Overview of regulatory strategies of European Data Protection Authorities for 2023 and beyond

FUTURE OF PRIVACY FORUM

February 2023

AUTHOR

Sebastião Barros Vale
Senior Counsel, FPF

The author would like to thank FPF's Vice-President for Global Privacy Gabriela Zanfir-Fortuna, Senior Counsel for Global Privacy Lee Matheson and former FPF interns Dale Rappaneau and Kavisha Patel for their valuable contributions to the Report.

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

FPF Europe maintains strong partnerships across the EU through its convenings and knowledge-sharing with policymakers and regulators. This transatlantic engagement helps regulators, policymakers, and staff at European Union data protection authorities better understand the technologies at the forefront of data protection law. By building this bridge between European and U.S. data protection cultures, FPF hopes to build a common data protection language. Learn more about FPF Europe by visiting fpf.org/about/EU.

Table of Contents

FOREWARD

by Gabriela Zanfir-Fortuna and Sebastião Barros Vale

Enforcement of data protection law is at an inflection point in the European Union (EU), five years after the General Data Protection Regulation (GDPR) became applicable. On the one hand, GDPR enforcement seems to have finally reached a certain level of maturity, with consequential decisions that tackle the fundamentals of data protection law as applied to core business models in the digital economy.[1]

On the other hand, Data Protection Authorities (DPAs) have started to realize, and act upon the fact, that the law they are already enforcing is applicable in many cases to the most complex and impactful new technologies, like artificial intelligence (AI)[2] and algorithmic decision-making.[3] In fact, some DPAs have recently created new internal structures dedicated to enforcement of the GDPR on AI systems and algorithms.[4]

Importantly, the effectiveness of enforcing the GDPR was subject to ample debate in 2022 in the European Parliament[5] and during a dedicated conference organized by the European Data Protection Supervisor[6] (EDPS). The need for such a debate was amplified by the shift in governance from national supervisory authorities to primarily the European Commission that the EU legislators are proposing in the Data Strategy legislative package, such as in the Digital Services Act (DSA) and the Digital Markets Act (DMA).

The consensus in Brussels remained that the enforcement model of the GDPR centered around national DPAs and the One-Stop-Shop should not yet be subject to legislative reform. However, as a result of this debate largely initiated by the EDPS and the European Parliament, several initiatives to reform the way DPAs are working together were launched or proposed.

Perhaps most significantly, the European Commission included in its Work Program for 2023 plans "to harmonize some national procedural aspects," with the purpose of

[1] Irish DPC, "Data Protection Commission announces conclusion of two inquiries into Meta Ireland", January 4, 2023, available at https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland
[2] "Replika, a 'virtual friendship' AI chatbot, hit with data ban in Italy over child safety", TechCrunch, February 3, 2023, available at https://techcrunch.com/2023/02/03/replika-italy-data-processing-ban/ .
[3] S. Barros Vale, G. Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities", May 2022, available at https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf
[4] CNIL, "The CNIL creates an Artificial Intelligence Department and begins to work on learning databases", January 26, 2023, available at https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases; and IAPP, Dutch DPA to enhance algorithm supervision, January 3, 2023, available at https://iapp.org/news/a/dutch-dpa-to-enhance-algorithm-supervision/
[5] European Parliament, LIBE Committee Hearing on "General Data Protection Regulation implementation, enforcement and lessons learned", March 17, 2022; Press release available at https://www.europarl.europa.eu/committees/en/general-data-protection-regulation-imple/product-details/20220301CHE09983
[6] EDPS Conference, "The Future of Data Protection: Effective Enforcement in the Digital World", June 16 and 17, 2022, Brussels. Read the Conference Report at https://edps.europa.eu/system/files/2022-11/22-11-10-edps-conference-report-2022_en.pdf

improving cooperation between national DPAs.[7] In fact, the European Data Protection Board (EDPB) itself adopted a "wishlist" of procedural reforms at national levels[8], which were included in a letter to Commissioner Didier Reynders just a week prior to the Commission Work Program being published.

In this list, the EDPB highlighted the need for harmonization of practical procedural issues, such as the status and rights of the parties to the administrative procedures, procedural deadlines, requirements for admissibility or dismissal of complaints, investigative powers of DPAs, and the practical implementation of the cooperation procedure.

Prompted by the lively debate in Brussels on the effectiveness of GDPR enforcement, and in order to streamline enforcement and make it more effective particularly in cross-border cases, in March 2022 the EDPB adopted the Vienna Declaration[9] where it set out goals to enhance cooperation among its members. One of the commitments made was "further exchanging information on national enforcement strategies with a view to agreeing on annual enforcement priorities at EDPB level, which can be reflected in national enforcement programmes." The DPAs also agreed that, for those among them who wish to do so, they can prepare "a common enforcement framework, including common instruments for inspections."

The Vienna Declaration also touched on potential areas of conflict of competences between DPAs and the enforcers of the legal instruments in the EU Data Strategy package. The EDPB wrote that, "it will be crucial to solidly embed the GDPR and DPAs in the overall regulatory architecture that is being developed for the digital market (Data Act, DMA, DSA, AI Act, DGA)," signaling a potential area for intense scrutiny in the upcoming years. The DPAs pleaded for "a clear distribution of competences among the regulators."

Finally, as part of the same effort to increase efficiency of cooperation between its member DPAs, the EDPB adopted criteria for the selection of cases of strategic importance that regulators should more closely focus on.[10] According to the July 2022 document, criteria that DPAs should consider when submitting proposals to the EDPB Plenary on cases to prioritize in investigations and enforcement efforts include:

1. The structural or recurring dimension of the compliance issue;
2. The intersection of data protection with other fields (such as consumer or competition law); and

[7] Commission Work Program 2023, COM(2022) 548 final, October 18, 2022, Strasbourg, p. 13.
[8] EDPB, Letter to Commissioner Didier Reynders, October 10, 2022, available at https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf
[9] EDPB, Statement on Enforcement Cooperation, April 28, 2022, available at https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf
[10] EDPB, Selection of Cases of Strategic Importance, July 29, 2022, available at https://edpb.europa.eu/system/files/2022-07/edpb_document_20220712_selectionofstrategiccases_en.pdf.

3. Whether there are high risks to individuals, notably where special categories of data or vulnerable populations are involved.

These are the broad strokes that characterize the framework of GDPR enforcement this year. In order to gain insight into the substantial priorities of DPAs, we looked at strategic documents and public announcements made by authorities and identified common trends, such as an increased interest in **online advertising**, **children's privacy**, **international data transfers, AI, and biometrics** across the board. **Codes of Conduct and certification mechanisms** are garnering more attention and appear in the plans of several DPAs. In addition, most strategic plans reveal a desire to complement investigations with **awareness-raising and training opportunities** for individuals and in-house compliance functions of companies. This Report provides valuable insight into the immediate plans of European DPAs.

