FUTURE OF PRIVACY FORUM
1400 Eye Street NW, Suite 450 | Washington, DC 20005 · 202-768-8950 · fpf.org

New Decade, New Priorities: A summary of twelve European Data Protection Authorities' strategic and operational plans for 2020 and beyond

Published on: May 12, 2020

by Charlotte Kress, Rob van Eijk, & Gabriela Zanfir-Fortuna, Future of Privacy Forum

Data Protection Authorities (DPAs) across the European Union (EU) are in a unique position to shape the future of digital services and how they impact individuals and societies both through their outstanding enforcement powers and through their policymaking. To address the complexities of digital services and individual rights in the new decade and beyond, several DPAs have published strategic and operational plans, and have set new data protection policy goals to meet these challenges head-on.

Organizations subject to the General Data Protection Regulation (GDPR) must understand these priorities in order to assess how existing and proposed policies, systems, and laws will address them, and to support appropriate guidance for the implementation of new digital products and services.

The Future of Privacy Forum (FPF) reviewed twelve publicly available strategic plans, roadmaps, and outlines to identify the priorities and focus areas that are considered top concerns amongst DPAs for the 2020s and beyond. The plans are from the DPAs in Germany (DE), France (FR), the United Kingdom (UK), Italy (IT), Poland (PL), the Netherlands (NL), Belgium (BE), Greece (GR), Norway (NO), Sweden (SE), Ireland (IE) and the European Data Protection Board (EDPB)[1].

Our findings indicate that both the local DPAs and the EDPB are concentrating on guidelines for the consistent application of the GDPR, which aligns with ongoing harmonization efforts across the EU and the European Economic Area (EEA). In addition, DPAs are focusing their resources on "high-impact" areas, which they identify by accounting for the complexity of processing, the size of controllers and the complexity of

[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).

their operations, the vulnerability of data subjects, and the potential long term effects of the DPA's intervention on compliance. These high-impact areas include specified enforcement priorities (such as big tech), sectoral priorities (such as ad tech), and societal priorities (such as child privacy).

In detail, DPAs aim to:

> (1) clarify how (relatively) recent technologies and business practices should operate under the GDPR, such as cookie consent mechanisms;
> (2) prepare for the implications and proliferation of newer technologies, such as artificial intelligence and automated decision-making; and
> (3) protect those most vulnerable to the risks of data use practices such as data profiling.

Together, the categories of priorities outlined below provide important insight into the privacy risks that will grow in prominence during the 2020s, as well as the specific technologies and use-cases that give rise to these risks.

This report consists of a **summary** of findings, plus an **annex.** Section one of the summary examines guidelines for the consistent application of the GDPR as articulated by the EDPB and by several national DPAs. Section two highlights the topic areas identified by national DPAs as focus points for enforcement actions arising from DPAs' "own motion", such as advertising & marketing, health, and banking & finance. Lastly, section three provides an overview of the most common policy-related topics that were enumerated in the DPA strategies, such as artificial intelligence and children & youth privacy.

The annex includes details about each DPA strategy that FPF studied, organized per country. The annex also includes resources about each of the DPA's COVID-19 response guidance, which are more or less strategic in nature.

The summary of findings is a vital resource for understanding how European data protection and privacy law, enforcement, and policy will take shape in the years to come. The inclusion of COVID-related strategies and priorities provides a holistic view of what has become the new, unexpected focus area of DPAs across the continent. Currently, for example, the European Data Protection Board[2] meets weekly for remote working sessions in an effort to fast track work on COVID-19 guidance related to geolocation and other contact tracing tools, and the processing of health data for research purposes. At the national level, DPAs have issued COVID-related guidance primarily on the use of personal data in the employment context, in addition to guidance on online schooling, health research projects, and the collection of telecommunications data. Beyond following COVID-related guidance, businesses and public authorities alike must consult their relevant DPA prior to processing personal data that would result in a "high risk" to citizens, as revealed by the conclusion of a Data Protection Impact Assessment for specific projects.[3] During these prior consultations, the DPAs will verify, for example, whether or not a contact tracing app meets the requirements of the GDPR; whether important data protection principles are embedded, such as data minimization, proportionality, and purpose limitation; and whether or not data security measures are in place to prevent unlawful processing of the personal data.

1. Guidelines for consistent application of the GDPR

European Data Protection Board: The work program for the EDPB was published last year to cover both 2019 and 2020.[4] Providing guidance on the application of the GDPR is central to the EDPB's work program, especially regarding topics that were not covered in previous guidelines by the Article 29 Working Party (the body preceding the EDPB, pre-GDPR). For example, the EDPB announced guidelines on data subject rights, which will focus on the rights of access, rectification, erasure, objection and restriction, as well as on the limitations of these rights. These guidelines will build off of the feedback gathered at the EDPB's dedicated stakeholder workshop, held in November 2019.

The EDPB already adopted some of the guidelines announced in the Work Program[5]. In addition, the following Guidelines, which were included in the 2019-2020 activities, will be concluded, or at least initiated, by the end of this year:

- Guidelines on the Payment Services Directive 2 (PSD2) and GDPR.
- Guidelines on Certification and Codes of Conduct as a tool for transfers.
- Guidelines on targeting of social media users.

[2] EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic.

[3] GDPR Articles 35, 36 & Recital 94.

[4] EDPB Work Program 2019/2020.

[5] GDPR: Guidelines, Recommendations, Best Practices.

- Guidelines on children's data.
- Guidelines on concepts of controller and processor (Update of the WP29 Opinion).
- Guidelines on the notion of a legitimate interest of the data controller (Update of the WP29 Opinion).
- Guidelines on the powers of DPAs in accordance with Art. 47 of the Law Enforcement Directive.

Other Activities of note that the EDPB announced include:

- An EDPB Enforcement Strategy.
- Procedural rules on the Supervision of EU large scale IT systems.
- A reflection paper on international mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50).
- A statement on the use of personal data in the context of elections.
- Enhancement of existing IT solutions and the development of new IT solutions.
- Data breach notifications.

National DPAs: Given the challenge of navigating complexities such as national variation of implementation, nuanced meanings, and multiple interpretations of the law, DPAs are focusing on how to clarify GDPR requirements so that companies have a strong understanding of their obligations.

Transparency and consent were the most frequently cited aspects of the GDPR that were identified as focus areas. Specifically, DPAs across the board aim to establish and monitor for clear boundaries that distinguish between data obtained without consent that can be used to the detriment or disadvantage of data subjects and data obtained for the benefit of data subjects and with their consent. For example, Sweden notes that the GDPR's consent requirements must be specified so that organizations can follow them, especially with respect to voluntariness, delineation of categories of information collected, and the scope of consent. Other DPAs, such as the Dutch DPA, note that organizations must be sufficiently transparent about what data is collected and the associated risks. Those engaged in digital processing of all kinds, ranging from artificial intelligence and machine learning, to IoT devices, to big data, were singled out in relation to the need for further clarifications on transparency and consent requirements.

Data Protection Officers (DPOs). The role of DPOs is another focal point for further clarification, the primary goal of which is ensuring that DPOs have sufficient expertise and an understanding of their role. DPAs will also monitor companies that have appointed a DPO without allowing them to act in accordance with the GDPR.

