Insights into the Future of Data Protection Enforcement:

Regulatory Strategies of European Data Protection Authorities for 2021-2022

Authors

Sebastião Barros Vale, LL.M
Dr. Gabriela Zanfir-Fortuna
Dr. Rob van Eijk

July 2021

Content

1. Introduction

The **European Data Protection Authorities (DPAs)** are arguably the most powerful data protection and privacy regulators in the world, having been granted by the European Union's General Data Protection Regulation (GDPR) broad powers and competences, in addition to independence. With GDPR enforcement visibly ramping up in the past year, it is important to get insight into the key enforcement areas targeted by regulators, as well as understanding what are those complex or sensitive personal processing activities where DPAs plan to provide compliance guidelines or to shape public policy.

The regulatory plans of DPAs, as revealed by annual reports, strategic documents and operational plans published in the first half of 2021, provide useful predictors of where the watchdogs will devote their broad investigative, advisory, and corrective powers. Following our May 2020 comprehensive analysis of European Economic Area (EEA) DPAs' priorities and focus areas for the new decade, the **Future of Privacy Forum** has conducted a new analysis that resulted in this Report presenting an overview of the regulatory strategies of DPAs for 2021-2022.

The strategic documents and operational plans published by DPAs since the initial FPF report offer a unique view into how the COVID-19 pandemic and the dissemination of digital tools will be shaping their regulatory action in 2021 and in coming years. This is why FPF has reviewed and summarized an additional fifteen available DPA strategies, roadmaps and annual reports, namely the ones released by DPAs in France (FR), Portugal (PT), Belgium (BE), Norway (NO), Sweden (SE), Ireland (IE), Bulgaria (BG), Denmark (DK), Finland (FI), Latvia (LV), Lithuania (LT), Luxembourg (LU) and Germany (Bavaria). FPF's analysis also included documents published by the European Data Protection Board (EDPB)[1] and the European Data Protection Supervisor (EDPS)[2].

[1] The European Data Protection Board (EDPB) is composed of representatives of the national European Union (EU) and European Economic Area (EEA) European Free Trade Association (EFTA) data protection supervisory authorities, and the European Data Protection Supervisor (EDPS).
[2] The European Data Protection Supervisor (EDPS) is the European Union's independent data protection authority, set up by Regulation (EU) 2018/1725, tasked with ensuring that the institutions and bodies of the EU (EUI) embrace a strong data protection culture. It also serves as an impartial advisor to EU lawmakers.

Our findings reveal that the **risk-based approach**, as mandated by the GDPR concerning a number of controller and processor compliance efforts, is preferred by DPAs when it comes to establishing priorities on the usage of their (often limited) resources. While some DPAs (like the **Latvian DPA**) seem to focus on risk areas that surface from their past enforcement record, others are committed to investing in own-initiative investigations in critical areas where the potential consequences for data subjects are the most dire. In this respect, the **Danish DPA** plans to create controller "risk profiles", based on factors such as their line of business and their industry's reported data breaches.

Our research also reveals that DPAs seem to be responding to the recent Court of Justice of the European Union's decisions on **online tracking technologies** (see Fashion ID and Planet49 rulings) and **international data transfers** by ramping up their corrective actions. Additionally, DPAs have announced plans to publish new guidance on various **Privacy Enhancing Technologies (PETs)** and to increase **awareness-raising** activities, as media reports on data breaches have exposed the vulnerability of information systems in essential sectors and the lack of data protection knowledge and skills at various levels of responsibility inside organizations.

The pandemic has also exposed the vulnerabilities of certain groups, such as employees and patients, to questionable data processing practices. To address data subjects' concerns, and moving beyond the mere publishing of guidance for organizations, DPAs plan to better explain to individuals how their "data subject rights" work, and make controllers accountable for alleged wrongdoings. They plan on doing so in response to complaints they receive, but also following **proactive audits and inspections**.

In terms of their regulatory toolbox, the DPAs seem to be more and more inclined to promote **sandboxes**, especially when it comes to the development of AI/ML applications and services, or more broadly for processing of personal data for research purposes.

Like FPF's previous report, this analysis consists of a **summary** of findings and an **Annex**. The initial part of the summary will cover the EDPB's and national DPAs' expected guidelines and clarifications for the consistent application of the GDPR. The second chapter outlines some thematic and sectoral enforcement priorities announced by DPAs in light of technological advancements and new risks posed to individuals, especially vulnerable populations, such as children.

---

on policies and proposed laws which might affect the rights to privacy and data protection. The EDPS also provides the secretariat to the EDPB.

The **Annex** includes translated excerpts of each national DPA strategic document analyzed, allowing the reader to dive deeper into the relevant details. It also includes a summary of the EDPS' 4-year strategy, covering the 2020-2024 period, which promises to deeply influence how DPAs across Europe understand and approach data protection challenges brought by emerging technologies.

With this report, FPF hopes to shed light on the general regulatory aims of DPAs across Europe for the coming year. The summary highlights the trends, but also some noteworthy outliers when it comes to planned enforcement of data protection standards in the continent.

Note: this report does not include findings outlined in the first FPF report on the European DPAs' strategies released on May 5, 2020. Therefore, this overview does not contain the analysis of materials published by DPAs in the first half of 2020, that were covered in said report, some of which outline regulators' (such as German, British and Italian DPAs) priorities for 2021 and beyond. Therefore, for a comprehensive view on the DPAs' near future plans, we invite readers to consult the two reports together.

2. Guidelines for consistent application of the GDPR

European Data Protection Board: In late 2020, the EDPB published its 2021-2023 Strategy, which builds on **4 key pillars:** (i) Advancing harmonization and facilitating compliance; (ii) Supporting effective enforcement and efficient cooperation between DPAs; (iii) A fundamental rights approach to new technologies; and (iv) the global dimension. The Strategy is further concretized in the EDPB's 2021-2022 Work Program, publish in March 2021, which sets out specific actions - notably, upcoming guidance - that the Board will take to address each of the 4 pillars:

i. **Advancing harmonization and facilitating compliance**, by
    a. Issuing guidance on key concepts of data protection law: **controllers and processors; restrictions of GDPR principles and rights (Article 23 GDPR); data subjects' rights; legitimate interests; medical and scientific research; children's data; and remuneration against personal data**.
    b. Advising the EU legislator on data protection-related policies (e.g., Data Governance Act, ePrivacy, AI regulation proposal etc.) and intensifying engagement and cooperation with other regulators and policymakers.

ii. **Supporting effective enforcement and efficient cooperation between DPAs**, by
    a. Issuing guidance on Chapter VII DPA cooperation tools (e.g., the **One-Stop-Shop mechanism**; mutual assistance; EDPB dispute resolution; **calculation of administrative fines**);
    b. Implementing a Support Pool of Experts (SPE), to provide material support to DPAs in the form of expertise that is useful for investigations and enforcement activities.

iii. **A fundamental rights approach to new technologies**, by issuing guidance on the data protection implications of such technologies (e.g., **blockchain**, facial recognition for law enforcement, **anonymization and pseudonymization, cloud computing, Artificial intelligence/Machine Learning, Digital Identity & Identity Federation, Data Brokers, Internet of Things and payment methods**);

iv. **The global dimension**, notably by providing **guidance on the use of tools for transferring personal data outside of the EEA** (e.g., final version of Recommendations 01/2020 on supplemental measures, opinions on and review of adequacy decisions - such as the UK's -, codes of conduct and certification for international transfers, the interplay between the GDPR's territorial scope and such tools).