1. Introduction

Following our May 2020[11] and July 2021[12] comprehensive analyses of European Economic Area (EEA) DPAs' priorities and focus areas for the new decade, the Future of Privacy Forum (FPF) has conducted a new analysis that presents an overview of the regulatory strategies of DPAs for 2023 and the ensuing years.

The regulatory plans of DPAs, as revealed by annual reports, strategic documents, and operational plans published between July 2021 and February 2023, provide useful predictors of where the watchdogs will devote their broad investigative, advisory, and corrective powers. Notably, the majority of EU DPAs have reported[13] a shortage of the adequate human and financial resources considered necessary to perform DPAs' supervisory duties under the GDPR, prompting calls for budgetary increases[14] at national levels.

DPAs from eight different European Economic Area (EEA) jurisdictions - in addition to the United Kingdom (UK)'s Information Commissioner's Office (ICO), the EDPB, and the EDPS - have published relevant documents. These include annual reports and brief outlines in the form of blog posts, which discuss some of their regulatory priorities for 2023 and upcoming years. Such jurisdictions are Belgium (BE), the Czech Republic (CZ), Denmark (DK), Estonia (ET), France (FR), Ireland (IE), Spain (ES), and Sweden (SE).

Our findings reveal that most DPAs are committed to **ramping up their investigatory and sanctioning efforts** in response to individuals' complaints and on their own initiative. They also show an increasing willingness to **cooperate** closely with other DPAs - both bilaterally and multilaterally - and regulators from other fields, such as competition and

[11] Available at https://fpf.org/blog/fpf-charts-dpas-priorities-and-focus-areas-for-the-next-decade/
[12] Available at https://fpf.org/blog/insights-into-the-future-of-data-protection-enforcement-regulatory-strategies-of-european-data-protection-authorities-for-2021-2022/
[13] Available at https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf
[14] Available at https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf

audiovisual regulators. In the aftermath of the landmark Schrems II ruling from the Court of Justice of the European Union (CJEU), **international data transfers** - notably, the ones that occur through cloud-based services - will likely remain a focal point of DPAs' enforcement endeavors. **Online marketing and advertising** mark another area of regulatory focus where DPAs have manifested an appetite for using the coercive tools at their disposal to achieve broad compliance with privacy and data protection rules.

However, the planned actions of DPAs are focused on more than enforcement. European watchdogs perceive the **upskilling of internal privacy roles** (such as Data Protection Officers) as crucial to achieving data protection on the ground, and they wish to contribute to that goal through knowledge-sharing. For DPAs, **awareness-raising and training** initiatives for both individuals concerned ("data subjects") and compliance functions remain essential.

Guidance on children's privacy (such as on age verification technologies), artificial intelligence (AI), and biometrics will continue to be developed by several DPAs. Moreover, DPAs will stimulate the drafting and approval of **Codes of Conduct (CoC) and certification mechanisms** as tools for attaining broad compliance with data protection standards, including from the international data flows perspective.[15]

This analysis consists of a **summary** of findings and an **annex**. The initial part of the summary will cover the EDPB, the EDPS, and national DPAs' non-enforcement-related objectives and planned actions, providing an overview of their planned "soft law" advisory and guidance commitments. The second chapter explores some thematic and sectoral enforcement priorities announced by DPAs in light of legal and technological advancements, focusing on their "hard law" plans.

The **annex** includes translated excerpts of each analyzed national DPA strategic document, allowing the reader to dive deeper into the details of DPAs' plans. This annex also includes the planned initiatives of EDPB and EDPS to support compliance and enforcement across the EEA.

With this report, FPF hopes to shed light on the general regulatory aims of DPAs across Europe for the coming years. The summary highlights the trends, as well as some notable outliers in planned enforcement of data protection standards in the continent.

Note: This overview does not contain the analysis of materials published by DPAs between 2019 and June 2021, some of which outline regulators' priorities for 2023 and beyond (such as the Belgian, Norwegian, Latvian, and Lithuanian DPAs, plus the EDPS and the EDPB). Therefore, for a comprehensive view of the DPAs' immediate plans, we invite readers to consult our previous Reports published in May 2020 and July 2021.

[15] EDPB, Guidelines 07/2022 on certification as a tool for transfers, adopted on June 14, 2022, version for public consultation, available at https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf.

2. “Soft-law”: Consolidating data protection through guidance and awareness

In the past two years, DPAs across the EEA, the EDPB, and the EDPS have published several **guidelines** that clarify the meaning of key concepts under EU data protection law and support organizations in implementing its requirements. At the EDPB level, this included guidelines on controllers and processors[16], the right of access[17], manipulative online interfaces (so-called “dark patterns”)[18], the GDPR’s cooperation and consistency mechanisms for DPAs[19], and alternative data transfer mechanisms (such as CoC[20] and certification mechanisms).[21]

National regulators have also contributed to this effort, with several DPAs - including ones from Austria, Luxembourg, and the Czech Republic - publishing guidelines on cookies and other tracking technologies.

The EDPS focused on delivering Opinions to EU policymakers about the interplay and inconsistencies between some of the EU’s Data Strategy legislative initiatives and data protection law, including on the Regulation on the transparency and targeting of political advertising.[22] The EDPS also worked with the EDPB on Joint Opinions regarding the Data Act[23] and the AI Act.[24]

What are some of the guidance papers in the pipeline of the EDPB and national DPAs for the coming year?

From the EDPB’s 2021-2022 Work Programme[25], which was not entirely executed by the end of 2022, we expect the Board to publish specific views on the “**legitimate interests” lawful ground, processing personal data for scientific research, children’s personal data, and several emerging technologies**. The latter include **blockchain, anonymization and pseudonymization, cloud computing, AI/machine learning, digital identity, Internet of Things (IoT), and payment methods.**

[16] Available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
[17] Available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en
[18] Available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en
[19] Available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_en
[20] Available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en
[21] Available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en
[22] Available at https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-transparency-and_en
[23] Available at https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en
[24] Available at https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
[25] Available at https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf

At the national level, the topics that DPAs intend to clarify through interpretative guidance and practical recommendations are varied and include the following:

- **Children's data, age verification, and online learning** (BE, IE, UK): in this regard, the Irish DPA (DPC) has recently published its "Fundamentals" guidance on children's data protection rights[26] to help organizations provide the special protection children require when processing their data. According to the DPC's final version of its 2022-2027 Regulatory Strategy[27], this guidance will be complemented by the development of a CoC on processing children's personal data. The UK DPA (ICO) will seek to amplify and disseminate its children-specific guidance through the UK's communications regulator (Ofcom) and the Digital Regulation Cooperation Forum.
- **AI and biometrics** (FR, UK): the French DPA (CNIL)'s newly-created AI department[28] will develop guidance and recommendations on AI, notably, on building and using datasets for training algorithms, and the regulator's Innovation Lab (LINC) will study and publish on new forms of AI-driven data collection, such as emotional recognition and analysis.
- **Online ads and tracking, direct marketing, and dark patterns** (BE): the Belgian DPA (APD) will clarify its position on cookies by aligning it with other regulators' positions and dedicate efforts to answering individuals' queries about direct marketing and online privacy.
- **Data Protection Impact Assessments, or "DPIAs"** (BE, UK): the APD will also develop expertise and dedicate resources to advise organizations in the context of Article 36 GDPR prior consultations, which are due when DPIAs reveal residual risks for individuals. The ICO aims to respond to 70% of external DPIA requests for advice in eight weeks and to all DPIA prior consultations within the legal timeframes.

*Additionally, DPAs are committed to **increasing*** data subjects, policymakers, controllers, and processors awareness of data protection law and its rights and obligations, as well as improving Data Protection Officers (DPO)'s qualifications. These initiatives include:

- **Explaining and enabling data subjects' rights** (BE, IE, UK): the DPC will leverage mainstream media channels for awareness-raising campaigns and explain its complaint-handling process, including how it identifies systemic risk. On a more practical level, the ICO will make available a novel online tool that data subjects will be able to leverage when addressing data access requests to organizations.
- **Advising lawmakers on draft laws and government initiatives that have data protection impacts** (BE, EDPS, UK).
- **Developing specific information and training for DPOs and other privacy professionals** (BE, IE, UK): the DPC plans to expand the scope of its DPO Network to ensure that non-DPO data protection-focused personnel are included in the scope of the network. The ICO will publish a range of "data essentials" training

[26] Available at https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing
[27] Available at https://www.dataprotection.ie/sites/default/files/uploads/2021-12/DPC_Regulatory%20Strategy_2022-2027.pdf
[28] Available at https://www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de

and development modules and products specifically aimed at small and medium businesses.

Moreover, several DPAs plan to ***stimulate the approval of CoC and certification mechanisms*** *at national levels* as tools that enable organizations to attain and demonstrate compliance with the GDPR's requirements. This activity comes after a period during which the Belgian[29] and French[30] DPAs approved groundbreaking CoCs for use in the cloud sector, although these mechanisms may not be leveraged for carrying out data transfers to non-EEA jurisdictions. The French, Irish, and UK DPAs have committed to promoting such tools in the near future, including by approving CoC monitoring bodies, which are responsible for overseeing compliance by the CoC's subscribers. The Irish DPC's efforts will specifically focus on developing a CoC on the processing of children's and other vulnerable groups' personal data.

3. Bolstering enforcement actions: priorities

At a time when many stakeholders are alleging that the GDPR's cooperation and consistency mechanisms have not been delivering on promises of harmonious and speedy enforcement of data protection law, the EDPB has proposed to tighten cooperation between EU regulators through various means. In this respect, three different initiatives are noteworthy highlighting:

- **Coordinated enforcement on the use of cloud-based services by the public sector[31]**, in the context of an EDPB Coordinated Enforcement Framework (CEF): in 2022, 22 DPAs (including the EDPS) decided to launch investigations on the use of cloud-based solutions in their respective jurisdictions' public sector. In such context, DPAs looked into the processes and safeguards public bodies implement when acquiring cloud services, provisions governing the controller-processor relationship, and how they seek to comply with international transfer rules. From our extensive analysis, many national DPAs (including the Belgian and the French) put these investigations high on their agenda. The EDPB has recently published a Report outlining the findings and outcomes of this initiative, including those related to the performance of DPIAs, the negotiation of data processing agreements, the use of telemetry data by cloud providers, the engagement of sub-processors, and international data transfers. Moreover, the EDPB has chosen the topic for its 2023 coordinated enforcement effort[32]: the appointment and position of organizations' DPOs.

[29] Available at https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct
[30] Available at https://www.cnil.fr/fr/la-cnil-approuve-le-premier-code-de-conduite-europeen-dedie-aux-fournisseurs-de-services
[31] Available at https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en
[32] Available at https://edpb.europa.eu/news/news/2022/edpb-adopts-statement-european-police-cooperation-code-picks-topic-next-coordinated_en

- **Closer cooperation for strategic files**[33]: in April 2022 in Vienna, European DPAs agreed to enhance cooperation on strategic cases and to diversify the range of cooperation methods used. These cases will be identified yearly based on quantitative and qualitative criteria that the EDPB is still currently discussing (e.g. cases affecting a large number of data subjects, cases dealing with a structural or recurring problem in several countries, cases related to the intersection of data protection with other legal fields).
- **A Support Pool of Experts (SPE)** will assist DPAs in their enforcement actions: following its call for expressions of interest in early 2022, the EDPB has selected multiple experts that will be called upon to assist national DPAs in specific investigations related to their subject matter expertise. Such subject matters include **IT auditing, IoT, mobile apps, cloud computing, behavioral advertising, anonymization techniques, Privacy Enhancing Technologies (PETs), digital identity, age verification, biometrics, AI, dark patterns, DPIAs, personal data breaches, fintech, and policy monitoring (digital laws)**.

Since the 2021 FPF Report, national DPAs have shifted gears[34], with the top 9 administrative fines since the GDPR became applicable in May 2018 coming since July 2021. This **change in approach, away from an awareness-raising-first attitude and towards a strict enforcement paradigm**, is also reflected in the strategic documents we have analyzed, as DPAs are committed to increasing their investigatory and sanctioning efforts. Aside from coordinated investigations on the use of cloud services in the public sector - an area the EDPS is also devoted to - DPAs' public stances reveal a few other trends regarding enforcement priorities:

a. **Children's data** (BE, DK, UK): the Danish DPA (Datatilsynet) will monitor CCTV surveillance systems in residential institutions for children and young people. The ICO will continue to investigate compliance with and enforce the ICO's Children's Code[35], which includes restrictions on profiling of children and data sharing, plus the promotion of age-appropriate privacy notices.

b. **AI and biometrics** (FR, NL, UK): the CNIL - who earlier this year created an AI department[36] to increase its subject-matter expertise and better address the data protection risks posed and the breaches facilitated by AI systems - will monitor controllers who use augmented cameras and related predictive algorithms, including for policing and commercial purposes. A new "algorithmic supervisor" has been established within the Dutch DPA, whose priority areas of focus for 2023[37] include the identification of AI risks and cross-sector impacts. The UK DPA will tackle AI-driven discrimination in the job market, access to social benefits, and consumer credit.