2. Enforcement Priorities

From our analysis, it follows that DPAs' enforcement priorities across the board are specified as narrowing in on "high-impact" areas, which are areas that are most likely to have the largest impact and that will reach the most consumers. Two examples of such areas are *big tech*, i.e., the largest and most dominant companies in the information technology industry, and *privacy by design*.

Big tech is the high-impact area most frequently identified as an enforcement priority by DPAs. In this regard, countries are focusing on acting against tech companies, with many cases relating to the transparency and legitimacy of the processing of online behavioral data (including the use of cookies). For example, the Irish DPA, the Data Protection Commissioner, currently has 23 investigations into "big tech" companies, at least some of which are related to online data processing.[6]

Privacy by design is another high-impact enforcement area that is frequently mentioned by DPAs. For example, the Dutch DPA states that it will increase enforcement against parties that have not taken responsibility to implement the relevant rules in the GDPR (i.e. Article 25 - Data Protection by Design and by Default). It expects organizations to apply privacy by design to ensure GDPR compliance and thereby avoid enforcement actions.

Advertising and (direct) marketing was by and large the most frequently mentioned sectoral priority. Specifically, DPAs are focusing on the processing of personal data carried out for advertising purposes, particularly in the online environment. The concern with online advertising is wide-ranging, covering both technical topics, such as the use of cookie technologies, and broader aspects of the ecosystem such as the resale of personal data to third parties, behavioral advertising, profiling, and direct marketing. At a more granular level, DPAs will monitor for and review companies to ensure that they are processing personal data fairly and that they are transparent about how they compile and use individual user profiles, how they target personalized advertising, and how they share personal data with third parties. Belgium, for example, noted that direct marketing (including data brokers) will receive "special attention," and that it will conduct a critical review of business models aimed at predicting citizens' behavior. Many DPAs are also working to develop new codes of conduct or recommendations related to online advertising and marketing that focus on the requirements of fairness, transparency, and consent. For example, the ICO recently released its draft direct marketing code, which aims to take a practical life-cycle approach to direct marketing and covers areas such as

[6] https://www.independent.ie/business/technology/data-protection-commissioner-signals-blockbuster-fines-for-multinationals-on-the-way-38972780.html.

planning marketing, collecting data, delivering marketing messages, and individuals rights.[7]

Telecommunications and media was also a top sectoral priority among DPAs. Closely related to advertising, the concerns in this sector relate to the reuse of personal data and the general processing of personal data via telematic and electronic communication networks. Italy, for example, prioritizes the processing of personal data carried out for telemarketing purposes, as well as the retention of telephone and telematic traffic data for the purpose of a criminal investigation.

Health. Although the issue areas identified by DPAs relating to the topic of health were more general in nature, they focused on the processing of biometric data, health data, and genetic data. For example, Sweden's focus on the health sector will be on the basic structures of data processing, such as responsibility, transparency for patients, and the protection of data from unauthorized access and sharing.

(Open) Banking. Banking has undergone rapid change as a result of new technologies and monitoring systems, which will only become more important in the future.[8] With respect to banking, multiple data protection concerns arise as a result of new payment methods and the proliferation of payment intermediaries.[9] DPAs focus their supervision of banking to include questions about basic principles, legal basis, and information to the employees (the people who are recorded).

SMEs. Another topic of interest is scaling GDPR compliance for **small and medium-sized enterprises** (SMEs). Specifically, DPAs aim to develop new, more practical guidance and compliance tools for small and medium-sized enterprises so that such organizations are able to self-assess their level of accountability and take appropriate compliance actions that may need to be implemented.

3. Societal Priorities and Forward-looking Technologies

In addition to specific guidance and enforcement priorities, our review makes it clear that several general topic areas are likely to gain more attention in 2020 and beyond. These areas are heavily focused on general societal concerns and on technologies that will play an increasing role in citizens' lives going forward.

---

[7] Direct marketing code of practice.

[8] See, e.g., I. van Zeeland, J. Pierson, "PSD2 and other challenges to the protection of personal data in the financial sector", https://smit.vub.ac.be/wp-content/uploads/2019/09/POLICY-BRIEF-data-protection-in-the-financial-sector_def.pdf, 2019, Published: Policy brief.

[9] See, e.g., I. van Zeeland, A.P. Stefanija, J. Pierson, "Personal data protection in the financial sector", 2019, Published: Report.

Artificial Intelligence. DPAs are motivated to understand the impact of artificial intelligence on data protection, including in the areas of big data, machine learning, and automated decision-making. The Dutch DPA, for example, states that AI is its own focus area because of the many social questions at play around such topics. In addition to simply understanding AI and its impact, several DPAs aim to develop monitoring systems focused on how AI systems use personal data and on automated decision-making without human intervention. Ultimately, the common goal appears to be an initial framework of obligations that affects how AI models are constructed and used.

Children and youth privacy was a common theme among DPAs both as a standalone topic and in relation to other identified priorities such as online advertising. For example, the Irish DPC aims to initiate and actively promote the development of codes of conduct on the processing of children's personal data and is working on draft guidance for the protection of children under the GDPR. Similarly, the ICO recently released guidance on how the GDPR applies in the context of children using digital services. Part of the focus on children's privacy also relates to strengthening education about privacy and digital skills.

Public awareness. Further, many DPAs are focused on **educating the public** about their privacy rights, emphasizing the desire for helping citizens better understand the protections that the GDPR provides. Education efforts include building a public understanding of substantive legal rights and raising awareness about how information may be stored, tracked, etc. Norway, for example, is developing guidance materials and self-help tools to help individuals safeguard their rights.

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

	DE	FR	UK	IT	PL	NL	BE	GR	NO	SE	IE
Ads & marketing	✔	✔	✔	✔		✔	✔				
AI		✔	✔	✔		✔	✔	✔	✔		
Banking					✔					✔	
Big Tech	✔	✔	✔			✔			✔		✔
Children		✔	✔				✔		✔	✔	✔
DPOs (GDPR)		✔				✔	✔		✔	✔	✔
Employment				✔				✔		✔	
Health		✔		✔			✔			✔	
Public Awareness	✔	✔	✔	✔		✔	✔		✔		✔
SME		✔					✔				✔
Telecom		✔		✔			✔			✔	
T&C	✔	✔	✔	✔		✔	✔		✔	✔	

6. Conclusion

New technologies and use-cases give rise to novel complexities in GDPR compliance and in the protection of individual rights. Preparations are already underway by DPAs across the EU to address these issues: they have set new data protection policy goals, published strategic and operational plans, and are committed to developing additional guidance to meet current and future data protection challenges head-on. The strategic and operational plans outlined above provide insight into how European data protection and privacy law, enforcement, and policy will take shape in 2020 and beyond, and give stakeholders a glimpse into how best to design and implement new digital products and services going forward.