National DPAs and the European Data Protection Supervisor: Data protection watchdogs have the difficult task of defining the domains where their action - either through guidance, investigations, or sanctions - would have the most impact on raising the data protection bar in Europe. Their strategic documents outline some of their plans to achieve that goal.

Transparency around online data collection. Various DPAs, such as the **French**, **Spanish** and **Irish DPAs**, have recently approved revised guidance around the **use of cookies** and other tracking technologies, with a particular focus on notice and consent. The **Portuguese DPA** has also recently announced it will issue its own guidance on online tracking. While some DPAs have already started their enforcement efforts in that domain, they are expected to increase supervisory action in the coming months and years, with other DPAs following suit. **Manipulative design choices** (or so-called "dark patterns") in online User Experience (UX) and User Interfaces (UI) are also expected to occupy DPAs across the board, from providing guidance, to enforcing the law against them.

Data Protection Officers (DPOs). DPAs have identified a need to check whether organizations across the board have appointed DPOs where such appointment is legally mandatory. Also, regulators are concerned that some acting DPOs have not been granted enough resources and independence to effectively perform their duties.

Regulators are expected to directly engage with DPOs - individually or through established knowledge networks - and to conduct *ex officio* inspections to verify compliance with DPO-related GDPR obligations.

Data integrity and confidentiality. Several DPAs are committed to guiding controllers in improving their data security standards. The **ICO** is currently revising its Anonymization guidelines, taking stock of technical developments in this space and the emergence of Privacy Enhancing Technologies (such as synthetic data). The **Belgian DPA** is also committed to assisting the EDPB with the revision of the Article 29 Working Party Guidelines from 2014 on Anonymization.

3. Sectoral and Thematic Enforcement Priorities

Big tech is listed by several DPAs' strategic plans as a priority for oversight. As Europe, led by France and its national cloud strategy, aims to build its "digital sovereignty", reducing European businesses' and public administration's dependence on US-based large online providers is seen as a priority. Recently, the European Commission launched two new Industrial Alliances, one for Processors and Semiconductor technologies, and the European Alliance for Industrial Data, Edge and Cloud, as key components of a strategy to "provide the EU with the capabilities needed to strengthen its critical digital infrastructures, products and services." As for DPA action in this respect, the **Norwegian DPA's** strategy mentions the need for attaining a fairer balance between large foreign technology companies and Norwegian actors, while other DPAs are announcing potential large scale enforcement actions against US-based big tech companies (e.g., the Luxembourgish DPA[3] and the EDPS[4]).

Privacy by design. This principle is mentioned as one of the focuses of DPAs' regulatory sandboxes, which aim to assist start-ups with ensuring privacy is embedded into innovative products and services. The **Luxembourgish DPA** plans to roll-out awareness-raising activities on privacy by design practices and the **EDPS** intends to share knowledge on the risks and opportunities posed by new technologies in that context.

Employment relationships. Data processing in the **employment context** was also a top sectoral priority among DPAs. This is likely due to the fact that, during the COVID-19 pandemic, there was a significant increase in the number of remote workers in Europe, which led to the use of electronic monitoring tools by employers. While DPAs (such as the **Portuguese DPA**) have issued guidance on the data protection rules in that context,

[3] *Amazon faces record privacy fine as Europe wields tougher rules* (Bloomberg, 10 June 2021).
[4] *The EDPS opens two investigations following the Schrems II judgment* (EDPS, 27 May 2021).

as well as on temperature screening and the collection of employees' health data, they are expected to conduct audits and inspections to verify compliance.

Health & Research. Researchers and healthcare providers may come under scrutiny by DPAs (such as the **French** and the **Bulgarian DPAs**) regarding the processing of health-related data for the management of the COVID-19 pandemic. In Luxembourg, the DPA is planning to issue specific guidance on digital health and associated data practices.

SMEs. European DPAs aim to increase **small and medium-sized enterprises'** (SMEs) data protection knowledge through training and personalized consultations. The **Belgian DPA** will publish a brochure and specific tools to facilitate their understanding and compliance with applicable laws. The DPA from the **German State of Bavaria** (BayLDA) will seek to assist SMEs to comply with the GDPR's international data transfer rules and the Schrems II ruling through awareness-raising sessions.

Data breaches. DPAs across the continent will conduct investigations on data breaches that are reported by controllers, or others they otherwise become aware of (e.g., through media reports). DPAs, such as the **Danish DPA**, will also consider the amount and specific characteristics of data breaches in specific sectors when deciding on their own-initiative investigation priorities.

International Data Transfers. After the Schrems II ruling of the Court of Justice of the European Union (CJEU), of July 2020, which annulled the European Commission adequacy decision for the Privacy Shield framework, regarding transfers of personal data from the EU to the US, the topic of international data transfers promises to be high on a number of DPA's enforcement agendas. The **French**, **German** and **Portuguese DPAs** seem to be leading the race, with the latter having prohibited the Portuguese National Statistics Institute to stop the transfer of personal data to the US, which was occurring through the use of Cloudflare's servers to host citizens' data collected in the context of the 2021 Census[5]. The BayLDA announced it will also take action with regard to international data transfers in the context of the supervision of specific service providers, notably in the email, cloud computing and video conferencing spaces.

AI/ML. Just like in 2020, DPAs seem committed to tackling the privacy and data protection risks posed by the uptake of AI and Machine Learning (ML) technologies across society. The **Bulgarian DPA**, for instance, announced it will devote efforts to ensuring facial recognition and profiling techniques comply with legal standards. Additionally, the **EDPS** plans to develop oversight, audit and assessment capabilities for such technologies, while the **Luxembourg** watchdog is still focusing on issuing relevant

[5] *CNPD orders Statistics Portugal to Stop Sending Census Data to US* (IAPP, 28 April 2021).

guidelines for stakeholders. In **Norway**, the DPA is planning to roll-out a regulatory sandbox for granting a green light to AI-driven products and services.

The protection of minors' privacy was identified by several DPAs as a priority, considering the specific vulnerabilities of and the online products used by such audiences. This is also due to the fact that the GDPR provides for specific provisions when under-aged data subjects are involved, notably when it comes to consent. For example, following its 2020 public consultation, the French DPA (CNIL) is expected to dedicate efforts to guiding controllers (e.g., schools) and enforcing the GDPR's rules on minor age verification and exercise of children's data protection rights. The Swedish DPA (IMY) is planning to conduct an investigation on the use of children's data in research contexts.

Cookies and online tracking. Several of the DPAs whose strategies we analyzed mention a focus on cookies and other tracking technologies for their near-term plans. For example, the CNIL is expected to conduct several audits and inspections of websites and apps to verify online tracking practices' alignment with its guidance, since the grace period to comply with it has ended in March 2021. The Portuguese and Belgian DPAs also included references to cookies and tracking technologies in their strategic plans, while the Bavarian DPA plans to analyze how the changes to the German Telecommunications Data Protection Act following the CJEU's *Planet 49* ruling, end up shaping Bavarian operators' consent collection for online tracking.