[33] Available at https://edpb.europa.eu/news/news/2022/dpas-decide-closer-cooperation-strategic-files_en
[34] Available at https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
[35] Available at https://ico.org.uk/for-organisations/childrens-code-hub/
[36] Available at https://www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de
[37] Available at https://www.rijksoverheid.nl/documenten/kamerstukken/2022/12/22/kamerbrief-over-inrichtingsnota-algoritmetoezichthouder

c. **Cookies and online tracking** (FR, DK, UK): DPAs in the EEA promise to increase alignment on the enforcement of cookie banner standards, after the January 2023 Report by an EDPB Taskforce[38] was set up after multiple complaints were filed across Europe by privacy organization NOYB. In a recent interview, CNIL's Deputy Secretary General Mathias Moulin revealed that the authority may apply its cookie consent standards[39] to enforcement actions in mobile apps, smart cameras, and cloud data transfers contexts, notably regarding concerns about obtaining consent to access individuals' contacts, cameras, and geolocation.[40] While supporting the phase-out of third-party cookies and cookie consent banners, the ICO will seek to ensure meaningful control for individuals through its enforcement actions, which is in line with the UK government's data protection law reform plans.[41]

d. **Direct marketing and data brokerage** (BE, CZ, FR, UK): the Belgian DPA's Inspection Service and Litigation Chamber will devote efforts to investigating and sanctioning data brokers and resellers. The Czech DPA will investigate the dissemination of marketing communications via SMS, notably the lawfulness of such communications and their content. The CNIL will prioritize checks of commercial prospecting actions and their related data processing activities, whereas the ICO will focus on predatory marketing calls and data-enabled scams and frauds.

e. **Auditing public bodies** (CZ, DK, UK): the Czech DPA is committed to investigating data protection infringements from the country's ministries and the police, including the former's usage of social media outlets to engage with the general public. The Danish DPA will supervise compliance by the national parliament, law enforcement agencies, and local authorities that rely on pan-European databases (such as Eurodac and VIS). The ICO will revise its public sector enforcement approach, diverting away from fines and prioritizing warnings, reprimands, and enforcement notices.

f. **International data flows** (FR, UK): the CNIL will systematically investigate international transfers of personal data in the context of cloud services beyond the public sector and data flows in the mobile apps ecosystem. Conversely, the ICO has stated that it will seek to enable personal data transfers from the UK to other countries through regulatory certainty, focusing on advising the UK government and parliament on adequacy assessments and swiftly approving Binding Corporate Rules (BCRs) to that effect.

[38] Available at https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf
[39] Available at https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-orders-20-organisations-comply
[40] MLex, *French privacy watchdog's sees cookie consent decisions as model for enforcement, official says*, October 3, 2022, available at https://content.mlex.com/#/content/1413642.
[41] Available at https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

g. **Prioritizing complaint-triggered investigations and simplifying enforcement action** (FR, IE, SE, UK): for non-complex files or less serious infringements, the CNIL can, from April 2022, follow a simplified sanctioning procedure[42], which does not involve public hearings and has a low fine ceiling (with a maximum 20,000 EUR amount). The DPC is committed to "taking a fair and balanced approach to complaint-handling" and "sanctioning proportionately and judiciously." In its complaint-handling activities, the Swedish DPA will prioritize cases whose resolution may have benefits for multiple individuals, while also seeking to improve its handling of more complex cases. The ICO has committed to assessing and responding to 80% of data protection complaints within 90 days and 90% within six months. In this regard, the Danish DPA is an **outlier**, since it decided to prioritize cases with far-reaching consequences on the basis of own-volition inquiries.

h. **Deepening ties with other DPAs and sectoral regulators** (FR, NL, UK): the CNIL will seek to improve cooperation with both other EU DPAs and the French competition and audiovisual authorities to align views on data processing practices of large online players. The Dutch DPA's "algorithmic supervisor" will seek to optimize collaboration with Dutch market regulators and state inspectors to achieve consistent supervision of AI systems in the Netherlands.

[42] Available at https://www.cnil.fr/fr/reforme-des-procedures-correctrices-de-la-cnil-vers-une-action-repressive-simplifiee

	BE	CZ	DK	ET	FR	IE	ES	SE	UK	EDPB	EDPS
CCTV		✔	✔						✔		
Children, age verification, edtech	✔		✔		✔	✔			✔	✔	
DPOs	✔	✔	✔			✔				✔	
AI, biometrics					✔				✔	✔	
Ads, marketing, dark patterns, cookies	✔	✔	✔		✔				✔	✔	
Awareness & Training	✔			✔	✔	✔	✔		✔		
Public Sector	✔	✔	✔						✔	✔	
Cloud	✔				✔					✔	✔
Scientific research and health			✔		✔				✔	✔	
Data breaches			✔						✔	✔	
Data subject rights	✔	✔							✔		
Complaint-handling		✔			✔	✔		✔	✔		
DPIAs	✔								✔	✔	
Certification and CoC					✔	✔			✔	✔	
International data transfers	✔				✔			✔	✔	✔	✔
Inspections and Sanctions	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Cooperation with other DPAs and regulators		✔			✔	✔	✔	✔	✔	✔	✔
EU Data Strategy					✔						

***Table 1* — Overview of strategic and operational topics per DPA/jurisdiction**

4. Conclusion

In the last year, we have witnessed a significant increase in GDPR enforcement activities, with an increase in both the initiation and conclusion of infringement procedures and an increase in the administrative fines imposed on controllers and processors. This change could be interpreted as a shift from creating a data protection culture through guidance and awareness-raising and towards more punitive, hardline priorities in enforcement decisions.

However, DPAs have not overlooked their advisory role in the strategic documents they have published since July 2021, as they mention several areas they intend to clarify through guidelines and public-facing activities. This includes the **completion of DPIAs, the scope of data subjects' rights, and training of privacy professionals**. DPAs will also seek to promote the approval and adoption of Codes of Conduct and certification mechanisms as ways to enable organizations to easily demonstrate compliance with the EU's privacy acquis.

