EVIDENCE-BASED GDPR OPTIMISATION

WHAT PROFESSIONALS REALLY NEED

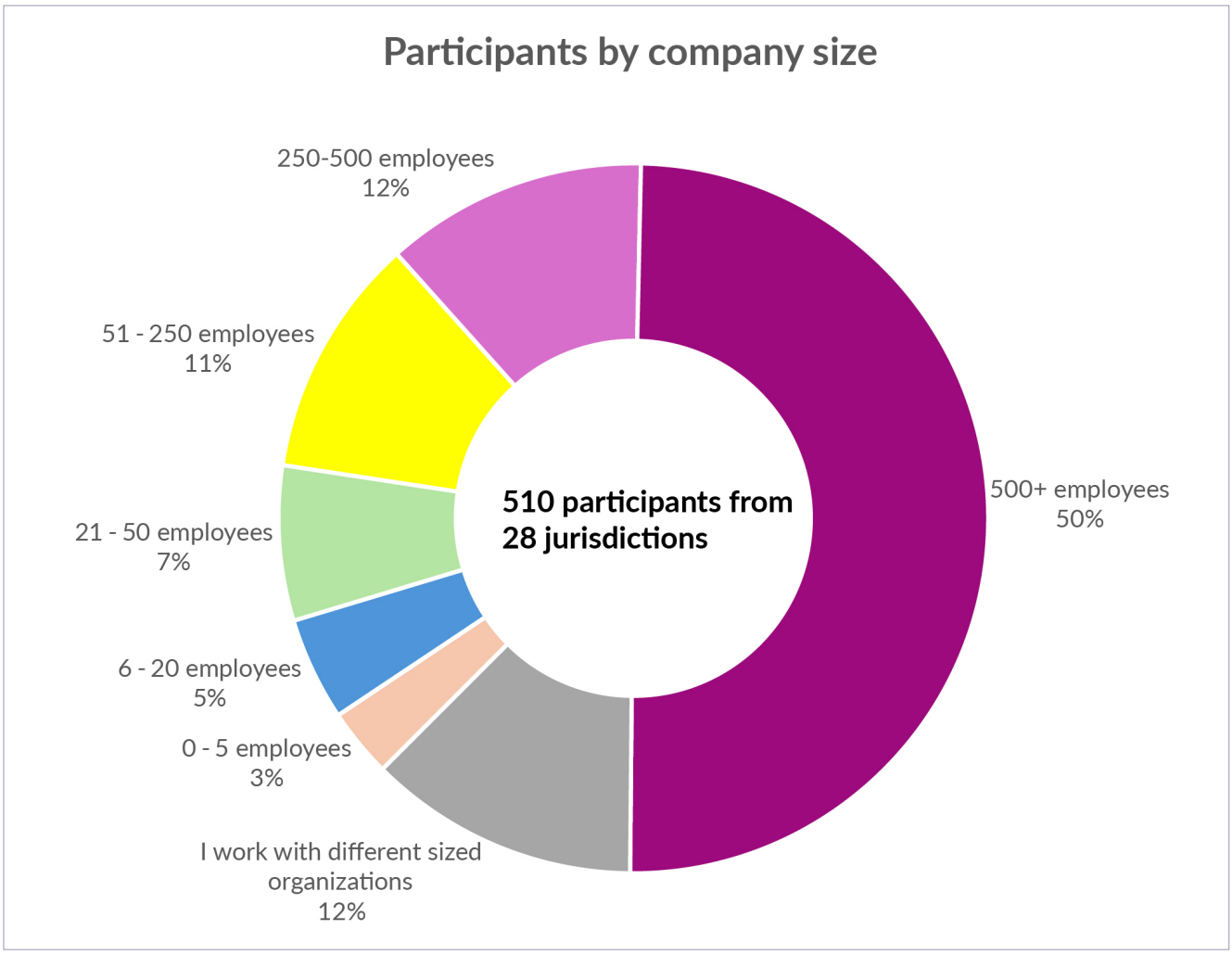
noyb.eu

Table of Contents

Preface

There is currently a lot of talk about the workload the GDPR creates for businesses in Europe, and what would be needed to limit it. With this survey, *noyb* wanted to find out which elements actually take up the most time for DPOs and Privacy Professionals in practice - and where time is best spent to ensure people's data protection. In addition, *noyb* asked the participants of this survey whether new regulatory approaches like "whitelisting" of standardised data processing activities and providing "blacklists" for clearly prohibited processing would be practicable. In practice, the various B2B relationships between controllers and processors often create the most paperwork. Consequently, possible new approaches to this issue were also subject of the survey.

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 the compliance of controllers or processers from within the company, we consider this target audience the most relevant to achieving an accurate, insightful and neutral view on the implementation of the GDPR on the ground.