Self-regulation. Aiming at increasing legal certainty for controllers and processors in specific sectors, several DPAs are looking to approve Codes of Conduct (CoC) under Article 40 GDPR and accreditation criteria for certification bodies. In 2021, both the **Belgian** and **French DPAs** approved their own cloud computing CoC, after positive opinions from the **EDPB** on the draft texts. Moreover, some supervisors, such as **Norway**'s and **France**'s, also wish to advise researchers and start-ups on data protection requirements at the design stage of their projects, through dedicated regulatory sandboxes. Some DPAs (such as the **Spanish DPA**[6]) have approved or are in the process of approving new industry-drafted Codes of Conduct focusing on online advertising and marketing, to ensure the lawfulness, transparency and security of such practices.

[6] *Código de Conducta Tratamiento de Datos en la Actividad Publicitaria*.

Table 1 — Overview of strategic and operational topics per European country

	FR	PT	BE	NO	SE	IE	BG	DK	FI	LV	LT	LU	DE	EDPB	EDPS
Children	✔	✔	✔	✔	✔	✔	✔					✔		✔	
SME	✔		✔			✔				✔		✔	✔		
DPOs (GDPR)	✔			✔		✔					✔	✔			
AI	✔	✔	✔	✔	✔		✔					✔	✔	✔	✔
IoT			✔									✔	✔	✔	✔
Ads, marketing & cookies	✔	✔	✔									✔	✔	✔	✔
T&Cs	✔	✔	✔										✔		
Public Awareness	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔			✔
Big Tech	✔			✔		✔							✔	✔	✔
Telecom	✔		✔										✔		
Employment	✔	✔			✔						✔				
Health & research	✔	✔	✔		✔		✔					✔		✔	✔
Banking	✔	✔			✔							✔			
Data breaches			✔		✔			✔	✔		✔	✔			
CCTV		✔	✔		✔		✔					✔			
Large scale data processing				✔	✔	✔	✔			✔			✔		
Certification and CoC		✔	✔	✔		✔					✔	✔		✔	
PETs			✔	✔										✔	✔
Regulatory sandboxes	✔			✔								✔			
International data transfers	✔		✔			✔			✔			✔	✔	✔	✔

4. Conclusion

The regulatory activity of DPAs is becoming increasingly complex and nuanced, three years after the GDPR empowered them with unprecedented enforcement powers and competences. After gaining insight into their plans for the immediate future, we could identify:

- responsiveness with regard to the protection of data related to **health** and other sensitive personal data processed in the context of the **COVID-19 pandemic**, as some DPAs announced they plan on following up on the specific guidance issued last year with enforcement actions;
- preoccupation with the protection of **children** with regard to processing of their personal data – most DPAs plan to issue guidance or to act in this area;
- prioritization of **international data transfers** enforcement, as a follow-up to the Schrems II judgment, with 8 out of 15 DPAs mentioning it in their strategic plans and related documents (see Table 1 above and the Annex);
- concern for the impact of **emerging technologies** on society and individual rights – with many initiatives to provide **guidance on AI/ML** and **Facial Recognition**;
- focus on **raising awareness** for the public about data protection rights – an astounding 12 out of the 15 DPAs whose published strategies we have analyzed for this overview indicate that they plan public awareness campaigns or related activities (see Table 1 above and the Annex);
- efforts to make GDPR compliance work in practice on a large scale, by applying a risk-based approach in their regulatory activity, as well as by targeting the empowerment of **DPOs** and by adopting tailored guidance for **SMEs;**
- a trend to modernize their regulatory approach, by proposing **sandboxes** and pushing for more self-regulation, like the adoption of Codes of Conduct.

In addition, when looking at their strategies, it is important to keep in mind that DPAs in Europe have quasi-rulemaking powers, through their ability to issue guidance on complex topics, and setting interpretation and informal enforcement precedents when imposing sanctions. Moreover, their approach often influences newer data protection regulators in jurisdictions outside of Europe, considering that they already have a history of guidance and enforcement activity related to some of the key concepts of emerging data protection laws around the world. The EDPB will continue to work for a consistent application of privacy and data protection instruments across the EU, by issue guidance

on key concepts (e.g., **data subjects' rights, legitimate interests, scientific research, children's data**) and on data protection compliance aspects of new technologies (e.g., **blockchain**, **PETs, AI/ML, Digital Identity, IoT and payment methods**).

ANNEX

Overview of strategic and operational plans per country

A.1 France

- ***Materials:***
  - 2020 Annual Report, outlining the CNIL's regulatory priorities for 2021
- ***Summary:***
  - **Specified 2021 Priorities:** the CNIL's 2020 Annual Report identifies some areas to which the regulator will devote its focus in 2021:
    - ***(1) Processing of children's data in online environments:*** the CNIL launched a public consultation on the matter in late 2020. Its results are available here. The authority is expected to dedicate efforts to guiding controllers (e.g., schools) and enforcing the GDPR's rules on minor age verification and exercise of children's data protection rights.
    - ***(2) COVID-19-related data processing:*** health authorities and providers may watch out for CNIL audits and inspections, aiming at verifying whether the processing of health data for the management of the COVID-19 pandemic complies with data protection rules. Also in the pandemic context, the authority will tackle the dissemination of surveillance technologies in several domains, including for public safety, employee monitoring and online proctoring.
    - ***(3) Cooke guidelines enforcement:*** the grace period granted by the CNIL to providers to comply with its cookie and other tracking technologies final guidance has ended in March 2021. Thus, the authority is expected to conduct several audits and inspections of websites and apps to verify online tracking practices' alignment with its guidance. Very recently, the CNIL has imposed heavy fines against companies that it found to be placing non-essential cookies

in their website visitors' devices without proper valid consent (e.g., Google, Amazon, and Carrefour fines). Since then, further 20 companies have received formal notices because they did not provide users with a button to refuse all cookies which was as clear as the button that allowed them to accept all.

- ***(4) Schrems II enforcement:*** the CNIL promises to be one of the most active and stringent DPAs in the aftermath of the July 2020 CJEU Schrems II ruling. As an illustration, in May 27, 2021, the CNIL **issued a public call addressed to higher education and research institutions in France to "bring changes" in their use of US EdTech services**, reminding that the **EDPB has not identified "additional measures that could ensure an adequate level of protection** when a transfer is made to a cloud IT service provider or other subcontractors who, as part of their services, need to access unencrypted data or have encryption keys, and who are subject to US legislation".