Annex
Overview of strategic and operational plans per country

A.1 Germany

On January 23, 2020, the Federal Commissioner for Data Protection and Freedom of Information, Ulrich Kelber, took part in the expert hearing at the Federal Chancellery on the "Data Strategy for Germany".[10]

- The statement stressed the use of data protection as an innovative driver toward digitalization. The digital-life is now heavily intertwined with the non-digital life. Data no longer consists of a mere few bits of our personhood. Technological advancements make it possible to collect, store, and save every detail about a person. Storage space is no longer a financial concern and today's computing capabilities enable new, real-time evaluations.
    - These advancements are what makes personal data so valuable; building profiles and scoring citizens exposes individuals to private entities and the government alike. While these possibilities have positive applications, like health and planning research, they also pose dangers like manipulation and marginalization.
    - All who decide the rules of data handling should know that profiling and scoring are no longer limited to the niche application of targeted advertising.
- Therefore, clear boundaries must be established that distinguish data obtained without citizens' consent that can be used to their detriment or disadvantage from data obtained for citizens' benefit and with their consent. These boundaries will only be workable through functioning data protection that has clear rules and effective sanctions. Such rules and sanctions can uphold good data protection without hindering digital innovation. Digitalization and tracking are not the same things, and profiling is not the only way to add value to digital offers.
- The digital strategy should give citizens sovereignty over their digital life. Knowing what information is available about you and where, plus what conclusions can be drawn from such information are elementary prerequisites for deciding how to handle your data and to whom you want to make it available. Yet, nobody knows the answer to these questions today.
- Credible data protection by design not only protects German values but can be a unique selling point for products and services in world markets. There is demand for such offers everywhere. In countries without data protection regulations and even more where the EU GDPR is the inspiration for its own regulations.

[10] https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/Stellungnahme_Datenstrategie_BReg_Anh%C3%B6rung.html?nn=5217016.

- Some parts of the CCPA are even more strict than the GDPR. According to data protection critics, digital innovation coming out of Silicon Valley will stagnate in light of the new law. However, Ulrich believes instead that American Big Tech will position data protection as a competitive product feature. He hopes that the local economy also takes this approach. Other countries are also orienting themselves around the GDPR, and German companies with existing know-how in this area should take the opportunity to capitalize on that fact and market themselves rather than lament new changes.
- The Data Ethics Commission has already given the Federal Government important recommendations, such as data protection-friendly innovations that can be specifically promoted. Germany could easily take the lead in the area of data spaces, personal data management systems and data trustees as well as decentralized learning. The government can also work in the area of interoperability
- Finally, Ulrich hopes that the government's data strategy does not follow the dead-end path of "lowering data protection requirements".

- ***COVID-19 Materials:*** Guidance of the Conference of German DPAs ("Datenschutzkonferenz") (in German) & Guidance of the DPA of Baden-Wuerttemberg (in German)

A.2 France

- ***Materials:***
  - Strategic Roadmap 2019 - 2021 & corresponding blog post
  - Control Strategy for 2020: Quelle stratégie de contrôle pour 2020
- ***Summary:***
  - **Mission & Priorities (general):** The CNIL's overall mission is "appropriation and achievement, for one and all (private individuals, professionals, and the European collective alike), of all of the GDPR's promises and potentialities." To effectuate its mission, CNIL has identified five strategic focuses to guide its action up to 2021:
    - ***(1) Giving priority to digital issues in everyday life:*** Priority will be given to whatever affects citizens' lives most directly, with a view to making the CNIL a trusted ally in citizens' digital daily lives. The four goals to facilitate this priority are:
      - **(a)** Maintaining and prioritizing the quality of processing referrals from private individuals. To be most effective, the CNIL will use all possible means to facilitate recourse, simplify internal processing, and increase the usefulness of solutions obtained.

    - **(b)** Bolstering the CNIL's educational role towards private individuals, particularly with young people. New communication formats (videos, tutorials, practical advice, etc.) will be developed to enable a better understanding of privacy issues.
    - **(c)** Providing greater clarity in communications to private individuals, including by focusing key responses, practical recommendations, and digital tools on questions that affect people most directly.
    - **(d)** Increasing the focus on digital daily life in all of the CNIL's actions, including by centering CNIL work around the questions and devices that affect people most directly in their private and professional lives.
- ***(2) Ensuring balanced data protection regulations in the era of the GDPR:*** The CNIL will continue to "walk on both feet" in a balanced and coordinated way, by providing support and taking repressive action. The four goals to facilitate this priority are:
    - **(a)** Improving the CNIL's visibility to increase the effectiveness of its actions, seeking partnerships with key players closely connected with companies of all sizes, and better resources and support services for collectives, professionals, and civil society.
    - **(b)** Ensuring that what the CNIL produces is easily understandable by all professionals. The CNIL will provide new, more practical compliance tools that consider the specificities of various types of bodies – SMEs/VSEs, local authorities and their groupings, various associations, etc. Eventually, organizations should be able to self-assess their levels of preparation and draw their conclusions on compliance actions they possibly need to implement.
    - **(c)** To make repressive action more visible so that organizations have better knowledge of control and sanction procedures. The many actions carried out by the CNIL in the context of complaint processing and oversight missions should be highlighted (on the website and with professional federations) with a view to relaying the best and worst practices observed.
    - **(d)** To better coordinate sanctions and support in light of an increased risk of litigation.
- ***(3) Promoting data diplomacy:*** The CNIL will contribute to the EU's success by promoting its own vision, based on its long experience

as regulator. Further, the CNIL will play an active part in international data geopolitics in concert with French diplomacy. The three goals to facilitate this priority are:

- **(a)** To incorporate European cooperation into the CNIL's work on a daily basis and to reinforce a strategy of cooperation with other national supervisory authorities.
- **(b)** To play a leading role within the EU by optimizing CNIL's targeting strategy at the European level and by efficiently managing its activities relating to the EDPB.
- **(c)** To make the CNIL's voice heard internationally by continuing to carry weight at the international level as major data privacy geopolitical balances come into play. The CNIL will develop new relays and levers of influence at this level with other public authorities on legal and technical matters of major strategic importance.

- ***(4) Providing up-to-the-minute public expertise on digital technology and cybersecurity:*** The CNIL aims to actively participate in the implementation of new forms of IT regulation, and will promote and participate in the networking of expertise and tools with other components of the digital State, including other approaches such as economic and ethical approaches. The four goals to facilitate this priority are:
  - **(a)** Deepening the CNIL's technical expertise to remain capable of legal and technical mastery of an increasingly complex ecosystem.
  - **(b)** Promoting the CNIL's vision of digital technology and innovation by contributing to the debates that shape the vision of digital technology and its regulation.
  - **(c)** Making inter-regulation more of a reality via exchanges on specific projects and further joint work between regulators.
  - **(d)** Continuing the CNIL's commitment to the field of ethics in collaboration with other public operators involved in the debate to further promote the ethical considerations already presented in CNIL products.
- ***(5) Embodying an innovative public service that holds fast to its values:*** The four goals to facilitate this priority are:
  - **(a)** Assessing the impact of the CNIL's actions and measuring the satisfaction of the CNIL's public.
  - **(b)** Consolidating CNIL's collective identity by increasing work on integration around a core of shared values.

