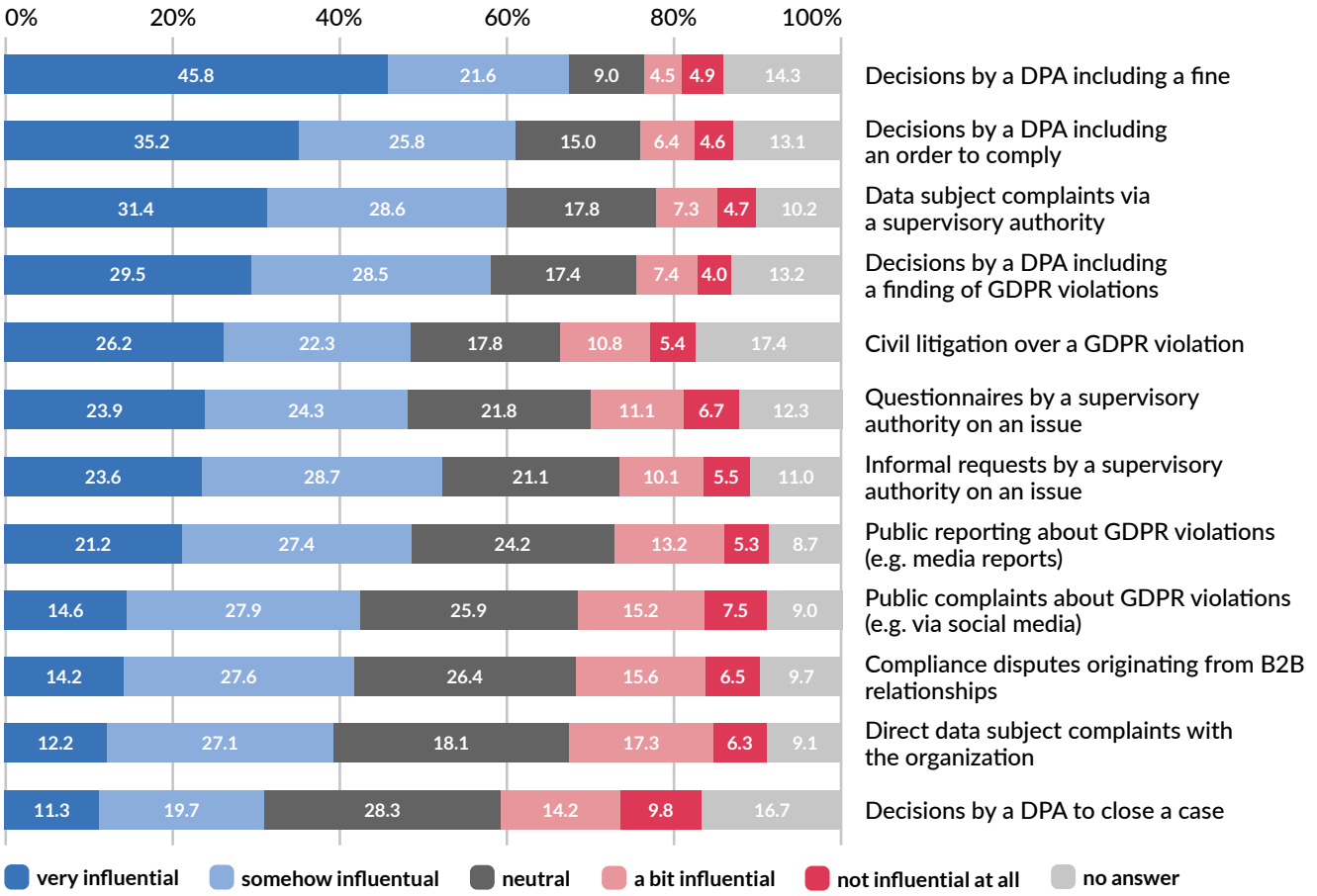
– According to respondents, the least influential external action would be a DPA decision to just close a case against their company, as commonly done via so-called "amicable resolutions" or "informal decisions". While only 30.9% said that this would not be *"somehow"* or *"very"* influential, this is the most common DPA action in many EEA/EU jurisdictions.

As part of an open question in the survey, the respondents added that data breaches and commercial losses can drive their companies towards improving their compliance.

Conflict between DPA strategies and DPO feedback? All in all, the survey clearly shows that the biggest drivers for improved compliance are large fines, orders to comply and reputational damage.

However, the actions most commonly chosen by DPAs are considered to be least influential by respondents: simply closing cases against organisations, requesting data subjects to directly raise issues with companies, finding that there is a GDPR violation without any further consequences and publishing (general) guidelines are consistently rated as the least efficient approaches.

Which types of direct GDPR disputes do you think influence compliance most? Which type of disputes are the biggest drivers so that decision makers in your organization actually opt for more compliance?