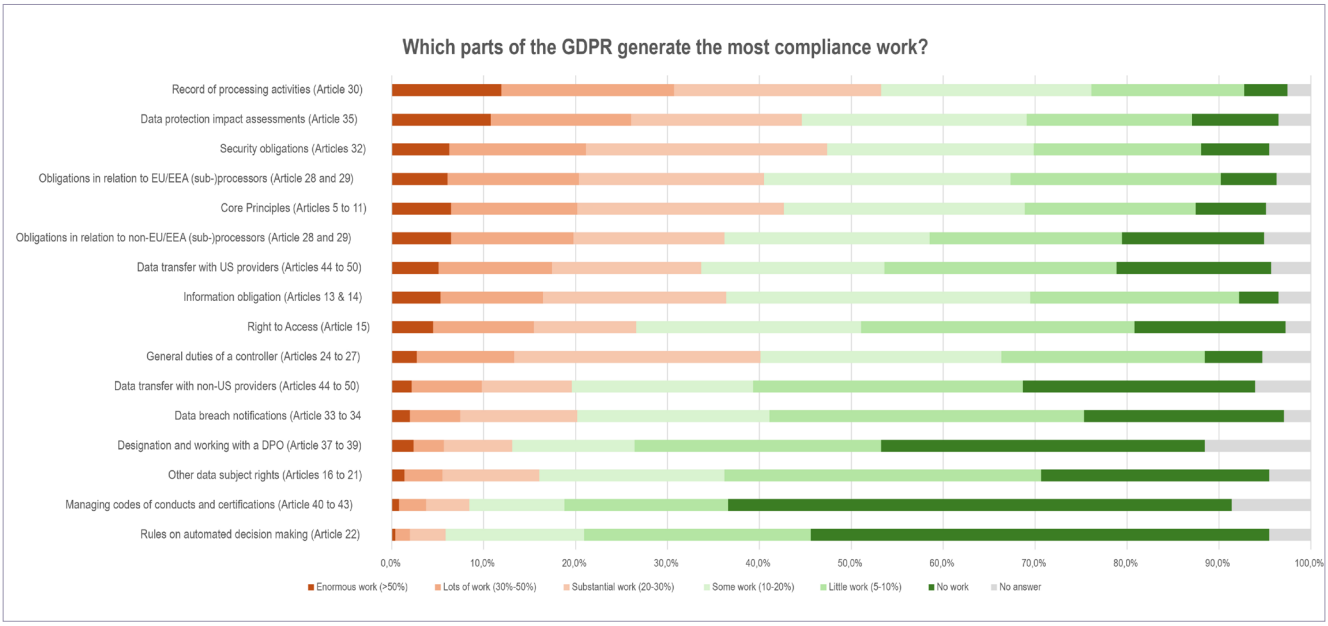
Data collection. We initially shared the survey online, both on *noyb*'s social media accounts (for example, on LinkedIn and Twitter/X) and in our weekly newsletter GDPRtoday. GDPRtoday is sent out to more than 13,000 business subscribers. Traditionally, the followers of these accounts and newsletters have a corporate background (e.g., data protection officers, lawyers, consultants and alike) with a strong geographic focus on the EU/EEA region.

Received data. Between July 3rd and July 14th 2025, we received 1,190 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 510 respondents for the following analysis.
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 over-represented (e.g., Ireland, Denmark and Germany) and others are under-represented (e.g., Italy, Spain and Poland). Some divergence is likely based on the higher number of controllers in some jurisdictions (e.g. Ireland) or additional national duties to appoint DPOs (e.g. Germany). 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.
noyb has indicated hours spent per week to the categories of workload ("enormous" to "no work"). Interestingly, survey participants have, on average, overestimated the total time spent per week far beyond the point of realistic weekly work time. While the absolute number of hours spent per item was therefore clearly inaccurate - the relative comparison of time spent should be reflective of real-life workloads.

Structure of survey. First, we tried to generate a baseline understanding of all elements of the GDPR. We did this by measuring both the workload and the benefits that various GDPR chapters or elements generate according to DPOs and Data Protection Professionals. While they typically have a very good understanding of the workload, some benefits may be seen from a more selective point of view when compared to data subjects. Nevertheless, the general tendency, in the view of DPOs and privacy professionals, seems to be a useful basis for further discussions.
Three regularly debated issues were surveyed in more detail, namely (i.) the current "risk based approach" in an otherwise "one size fits all" law, (ii.) compliance work between businesses under Article 28 and 29 GDPR and (iii.) a "blacklist / whitelist" approach to limit the need of controllers and processors to correctly apply often vague or unclear terms in the GDPR themselves.

Start of a debate. While this is just the beginning of a larger debate sparked by the Digital Omnibus proposal, we believe that evidence-based changes to the GDPR could be beneficial for everyone: controllers, processors, data subjects and authorities. We hope that these first results could guide our way towards useful solutions for actual problems, instead of chasing buzzwords.