A.2 Portugal

- ***Materials:***
  - 2021 Activities Plan
- ***Priorities and focus areas:***
  - ***(1) Deepening of thematic areas,*** notably:
    - Conditions and procedures for the approval of codes of conduct under Article 40 GDPR;
    - Measures and procedures for ensuring Privacy by Design & by Default;
    - Analyzing the impact of AI/ML technologies on data protection.
  - ***(2) Monitoring specific issues***, including:
    - ePrivacy Regulation negotiations;
    - 2021 Portuguese Census
    - Remote working data processing
  - ***(3) Issuing guidelines,*** notably on:
    - Children's data processing;
    - Cookies & other tracking technologies;
    - Transparency and privacy notices.
  - ***(4) Audits and inspections***, with a particular focus on:
    - Video surveillance in publicly accessible areas;
    - Call centres;
    - Ride hailing services.
  - ***(5) Institutional cooperation*** with several entities:

        - The Justice Ombudsperson;
        - Cybersecurity National Centre;
        - Higher education institutions;
        - Safe Internet Centre;
        - DPAs of Portuguese-speaking countries (Cabo Verde, São Tomé e Príncipe and Macau).
    - *(6) Awareness-raising*, notably by:
        - Promoting conferences and webinars;
        - Issuing a periodic newsletter;
        - Publishing its Data Protection Forum journal;
        - Participating in sessions hosted by other bodies, schools and universities.
    - *(7) International activities*, including within the EDPB, the International Working Group on Data Protection in Telecommunications (Berlin Group), the Iberia-America Data Protection Network, the International Conference of Data Protection and Privacy Commissioners and the Global Privacy Assembly.
    - *(8) Improving the internal functioning of the DPA*, notably by:
        - Spreading the DPA's workforce and services in other regions of the country (North, Azores and Madeira archipelagos);
        - Recruiting specialized workers;
        - Approving and publishing an inspection methodology/checklist;
        - Making available electronic means for notifying DPIA prior consultation requests and codes of conduct.
- ***COVID-19 Materials:*** the Portuguese DPA has published several guidance papers on the processing of personal data in the context of the COVID-19 pandemic, including the processing of health data for research, remote monitoring of employees and online proctoring.

A.3 Belgium

Materials: 2021 Management Plan (*Plan de Gestion*), aimed at defining concrete strategic and operational objectives to set the goals of the 2019-2025 Strategic Plan goals in motion, throughout 2021.

The evaluation criteria used by the Belgian DPA to assess the execution of the Management Plan include: (i) the timely and quality handling of files; (ii) data protection awareness-raising and education; (iii) the DPA's visibility; (iv) cooperation with partners; (v) the DPA's effectiveness.

The Management Plan is centered around the six Strategic Objectives outlined in the 2019-2025 Strategic Plan, setting out specific action points for the DPA, during 2021, on each of such objectives:

- *(1) Better data protection through awareness*, by*:*
  - Optimizing and integrating prior consultation opinions in data protection impact assessments (DPIAs) (e.g. guidance on the concept of "high risk", publication of socially relevant prior consultation opinions);
  - Implementing and apply codes of conduct approval criteria and expertise (at national and European level);
  - Compiling and publishing the DPA's decisions (including opinions and recommendations, codes of conduct and certification and administrative sanctions);
  - Developing clear and precise publications, notably answers to data subjects' and controllers' FAQs;
  - Submitting opinions on draft legislative texts and data protection-related matters upon lawmakers' requests and replying to the latter's questions on such opinions;
  - Publishing a data protection "legislator's checklist" for the benefit of Belgian lawmakers
- *(2) Better data protection through law enforcement*, by:
  - Supporting international data transfers, with a particular focus on recent case law (Schrems II) and Brexit;
  - Simplification and improvement of notification procedures (e.g. DPOs and data breaches), taking into account DPOs' views;
  - Devoting particular attention to data processing activities mentioned in the Strategic Plan, including direct marketing, data brokerage, e-ID, cookies and video surveillance;
  - Examining the appointment, accessibility, competences and tasks of Belgian organisations' DPOs, as well as the activities they pursue;
  - Improving information collection from complainants, notably by proposing a clear complaint form, allowing the qualitative identification of the complaint;
  - Handling cases effectively, within 3 months (save for complex cases);
  - Creating a web page outlining the reasoning and the procedure behind the DPA's decisions;
  - Developing a methodology for choosing the appropriate corrective measures, including the amounts of fines;
  - Effective monitoring of imposed sanctions.
- *(3) Better data protection by identifying and adjusting to the changes*, by:
  - Optimizing the General Secretariat's monitoring procedures;

- Regularly reporting to and exchanging information with the DPA's other departments and with its Board;
- Actively and passively participating in conferences on key matters, notably around data subjects' rights;

- *(4) Better data protection through national and international cooperation*, by:
  - Cooperating with other regional and sectoral regulators (e.g. Consumer protection, telecommunications, competition, energy and financial regulators);
  - Partnering with experts and training centres (e.g. researchers with expertise in novel technologies);
  - Collaborating with the Belgian Federal Public Service and the State Secretary for Privacy, notably in replying to Parliament's questions on privacy and data protection;
  - Boosting international cooperation:
    - Multilaterally, within the EDPB, including by (i) issuing guidelines and opinions on legitimate interests and anonymization, data monetization, dark patterns, IoT; and (ii) improving cooperation in cross-border cases (e.g. participating in EDPB cooperation subgroups); and
    - Bilaterally, with European and other DPAs, in particular with neighbouring countries' DPAs.
- *(5) Better data protection with the Belgian DPA as leader/guide and reference center*, by:
  - Publishing a new information brochure for small and medium enterprises and non-profits, as well as providing support and developing tools with a view to ensuring a generalized understanding of and compliance with the existing laws (e.g. the BOOST project);
  - Publishing specific information for DPOs, organizing and supporting DPO networking meetings (Lunch & Learn);
  - Increasing citizens' protection and legal certainty for controllers, through individual consultations and the approval of codes of conduct;
  - Publishing a GDPR toolbox, including templates of simplified records of processing activities, DPO opinions and exchanges of personal data with public authorities;
  - Issuing recommendations on certain usages of biometric data and updating the DPA's guidance on the use of employee electronic monitoring tools.
- *(6) Enhancing data protection by being an efficient regulator (internally)*, by:
  - Optimizing the usage of IT tools;
  - Increasing the DPA's visibility through modern and effective communication;
  - Boosting the quality of reports;

- Ensuring internal GDPR compliance (e.g. records of processing activities, management of data subjects' requests, DPO opinions, awareness-raising);
- Publishing information about the numbers and contents of requests received from data subjects.

Lastly, the Belgian DPA asked for a structural increase of its budget, with the aim of keeping its current staff and hiring 14 more officials over the next 5 years.

A.4 Norway

- ***Materials:***
  - Overall DPA Strategy for 2021-2023
- ***Summary:***
  - **Mission & Priorities:** The Norwegian DPA has statutory core tasks that involve case processing, supervision and communication activities, It therefore prepared six strategic objectives that will govern its work over the next three years.
    - *(1) A fairer balance of power between individuals and commercial actors/public sector*. The latter often hold vast amounts of data about the former, who struggle to exercise control over it. Therefore the DPA proposes to:
      - Actively enforce data protection laws to promote compliance by data-driven organisations;
      - Collaborate with other DPAs and regulators, as well as other organisations, to strengthen data protection rights;
      - Influence the political and legislative processes that determine how data is processed;
      - Work for a fairer balance between large foreign technology companies and Norwegian actors;
      - Bolster awareness-raising activities for the benefit of individuals.
    - *(2) Promoting privacy-friendly digitisation, innovation and development*. The use of big data has potential to improve society, but also entails risks to fundamental rights. Therefore, the DPA will:
      - Operate and further develop a regulatory sandbox for AI;
      - Hold data-intensive actors accountable for their use of data;
      - Work to ensure that relevant authorities set aside more funding for research on Privacy Enhancing Technologies (PETs);
      - Promote the use of built-in privacy and sanction associated breaches;