In the use of their investigative and corrective powers, EU DPAs will seek to make better use of the GDPR's cooperation and consistency mechanisms. Following the lead of their collegial body (the EDPB), most DPAs in the EEA have committed to participate in a **coordinated enforcement initiative on the appointment and position of Data Protection Officers (DPOs)**, to cooperate more closely on to-be-identified "**strategic files,**" and to rely on a multinational **Support Pool of Experts** during their national and cross-border investigations. Furthermore, DPAs like the CNIL will seek to **improve their collaboration with other sectoral regulators** (such as competition authorities), something that DPAs will be expected to do in the context of emerging regulations, such as the EU's Digital Markets Act (DMA). **International data transfers** remain a high priority for EU DPAs' enforcement efforts.

We also note a significant **overlap** between the areas that DPAs aim to clarify through guidance and areas that are targeted for investigations and enforcement. Topics that appear in agendas of several DPAs from both approaches include the **processing of minors' personal data** (including in online schooling environments), the use of **personal data-driven AI systems**, **advertising technology, and direct marketing activities**.

In parallel with the answers that the CJEU is expected to give in response to multiple national courts' preliminary ruling requests,[43] upcoming DPA guidance and enforcement actions will hopefully provide clarity as to the interpretation and application of key GDPR requirements in the EEA. Closer cooperation in the context of EDPB Subgroups and Coordinated Enforcement Frameworks may help ensure consistency in the guidance and decisions issued by these regulators and guarantee a high degree of data protection in EEA jurisdictions.

[43] https://fpf.org/blog/upcoming-data-protection-rulings-in-the-eu-an-overview-of-cjeu-pending-cases/.

ANNEX
Overview of strategic and operational plans per country

A.1. BELGIUM

- ***Materials:***
  - Press release[44] on priorities for 2023.
- ***Summarized Priorities for 2023:***
  - Clarifying the DPA's position on **cookies**, by aligning it with other EU regulators' stances.
  - Supporting **DPOs** in their role by ensuring their appointment and involvement, and investigating their position within organizations.
  - Establishing prevention actions and a dialogue with the players involved in the "**Smart City"** data processing ecosystem (e.g., intelligent transportation).
  - Awareness-raising activities for **children**, parents, and teachers.
  - Investigating and sanctioning **data brokers** and resellers.

A.2. CZECH REPUBLIC

- ***Materials:***
  - Control Plan 2023[45]
- ***Planned Inspections for 2023:***
  - **By the Inspector of the Czech DPA, Jiřina Rippelová:**
    - Following up on the audits to bailiff officers from 2021 and 2022, and carrying out two additional inspections. These will focus on breaches of data subjects' rights under Articles 15 to 21 GDPR, and follow from complaints received by the DPA or *ex officio* knowledge it recently acquired.
  - **By the Security Agendas Department:**
    - Checking Eurodac Regulation compliance by the Ministry of the Interior. The focus of the audit shall be on the processes that the ministry is currently setting up for implementing the Eurodac Regulation, and how they comply with data protection requirements.
    - Controlling compliance of data processing in the context of visa issuance by the Ministry of Foreign Affairs, consulates, and embassies.
    - Verifying data protection compliance of CCTV systems equipped with biometric functions, both by private and public bodies.

[44] Available at https://www.autoriteprotectiondonnees.be/lapd-definit-ses-priorites-pour-lannee-2023
[45] Available at https://www.uoou.cz/urad-zverejnil-svuj-kontrolni-plan-pro-rok-2023/d-56742

        - Monitoring compliance of local police databases and information systems.
    - **By the Private Sector Inspection Unit:**
        - Controlling data processing operations carried out by a prominent (unnamed) processor. The inspection should focus on the engagement of sub-processors, compliance of contractual arrangements with Article 28 GDPR, and the documentation of audits.
        - Processing of personal data in the context of telemarketing. The audit will focus on one telemarketing company, will evaluate compliance with lawfulness and transparency requirements, and will be conducted together with the Czech Telecommunications Office (TCU).
        - Employer processing of employee attendance data. The Czech DPA will monitor “selected employers” - through preliminary questionnaires and ensuing inspections - for the categories of personal data processed by their attendance-keeping systems, the duration of the processing, and whether the data is strictly necessary.
    - **By the Public Entity Audit Unit:**
        - Processing of personal data in the context of the issuance of identity cards by the Ministry of Interior.
        - Processing of complainants’ personal data by an unnamed public body. The audit will focus on the applicable data retention period, the fulfillment of transparency obligations, the exercise of data subjects’ rights, and the involvement of the DPO.
        - Monitoring the use of social media by ministries to communicate with the general public. The DPA will send questionnaires to public bodies that use Linkedin, Twitter, Facebook, Instagram, and Mastodon for public engagement, which will focus on compliance with Article 5 GDPR principles and data protection by design.
        - Coordinated Enforcement Framework with other EU DPAs on the appointment and position of the DPO.
    - **By the Commercial Communications Department:**
        - An inspection of two companies in the area of dissemination of marketing communications via SMS, notably about the lawfulness of such communications and their content.

A.3. Denmark

- ***Materials:***

- Special focus areas for the Danish Data Protection Authority's supervisory activities in 2023[46]

- ***Summarized Focus Areas:***
  - **Better balance between targeted supervision and complaint-handling**: while complaints will continue to be an important source for focusing on the real issues, the DPA has decided to prioritize cases with far-reaching consequences on the basis of own-volition inquiries. This means that the DPA will more seldom treat individual complaints in a thorough and detailed manner, and will rather more often select instances of high-risk infringements that come to its attention via other means, like personal data breach notification, media coverage, and tips. With regards to complaints, the DPA will often limit itself to contacting the data controller and informing them of the complaint and the relevant rules, but not necessarily carrying out "extensive and time-consuming investigations."
  - **Protection of children's data:** the DPA's investigations will focus on the monitoring of CCTV surveillance in residential institutions, covering children and young people, but also the institutions' employees.
  - **Data Protection Officers (DPOs)**: in the context of the EDPB's Coordinated Enforcement Framework for 2023, the DPA will monitor the appointment and position of DPOs in organizations across Denmark and align its enforcement efforts and stances with other European regulators.
  - **Medical devices and other personalized healthcare products**: the DPA will supervise a number of companies that process sensitive data in the context of manufacturing and selling medical devices and other products that are supplied directly to citizens on the basis of orders from municipalities, hospitals, etc. The inspections will target the companies' storage of and disclosure of information, data minimization, and security standards.
  - **Inspecting the Danish Parliament (Folketing)'s** data processing practices.
  - **Processing of personal data about website visitors.**
  - **CCTV surveillance** by parking companies in the context of the issuance of parking fines.
  - **Disclosures of personal data for statistical or scientific research purposes**: such disclosures may only occur where the studies at stake are of significant social importance. The DPAs prior permission for disclosures - subject to strict conditions - must be obtained in three instances: (i) when the transfer takes place for processing outside the territorial scope of the GDPR; (ii) when the disclosure concerns biological material; and (iii) when the disclosure takes place for the purpose of publishing information in recognized scientific journals. In 2023, the DPA will check whether the conditions set out in a number of authorizations it has issued for such disclosures in recent years are being complied with.