1. Workload and impact on data subjects for different Articles of the GDPR



• Article 5 to 11 – Core GDPR rules

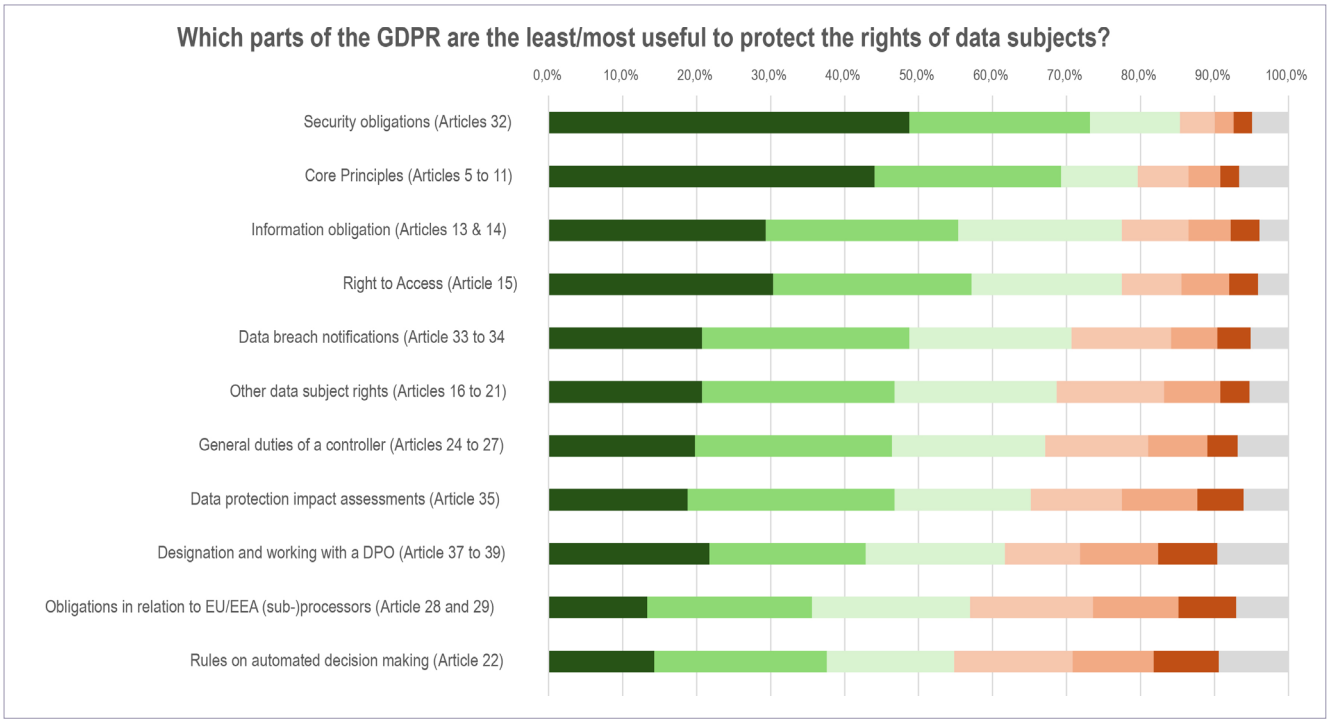
Unsurprisingly, the core rules of the GDPR generate a relevant workload, but they also provide protections (see on the right). Given that these rules largely mirror Article 8(2) of the EU Charter of Fundamental Rights, there are very few options for reform. Mirroring the workload, company representatives also highlight that these rules are the second most useful for protecting data subjects. This is in line with our experience and indicates little to no need for change.

• Articles 13 and 14 – Transparency duties

Unsurprisingly, the documentation duties that result in a public privacy policy rank rather high in workload (see also Articles 24 to 30 below). However, transparency is strongly linked with the notion of 'fairness' in Article 8(2) of the Charter and is a pre-condition for the exercise of rights by the data subject.

Corporate Data Protection Professionals, however, rank the benefit of Articles 13 and 14 very high, indicating that the need to document and publish practices does also provide very useful protection.

Transparency in data processing is also a global principle that even the US has embraced in its laws. As the answers on page 9 show, templates for privacy policies that are approved by authorities could be a tool to simplify the drafting, improve the quality and increase legal stability – especially for daily processing operations at smaller companies.



Article 15 to 21 – Data subject rights

Data subject rights rank comparably low in terms of workload. Article 15 (Right of Access), the most commonly exercised right, also ranked comparably low in terms of workload. At the same time, it is seen as a very useful tool for the protection of data subject rights. The other rights are ranked slightly lower in terms of workload and usefulness. This seems to match real-life experiences, since most controllers hardly get subject access requests(SARs) and specific controllers (VLOPs, data brokers or credit ranking agencies) usually have automated SAR responses. Surprisingly, The European Commission's Digital Omnibus proposal nevertheless suggests a limitation of Article 15.

Article 22 – Automated decision-making

Despite being rather complex, the rules in Article 22 (automated decision making) ranked exceptionally low in terms of workload, indicating that most controllers do not engage in automated decision-making. The small number of controllers that do engage in automated decision-making have streamlined the process. Surprisingly, the Digital Omnibus proposal also included a limitation on Article 22.

