DPAs on the Ground

By IAPP Legal Extern Bailey Sanchez

DPAs on the Ground

By IAPP Legal Extern Bailey Sanchez

As of May 25, 2020, the EU General Data Protection Regulation has been in force for two years. The GDPR provides that by this anniversary (and every four years thereafter), the European Commission must submit a report on the evaluation and review of the GDPR to the European Parliament and Council. To support the first mandated evaluation of the GDPR, the commission sent a questionnaire to data protection authorities to be completed by January 2020. The questions focus on the GDPR's international transfers regime and its mechanisms to support cooperation and consistency across the European Union. The European Data Protection Board published an informative synthesis of DPA responses. To understand DPAs' work in practice, though, a closer look at DPAs' separate circumstances and resources is needed. This piece focuses on the resources available to each DPA and its progress so far in addressing complaints, both individually and in coordination with other member states. Additionally, it highlights GDPR's impact on budget and staffing levels in relation to a country's GDP. Results from the questionnaire provide an illustrative snapshot into DPAs' work "on the ground."

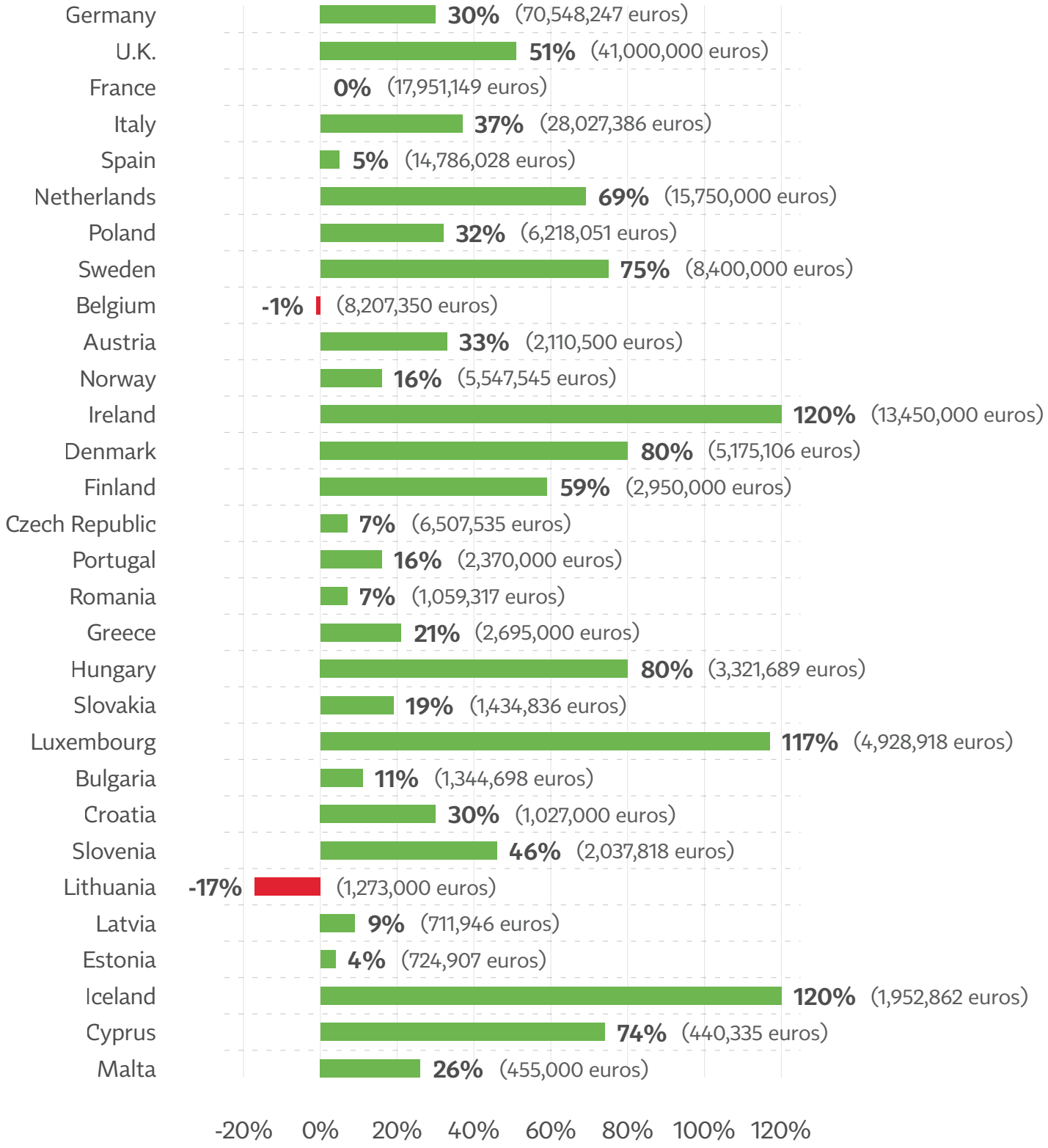
A DPA's resources

The commission's questionnaire asked each DPA to indicate the number of staff employed and its yearly budget from 2016 through 2020. The inclusion of 2016 and 2017 offers insight into how the GDPR impacted staffing. In most cases, DPAs' staff grew each year. However, in a few cases, staffing remained constant or even shrank. While staffing has generally increased each year, several DPAs indicated that more staff is needed to effectively accomplish their tasks. As staffing increased, so did budgets. Most DPAs entered 2020 with their largest budget to date, though a few are working from the same budget as in 2019.

Almost without exception, DPAs must deal with tasks beyond those mandated by the GDPR, with clear implications for staffing and budget. The number of tasks for which each DPA is responsible and the level of detail with which each described them varied by response. DPAs' non-GDPR tasks include enforcing and providing guidance concerning domestic laws implementing the ePrivacy Directive and Data Protection Law Enforcement Directive, as well as laws and regulations governing freedom of information, consumer protection, and criminal and national security matters. A given DPA could be responsible for one, a few or all these tasks.