Comments by Participants

"The risk based approach to compliance is focused on risks to the organisation, not to the data subjects. As long as companies get away with lack of compliance, they will continue to do so."
– DPO working in multiple jurisdictions

"Economics beats human rights. The last Meta issue and how DPAs tolerate and explain legitimacy of paywalls illustrates the point. It is disappointing."
– DPO working in multiple jurisdictions

"There is no real enforcement and most DPAs openly favour the companies in their territory. For example, the CNIL advertised that they get 14,000 complaints per year but only do 25 deep investigations per year."
– DPO from France

7. Overall Status after 5+ Years

In order to gain a general insight into the respondents' experience with the GDPR since it came into force almost six years ago, we picked some typical or pointed claims about the law for the last question of the survey. The respondents were asked if they agreed or disagreed with these claims.

– The **lack of compliance and on-premises factual** investigation is further illustrated by the fact that 74.4% of respondents think that if a DPA would walk through the door of an average controller tomorrow, they would surely find "relevant" GDPR violations.

– Equally, 70.9% think that we need more clear decisions by DPAs and courts to improve compliance. The responses to previous questions in this survey already showed that current **soft-law approaches via guidelines** are not really leading to more compliance.

– 69.9% of respondents think that we need more DPA enforcement to actually improve user privacy in practice. This confirms previous responses, which showed that only large fines and reputational damage can really improve GDPR compliance.

– 35.8% find that the *"deterring effect"* of the GDPR has been lost over the last five years, only a combined 31.2% do not support such a claim.

– While 7.9% see less compliance by controllers that *"rely on personal data to make profits"*, there seems to be only a slight uptick compared to companies that do not focus on making profits from personal data.

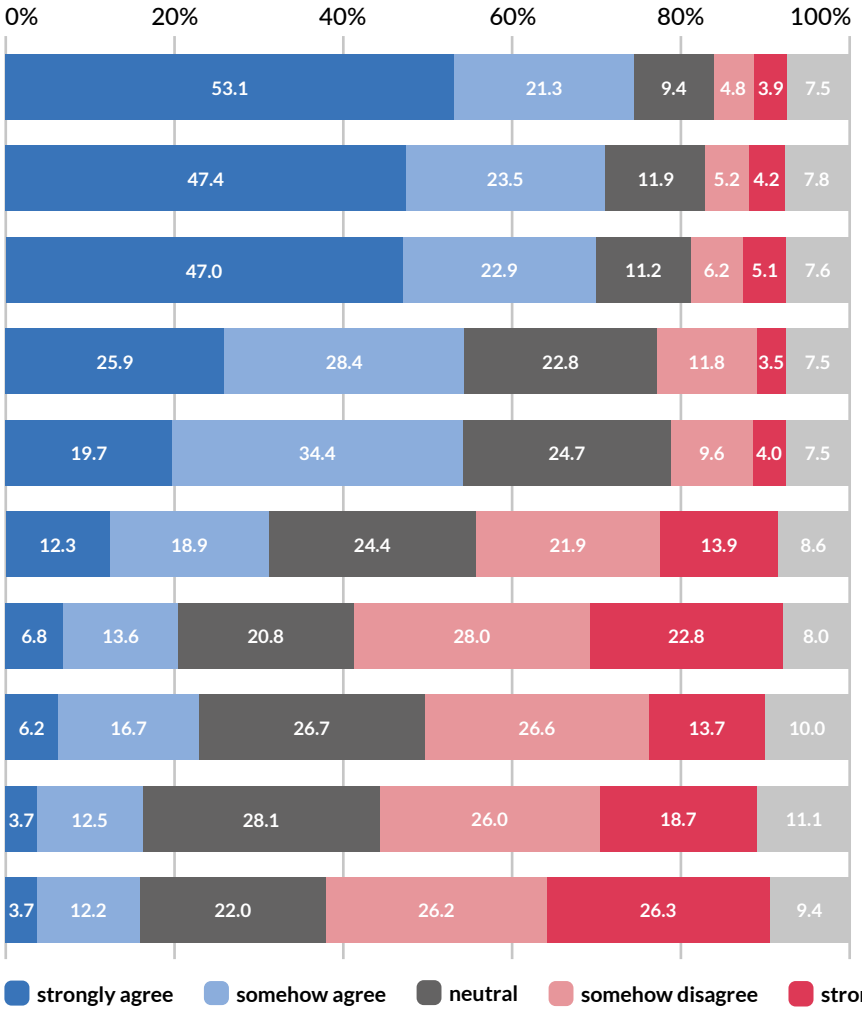
– When it comes to the real effect of the law, 19.7% of the respondents *"strongly agree"* that - independent of compliance on paper - the GDPR has significantly improved the processing of data by companies. Another 34.4% *"somewhat agree"*. Not surprisingly, for respondents from large companies reacting to a major shift in European law, a combined 54.1% see a positive effect on the processing of personal data. 50.8% also disagree that the GDPR is merely a *"bureaucratic exercise"*, while a combined 20.4% show some sympathy for that claim.