Articles 24 to 27 – General duties of a controller

The general duties of a controller seem to take quite some work. However, given that Articles 24 to 27 do not have a lot of specific duties, it can be assumed that participants have accounted for much of the undefined time when working for a controller under this heading. Mirroring the work on these elements, participants also take the view that this work does protect the rights of data subjects.

Article 28 and 29 – Monitoring of processors

The survey asked for the workload under Article 28 GDPR, split between EU/EEA and non-EU/EEA processors. There is generally an argument that EU/EEA processors are easier to deal with. However, in practice, they may also be less relevant. If the time spent on both categories is added together, it would top the list of time spent altogether. However, given that the survey participants tend to overestimate time spent, such a calculation may be unfair.

In any case, the more detailed question under section 2 shows that there is enormous appetite to simplify these requirements – ideally towards a direct duty of the (sub-)processors under the GDPR.

Article 30 – Record of processing activities

Privacy Professionals invest a lot of work on Records of Processing Activities (ROPAs). The views of Privacy Professionals on the usefulness of Article 30 is very much split, with a favour for ROPAs.

Surprisingly, 43% of professionals working for companies with less than 250 employees say that they invest more than 20% of their time into ROPAs – indicating that ROPAs are a tool that is used beyond controllers that are legally obliged to have one. This indicates that changes to Article 30(5) GDPR, as proposed by the European Commission's Omnibus package, will have little impact - given that controllers follow the rules even if they are not obliged to do so.

Article 32 - Security

Unsurprisingly, security obligations are seen as extremely useful for the protection of the rights of data subjects, but also create relevant workload. Different to other elements of the GDPR, this obligation is usually in the interest of both controllers and data subjects and hence sees less criticism by controllers.

Article 33 and 34 – Data breach notifications

Contrary to the common argument, data breach notifications do not seem to be a major burden for controllers. They also rank reasonably well when it comes to the usefulness for data subjects. It is therefore surprising that the Commission's Digital Omnibus proposal suggests to limit Article 33 GDPR to only "high risk" breaches.

Article 35 – Data protection impact assessment

Data protection impact assessments seem to generate quite a substantial workload and are seen as providing limited protections for data subjects. This assessment could be linked to the response to another question, where professionals report that such assessments usually arrive at a "pre-determined" outcome in favour of a controller – calling into question the self-regulatory approach.

- ## Article 37 to 39 - Data Protection Officers

The appointment and work with a DPO is seen as a low-workload task and rather useful. However, given that the vast majority of survey participants identified as DPOs, it seems clear that these answers may suffer from bias and controllers may take a different view.

- ## Article 40 to 43 – Codes of Conduct and Certifications

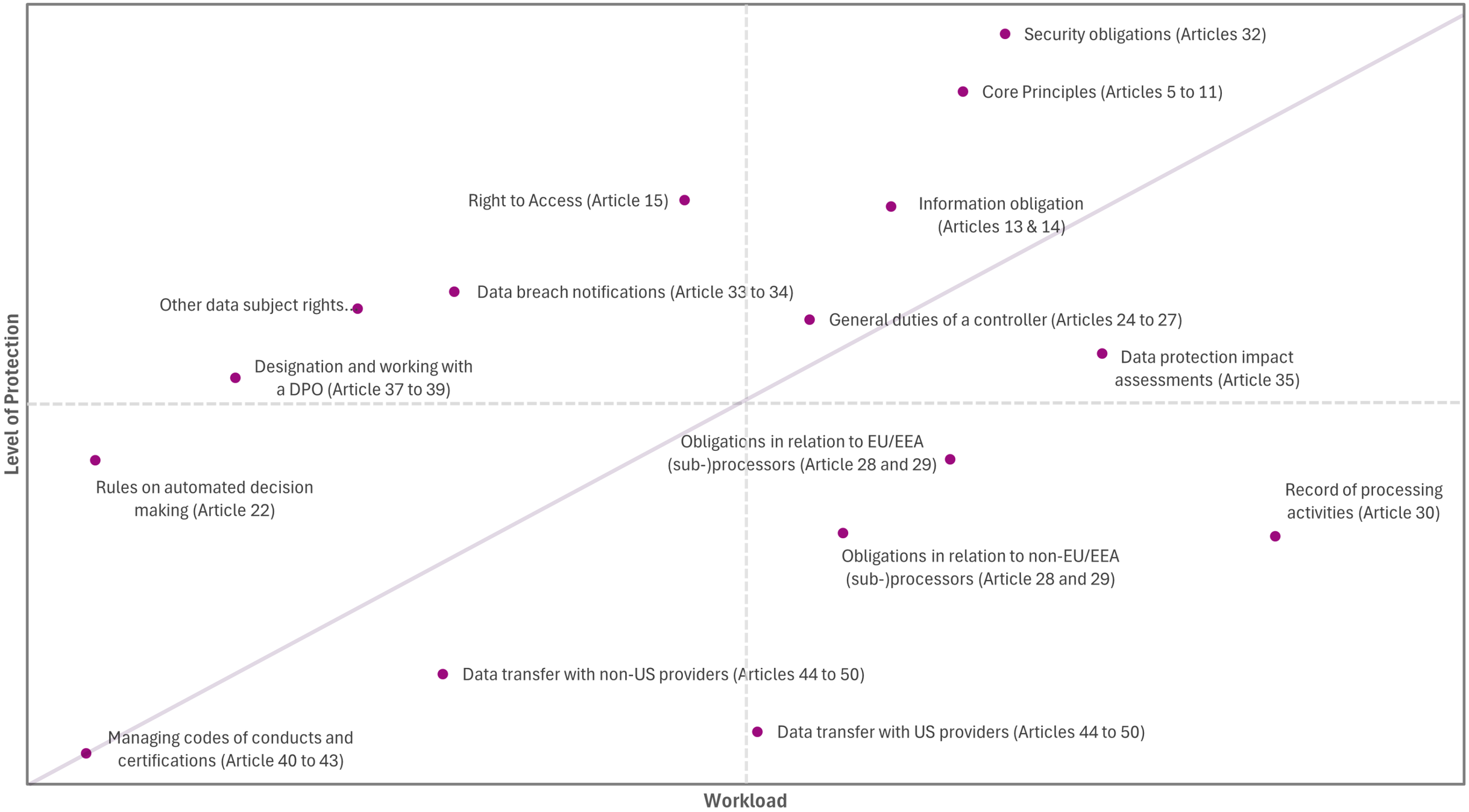
Given the limited practical use of Codes of Conduct and Certifications, it is not surprising that little time is spent on them and little benefit is being derived.