        - **(c)** Improving the CNIL's internal cohesion to ensure the legal security of its actions and to facilitate its employees' work.
        - **(d)** Creating a CNIL "employer brand" through efficient management of its members of staff's careers and skills, which needs to be further formalized.
    - **Specified 2020 Priorities:** In addition to the above mentioned priorities the CNIL has identified three specific priorities for 2020, all of which relate to the daily lives of French citizens:
        - ***(1) Health data security:*** The CNIL notes that health data is sensitive data, and that it is therefore subject to special protections. The CNIL aims to focus more specifically on the safety measures implemented by healthcare professionals or by others on their behalf.
        - ***(2) Mobility & local services; the new uses of geolocation data:*** Due to the rise of mobility and location services aimed at optimizing daily life such as travel routes, the CNIL is particularly concerned with the use of geolocation data and the associated risks to privacy. The CNIL will develop controls related to the proportionality of the data collected in this context, the defined retention periods, the information delivered to individuals, and the security measures implemented.
        - ***(3) Compliance with the provisions applicable to cookies and other tracers:*** The CNIL aims to ensure full compliance by professionals related to their obligations in terms of monitoring internet users based on cookies or other tracers, particularly with respect to use for targeted advertising and user profiling. Throughout 2020, the CNIL will continue to verify compliance with the requirements of the obligation to obtain prior consent, the obligation to inform the user about the purposes of the cookies placed, etc.
            - Further the CNIL emphasizes that consent must be free, informed, explicit, and unequivocal. In particular, the simple pursuit of navigation on a site can no longer constitute valid consent of the user to the deposit of cookies. The CNIL referenced related guidelines that it adopted in July 2019, and stated that it will develop a recommendation in spring 2020 to guide operators in implementing the new requirements from those guidelines. It will allow organizations 6 months from the publication of this recommendation to comply with the new obligations resulting from the GDPR. "Controls" will thus start in fall 2020 and continue in 2021.

- ***COVID-19 Materials:*** Coronavirus (Covid-19): reminders from the CNIL on the collection of personal data (in French)

A.3 United Kingdom

- ***Technology Strategy 2018 -2021:*** This Technology Strategy supports the Information Rights Strategic Plan 2017-2021, particularly Goal #4: 'Stay relevant, provide excellent public service and keep abreast of evolving technology' and the specific strategic priority to 'Develop a Technology Strategy' that will 'outline our means of adapting to technological change as it impacts information rights and enable us to plan ahead for the arrival of new technologies.' The ICO will review and update the Strategy annually.
    - **Technology goal #1**: To ensure effective education and awareness for ICO staff on technology issues.
        - Develop training programs for ICO staff to develop their technical knowledge and understanding at a level appropriate to their role. This training will aim to develop core knowledge of how essential technologies work and further learning on new and emerging technologies.
        - Develop competencies for staff in roles connected to technology and add these to job descriptions.
        - Develop internal knowledge resources and briefings to ensure that ICO staff can refer to key information about technology.
        - Further develop internal technology advice service that will ensure ICO staff can access in-depth or specialist technical knowledge and understanding when required.
    - **Technology goal #2:** To provide effective guidance to organizations about how to address data protection risks arising from technology.
        - Develop guidance to support identified technology priority areas
        - Update existing technology guidance to reflect the requirements of the new provisions in the GDPR, the Directive on security of Networks and Information Systems (NIS) and ePrivacy Regulation.
        - Promote the use of data protection design by default, and write new guidance about these provisions in the GDPR that is technical and proportionate.
        - Produce further reports on emerging technology issues.
        - Publish a report on 'lessons learned' from cyber breaches reported to the ICO and technology issues emerging from Data Protection Impact Assessments annually.
        - Keep organizations informed about emerging risks and opportunities arising from technology in an appropriate and timely manner, including via blogs, social media, and webinars.

- **Technology goal #3:** To ensure the public receive effective information about data protection risks arising from technology.
    - Write new content for the ICO website to ensure that individuals are informed about emerging risks and opportunities arising from technology in an appropriate and timely manner.
    - Develop new partnerships to broaden public messaging about data protection risks and opportunities arising from technology.
- **Technology goal #4**: To support and facilitate new research into data protection risks and data protection by design solutions.
    - Develop a comprehensive understanding of related technologies.
    - Build relationships with research and development stakeholders to inform and educate ICO policies.
    - Use the ICO's Grants Program to support research and data protection by design solutions.
    - Use business intelligence, including annual track surveys, to understand new areas of public concern and address FAQs
    - Carry out research and investigations into new and emerging technologies.
- **Technology goal #5:** To recruit and retain staff with technology expertise to support delivery of the strategy.
    - Use secondees from external organizations to complement and support the established technology team.
    - Establish a panel of forensic investigators to support regulatory work.
- **Technology goal #6:** To establish new partnerships to support knowledge exchange with external experts.
    - Develop a new stakeholder engagement map focused on technology. The ICO will seek to engage with the following communities to develop stronger or new partnerships:
        - Professional bodies focused on technology
        - Academic technology networks and University departments focused on technology
        - Public sector technology networks
        - Industry bodies focused on technology
    - Work with cross-sector bodies to embed data protection by design in emerging standards.
    - Establish Technology Fellowships for post-doctoral experts to enable increased in-house advice and expertise on technology priority areas. The first appointment will be a two-year post-doctoral role to investigate and research the impact of artificial intelligence on data privacy, encompassing big data and machine learning.

        - Revise and reconstitute our technology reference panel with new terms of reference to ensure we receive expert advice and strategic insight into emerging technologies.
        - Develop a new 'call for evidence' process to enable receipt of insight into the data protection risks and opportunities posed by different technologies, linked to the priority areas listed above.
        - Establish a new annual ICO conference on Data Protection and Technology to showcase the latest research on data protection risks and data protection by design solutions, including outcomes from the ICO's grants program.
    - **Technology goal #7:** To engage with other regulators, international networks and standards bodies on technology issues related to data protection.
        - The ICO will prioritize international engagement on issues related to global privacy risks arising from the application of new technologies.
        - Explore new links with international bodies and regulatory networks that do not focus on data protection but have an important influence on developing global technology standards that affect data protection.
    - **Technology goal #8:** To engage with organizations in a safe and controlled environment to understand and explore innovative technology.
        - Establish a 'regulatory sandbox', drawing on the successful sandbox process that the Financial Conduct Authority has developed.
        - As part of the sandbox process the ICO would provide advice on mitigating risks and data protection by design.