        - Work actively to ensure that universities and university colleges incorporate privacy in all relevant education programmes.
    - ***(3) Ensuring that undertakings have the necessary expertise and that they understand the importance and comply with privacy regulations.*** In that view, the DPA will work to:
        - Actively engage with partners and key actors in different sectors to ensure they are equipped for compliance;
        - Encourage the development and use of self-regulation mechanisms, such as national guidelines, industry norms, standardisation and certification solutions;
        - Increase organisations' competences in DPIAs;
        - Provide guidance and develop tools that help enterprises comply with the regulations;
        - Ensure that businesses appoint DPOs in mandatory cases, and that the latter have adequate competences and understand their role.
    - ***(4) Ensuring that individuals can safeguard their own privacy.*** It is important to ensure that individuals are aware of their rights and know how to exercise them. Thus, the DPA will:
        - Develop guidance materials, self-help tools and templates to help individuals safeguard their rights;
        - Influence businesses and industries to develop good solutions that help individuals safeguard their rights;
        - Work to strengthen training on privacy and digital competences in schools, as well as connect with external youth councils or privacy ambassadors in target groups.
    - ***(5) Influencing, leading and exchanging knowledge in selected privacy-enhancing international processes***, within the Nordics, Europe and also globally, sharing the DPA's guidance, reports and decisions, but also to learn from other regulators.
    - ***(6) A competent, flexible and forward-looking DPA.*** This will include:
        - Being at the forefront of societal and technological trends that affect privacy;
        - Cooperating with relevant research communities, influencing them to focus on important developments that affect privacy.

A.5 Sweden

- ***Materials:***

- Strategic Supervision Plan 2021-2022
- ***Summary:***
  - **Mission & Priorities:** The DPA's overall mission until 2022 is to carry out efficient and legally sound supervision that leads to the protection of individuals in concrete cases, but also to the protection of privacy in society at large.
    - ***Supervision will generally be based on complaints:*** the Swedish DPA will deal with and, where appropriate, examine the substantive issue of the complaints it receives from individuals. The EDPB has approved an internal guiding document to harmonize the handling of complaints by EEA DPAs ("Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements", 2 February 2021). In line with said document, the DPA will only initiate investigations where answering complaints in writing is not enough. In any case, the investigations should be limited to the facts described in the respective complaint.
    - ***Risk-based supervision:*** the Swedish DPA may initiate own-initiative investigations, based on data breach notifications, information obtained from media reports and other sources. It may also decide to extend complaint-based investigations to other matters. It shall only pursue one of those avenues after concluding there is a **risk of serious infringement** of data protection law. For that conclusion to be drawn, at least two of the following criteria need to be met (unless one of them is poignantly identified):
      - **(1) serious risk to or breach of individuals' right to privacy**, considering the nature of the personal data at stake, the vulnerabilities of data subjects, the purpose, means and the context of the processing (eg. illegal sharing of personal data with many stakeholders);
      - **(2)** the processing affects or is likely to have consequences for many data subjects, considering whether there are systematic shortcomings and the need for speedy regulatory action;
      - **(3)** there is a use of a **new technology** that can significantly affect individuals' right to privacy, notably in case where it can increase the risk of illegal data processing;
      - **(4)** there is a **significant need for guiding controllers' practices**, notably in cases involving new practices or phenomena that need to be addressed by the DPA before they become established;

- **(5)** there is a **serious violation of good practice in debt collection or credit reporting activities**, notably where a debtor suffers unnecessary damage or is subjected to undue pressure.

In any case, the Swedish DPA shall notify the organisation's management before the initiation of the inspection. .

- ***Annual planned inspections:*** in addition to the aforesaid supervision activities, the Swedish DPA is required to conduct supervision over certain activities or systems. Also here, the DPA will have a risk-based approach when deciding on the inspections to conduct. The DPA's planned inspections include:
  - An examination of **public authorities' use of consent** as a legal basis for processing personal data and of their DPIA-related duties;
  - An examination of **children's data processing in research contexts**;
  - A review of **video surveillance** practices at the workplace and in publicly accessible spaces;
  - **Debt collection operations.**

A.6 Ireland

- ***Materials:***
  - Draft 2021-2026 Regulatory Strategy & corresponding blog post
    - The Irish Data Protection Commission (DPC) published a draft version of its Regulatory Strategy for 2021-2026, which is open for public consultation until June 30, 2021. The draft document itself was adopted following two rounds of open public consultation. Taking account of academic theories that are emerging in respect of effective regulation and behavioral economics, the DPC also considered the needs of its diverse stakeholders and the evolving nature of the fast-paced and non-traditional sectors it regulates.
- ***Summary:***
  - **Mission:** Upholding the consistent application of data protection law through engagement, supervision and enforcement.
  - **Vision:** being an independent, internationally influential and publicly dependable regulator; applying a risk-based regulatory approach to its work, so that its resources are always prioritised on the basis of delivering the greatest benefit to the maximum number of people.

- **Values:** fairness, expertise, consistency, transparency, accountability, engagement, independence and forward-looking.
- **Strategic goals and associated planned action:**
  - *(1) Regulating consistently and effectively*:
    - (a) Clarifying the limits of legislation and setting expectations for stakeholders, including how and when corrective measures are imposed.
    - (b) Improving guidance to individuals, including vulnerable groups.
    - (c) Standardizing and publishing the procedures for complaint handling and inquiries.
    - (d) More frequent publication of case studies illustrating how data protection law is applied, how non-compliance is identified and how corrective measures are imposed.
    - (e) Seeking clarification and consistency on procedures under the One-Stop-Shop mechanism and international cooperation.
    - (f) Working with the EDPB to develop legal certainty for international transfers of personal data.
  - *(2) Safeguarding individuals and promoting data protection awareness.* This should help individuals to exercise their rights and to escalate their issues to the DPC when necessary. There is also a need to rebalance the way the DPC handles individual complaints against assisting individuals to make more informed data protection choices. The DPC will prioritise cases that are likely to have the greatest systemic impact for the widest number of people over the longer-term. To achieve these outcomes, the DPC proposes: .
    - Taking account of how data protection impacts vulnerable groups and engaging with advocacy groups to communicate this appropriately;
    - Identifying trends and themes within individual complaints so that we can achieve strong collective outcomes;
    - Regularly communicating with organizations on investigation procedures and final outcomes;
    - Engaging fairly with organizations to promote openness, trust and compliance culture;
    - Working with peer DPAs to introduce consolidated and consistent enforcement across Europe.
  - *(3) Prioritizing the protection of children and other vulnerable groups (e.g. elderly, non-native speakers and the homeless).* This includes publishing specific and accessible guidance, notably

on data sharing with third parties and consent. Other proposed initiatives include:

- Actively promoting the development of codes of conduct on the processing of children's personal data;
- Conducting detailed research on how data protection law applies to children, both internally and through research partnerships, for example on the use of age verification mechanisms and methods for obtaining parental consent for online services;
- Clarifying the bases for data sharing, so that individuals are not disadvantaged or at risk as a consequence of over caution on the part of data controllers.