While controllers call for "whitelists" and "blacklists" the current approach taken under Articles 40 to 43 GDPR cannot be operationalised properly in practice - calling for a different approach.

- ## Article 44 to 50 – Data transfers

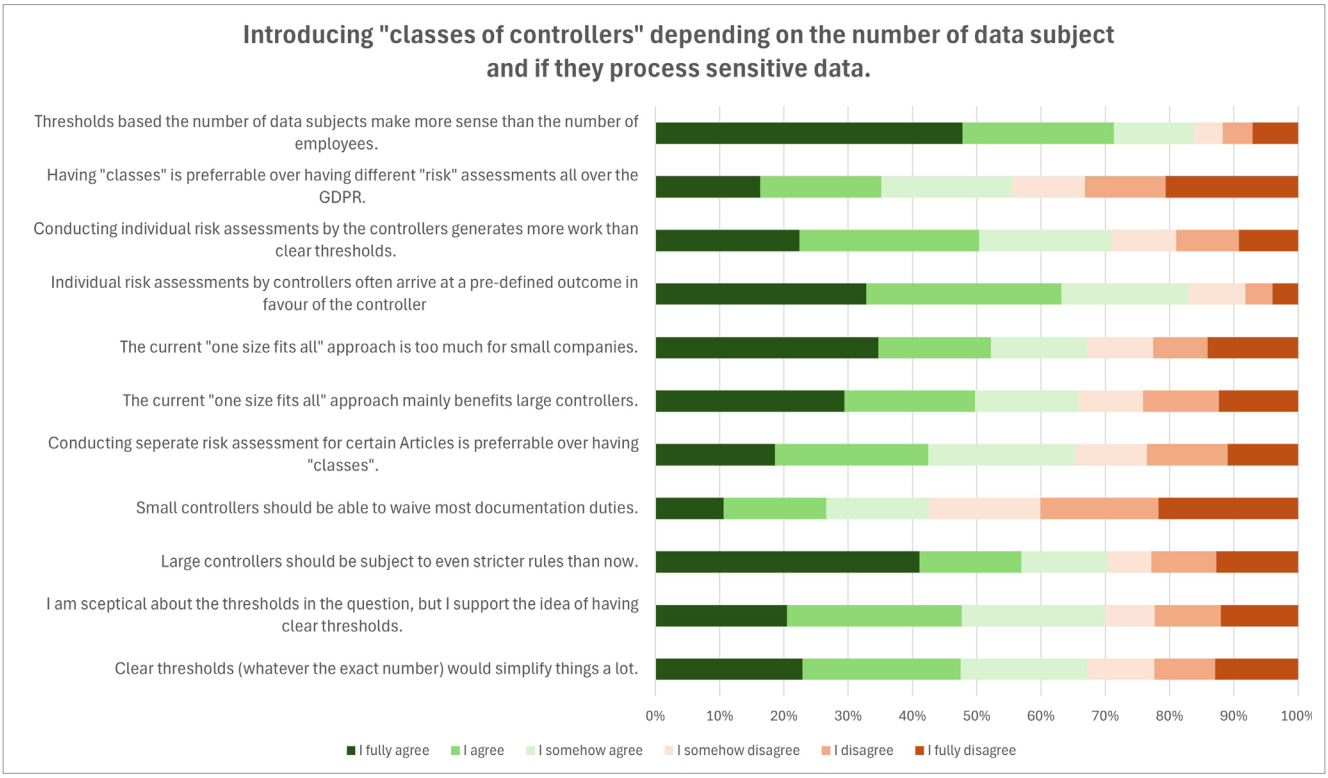
Surprisingly, controllers report relevant, but not extreme workloads from managing data transfers, despite unresolved issues with EU-US data transfers and increasing geopolitical tensions. At the same time, controllers see little benefit from the relevant regulations for data subjects. It is unclear whether this is due to disbelieve in regulating transfers at all or because of regulations not delivering for protections.