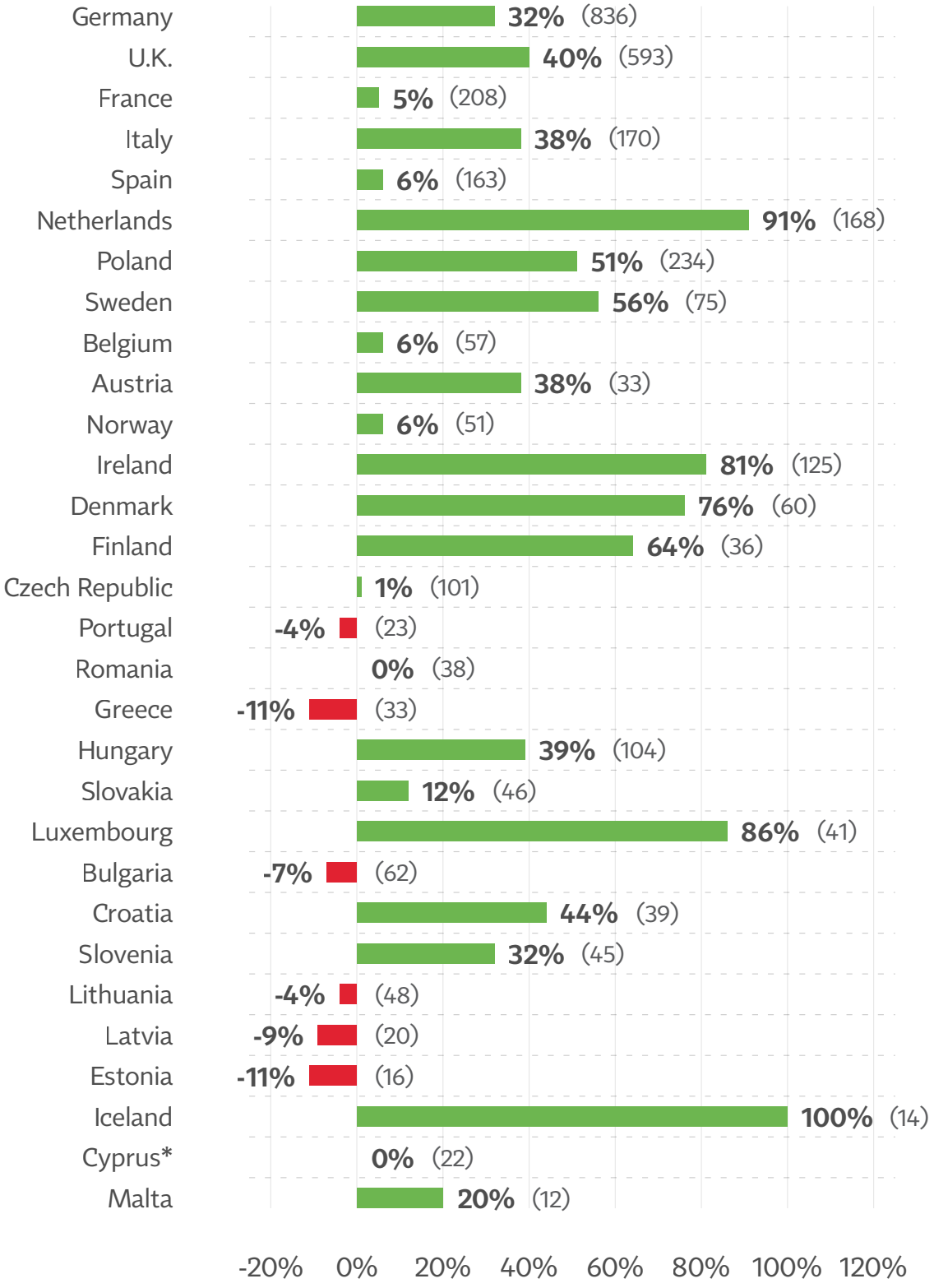
Percentage Change in Budget

When comparing average post-GDPR (2018–19) to average pre-GDPR (2016–17) budget. Countries organized by GDP. Average post-GDPR budget in parenthesis.



Percentage Change in Staff

When comparing average post-GDPR (2018–19) to average pre-GDPR (2016–17) staff. Countries organized by GDP. Average post-GDPR staff in parenthesis.



**Pre-GDPR staff data not provided.*

A DPA's work to date

The commission questionnaire sought information on the number of complaints each DPA received since May 2018, as well as the number of fines imposed. It is important to note that respondents were also asked to explain what qualifies a particular communication as a complaint. Interpretations varied, with some DPAs adopting a broader notion of complaints than others. For this reason, as well as others, including member state population, the number of complaints varied widely among DPAs. Some reported less than 1,000, while Germany and the U.K. recorded more than 60,000. The number of fines imposed also varied greatly. Seven DPAs reported that at the moment of their response, they had not yet imposed any fines, though some DPAs noted they were in the final stages of resolving complaints where a fine would be imposed.

All but the Hellenic Data Protection Authority supplied national statistics on breach notifications since May 2018. The number of breach notifications ranged from 92 in Cyprus to 46,561 in Germany, with Germany noting that even this large number is an underestimate because not all German DPAs responded to the question. Given this wide range, there is no true average number of national breach notifications.

> ***... the number of complaints varied widely among DPAs. Some reported less than 1,000, while Germany and the U.K. recorded more than 60,000. The number of fines imposed also varied greatly.***

The complaint, breach and enforcement statistics make clear that each DPA is dealing with its own unique workload.