– In general, the respondents also said that at least awareness about data protection and privacy has improved in the last five years.

In summary, the respondents' feedback clearly shows that the ultimate goal of achieving broad and consistent compliance and enforcement across the EU has not yet been reached.

In their individual written responses, the respondents also repeatedly stated that the only things that truly make a company comply are fines and bad press. Some of them stated that without real enforcement, the GDPR is a *"toothless tiger"*, emphasizing the need for more enforcement. In addition, some respondents said that while there was a fear of enforcement in 2018, but that it has vanished due to a lack of enforcement action. This makes it increasingly harder to ensure compliance.

General status after 5+ years of GDPR Do you disagree or fully agree with the statements below?



Comments by Participants

"If Big Tech gets away with not complying with the GDPR, then why should small companies bother to comply?"
– GDPR lawyer from the Netherlands

"Things have significantly improved, but getting rid of 20+ years of organizations doing what they feel like with personal data will take longer than 5 years to remedy."
– DPO from Belgium

"Lack of enforcement weakens the right to privacy and data protection"
– DPO from Denmark

8. Suggested Action

The results of this survey paint a clear but alarming picture of the practical state of GDPR implementation. It also clearly identifies the lack of enforcement by European data protection authorities. While the GDPR led to improvements regarding the awareness of companies and the processing of personal data, the original promise of the GDPR of consistent compliance and enforcement was clearly not delivered. Therefore, based on the analysis of the results, we would make the following suggestions:

– A vast majority of respondents stressed that there is a **lack of compliance** and a **clear need for more enforcement from DPAs and courts** in order to make organisations improve their GDPR compliance. While courts were not the main focus of this study, an overly restrictive approach by the courts in some Member States, which limits the work of DPAs even further, seems highly problematic in the light of these results.

– The survey shows that many known enforcement tools of DPAs have a positive impact. However, the survey also shows that two of those options clearly need to be prioritised: **high fines and the publication of findings and decisions**. Both are typical forms of deterrence that are well-known and studied in many other areas of the law.

– Companies are largely looking at local enforcement. Spill-over effects from other jurisdictions are not overly relevant. It therefore seems that DPAs would have to **"relay" European decisions or guidelines** to ensure that companies react to these decisions.

– The fear of reputational harm could **also be an indication that DPA's public relations and publication efforts** may be a good investment when it comes to the enforcement of the GDPR – even if their options are often regulated by applicable procedural laws. Currently, a lot of DPA decisions and investigation reports can't be publicly accessed, leaving controllers and processors without an option to even know what DPAs have decided. If decisions are published, they should ideally include the names of the organisations involved.

– Relatively **broad enforcement actions** (like a "cookie raid" on random websites or questionnaires sent directly to controllers) may not be the most feared instruments but are seen as having an overall positive impact, while limiting the need for DPA resources. noyb's experience shows that a mere email by a non-profit can get up to 40% compliance rates without even the need for a procedure.

– Written responses show, that most companies clearly follow a "risk-based approach" when it comes to compliance with the GDPR. As long as they can see that there is a lack of enforcement – and therefore little risk of having to pay a substan-

tial fine or even reputational damage – it pays off for controllers and processors to violate the law or cut corners in compliance. The only way to change this equation seems to substantially **increase the "risk" of enforcement.**

– Responses that see relevant compliance issues being found when DPAs "walk into" the offices of a controller also indicate that **on-premises checks** seem to be most feared – this question got the highest number of agreeable responses in the entire survey.

– In practical terms, broad and consistent enforcement and deterrence would require **technical, financial and organisational resources** that allow DPAs to engage in efficient and effective enforcement. To our knowledge, only some DPAs started to experiment with technical solutions, while many still operate in a rather analog way that requires human resources that are not available to them.

– On the other hand, DPAs cannot expect a shift in compliance from publishing more **guidelines or from "informal" solutions** that lead to the closing of cases. If guidelines are published, they should be clearer and more precise, even when there are diverging views within the EDPB.

While this study was able to identify some high-level trends, obstacles and options to enforce the GDPR more efficiently, further research would be needed to identify the efficiency of specific enforcement strategies. The view of privacy professionals allows a good general understanding of expected factors, but these views would have to be matched with real-life data on various enforcement projects.

Currently, there is very little research and available data. We therefore see an urgent need to **gather more objective evidence** during ongoing compliance and enforcement work to ensure that the work of DPOs and DPAs is undertaken in the most efficient way. We would expect that the use of public and private resources, effort and time when ensuring GDPR compliance could be greatly improved when further developing an approach to evidence-based compliance and enforcement work.

European Center for Digital Rights

Imprint:
noyb – European Center for Digital Rights

Goldschlagstraße 172/4/3/2
1140 Vienna – Austria

ZVR: 1354838270