Ratio of Workload for DPOs and Level of Protection for Data Subjects



2. Differentiation between larger and smaller controllers as functioning "risk-based approach"

While many call for a "risk based approach" from which smaller SMEs could benefit, the current approach largely leads to uncertainty and an even greater need for legal advice to apply open and undefined "risk" metrics. We have asked various questions to see if a more regulated risks based approach would be seen as beneficial by DPOs and Privacy Professionals.



- **Professionals favour clear thresholds, but favour metrics like affected people instead of employees**

Overall, respondents show a strong tendency to favour clear thresholds instead of undefined risk elements. While this may not always be possible, the GDPR and implementation work could focus on such clearer thresholds to ensure more legal certainty and more compliance.

- **Current “risk assessments” by controller are seen as dysfunctional**

Notably, 82% of data protection professionals working at controllers take the view that current risk assessments result in a predefined outcome. This means that these risk assessments are not a genuine tool to ensure that overly risky processing is stopped, but a way to legitimise processing in the interest of the controller. It would therefore be advisable that any “risk-based approach” ensures that it does not only amount to a paper exercise.

- **A “one size fits all” approach is seen as favouring large companies over SMEs. A “class” system is favoured**

While the “risk-based approach” of the GDPR was seen as a way to limit the burden on smaller controllers in a “one size fits all” law, professionals report the exact opposite. In practice, it is a common complaint that large controllers can manage unclear texts and "risk" assessments that are open to interpretation, while smaller controllers do not have the resources to use flexible wordings to their benefit.

- **Professionals want stricter rules for larger controllers, but are slightly negative on less documentation duties for smaller controllers.**

Even though the survey participants mostly represent controllers with 500+ employees, there is a large (70%) consensus that the current GDPR rules are not sufficient for large controllers. This hints at the need for stricter rules for VLOPs and other large controllers or processors.

Surprisingly, there is a rather diverse view on lowering the documentation requirements for smaller controllers. There is no clear indication as to the reasons, which may be that the current definition of “small” based on the number of employees is not seen as useful, the fact that most respondents in the survey work at large controllers, or a general feeling that documentation duties are important no matter the size of a company.

3. Getting rid of millions of contracts: Reforming Article 28(3) GDPR

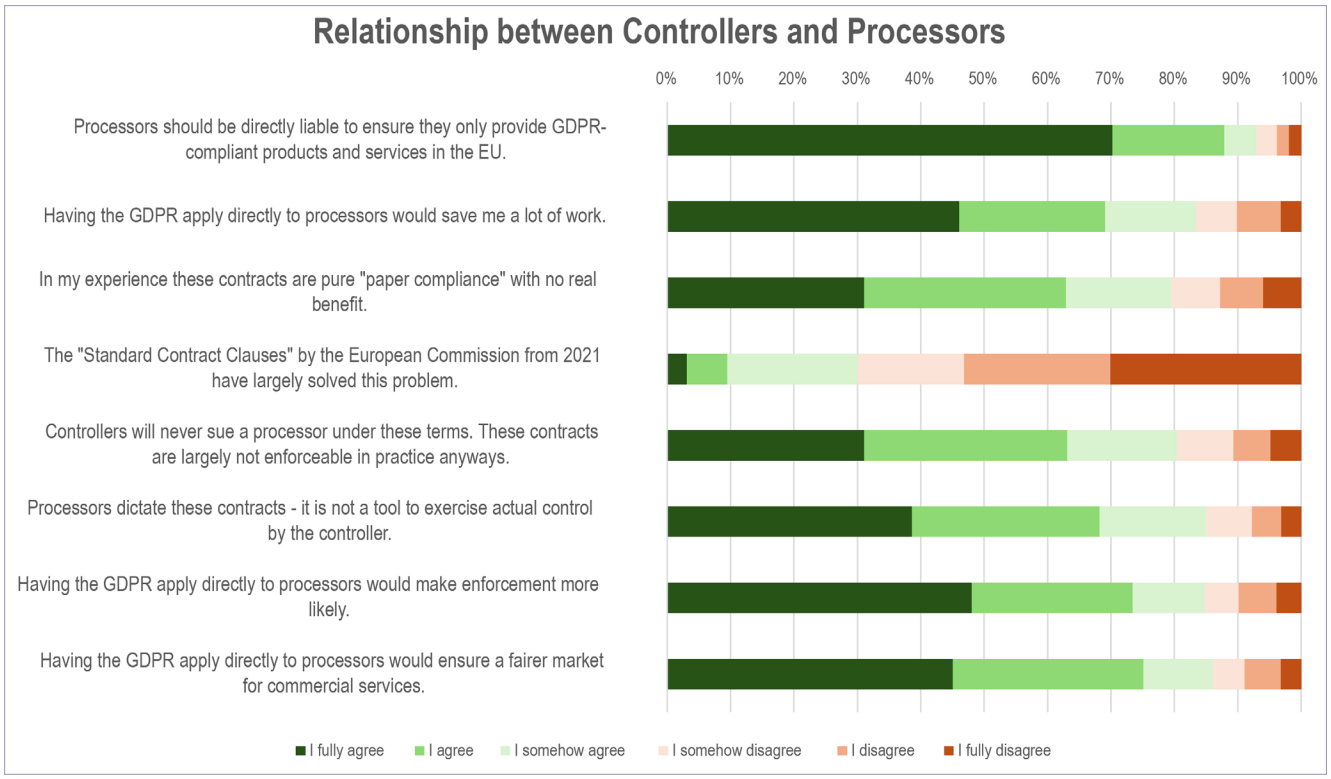
A regular complaint is the need to sign individual contracts between each controller and processor or sub-processor. Given that almost any of the 30 million EU businesses processes personal data and likely manages multiple of these contracts, there must be easily 100+ million of such contracts. Notably, under Article 28(3) GDPR they must all have the same elements in them, leading to enormous copy/paste efforts.