- *(4) Bringing clarity to stakeholders* on how the DPC uses its resources to follow-up on complaints and conduct investigations. On this basis the DPC may, in the future, adopt a collective approach to investigating systemic issues, rather than run multiple investigations into individual complaints about the same matter. The DPC will also look to further guide controllers on how to operationalise their GDPR obligations, in parallel to increasing the use of its corrective powers. In this regard, the DPC proposes:
  - Applying corrective powers proportionately – including fines, where appropriate – to produce changed behaviours and an improved culture of data protection compliance;
  - Working with the EDPB to develop consistent procedures for the IMI system (for cross-border cases) and improving the metrics it generates.
- *(5) Supporting organizations and driving compliance .* The DPC observes that there is a "tendency to conflate fining with regulatory success and to use the imposition of fines as a means to measure effectiveness". However, the DPC believes that hard enforcement is not the limit of the regulatory role. The DPC favors changing cultural approaches to data protection by extensive engagement. This is also true in cross-border cases, where it commits to improving its work with peer DPAs in Article 60 GDPR cooperation cases. The DPC will prioritize prosecution, sanction and/or fining those infractions that result from willful, negligent or criminal intent. It It will also:
  - Produce indicative guidance on scope-setting for large-scale and multinational inquiries;
  - Communicate proactively with other EDPB supervisory authorities on emerging issues;

- Prioritize the development of guidance for micro, small and medium sized enterprises;
- Work with DPOs to increase the knowledge and impact of their role;
- Regularly review and communicate our supervision and enforcement priorities.

A.7 Bulgaria

- ***Materials:***
  - 2020 Annual Report. The last part (Chapter XII) of the Report outlines the objectives and priorities of the Bulgarian DPA for 2021.
- Priorities and objectives:
  - ***(1) Continuation of the analysis of modern threats and challenges to the protection of personal data,*** including artificial intelligence, facial recognition, the protection of children's personal data on the Internet, large databases and profiling. Based on the analysis, the DPA will determine its focus areas of preventive outreach and control;
  - ***(2) Upcoming EU legislation,*** including the ePrivacy Regulation, the Data Governance Act and the Digital Markets Act. The DPA notes that some of its representatives are actively involved in the development and negotiation of these documents. These new forms of regulation will require the creation of new focus groups and new regulatory approaches within the DPA;
  - ***(3) Intensified controls on the processing of personal data in certain sectors***, including insurance, energy, courier, education, healthcare, online sites and gambling.
  - ***(4) New focus on awareness-raising activities***, notably within schools and the use of social media tools, in partnership with the Ministry of Education. The DPA plans to roll-out e-learning tools, targeted at specific sectors and groups (e.g. security companies on video surveillance activities).

A.8 Denmark

- ***Materials:***
  - Data and risk-based 2020-2023 action strategy.
  - Press release. "*Responsible use of citizens' data in a digitised society*". The Danish DPA's mission entails its openness, independence, visibility, focus

on guidance and targeted supervision. Its values: high professionalism, integrity, proactivity and keeping up-to-date with trends in society, technological developments and the needs of stakeholders.

- Priorities and objectives: the Danish DPA's strategy rests on 4 pillars, each of them with two main efforts, which are materialized in concrete planned action, as outlined below:
    - *(1) How do we ensure a high quality of the DPA's data?* This includes records of received complaints, data breach notifications, the analysis of which would allow to identify priorities in enforcement areas (e.g. specific sectors or processing activities).
        - Evaluation of data quality and registration of metadata
            - Ensuring the DPA's data is accurate, complete, relevant, objective, credible and usable, through a systematic overview of the DPA's data sources and information (in Q2 2021)
            - Identifying companies that often breach data protection rules, as well as others who may need specific guidance
        - Systematized data collection
            - Changing the standard complaints form, to fully digitise the complaints-handling procedure
            - Making collection of information in appeal cases (e.g. in hearings) more uniform
            - Standardized inspections in selected areas (e.g. IT security)
    - *(2) How does the DPA ensure access to relevant data sources?* This has the goal of ensuring guidance and controls where data protection risks are greatest.
        - Experiment with new supervision concept (new internal data sources) leading to uniform and scalable inspections of various data controllers and to the gathering knowledge for the DPA's efforts
            - Phase 1: auditing a large number of data controllers, in a standardized and largely automated fashion, with a high degree of controller self-assessment;
            - Phase 2: selection of data controllers and collection of further information and documentation. Random checks of the submitted inputs should then be performed
            - Phase 3: selection of data controllers for in-depth inspections and visits.

              The ultimate goal is to compile all controllers' answers in a database to analyze non-compliance trends across controllers and industries (e.g. impact of the organisations'

size, number of employees, location, etc.). The DPA aims to carry out preliminary Phase 3 inspections by the end of 2021.

- Access to external data sources (e.g. from legal persons' registries and other regulators). The possibility of collecting information from two other authorities should be assessed by the DPA until Q4 2021.

- *(3) How does the DPA become good at using data, both for large and small activities?*
  - **Clear criteria for selecting control areas in own-initiative investigations** (e.g. pursuant to data breach notifications or media reports). Typically, in cases where it becomes aware of potential wrongdoing, **the DPA will consider**:
    - The purpose of the processing, notably if it is a profit-seeking one;
    - The sensitivity and the amount of personal data;
    - The potential negative consequences for data subjects;
    - Whether the breach is ongoing or completed, and whether it is wilful or negligent;
    - Whether the organisations is a recurring offender;
    - Whether an investigation could lead to a better understanding of data protection requirements for other operators.

    By the end of 2021, the DPA also intends to create controller risk-profiles to decide when to conduct investigations where no signs of wrongdoing have been collected. Such profiles will include:

    - The general profile of the controller (activities and size, categories of processed personal data, number of affected data subjects, etc.)
    - Company-related events (e.g. number of reported breaches and previous audits by the DPA)
    - The specific industry's conditions and events (e.g. reported breaches, number of complaints handled)
  - Multiple database-informed decisions, to avoid discretionary risk assessments by the DPA, **by the end of Q2 2021**:
    - Systematised and automated data collection and analysis
    - Experimenting with database and risk-based selection of supervisory targets
    - Publication of automated statistics of personal data breaches

        - Preparation of guidance and news based on statistical information.
    - ***(4) How does the DPA document and evaluate its control and guidance efforts?*** This should increase transparency and enable the establishment of a link between the DPA's decision-making processes and controllers' knowledge and understanding of data protection and the DPA's focus areas
        - Documented processes, decisions (e.g. risk assessments) and results, as an ongoing effort
        - Experiment with effect measurement (to controllers and to society as a whole - e.g. better information security in DK?), for the benefit of the DPA's targeted action. **By the end of Q3 2021, the DPA wants to have identified targets for the effects of its supervisory efforts. It will also annually reevaluate such metrics to ensure its action benefits citizens.**

A.9 Finland

- ***Materials:***
    - Finish DPA's planned action. The DPA's priorities for action in 2021 include:
        - Informing data subjects;
        - Data protection impact assessments;
        - Data transfers to third countries;
        - Accountability principle, in particular in the application of the Criminal Data Protection Act and in cases of data breaches;
        - Improving data security in Finland.