- ***Openness by Design Strategy 2019 - 2022*** The major priority in this new strategy is to ensure focus on the ICO's role to enforce access to information rights through the use of all of regulatory powers. Over the next three years, the ICO will continue to make the case for information work funding.
    - **Vision:** To increase the impact of ICO oversight of access to information legislation and to encourage public bodies to comply with the law in the first instance, reducing the need for citizens to raise appeals with the Information Commissioner. In framing this new strategy, the ICO also supports delivery of the goals set out in the IRSP:
        - ***Goal #1 To increase the public's trust and confidence in how data is used and made available.*** To achieve improvements in compliance the ICO will:
            - Prioritize increasing FOIA and the EIR compliance through targeting non-compliance and taking enforcement action

consistent with the approaches set out in their Regulatory Action Policy;
    - Use insights from casework and policy analysis from the external environment to scope and publish a series of special or own-motion studies that make recommendations for improvements in understanding, accountability, openness and transparency;
    - Develop, pilot and roll out a self-assessment toolkit for public authorities, targeted to increase compliance and include opportunities for advisory ICO audits;
    - Explore the feasibility of developing an online portal to share information about the performance of public authorities in responding to information requests;
    - Work in partnership with technology experts, FOIA practitioners and stakeholders to scope and publish a technology review to assess how public authorities are using technology to search for information; and
    - Work in partnership with public authorities and civil society organizations to research and promote new digital approaches to proactive disclosure of information, including making the most of open data opportunities.
- ***Goal #2 Improve standards of information rights practice through clear, inspiring, and targeted engagement and influence.*** To achieve improvements to the services provided, the ICO will:
    - Devise, pilot and roll-out a program for customer feedback;
    - Use this feedback to inform the development of a new service charter setting out expectations for the public and public authorities;
    - Review and implement improvements to core processes, systems and procedures to meet customer needs and improve efficiency and quality.
    - Review and develop new guidance for public authorities consistent with the ICO's Regulatory Action Policy, prioritizing those areas of greatest impact
- ***Goal #3 Maintain and develop influence within the global information rights regulatory community.*** To achieve this, the ICO will:
    - Draw on the learning from the 'Your data matters' campaign, to develop, deliver and evaluate a series of targeted information rights campaigns to raise awareness of FOIA and

the EIR rights and show how access to information makes a difference;
        - Scope and assess the demand for resources for schools to support the delivery of citizenship programs;
        - Develop new engagement channels to promote guidance, support and good practice for public authorities, including organizing practitioner workshops; and
        - Redesign online forms to make it easier for individuals to use.
    - ***Goal #4 Stay relevant, provide excellent public service, and keep abreast of evolving technology.*** To achieve this goal, the ICO will:
        - Continue to build and promote the case for changes to the scope of FOIA and the EIR legislation, working closely with colleagues in government and Parliament, public authorities, the private sector, civil society organizations, the media and the public;
        - Engage and consult with stakeholders to review other potential areas for legislative change; and
        - Work with regulators and stakeholders including The National Archives to explore the practical application of duty to document frameworks.
    - ***Goal #5 Enforce the laws we help to shape and oversee.*** To build and sustain international collaboration, the ICO will:
        - Promote standards of openness and transparency globally, and continue to support the strengthening of a global voice for access to information rights;
        - Work in partnership with UNESCO and international colleagues to contribute towards the promotion of access to information rights, as part of the achievement of the United Nations Sustainable Development Goals framework;
    - ***Goal #6 To be an effective and knowledgeable regulator for cyber related privacy issues.***

- **Draft Direct Marketing Code of Practice**
    - All organizations have an obligation to ensure their direct marketing activities comply with the GDPR, Data Protection Act 2018, and the PECR 2003. The draft code aims to help those undertaking direct marketing to comply.
    - The draft builds on the ICO's previously produced direct marketing guidance, taking into account the input received during the initial call for

views. The code takes a practical life-cycle approach to direct marketing, starting with a section looking at the definition of direct marketing to help organizations decide if the code applies to them, before moving on to cover areas such as planning marketing, collecting data, delivering marketing messages and individuals rights.
    - The code was out for consultation until 3/4/20 and the final version is expected later this year.

- ***Information Rights Strategic Plan* April 2017 - March 2021**
    - **Vision:** To increase public confidence in organizations that process personal data and those which are responsible for making public information available.
    - **Strategic Goals:**
        - ***Goal #1***: To increase the public's trust and confidence in how data is used and made available. Progress towards this goal will be measured annually through tracking research. To achieve this goal, the ICO has identified the following strategic priorities:
            - **(a)** Increasing transparency: The public should be able to easily find out and influence how their personal data is being used.
                - The public should have straightforward access to clear information about data processing. They should expect the highest standards of transparency for processing that has a serious impact on their lives.
                - All should be able to see, challenge and correct personal records, especially where these contain details of particular sensitivity.
                - Work to promote transparency of digital processing - including the use of big data, artificial intelligence and machine learning - where opaque or invisible practices can pose a particular risk to public trust and confidence.
            - **(b)** Creating a culture of accountability: Promoting accountability will be a priority activity for the ICO – in guidance, toolkits and other communications with stakeholders.
                - Define the parameters of good information rights practice and clearly explain what good practice looks like to both users of data and the public.
                - Develop a privacy management framework that supports implementation of accountability programs.

        - Develop frameworks to enable the ICO to accredit codes of conduct and certification schemes as mechanisms to enable organizations to demonstrate the effectiveness of their accountability measures.
        - Actively seek exemplar organizations to help illustrate good practice which protects people's personal information.
- ***Goal #2:*** Improve standards of information rights practice through clear, inspiring and targeted engagement and influence. In working towards this goal, the ICO will focus on the following strategic priorities:
    - **(a)** Leadership
    - **(b)** Excellent guidance
    - **(c)** Assurance: publish good practice guidelines and enable organizations to come to us and explain how they comply.
    - **(d)** Advising and influencing Government: giving particular focus to engagement, including in Scotland, Wales and Northern Ireland, with policy makers, legislators and other groups who represent the public.
    - **(e)** Partnership working: with key public, private and third sector stakeholders through co-operation agreements and direct engagement.
- ***Goal #3:*** Maintain and develop influence within the global information rights regulatory community. To expand and enhance international work the ICO will have the following strategic priorities:
    - **(a)** Develop an International Strategy designed to achieve global reach and influence for the ICO.
    - **(b)** Creating and maintaining effective relationships
    - **(c)** seize opportunities to engage with information rights regulatory regimes and communities outside the EU, with the aim of establishing effective networks and relationships in the UK public interest.
- ***Goal #4:*** Stay relevant, provide excellent public service and keep abreast of evolving technology. The ICO wants to ensure that privacy and data protection considerations are integral to big data analytics. To maintain relevance in an ever more technologically sophisticated world, the ICO will have the following strategic priorities:
    - **(a)** Working with innovators
    - **(b)** Develop a Technology Strategy
    - **(c)** Develop a Resource and Infrastructure Strategy

    - **(d)** Commission specific research or issue calls for evidence where appropriate
- ***Goal #5:*** Enforce the laws that the ICO helps shape and oversee. To maintain an effective and proportionate regulatory response, the ICO will have the following strategic priorities:
    - Develop a new Regulatory Action Policy as part of the ICO's preparations for the forthcoming EU data protection reform package. (laid before Parliament in 2018)
    - Use the information gathered from the public, those regulated, and other stakeholders to identify areas of poor practice or noncompliance.
    - Take regulatory action, where appropriate, in areas which most directly and effectively further the ICO's strategic vision.
    - Continue to ensure that lead generation and data broking organizations are compliant with the law.
    - Prioritize issues and cases of significant potential public impact
    - Develop an Intelligence Strategy to enable taking action on issues as they emerge and deal with those of significant potential impact as a high priority.
- ***Goal #6:*** To be an effective and knowledgeable regulator for cyber related privacy issues. To achieve this goal, we will prioritize the following actions:
    - Provide an effective service meeting an expanded range of customer's and stakeholder's breach reporting and incident response needs.
    - Prioritize response to significant data breaches affecting large numbers of UK citizens.
    - Strengthen relationships with other relevant agencies working in this area, including a program of secondments and apprenticeships to build in house capability and capacity.
    - Agree a core suite of information for the public, agreed with other stakeholders involved in the UK incident response mechanism, as the basis of communications to describe ICO and partners' respective roles during live incidents.
    - Participate in national incident response drills, to train staff and test the effectiveness and readiness of arrangements.
    - Debrief incident responses and investigations to gather learning and improve services in future.