This approach seems to be based on Directive 95/46, whereby each Member State had slightly different data protection laws and processors in another EU jurisdiction naturally needed to be bound to the national law of the controller. This was done via a contract. The need to indirectly (!) bind processors to the law applicable to the controller largely does not exist anymore – in particular because the geographic application of the GDPR also covers non-EU/EEA providers. It seems that today such contracts could be replaced by a direct legal duty of the processors – enforceable by controllers and SAs alike.

- **Processor contracts dictated by processors – not controllers**

Oftentimes, processors - not controllers - have a dominant market power. 85% of survey participants support that claim. The “big three” (AWS, Google and Microsoft) have an enormous market power. This turns the concept of a controller being in control of any processor upside down. Currently, the GDPR attributes responsibility to an entity that has no real control over processing operations. Supervisory

Authorities would have to take action against EU controllers to deal with unlawful processing by processors. Processors that do allow for individualised contracts, in turn, report that the management of deviating contracts on one IT system provided by the processor can be a huge challenge.



- **Processor contracts are seen as unenforceable and mere "paper compliance"**

Given that processors draft Article 28(3) contracts and that B2B contracts are hardly regulated, they often contain clauses like prohibitive costs for the exercise of controllers' rights or US jurisdiction for any claim or other barriers to enforcement. 80.4% see these contracts as hardly enforceable and mere "paper compliance", raising questions as to their value for the protection of data subject rights.

- **Professionals see a chance to shift responsibility from SMEs to the "Big Three" and ensure a fairer European market for processing services**

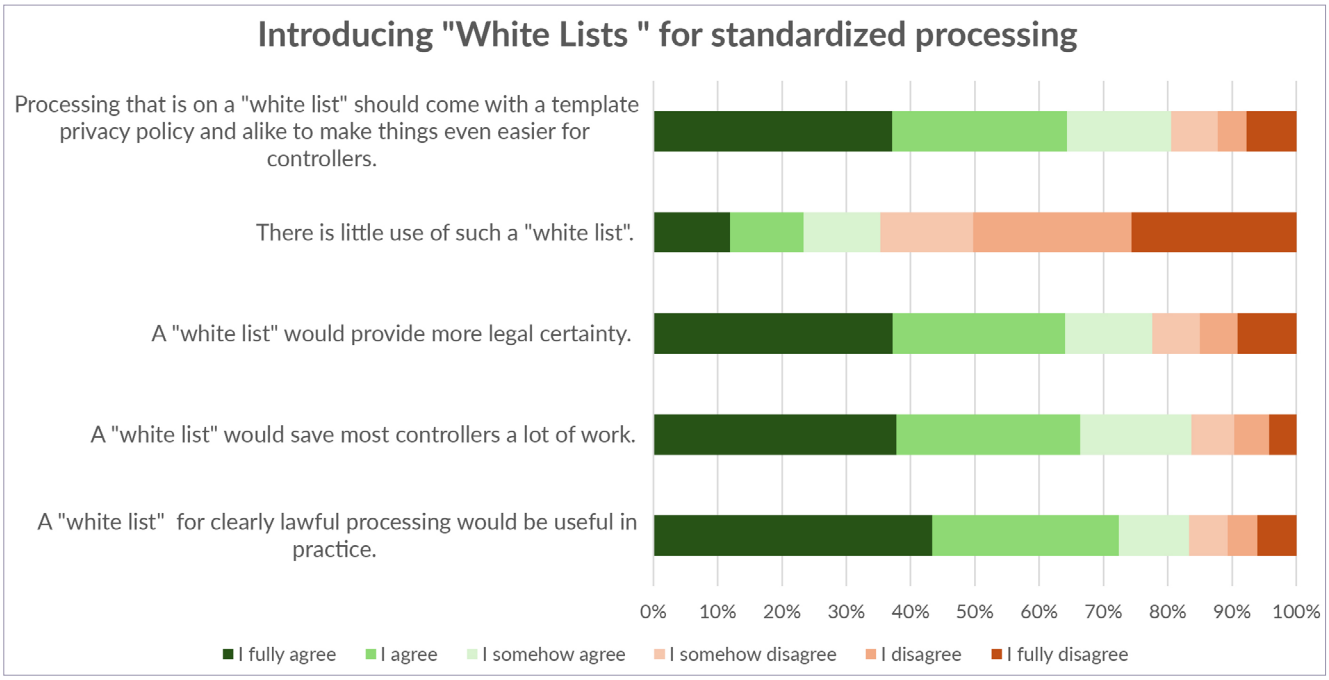
84.7% of all participants take the view that a direct application would make enforcement more likely and 86.1% of all participants take the view that this would ensure a fairer market for commercial services.