A.10 Latvia

- ***Materials:***
    - Operational strategy for 2021-2025. It outlines the lines of action, corresponding objectives and the results that the Latvian DPA intends to achieve over the next 4 years.
- **Values:** (i) professionalism and results-oriented action; (ii) development, openness to new ideas and technologies; (iii) cooperation, amongst its members and with other institutions; (iv) fairness, duly assessing data protection aspects together with other fundamental rights; (v) transparency.
- **Lines of action:**
    - ***(1) Raising awareness*** through: (i) coverage in the media, promoting and participating in events and webinars; (ii) improving the DPA's website and

social media accounts; (iii) publishing guidelines, recommendations and explanations on the topics raised in requests addressed to the DPA; (iv) establishing sector-specific exchanges with companies, NGOs and State institutions; (v) organizing qualification exams for data protection specialists and verifying the latter's qualifications and service provision.

- *(2) Effective controls*: ensuring fines are transparent and fair (effective, proportionate and dissuasive). The DPA intends to focus on the purposefulness, quality and achievements of inspections, instead of their quantity. Similarly to the Irish DPA, the Latvian DPA is committed to focusing inspections of cases involving a larger number of individuals, rather than individual complaints. The DPA formulated its main principles with regards to controls:
  - Supporting controllers as a rule, rather than sanctioning them, either through consultations or explanations, aiming at the prevention of data protection breaches.
  - Fair and proportionate use of corrective powers.
  - Identification of priority control areas, based on the DPA's risk analysis. This will require the DPA to look into its databases, analysing its sanctions history and sectoral specificities, as well as analysing court rulings following DPA decisions (which generally uphold the latter - 89.65% in 2020 alone).

  It also listed a number of tasks for the implementation of this second line of action:

  - Improving its monitoring activities, with a focus on the prevention of breaches.
  - Actively cooperating with other EEA DPAs in conducting joint investigations and providing mutual assistance.
  - Ensuring a uniform approach to monitoring activities and developing an effective sanctioning scheme.
  - In the event of non-compliance, choosing a solution that allows the controller to voluntarily remedy the breach.
- *(3) An efficient and developed DPA*, considered as an opinion leader who publishes useful resources and works for the benefit of society. This also involves attracting a motivated and cohesive workforce for the DPA.

- **Priorities:** cutting red tape and shifting away from sanctions, towards: (i) awareness-raising on lawful data processing; (ii) strengthening cooperation with the public and private sectors, by providing more advisory support; (iii) opinion leadership, by promoting controllers' understanding of data protection as a

fundamental right; (iv) trust-building, by responding in a timely and adequate manner to new technological developments and challenges.

A.11 Lithuania

- ***Materials:***
  - Strategic Activity Plan 2021-2023. It outlines the DPA's operational priorities for the next three years and the tasks it intends to carry out to address them. The general goal of the DPA is to further spread a culture of data protection in society, in particular by enhancing stakeholders' knowledge, competences and skills.
- Priorities:
  - ***(1) Increasing the knowledge and tools of controllers, DPOs and data subjects***, notably by:
    - Checking whether controllers' processing purposes comply with general data protection principles;
    - Enhancing the DPOs' skills and ensuring they are involved in decisions involving the processing of personal data;
    - Making data subjects aware of their rights and encouraging cooperation and mutual respect with controllers (e.g. a guide on data protection in the employment context);
    - Publishing more information on the DPA's decisions following own-initiative and complaint-driven investigations;
    - Coordination and adoption of codes of conduct, accreditation of certification bodies and approval of certification criteria;
    - Evaluating and approving BCRs.
  - ***(2) Building trust in public sector data processing***, notably by:
    - Increasing monitoring activities;
    - Delivering opinions on draft laws;
    - Checking public authorities' (e.g. courts, ministries, municipalities) data processing tools and recommending security best practices.
  - ***(3) Strengthen international cooperation***, notably by:
    - Initiating joint action on personal data breach notifications;
    - Handling and harmonising practices on cross-border complaints, investigations and prior consultations via the IMI system;
    - Actively contributing to the activities of the EDPB.

A.12 Luxembourg

- ***Materials:***
  - 2021 Annual Work Program.

    - 2020-2022 Strategy and Work Program. It acknowledges the societal challenges of the digital age (e.g. Big Data, public services digitisation, growth of the Luxembourgish tech sector) and the specific challenges that the DPA faces in its daily work (e.g. new competences around certification, lack of resources, stakeholders' needs for compliance tools).
- **Strategic goals and objectives:** the Strategy outlines 5 strategic and operational objectives, namely:
    - ***(1) To promote the rights to data protection and privacy***, making data subjects aware of the existence of and the ways in which they can exercise their rights.
    - ***(2) To facilitate stakeholders' access to the DPA***, offering a personalised service and various self-service tools.
    - ***(3) To develop and make available compliance tools***
    - ***(4) Regulation fit for a digital world***, bolstering balanced enforcement action
    - ***(5) To contribute to an European data protection culture***, working within the EDPB for better guidance and decisions, and participating in the workings of the Global Privacy Assembly (GPA).
- **Focus on specific sectors and subject-matters**, notably:
    - ***SMEs***, acknowledging their compliance struggles due to lack of expertise and resources.
    - ***Health and research***, particularly in the context of the COVID-19 pandemic and international data transfers.
    - ***National security.***
    - ***Training***, for its own staff and for organisations.
    - ***DPOs***, by publishing the results and conclusions of the DPA's audits on organisations that have appointed DPOs.
    - ***Geolocation***, by publishing guidance on the processing of location data, complaints management and specific investigations.
    - ***Video Surveillance***, notably by sanctioning breaches and assisting lawmakers in approving suitable legal basis for conducting such activities where they are needed.
    - ***Data breaches***, by informing the technical and organisational analysis component of data breaches assessments, through guidance that will also empower organisations to prevent and better manage and control breaches.
    - ***Certification***, by initiating the accreditation of certification bodies.
- **Priority action points**:
    - ***Awareness-raising and communication***, by:
        - **Targeted communications and campaigns** for organisations, to guide them in their data protection compliance efforts;

- **Training sessions**, both sectoral and thematic, remote and in-person, with several industry bodies and associations (e.g. Confédération Luxembourgeoise du Commerce, Chambre des Salariés Luxembourg, Association des professionnels des courtiers en assurances au Luxembourg, Association Luxembourgeoise pour la Formation Médicale Continue);
- Development of an **e-learning platform** for the National Institute of the Public Administration (INAP);
- Awareness-raising campaigns, through infographics and brochures (for the general public, professionals and vulnerable segments), public sessions for start-ups on specific topics (e.g. Privacy by Design, DPIAs);
- Sectoral workshops on several topics, including DPIAs for public research, **children's data**, interaction of the GDPR with PSD2 and MIFID, data sharing security in the financial and insurance sectors;
- Contributing to the Data Protection Working Group on Digital Education (DEWG) of the GPA;
- R&D collaborations, notably through the participation on Project Smart Schoul 2025's steering committee (aiming to develop a platform for the validation of artificial vision technologies) and the launch of a **regulatory sandbox** for researchers and start-ups to test their products and services.