- **International Strategy 2017 - 2021**
  - **Challenge 1:** To operate as an effective and influential data protection authority at European level while the UK remains a member of the EU and when the UK has left the EU, or during any transitional period.
    - 1.1 Provide expert advice to the UK Government on the data protection implications of leaving the EU, in particular about the ICO's relationship with the EDPB.
    - 1.2 Continue Strong engagement with the Article 29 Working Party and EDPB, seeking to maintain a strong working relationship with the EDPB when the UK exits the EU.
    - 1.3 Continue to engage with other European groups of data protection authorities, including the Council of Europe, to explore the role of Convention 108 as a data protection standard.
      - Seek to engage with specialist EU working groups that consider data protection related to law-enforcement data sharing.
  - **Challenge 2:** Maximizing the ICO's relevance and delivery against its objectives in an increasingly globalized world with rapid growth of online technologies. To meet this second challenge the ICO has identified the following priorities:
    - 2.1 Global relationships: continue to engage with leading international privacy networks and explore relationships with networks not previously engage, for example in the Asia Pacific region. The ICO will prioritize international engagement on issues related to global privacy risks arising from the application of new technologies.
    - 2.2 Enforcement: The ICO will invest in bi-lateral relationships, including enforcement cooperation, with the most strategically important economies and data protection/privacy authorities globally.
    - 2.3 Knowledge exchange, guidance and standards: seek to develop new relationships with think tanks, academic and civil society networks. The ICO's new Grants Program, launched in 2017, will be open to such bodies.
    - 2.4 Freedom of Information: The ICO will share information and knowledge with other independent bodies responsible for enforcing and promoting freedom of information laws. It will support work to identify common standards for freedom of information laws and progressive transparency.

- **Challenge 3:** Ensuring that UK data protection law and practice is a benchmark for high global standards. To meet this challenge the ICO has identified the following priorities:
  - 3.1 Collaborate with the international business community and other stakeholders to support work to turn the GDPR's accountability principles into a robust but flexible global solution.
- **Challenge 4:** Addressing the uncertainty of the legal protections for international data flows to and from the EU, and beyond, including adequacy. To meet this challenge the ICO has identified the following priority:
  - 4.1 Protecting personal data flows by providing expert advice to the UK Government and Parliament on international data flows. The ICO will seek to explore the concept of the UK as a 'global data protection gateway' – a country with a high standard of data protection law which is effectively interoperable with different legal systems that protect international flows of personal data.
    - Further, it will support the development of mechanisms to support better interoperability between the UK's data protection laws and other systems such as the APEC Cross Border Privacy Rules (CBPR).

- ***COVID-19 Materials:*** Data protection and coronavirus: what you need to know; Apple and Google Joint Initiative on COVID-19 contact tracing technology

A.4 Italy

- ***Materials:***
  - Priorities for 2020 (Italian)
  - Strategy Document 2020-2022 (Italian)

- ***Summary:***
  - **Mission & Priorities:** The Italian DPA will focus on operational activities related to the following specific areas of intervention:
    - ***Obligations established by relevant regulations:***
      - Guarantee measures relating to the processing of biometric data
      - Collaboration with relevant institutions for the purpose of adopting regulations concerning data related to criminal convictions and offenses
      - Guarantee measures relating to the processing of genetic data
      - Guarantee measures relating to the processing of health data

- ***Data Processing by Private Subjects:***
  - Assessments regarding the processing of personal data for journalistic purposes;
  - Verification of codes of conduct
  - Improving procedures for notice of violations of personal data;
  - The privacy role of OIV auditors;
  - BCR approval procedures where the Guarantor holds the role of lead authority;
  - Data processing in the employment context;
  - International data transfers
- ***Public Data Processing:***
  - Processing of personal data (including that contained in deeds and administrative documents) carried out for advertising purposes and transparency on the web by public entities and other obliged entities;
  - Data processing carried out for tax purposes;
  - Data processing carried out at local bodies;
  - Data processing concerning the healthcare sector with specific reference to the innovations introduced by the new regulatory framework;
- ***Data Processing via telematic and electronic communication networks:***
  - Checks on the processing of personal data carried out for the purpose of telemarketing;
  - Cyberbullying;
  - Checks against telephone operators following a violation;
  - Customer data;
  - Retention of telephone and telematic traffic data for purposes of investigation and repression of crimes;
  - Electronic identification processing and trust services for electronic transactions in the internal market;
- ***International Activity:***
  - Cooperation with other national DPAs across the EU through the IMI platform;
  - Participation in the procedures established through consistency with the EDPB;
  - Participation in international and European working groups;
- ***Data Processing in the Health Sector***
- ***Inspection Activities and Sanctions:***

        - Supervision of strategic or databases presenting greater critical issues, taking into account the seriousness of the violations disputed altogether.
    - ***Transparency and Corruption Prevention Activities:***
        - Implementation of the regulation on administrative transparency and corruption prevention at the Guarantor;
        - Adoption of the 2019 three-year corruption prevention plan-2021- Update 2020;
    - ***The DPA will also implement the following priorities to adopt suitable measures for improvement of the office organization:***
        - Strengthening of collaboration activities and mutual link between different Departments, Services, and Offices to create a wider circulation of information;
        - Progressive coverage of the places provided in the organic plan, giving priority to the completion of the bankruptcy procedures already started;
        - Consolidation of the DPA's necessary IT security activities, as well as IT procedures for archiving and the management of document flows.

- **Additional Information:** In addition to the above priorities, the Italian DPA identifies several other activities of "particular interest" that will be given close attention:
    - ***(1) Strengthening participation in EU institutions***, with particular reference to the concrete implementation of the new regulatory framework on personal data protection (GDPR?) and the need to support the work in the context of the participation of the Italian DPA in the Group of European guarantors; consolidation of collaboration activities undertaken with other national DPAs;
    - ***(2) Communication*** activities on data protection issues, including through the use of new technologies; dissemination of knowledge not only in the media, but also at representative institutions and bodies (e.g. trade associations of local authorities, private entities, etc.), both to educate them on privacy issues and to obtain greater dissemination;
    - ***(3) Strengthening of studies***, in part for the purpose of preparing functional files for the possible issuance of general measures of the Guarantor or for the purpose of deepening understanding of particularly topical issues; implementation of the provisions in administrative transparency and whistleblowing, and the structuring of the institutional website;

        - **Budget:** The DPA indicates the need for a greater budget and more bandwidth to be able to implement its Strategic Plan, as its workload has considerably increased since the GDPR became applicable. The process of increasing the DPA's bandwidth began in 2019.