A DPA's coordination across member states

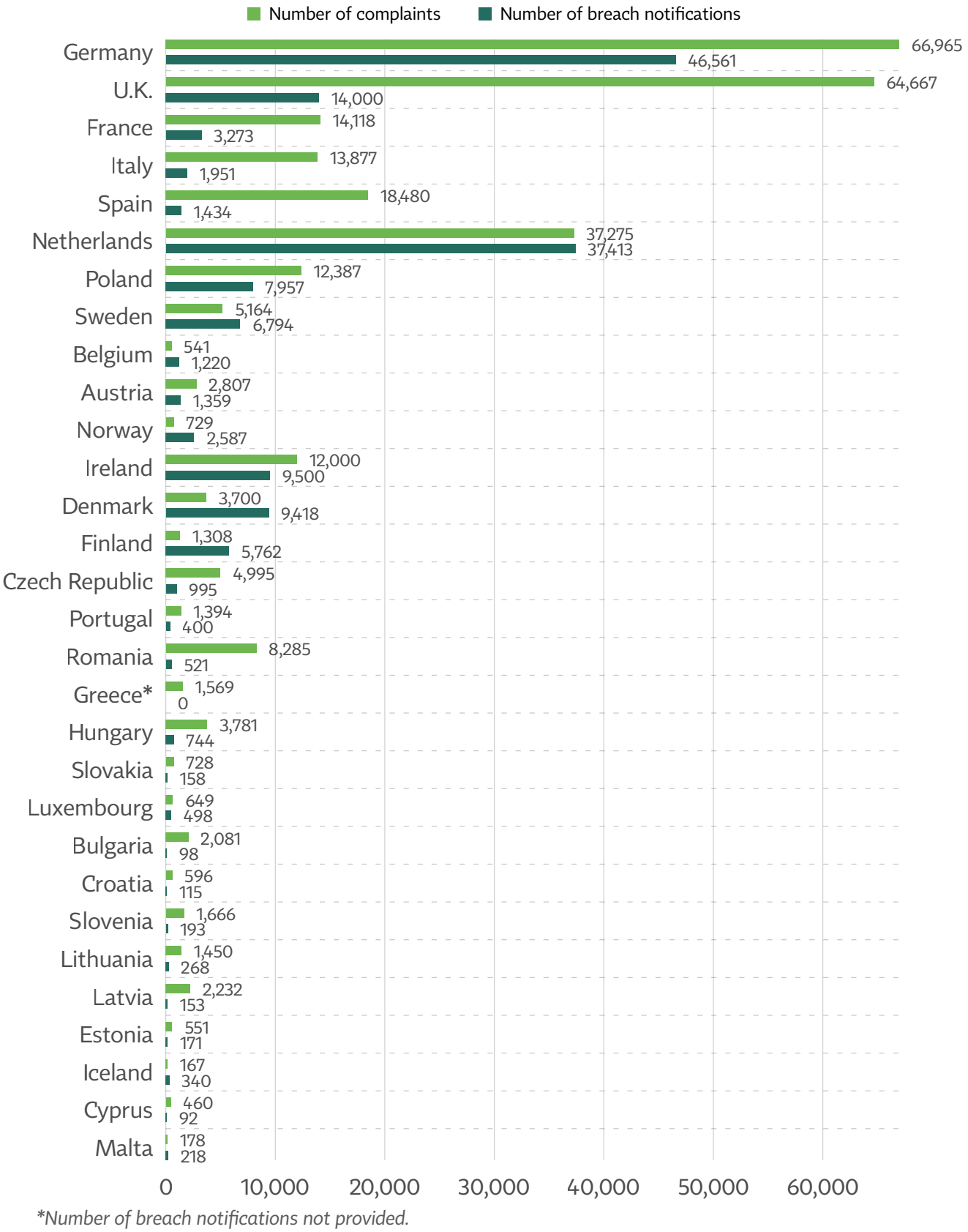
The commission's questionnaire also included a section dedicated to the one-stop shop. The one-stop-shop mechanism is intended to be a benefit of the GDPR, enhancing cooperation between member states and making it easier for companies to do business across the EU. The mechanism is used when a DPA is investigating a complaint that impacts more than one member state and the organization involved in the complaint or investigation has a "main establishment" somewhere in the EU. The member state in which the main establishment of the controller or processor is located becomes the lead supervisory authority, with other impacted member states acting as concerned supervisory authorities.

> ***The one-stop-shop mechanism is intended to be a benefit of the GDPR, enhancing cooperation between member states and making it easier for companies to do business across the EU.***

DPAs were asked about their participation in one-stop-shop procedures. All but the Croatian Personal Data Protection Agency have been involved in a one-stop-shop case, either as an LSA or CSA. DPAs were then asked to identify any problems or obstacles to cooperation with the other involved DPAs. Of the

Number of Complaints and Breach Notifications

Countries organized by GDP.



**Number of breach notifications not provided.*

DPAs who addressed the question, Cyprus, Estonia, Malta, Norway, and Romania noted no problems. The remainder noted some challenges or areas for improvement.

A handful of common themes emerged in the responses. First, DPAs identified differences in national procedural rules as the main obstacle to effective cooperation. As explained by the Icelandic Data Protection Authority, "Some have very flexible procedural laws while others have very strict provisions. This — along with a lack of understanding between member states when it comes to these differences — can be identified as a shortcoming." Generally speaking, these differences make the one-stop-shop mechanism more difficult for the DPAs to administer. They can also lead to conflicts in deciding outcomes of cases. For example, some DPAs may have the option to reach an amicable settlement, and some must issue a decision.