[46] Available at https://www-datatilsynet-dk.translate.goog/afgoerelser/generelt-om-tilsyn/saerlige-fokusomraader-for-datatilsynets-tilsynsaktiviteter-i-2023?_x_tr_sl=da&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp

- **Processing of personal data by national authorities in pan-European systems**: such systems include, among others, the Schengen Information System (SIS), the Visa Information System (VIS), the EU Fingerprint Register (Eurodac), the Customs Information System (CIS), and the Internal Market Information System (IMI).
- **Personal data processing for Law Enforcement**: the Danish DPA will monitor the processing of personal data by the police, the public prosecutor's office, the correctional institutions, and the Independent Police Complaints Authority for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses or enforcing criminal sanctions.

A.4. EDPB

- ***Materials:***
  - Coordinated Enforcement Framework (CEF): use of cloud by public sector[47]
  - Recruitment for Support Pool of Experts (SPE)[48] - call for expressions of interest
  - 2021 Annual Report[49]
- ***Summary:***
  - **CEF**: following the launch of the EDPB Document on the CEF in 2020, 22 DPAs (including the EDPS) decided to launch investigations on the use of cloud-based solutions in their respective jurisdictions' public sector ("Through coordinated guidance and action, the [DPAs] aim to foster best practices [in that context] and thereby ensure the adequate protection of personal data").
    - "The CEF will be implemented at national level in one or several of the following ways: fact-finding exercise; questionnaire to identify if a formal investigation is warranted; commencement of a formal investigation; follow-up of ongoing formal investigations. In particular, [DPAs] will explore public bodies' challenges with GDPR compliance when using cloud-based services, including the process and safeguards implemented when acquiring cloud services, challenges related to international transfers, and provisions governing the controller-processor relationship."
    - A report on the outcome of this analysis is expected in the coming months.
  - **SPE**: "The EDPB 2021-2023 Strategy has identified the need for improved collaboration between authorities. In particular, Pillar 2 of the strategy (supporting effective enforcement and efficient cooperation between national supervisory authorities) calls for the establishment of a [SPE], with

[47] Available at https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en
[48] Available at https://edpb.europa.eu/system/files/2022-02/call_for_expressions_of_interest_support_pool_of_experts.pdf
[49] Available at https://edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2021_en

a view of providing material support in the form of expertise that is useful for investigations and enforcement activities (...). The SPE involves both the EDPB and external experts."
    - The subject matter experts could be expected to perform any tasks in the area of enforcement support and coordination, including (i) Support / participate in investigation activities, (ii) Advise on the development of investigatory support tools, (iii) Provide legal advisory services, (iv) Produce sufficiently detailed contributions, and (v) Participate in any face-to-face meetings and teleconferences.
    - Fields of sought expertise include IT auditing, internet of things, mobile applications, cloud computing, behavioral advertising, anonymization techniques, Privacy Enhancing Technologies (PETs), digital identity management, age verification, biometrics, artificial intelligence, dark patterns, DPIAs, personal data breaches, fintech, policy monitoring (digital laws).
  - **2021 Annual Report**:
    - The EDPB will regularly organize stakeholder events to gather new information on specific regulatory issues in the interest of developing future guidance and drafting new laws and regulations.
    - The EDPB's Coordinated Supervision Committee (CSC) will gradually take responsibility for all coordinated supervision of large EU information systems, bodies, offices, and agencies. This includes the Schengen Information System (SIS), ETIAS, Eurodac, ECRIS, and Europol.

A.5. EDPS

- ***Materials:***
  - Annual Report 2021[50]
- ***Summary:***
  - **Acting on the 2020-2024 Strategy[51] "Shaping a Safer Digital Future"** (already covered in the 2021 FPF Report):
    - **Foresight**: the EDPS' commitment to being a smart institution that takes the long-term view of trends in data protection and the relevant legal, societal, and technological contexts.
    - **Action**: the EDPS will develop tools for EU institutions to be world leaders in data protection. It aims to promote coherence among EU enforcement bodies via a stronger expression of European solidarity, burden sharing, and a common approach.
    - **Solidarity**: the EDPS believes that justice requires privacy to be safeguarded for everyone, in all EU policies, while sustainability should be the driver for data processing in the public interest.

[50] Available at https://edps.europa.eu/system/files/2022-04/2022-04-20-edps_annual_report_2021_en.pdf
[51] Available at https://edps.europa.eu/edps-strategy-2020-2024/

A.6. ESTONIA

- ***Materials:***
  - Report On Compliance with the Public Information Act and Ensuring the Protection of Personal Data[52] (2020 Annual Report)
  - "A look into the future"[53] blogpost
- ***Summary:***
  - **Strategic Vision for 2024:** The Estonian DPA (AKI) conducted an anonymous survey of selected partners to obtain feedback on its efforts to date and forecast its forthcoming efforts. However, the AKI provided sparse details on its vision, stating only that the AKI will provide more information letters and training, will be funded and staffed, will partner with other entities, and focus on supervision and enforcement.

A.7. FRANCE

- ***Materials:***
  - 2022 - 2024 Strategic Plan[54] and corresponding article, outlining the CNIL's regulatory priorities from 2022 to 2024
  - Reform of the CNIL's sanctioning procedures: towards simplified action[55]
  - 2021 Annual Report[56]
  - CNIL's Innovation Lab (LINC) 2022-2023 research plan[57]
- ***Summary:***
  - **Specified Priorities for 2022 - 2024:** the CNIL identifies three priority areas it intends to focus on from 2022 to 2024, and three priority themes specifically for 2022:
    - ***(1) Promoting control and respect for the rights of people in the field:*** the CNIL is mobilizing to strengthen and promote information and awareness about the public's control over personal data, which includes creating tools to help individuals navigate complex and opaque digital services and products. To that end, the CNIL will prioritize investigating complaints and work to reduce the time required to conduct such investigations. The CNIL will also continue its efforts on the European level to protect individual rights from major digital players.