- ***COVID-19 Materials:*** Coronavirus: No do-it-yourself (DIY) data collection, says the Italian DPA (in Italian)

A.5 Poland

- ***Materials:***
    - Plan for 2020 (Polish)
- ***Summary:*** Due to the increased risk of violation of personal data protection laws in the below mentioned sectors and the increase in public interest on these issues, it is important that the following topics play a significant role with respect to the tasks carried out by the President of the Office for Data Protection of Personal Information.
    - ***1. Authorities processing personal data in the Schengen and Visa Information System Information System, including SISII / VIS security audit:*** consulates and administrative authorities tax in the scope of processing personal data SISII and VIS.
        - The purpose of the check is to check how these entities process SISNIS personnel data available via KSI (National Information System) or directly in SISII / VIS pursuant to the provisions of the Act of 24 August 2007 on the participation of the Commonwealth Polska in the Schengen Information System and the Visa Information System (Journal of Laws from 2019 item 1844.).
        - The Schengen Information System was established as a tool to lift border controls between the Schengen Area countries. Its essence lies in ensuring that each State party to the Convention implementing the Schengen Agreement has the same set of information allowing access to the system and searching for entries regarding persons and objects for border control and other police checks and customs kept within a given country and for issuing visas, documents residence permits and regulations on foreigners.
        - The Visa Information System was created for ensuring exchange of information between the Schengen States regarding issued visas and people applying for them.
    - ***2. Banks*** - processing of personal data in connection with making copies / scans of customer and potential customer identification documents.
    - ***3. Entities using the remote water meter reading system (so-called intelligent meters) -*** processing of personal data in connection with the use of these water meters.

- ***COVID-19 Materials:*** Statement by the President of UODO on the coronavirus (in Polish)

A.6 The Netherlands

- ***Materials:***
  - Focus areas in 2020 (Dutch)
  - AP Focus in 2020 - 2023 (Dutch)
    - Corresponding Leaflet in Dutch
    - Corresponding Leaflet in English
- ***Summary:***
  - **Mission & Priorities:** The AP's interventions are aimed at sustainable behavioral change. The AP will prioritize the following three focus areas:
    - ***(1) Data Trade (incl. data brokers):*** The AP notes an exponential increase in the unauthorized resale of personal data to third parties. The AP's goal is to have responsible data use become part of Corporate Social Responsibility (CSR) and the Corporate Governance Code. The most important areas within the category of data trade are:
      - **(a)** the supervision of resale data,
      - **(b)** IoT,
        - The AP expects providers, both public and private, to be sufficiently transparent about which data are collected and what risks are associated with the use of the various devices. The AP also expects IoT devices to be sufficiently protected.
        - Further, the AP plans to stimulate the development of production standards for IoT products in the coming period and certify these standards with the AVG.
        - The AP also wants to actively participate in the debate on the development of sustainable, socially responsible IoT. Data minimization, privacy by design and privacy by default will be important subjects here.
      - **(c)** profiling, and
        - The AP will monitor for companies and organizations to process data fairly and to be transparent about how they compile profiles and how they use profiling.
      - **(d)** behavioral advertising
        - The AP will aim for new codes of conduct related to online advertising that do justice to the requirements of, among other things, transparency and permission. Various sector and branch organizations are already working on this.

- ***(2) Data Government:*** The most important areas within the category of Data Government are:
  - **(a)** data security,
    - In the coming years the AP wants to check government organizations on their security level and encourage them to work on strong IT and data management.
  - **(b)** smart cities,
    - The AP will monitor the observance of the AVG by political parties by exploring and conducting research, formulating further standards, encouraging self-regulation and possibly enforcement.
    - In 2019, the AP launched an exploratory study into the development of Smart Cities, looking at the way in which municipalities deal with the privacy of residents and visitors in the development phase by requesting the DPIAs of a specific group of municipalities.
      - Prior to developing Smart City applications, municipalities must identify the privacy risks involved, such as by conducting a DPIA.
      - As of March 2020, the AP's exploratory study reached its second phase, in which a second, larger group of municipalities has been asked to provide information about Smart-City projects. At a later stage, the AP will conduct in-depth research on specific themes or specific examples based on the information provided
      - The AP is expected to complete the investigation in the summer of 2020.
  - **(c)** partnerships/unauthorized sharing, and
  - **(d)** elections and micro targeting.
    - Here, the AP attaches great importance to cooperation with European colleagues.
- ***(3) AI & Algorithms:*** The most important area of attention within AI & algorithms is:
  - **(a)** Monitoring system. Because both private and public parties use AI and algorithms and because there are many social questions that play around these topics, the AP will pay special attention to it - thus forming its own focus area.
    - In the coming period, the AP will focus on shaping a system of supervision of AI and algorithms in which personal data is used. It will focus, among other things, on clarity and clarity of automated decisions.

- **Vision, Strategy & Goals:** The AP uses a risk-based supervisory approach, assessing risk within a variety of sectors and topics based on the likelihood that they will occur and on its impact on people's daily lives. In the coming years, the AP will expand its knowledge of the consequences of digitization of different sectors on privacy protection. The AP aims to be an influential privacy regulator in Europe by 2023.
    - The AVG is an accountability based law, meaning that it is up to companies and organizations to show that they comply with privacy legislation. Consequently, the AP sets up broad information campaigns and communicates through their website and social media.
        - The AP encourages forms self-regulation based on clear frameworks set by the AP.
    - Since the AVG entered into force, the AP explicitly gave organizations space to properly implement the new rules. In the coming years, the AP will increase enforcement against parties that have not taken responsibility to implement these rules.
        - Further, the AP expects companies and organizations to apply privacy by design to ensure AVG compliance and thereby avoid AP enforcement actions.
    - ***Roles of the AP:*** The following roles are not mutually exclusive
        - **(1)** Legal order: The AP sees itself as a guardian of the foundations of democratic legal order.
        - **(2)** Ombudsperson assignment: The AP will focus on the opaque processes behind automated decision making.
        - **(3)** Supervisor in the data market: The AP considers it essential to have insight into the dynamics of the international data market and data economy.
    - ***Strategy:*** The AP chooses an enforcement instrument by looking at what is most desirable from the point of view of punishment or special and general prevention. Further, it considers the unlawful advantage that may have occurred as a result of unlawful processing.

- **Additional Information:**
    - The AP also identifies three major trends that influence the protection of personal data: Growth of the data society, increase in digital injustice, and increase in privacy awareness.

- ***COVID-19 Materials:*** My sick employee (in Dutch)

A.7 Belgium

- ***Materials:*** Final version of the 2019-2025 Strategic Plan
    - Summary (Dutch)
    - Press Release (Dutch)

- ***Summary:***
    - **Mission & Priorities:** The overall mission is "to guide citizens and organizations towards a digital world where privacy is a reality for all."
        - ***Sector Focuses:*** To effectuate its mission, the Belgian DPA will focus its priorities on the following sectors:
            - **(1)** telecom and media,
                - In this sector, the DPA will focus on the reuse of personal data by players and their partners.
            - **(2)** public authorities,
            - **(3)** direct marketing (including data brokers),
                - This sector will receive "special attention."
                - "Without delay," the DPA will conduct a critical review of the increasingly intrusive business models aimed at predicting citizens' behavior.
            - **(4)** education, and
            - **(5)** SMEs.
        - ***GDPR Focuses:*** It will also focus its actions on the following aspects of the GDPR:
            - **(1)** the role of the DPO, with a particular focus on companies that have appointed a DPO without allowing them to act in accordance with the GDPR;
            - **(2)** the lawfulness of data processing activities, and more particularly the (abusive) processing of personal data based on the legitimate interests legal basis; and
            - **(3)** data subjects' rights, specifically the scope of some of these rights.
        - ***Societal Focuses:*** Finally, the Belgian DPA will also focus on more general societal topics, including
            - **(1)** pictures and cameras;
                - The DPA "must" update its website information on pictures and cameras to be consistent with technological advancements.
            - **(2)** online personal data processing, including the use of cookies; and

        - The DPA considers it essential to act quickly and effectively against actors who do not respect basic rules relating to the transparency and legitimacy of the processing of online behavioral data (with particular emphasis on protecting young Internet users).
      - **(3)** sensitive personal data processing.
    - In addition to the main priorities outlined in the Strategy Plan, the DPA indicated that it will also pay attention to artificial intelligence applications, as well as applications using biometric data.