> ***Multiple responses noted that cross-border cases typically take much longer to resolve than national cases.***

Second, DPAs expressed general concern regarding the lengthy timeframe of one-stop-shop cases. The Danish DPA attributed the timeliness issue to the differences in national procedure rules. Multiple responses noted that cross-border cases typically take much longer to resolve than national cases. However, the Irish DPA noted the "long delays in transmitting complaint files are becoming less frequent." The Belgian Data Protection Authority also cited a problematic consequence of lengthy cases. The Belgian DPA believes "it poses risks to the level playing field, whereas it is much easier to resolve national cases, sometimes leading to sanctions imposed on companies operating within the country, whereas similar infringements by multinational companies remain unsanctioned." Some DPAs suggested instead that the timeliness issue resulted from slow communication between DPAs. German DPAs noted that case handling within the system is sometimes "sluggish."

Third, DPAs expressed concern with the functioning of the internal market Information system. The IMI is an IT system that allows DPAs to confidentially communicate with each other regarding cross-border cases. There appears to be technical shortcomings with the design of the system. The Irish Data Protection Commission explained, "The IMI is not designed or intended to be used as a case management system; rather, it is intended as a simple notifications or messaging system. This means that it is very difficult for supervisory authorities to search for IMI entries, to link relevant IMI entries and to track cases. Not only does this present challenges for CSAs, it also creates challenges for LSAs, in being operationally efficient and also in being transparent to CSAs. At the DPC, we have had to implement several spreadsheets and databases to mitigate the problems with the IMI." Other DPAs mentioned the time and translation costs associated with using the system, which may be too technically complicated to use.

> ***DPAs sought further guidance on procedures for implementing the one-stop-shop mechanism, suggesting that more detailed guidance and clarification on procedures could resolve the inconsistencies between national rules and assist with cooperation.***

The commission also asked respondents to share potential solutions to the identified problems. Broadly, multiple DPAs suggested that greater harmonization between member states would help. More specifically, DPAs sought further guidance on procedures for implementing the one-stop-shop mechanism, suggesting that more detailed guidance and clarification on procedures could resolve the inconsistencies between national rules and assist with cooperation. A few suggested additional staffing could help. Several DPAs also pointed to the administrative burden of one-stop-shop cases. As the Dutch DPA, the Autoriteit Persoonsgegevens, observes, DPAs are all interdependent. Therefore, the mechanism "depends on all SAs being provided with sufficient resources to carry out their tasks." In addition to potentially increasing staffing, another concrete solution suggested by many DPAs was to improve communication tools. Multiple DPAs suggested that this could be accomplished by improving the IMI system.

> ***In addition to potentially increasing staffing, another concrete solution suggested by many DPAs was to improve communication tools.***

A DPA's work continues

Before 2020 was even underway, DPAs had received 275,557 complaints and imposed 785 fines in total. These numbers relate to only a subset of DPAs' day-to-day responsibilities but clearly demonstrate just how busy DPAs have been since May 25, 2018. For most DPAs, the increased workload has been accompanied by staff and budget increases, but that experience has not been uniform or perfectly paralleled the uptick in responsibilities.

> ***Many entered 2020 with their largest budget to date, but 2020's global pandemic brought new responsibilities and new challenges for DPAs and those they regulate, making it difficult to know whether the upward trends from recent years are sustainable.***

Many entered 2020 with their largest budget to date, but 2020's global pandemic brought new responsibilities and new challenges for DPAs and those they regulate, making it difficult to know whether the upward trends from recent years are sustainable. Despite the current uncertainty, DPAs feedback offers a look into the functioning of the GDPR in its first two years and should help the European Commission assess and prioritize opportunities for improvement moving forward. As Latvia reflected, "The (one-stop-shop) mechanism is a useful and necessary tool in the context of cross-border data protection supervision, especially in view of the increasing number of cross-border data processing. In the view of the Inspectorate, as a result of practical application, OSS procedure will only evolve." It seems likely, that this "evolution" will occur across all of the work that DPAs undertake as they learn from their experiences on the ground and that of other DPAs implementing the GDPR.