[52] Available at https://aastaraamat.aki.ee/sites/default/files/aastaraamatud/aastaraamat_2020.pdf
[53] Available at https://aastaraamat.aki.ee/aastaraamat-2020/pilk-tulevikku
[54] Available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_plan_strategique_2022-24.pdf
[55] Available at https://www.cnil.fr/fr/reforme-des-procedures-correctrices-de-la-cnil-vers-une-action-repressive-simplifiee
[56] Available at https://www.cnil.fr/fr/la-cnil-publie-son-rapport-dactivite-2021
[57] Available at https://www.cnil.fr/fr/le-laboratoire-dinnovation-numerique-de-la-cnil-publie-son-programme-de-recherche-20222023

        - ***(2) Promoting the GDPR as a trusted asset for organizations:*** to further promote data protection as part of daily culture for data controllers, the CNIL will continue producing clear and practical guidelines to ensure data protection principles are understood and applied accordingly. This effort includes promoting and approving certification mechanisms and codes of conduct, developing tools to allow data controllers to control their compliance in a way that is adapted to their needs, and making compliance the best prevention against cyber risks and crime. Additionally, the CNIL will work to further its understanding of business models and the economic impact of regulatory choices.
        - ***(3) Prioritizing targeted regulatory actions on topics of high privacy concern:*** to meet the evolving challenges arising from technologies based on intensive data collection and processing, the CNIL will implement a global action plan targeting various sectors. This action plan will begin with a compliance strategy setting out doctrine for the sector, then establish sector-specific practical compliance tools, and finally the CNIL will conduct control campaigns and adopt corrective measures, if necessary, to ensure compliance. The CNIL intends to target three sectors: (a) augmented cameras and their use of predictive algorithms, including police uses, commercial uses, and support actors; (b) data transfers in the cloud, to secure the transfer of personal data of French citizens to countries outside the European Union; and (c) smartphone applications that collect personal data, focusing on making data flows visible to users and reinforcing the compliance of mobile applications and their ecosystems.
    - **The CNIL's LINC Lab** will host debates and studies on the environmental impacts of data processing (linked to the promotion of the data minimization principle), the data economy (ie., data exchanges), data subject perceptions and action, new forms of data collection (focusing on emotion recognition/analysis), and the data protection implications of the metaverse.
    - **Simplified enforcement action:** Since April 8, 2022, the CNIL can follow a simplified sanctioning procedure for non-complex files or less serious infringements.
        - This simplified procedure does not involve a public hearing and is solely led by the chair of the CNIL's restricted panel (*formation restreinte*). In this context, fines can only reach a maximum of 20.000 EUR, and periodic penalty payments are capped at 100 EUR per day. None of them can be made public.
        - The ordinary sanctioning procedure has also changed, extending the deadlines to produce observations and removing the possibility for the chair of the *formation restreinte* of deciding to impose a fine or drop an investigation on their own.

- Compliance orders issued by the President of the CNIL no longer require a written response from organizations, which must comply within the time limits set by the President. They do not need to submit evidence of compliance, but the latter can be checked via a subsequent audit. The mandatory 6 months deadline for compliance has also been removed.

A.8. IRELAND

- ***Materials***
  - Irish DPA's Regulatory Strategy for 2022-2027[58]
  - Irish DPA's 2021 Annual Report[59]
- ***Mission:*** Upholding the consistent application of data protection law through engagement, supervision, and enforcement, and driving compliance with data protection legislation. Planned goals include:
  - Educating stakeholders on their rights and responsibilities;
  - Taking a fair and balanced approach to complaint-handling;
  - Communicating extensively and transparently with stakeholders;
  - Participating actively at EDPB level to achieve consistency;
  - Cultivating technological foresight, in anticipation of future regulatory developments;
  - Sanctioning proportionately and judiciously; and
  - Retaining and amalgamating the expert capacities of its staff to ensure operational effectiveness.
- ***Achieving Strategic Goals***
  - *Regulating consistently and effectively*, through:
    - Quarterly publication of case studies on GDPR application and enforcement
    - Publishing the findings of an independent review into the resource capacity and future-state resourcing needs of the DPC
  - *Safeguarding Individuals and Promoting Data Protection Awareness*, through:
    - Utilizing mainstream media channels to make individuals more aware of data protection and their rights under the GDPR
    - Publishing separate and more expansive guidance on the DPC's complaint handling process, including how systemic risk is identified
  - *Prioritizing the Protection of Children and Other Vulnerable Groups*, through:

[58] Available at https://www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-regulatory-strategy-2022-2027?mkt_tok=MTM4LUVaTS0wNDIAAAGBgkqSzeXW5KBpvABjoO1bjqGWxXz-9dKepArR5YpDJoT_Wh1N1WDsQ1uSI0Ngwi8HxbaNlX8s6P0RbIByawSBandglvybJ0QIg907uzZ0MFzc
[59] Available at https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2021-annual-report

        - Defining the specific protections required to safeguard the rights of children and other vulnerable groups, and providing guidance
        - Collaborating with advocates and experts in the field of protection and promotion of the rights of vulnerable adults, including other regulators
        - Actively promoting the development of codes of conduct on the processing of children's personal data, and that of other vulnerable groups
    - *Bringing Clarity to Stakeholders*, through expanding the scope of the DPC's DPO Network, to ensure that non-DPO data protection-focused personnel are brought within the ambit of the Network.
    - *Support Organizations and Drive Compliance*, by engaging with the current – and future – legislation that intersects with the GDPR.

A.9. SPAIN

- ***Materials:***
    - 2021 Annual Report[60]
- ***Summarized Priority Areas for 2023 and Beyond:***
    - Improving and adding publicly-available resources (e.g., FAQs, also in English);
    - Enlarging the Inspection Sub-Directorate, adding 10 persons;
    - Defining the Convention 108+ Consultative Committee's 2022-2025 work programme

A.10. SWEDEN

- ***Materials:***
    - Annual Report 2021[61], detailing the DPA's name change and efforts from 2018 to 2021, along with a new strategic direction for 2022 to 2025
- ***Summary:***
    - **New Strategic Direction for 2022 - 2025:** in response to a review identifying a number of development issues, the DPA formulated a new strategic plan for 2022 to 2025. The DPA identified four success factors that are critical for the coming years: (i) clear and effective ways of working, (ii) digitalization, (iii) strategic collaboration, and (iv) upskilling of its staff. The DPA will focus on these factors when developing efforts during the coming years, though the Report does not expressly state how proposed future efforts will achieve these particular goals. The Report discusses:

[60] Available at https://www.aepd.es/es/documento/memoria-aepd-2021.pdf
[61] Available at https://www.imy.se/globalassets/dokument/arsredovisningar/imy-arsredovisning-2021.pdf

- ***(1) Changing approach to complaints:*** the DPA intends to improve processing times and case balances, and ultimately free up resources in order to remedy a failure to meet target times for processing complaints. Furthermore, the DPA recognizes that its practices in past years have led to a reduction in the number of inspections opened and closed. In the coming years, the DPA will strive to handle cases easily, quickly, and efficiently.
- ***(2) Increasing focus on complaint-based supervision:*** current inspection activities will shift to those based on complaints from individuals rather than own-initiative investigations and risk assessments. The DPA believes this shift will allow them to carry out significantly more enforcement cases. The DPA will continue working to create practices that contribute to many individuals, that are carried out in an effective and lawful manner, and that impact both individual cases and the broader protection of privacy in society.
- ***(3) Harmonizing the DPA within the EU:*** the DPA participated in the EDPB by issuing common guidelines, recommendations, and opinions in support of a harmonized application of the law. The DPA expects the number of cases escalated to the EDPB will increase as its work on cross-border cases increases. However, the DPA is currently satisfied with its participation in the EU.
- ***(4) Reducing processing times for complex cases:*** the DPA recognizes the need to improve its handling of cases involving binding corporate rules, lawfulness checks, and data processing infringements. This will be a priority for the coming years.