- **The Commission's Standard Contracts did not solve the problem**

The Commission has identified the problem and issued Standard Contracts in Implementing Decision (EU) 2021/915. When asked if this has solved the matter, 69,9% of privacy professionals say that it has not solve the underlying problem.

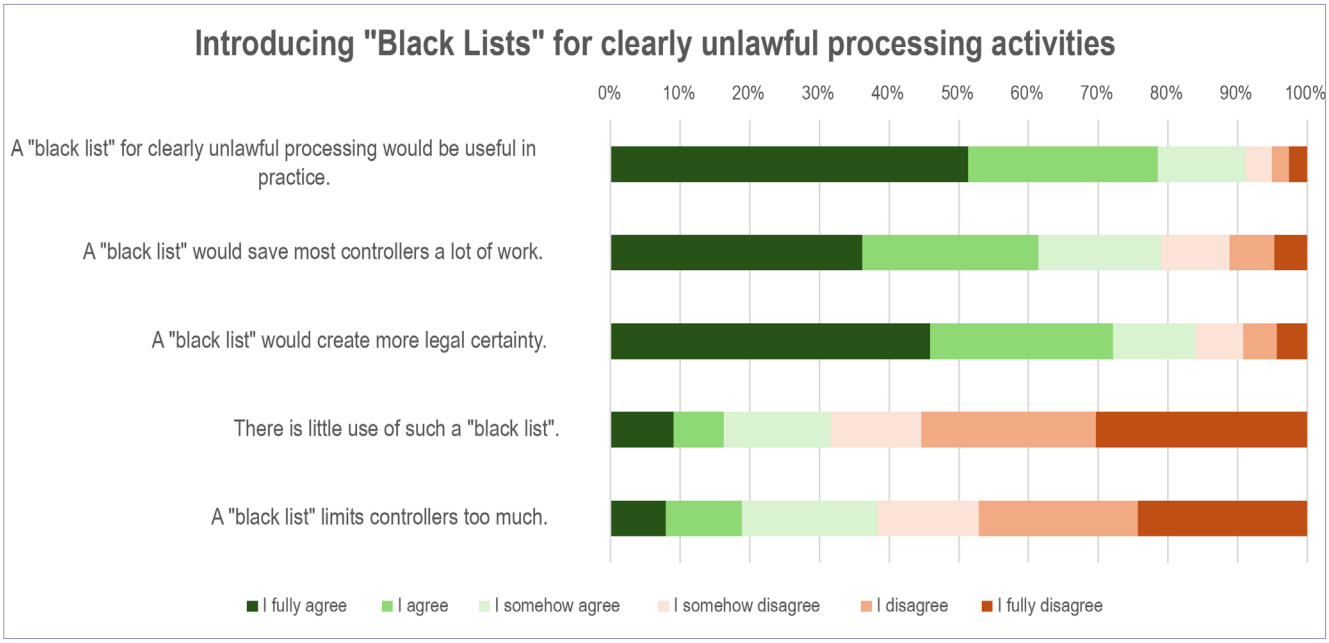
4. Professionals favour “whitelists” and “blacklists”

83.3% of professionals favour a “whitelist” and 91.1% favour a “blacklist” for processing activities. 83.7% and 79% respectively take the view that such lists would save controllers “a lot of work”. Respondents also say that such lists would create more legal certainty.



• Professionals wish for accompanying templates to comply with Article 13 and 14 GDPR

The idea that “whitelisted” processing could also come with approved templates to comply with requirements under Article 13 and 14 GDPR is widely supported. Such an approach may also be taken for other requirements under the GDPR, like compliance with Article 30 GDPR and alike.



- **Professionals do not think that a "blacklist" would limit controllers too much**

Surprisingly, privacy professionals working for controllers do not feel that a "blacklist" (similar to Article 5 of the AI Act) would limit controllers too much. It seems that legal certainty is preferred over flexible laws. It can only be assumed, that ensuring fair competition may be a factor that supports the issuing of "blacklists" – given that competitors would also be subject to clearer red lines.

Imprint:
noyb – European Centre for Digital Rights

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

ZVR: 1354838270