- *Guidance, information and opinions*, by:
  - Managing requests for information received from individuals and data protection professionals, within a reasonable timeline (preferably, within a week from receipt;
  - Issuing opinions on proposed laws and regulations;
  - Observing, documenting and analyzing technological, societal, economic and legal evolutions with a data protection impact, developing an internal knowledge base. Topics include **video surveillance 2.0, neuromarketing, connected vehicles, IoT, AI, blockchain, contactless payments and digital health**;
  - Drafting thematic guidelines, on **vehicle geolocation, human resource management, video surveillance, international data transfers and Brexit**;
- *Compliance-oriented actions*, including approving criteria for codes of conduct and opinions on DPIA prior consultations.
- *Complaints-handling*, both the ones received directly from data subjects and other directed by other DPAs, through:
  - Introducing automated acknowledgments of receipt;

        - Optimizing the IMI system for exchanges of information between EEA DPAs.
    - ***Investigatory and corrective actions***, including:
        - Large investigations of cross-border digital economy players, in cooperation with other DPAs;
        - Publishing a **practical investigations guide**, which makes the investigation process transparent for organisations;
        - Launching audit campaigns on specific matters against several organisations. The 2 matters identified for 2021 are **records of processing activities (Article 30 GDPR) and international data transfers**;
        - Improving the management of data breach notifications, by automatically classifying them from the information provided in the DPA's standard form. This will allow the DPA to prioritise the investigation of the most serious cases.

A.13 Germany (Bavaria)

- ***Materials:***
    - 2020 Annual Report and press release. The DPA's President's foreword and several passages throughout the report provide hints on the DPA's focus areas for the current year.
- **Focus areas and planned action:**
    - ***(1) Email, cloud computing and video conferencing service providers*** and their compliance with the GDPR's principles of lawfulness, transparency and minimisation.
    - ***(2) Raising SMEs' awareness on international data transfers compliance***, notably through public workshops and events.
    - ***(3) Approving Binding Corporate Rules (BCR)*** for international data transfers submitted by several companies, while adequately addressing the issue of government access to data in the recipients' jurisdiction.
    - ***(4) Data processing by Tesla vehicles***, in particular through sensors and cameras for driver assistance and lane departure/keeping, but also for product development purposes. The BayLDA is concerned about the use of dash cams, which may record persons in the vicinity of the vehicle, and how transparency requirements are considered by the company and the driver. The DPA also notes that the Dutch DPA is the lead DPA for Tesla's EU branch, responsible for verifying the company's compliance with data protection law. However, the BayLDA plans to test a Tesla vehicle and produce a report in 2021.

- ***(5) Analyzing how the changes to the German Telecommunications Data Protection Act (TTDSG)*** on cookies and other tracking technologies, following the CJEU's Planet49 ruling, ***end up shaping Bavarian operators' consent collection for online tracking.***

A.14 EDPS

- ***Materials:***
  - The EDPS Strategy 2020-2024 "Shaping a Safer Digital Future".
  - Press release. Key triggers: data protection as fundamental rights under the EU Charter; technological data-driven advances (e.g. IoT); domination of global information flows by a small number of players; COVID-19 crisis; widespread surveillance; business models relying on tracking, profiling and behavioral targeting; roll-out of AI and automated decision-making systems in various sectors; international data transfers post-Schrems II.
- **Strategy pillars and objectives:** the EDPS 4-year Strategy rests on 3 pillars, reflecting EU values around privacy and data protection, which the EDPS intends to implement through several initiatives, as outlined below:
  - ***(1) Foresight***. As a recognized and respected centre of expertise, the EDPS wishes to take a long-term view of trends in data protection and the legal, societal and technological contexts.
    - Being smart, gathering and sharing knowledge and expertise notably by:
      - Organizing evidence-based discussions on **intrusive, emerging or hypothetical practices**, such as eHealth, biometric technologies and automatic recognition systems, quantum computing, edge computing and blockchain;
      - Facilitating discussions between data protection experts, regulators and the research community, including ethics boards, to ensure that data protection enhances the efforts of **genuine scientific research**;
      - Encouraging and facilitating more exchanges between our staff and DPAs and between DPAs themselves;
      - Exchanging information and best practices with international organizations and interlocutors in third countries.
    - Accounting for trends, acknowledging potential risks and opportunities of new technologies and ensuring data protection by design & default in the innovation process, notably by:

        - Focusing on where tensions between data protection and other areas of law (such as competition, consumer and payments instruments) arise;
        - Promoting understanding of the "state-of-the-art" of specific technologies (e.g. anonymisation);
        - Advising EU lawmakers on the data protection impacts of new proposals;
        - Monitor the deployment of novel technologies by EU Institutions and the risks they pose to individuals and groups;
        - Talking to innovators in the private sector (e.g. Internet Privacy Engineering Network, or "IPEN").
- *(2) Action*, proactively developing tools for the EU Institutions to be leaders in data protection. The EDPS also aims to promote coherence in the DPAs' enforcement activities.
    - Acknowledging that EU Institutions need to outsource tasks to communications services and digital tools, but ensuring that this does not lower the level of data protection, which includes advising on possible standard contractual clauses and DPIAs, and minimising reliance on monopoly providers of communications and software services, to avoid detrimental lock-in;
    - Developing oversight, audit and assessment capabilities for technologies and tools, which are increasingly "endemic" to our digital ecosystem (e.g., profiling, machine learning, AI);
    - Support the idea of a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals;
    - Using enforcement powers to ensure EUI websites and mobile apps are complying with EU law, particularly in respect of third party tracking.

The EDPS also aims to promote coherence in the DPAs' enforcement activities.

- Ensuring the consistent application and enforcement of the GDPR, via its role as member and secretariat of the EDPB;
- Calling for the adoption of the ePrivacy Regulation with meaningful protections, not to the detriment of existing ones;
- Developing European and international cooperation measures, and promoting joint enforcement actions and active mutual assistance, by concluding Memoranda of Understanding with DPAs

- *(3) Solidarity*, promoting justice and safeguarding privacy for everyone, in all EU policies, together with ensuring sustainable data processing in the public interest.
    - Privacy and data protection should not be traded for access to essential services;
    - Protecting vulnerable data subjects (gig workers, consumers, women, people of colour and those with disabilities) against algorithmic decision-making-induced discrimination by EUIs;
    - Shifting the public discourse away from “data ownership”, as it would not comply with the Charter nor empower individuals;
    - Ensuring the independence of DPAs and the EDPB;
    - Providing guidance on policies and measures (such as the Digital Services Act) that hold private companies accountable for manipulation and amplification serving private gain;
    - Building practical cooperation and joint enforcement between digital regulators on specific cases;
    - Actively contributing to the development of a common EU vision on digitization and technology. For example, determining how AI can be used for humankind and re-engineered along the lines of EU rights and values and alongside strict liability rules;
    - Enforcing data minimization to reduce the carbon footprint of data processing;
    - Promoting access to privately held data by non-profit stakeholders to foster social and solidarity innovation and scientific research in the public interest, with due regard to proportionality and appropriate safeguards (including anonymization and pseudonymization).

***

Future of Privacy Forum
1400 Eye Street NW
Suite 450
Washington, DC 20005

Future of Privacy Forum
Avenue Marnix 17
1000 Brussels, Belgium

e-mail: info@fpf.org

www.fpf.org/EU