A.11. UNITED KINGDOM (UK)

- ***Materials:***
  - ICO25 plan[62], outlining the UK DPA's priorities and objectives for the 2022-2025 period. It also contains an Annual Action Plan (October 2022 - October 2023). The document was under public consultation until September 2022.
  - ICO's revised approach to public sector enforcement[63]
- ***Summarized Strategic Objects and Actions:***
  - **Safeguard and empower people, in particular vulnerable groups,** by:
    - Empowering them with information, notably through a novel data access request tool, and helping people to understand their rights (FAQs and support);

[62] Available at https://ico.org.uk/media/about-the-ico/documents/4020926/ico25-plan-for-consultation-20221407-v1_0.pdf
[63] Available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-sets-out-revised-approach-to-public-sector-enforcement/

- Focusing the ICO's intervention in areas of greatest harm and risk, and **evening up the power balance** between those who hold the most precious data and the **most vulnerable** who hand over their data. Some examples include:
    - **Children's privacy**, by continuing to investigate compliance with and enforce the ICO's Children's Code[64], as well as influencing industry (such as social media platforms, video and music streaming sites, and gaming platforms) to ensure children benefit from an age-appropriate online experience. This also includes restrictions on children profiling and data sharing, plus the promotion of age-appropriate privacy notices.
    - Publishing guidance on mitigating negative impacts of emerging technologies on vulnerable groups;
    - Addressing **AI-driven discrimination**, notably concerning access to job opportunities, social benefits, and credit.
    - Tackling the risks of **biometric technologies**, like gait analysis, facial recognition, iris scanning, fingerprint recognition, and emotion recognition. The ICO will consult and investigate the industry on how these technologies are and should be used.
    - Influencing **online tracking** practices to create a more privacy-friendly internet (e.g., phasing out of third-party cookies and cookie pop-ups, while promoting meaningful control for users).
    - Investigating and guiding the use of **CCTV**, in particular in care homes.
    - Exploring the use of targeted advertising (adtech) of gambling on social media and the use of personal information within the **gambling** sector.
    - Continue to focus on **predatory marketing calls** and data-enabled scams and frauds.
- Measuring attitudes, perceptions, and awareness of data rights (especially of vulnerable groups and communities), the work of the ICO, trade-offs between sharing personal information and access to products and services, and how organizations collect, use, share, and store personal data;
- Assessing and responding to 80% of data protection complaints within 90 days and 90% within six months. This includes **coordinating with sector-specific ombudsmen or representative groups**, which could become the first point of contact for data protection complaints in their area of expertise or responsibility.
- Ensuring that less than 1% of our data protection complaints caseload are over 12 months old.

[64] Available at https://ico.org.uk/for-organisations/childrens-code-hub/

        - Concluding 95% of all formal investigations within 12 months of them starting.
    - **Empowering responsible innovation and sustainable economic growth**, by:
        - Taking evidence-led action against those who try to gain unfair advantage through unlawful or irresponsible actions, with a predictable approach and a rapid response to complaints and new regulatory risks (e.g., biometrics, facial recognition, AI, algorithms, health data processing);
        - Cooperating and collaborating with regulatory counterparts in other jurisdictions;
        - Enabling international data flows through regulatory certainty, with a focus on advising the UK Government and Parliament on adequacy assessments, and swiftly approving Binding Corporate Rules (BCRs);
        - Producing and publishing a 'guidance pipeline', which will include guidance on direct marketing, journalism, employment practices, research, subject access requests, emerging technologies (e.g., AI and biometrics), and a program of guidance reviews in response to forthcoming legislative reform;
        - Amplifying advice and guidance through sectoral regulators and sector representative associations (Ofcom on children's privacy, through the Digital Regulation Cooperation Forum[65]);
        - Consulting with stakeholders to gain the widest possible input into the development of statutory guidance and codes;
        - Advising organizations in the Regulatory Sandbox, iAdvice (a fast, frank feedback service for innovators), and Innovation Hub;
        - Supporting SMEs, by publishing a range of "data essentials" training and development modules and products specifically aimed at SMEs;
        - Delivering a program of Codes of Conduct and certification schemes, tailored to the needs of sectors, and promoting their adoption;
        - Resolving 80% of written inquiries within seven calendar days and 99% within 30 calendar days;
        - Referring or closing 80% of personal data breach reports within 30 days;
        - Ensuring 90% of audit recommendations are accepted in full or in part;
        - Responding to 70% of external DPIA requests for advice in eight weeks and to all DPIA prior consultations within legal timeframes;
        - Acting as a "hub" for good information rights practice, so organizations can access real life examples of what the law requires (e.g., publishing training materials, templates, and recommendations made in complaint-handling and audit work).

[65] Available at https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/

- **Promoting openness, transparency, and accountability in the public sector**, while revising the ICO's approach for public sector fines/enforcement, to ensure that money is not being diverted away from the public services where it is needed. In this regard, the ICO will prioritize other powers, such as warnings, reprimands, and enforcement notices, with fines only issued in the most serious cases.
- **Continuously developing the ICO's culture, capability, and capacity,** by:
    - Providing quality and timely responses proportionately tailored to the needs and circumstances of individuals and stakeholders;
    - Communicating, both internally and externally, in ways which are understandable, accessible, and engaging;
    - Providing value for the money paid in fees by companies, in particular SMEs, by seeking to:
        - recover the costs of litigation, as far as is possible, from companies that have been fined;
        - ensure that all organizations that are required to register do so;
        - publish annually a value for money summary of how the data protection fees the ICO receives, and the funding the ICO gets from the government, is used to deliver efficient and effective services.

AVENUE MARNIX 13-17 | 1000 BRUSSELS, BELGIUM
FPF.ORG | info@fpf.org