- **Strategic Objectives:** The Strategic Plan outlines the following six strategic objectives:
  - ***(1) Better data protection through awareness:*** This objective reflects the DPA's vision of instilling a cultural change by reinforcing citizens' knowledge of their own data protection rights and obligations.
    - Further, the Belgian DPA makes clear that the ODA is available as a reference center for citizens, processing officials, and subcontractors.
  - ***(2) Better data protection through law enforcement:*** With this objective, the ODA is moving from a purely advisory role as a "Privacy Commission" to a supervisory role as an Authority.
    - To achieve this objective, two new bodies within the APD - the Litigation Chamber and the Inspection Service - will play a crucial role.
  - ***(3) Better data protection by identifying and updating the changes:*** This strategic objective reflects the importance of monitoring, understanding, and correctly assessing changes in technology, economics, and societal plans so that the ODA can follow them closely and react to them appropriately.
  - ***(4) Better data protection through cooperation (national & int'l):*** The DPA stresses that national cooperation cannot be limited to the DPAs, but should include a dialogue with other controllers, too.
  - ***(5) Better data protection with ODA as leader/guide and reference center:*** The goal is to be a known reliable partner in data protection, as well as a leader and recognized reference center.
  - ***(6) Better data protection by being an efficient controller (internally):*** In this context, the ODA will conduct a critical analysis of its current organization and be (more) attentive to a "methodical" approach to its activities.

- **Concrete Projects:** The BOOST project, which aims to support SMEs, will start in January 2020. The Strategic Plan also mentioned that preparations are currently underway for a completely new recommendation on direct marketing.

- **Additional Information:**
  - **Budget:** The DPA indicates the need for a greater budget and more bandwidth to be able to implement its Strategic Plan due to the workload increase since the GDPR became applicable.
  - **Drafting:** The strategic plan was drafted by the new ODA executive committee, appointed in April 2019. This new executive committee is made up of five different departments that work together to implement the ODA mission:
    - **(1)** the General Secretariat,
    - **(2)** the Knowledge Center,
      - This Center will issue positions and recommendations as to how to implement certain provisions of the GDPR in practice and will act as a safeguard so that the draft Belgian laws do not unjustly interfere with citizens' rights to respect for their private lives.
    - **(3)** the Front Line Service,
    - **(4)** the Inspection Service, and
      - This Service will investigate complaints received by the DPA, and intends to operate much more proactively in the coming years.
    - **(5)** the Litigation Chamber.

- ***COVID-19 Materials:*** COVID-19 and processing of personal data at work (in French)

A.8 Greece

- In honor of Data Privacy Day 2020, the Greek DPA held a conference entitled "The right to the protection of personal data after the implementation of Regulation (EU) 2016/679 and the transposition of Directive (EU) 2016/680." The conference included various presentations from members of the Authority, including the Minister of Justice, Costas Tsiaras, and the President of the DPA, Konstantinos Menoudakos. Below is a summary of the key points (Greek) made during the conference that relate to upcoming priorities and strategies.
  - *Judicial System updates:* The Ministry of Justice recognizes the need to develop interdisciplinary synergies to modernize the judicial system, and has already set up a Standing Scientific Committee consisting of legal, administrative, and computer technicians. The committee will examine the impact of introducing artificial intelligence into the judicial system.

        - A semi-automatic algorithmic method is already being used in the Supreme Court for the anonymization of court decisions posted on the online case-law database, pursuant to the GDPR.
        - The Ministry also announced its intention to contribute to a wide-ranging information campaign aimed at government officials, businesses and the general public.
    - *Practical application of principles:* The DPA President noted that "in an era of technological acceleration, a new culture with a focus on data security is becoming increasingly urgent as a fundamental requirement, which must be preserved not only as a legal right but also as a practical application."
        - He stressed that "the GDPR, Directive (EU) 2016/680, and Law 4624/2019 are not only a new legislative framework but also introduce a new concept of responsibility and compliance." He noted that "clearly more time is needed to draw comprehensive and secure conclusions on the difficult but necessary adaptation from the implementation of the new legislation."
        - The President also highlighted important decisions that the DPA has issued, some of which included fines and address recommendations, warnings, or reprimands to controllers. In particular, he referenced the fines imposed on 25/5/2018, with amounts totaling EUR 1,397,000. The DPA examines specific cases either on the basis of complaints or inspections carried out on its own initiative or in the context of its opinion work.
    - *Proposed Amendments:* The DPA will submit concrete proposals to the Ministry of Justice for any necessary amendments "based on the findings of the Authority to date and on the issues that arise in practice in the context of the implementation of Law 4624/2019."
    - *Areas of concern:*
        - **(1)** Labor relations: One area of concern is the personal data protection in labor relations post-GDPR and Law 4624/2019.
        - **(2)** AI models: Another area is "the development and operation of Artificial Intelligence models, [which] raises a number of issues of a moral, legal and purely technical nature. Part of these issues relate to the protection of fundamental rights, privacy, and the protection of personal data. Provisions of the GDPR and of Law 4624/2019 constitute a regulatory framework that affects the way artificial intelligence models operate and use."
        - **(3)** Automated Decision-Making: The conference also emphasized that 'data protection by design, privacy by design, the emphatically accountable principle, the principle of transparency, and the provisions of automated decision-making without human

intervention constitute an initial framework of obligations that affects how artificial intelligence models are constructed and used. This framework is analyzed in the light of the forthcoming more specific EU regulatory interventions in the field of Artificial Intelligence.

- ***COVID-19 Materials:*** Guidelines for processing of personal data in the context of managing COVID-19 (in Greek)

A.9 Norway

- ***Materials:***
  - National Strategy for AI (Norwegian) and corresponding article (Norwegian)
  - Overall DPA Strategy for 2018 - 2020
    - § Strategy (Norwegian) and corresponding article (Norwegian)
- ***Summary:***
  - **Background:** The Norwegian DPA is a separate independent administrative body under the Ministry of Local Government and Modernization and can therefore not be instructed by the Ministry in individual cases. They decide for themselves which sectors they prioritize and what methods they use.
  - Their most important tasks are to supervise, among other things, the Norwegian Personal Data Act, the Health Register Act and the Patient Record Act, and to be ombudsman in questions concerning privacy matters.
    - **Mission & Priorities:** The overall goal for the Norwegian DPA's strategy is to create a clear direction for their work and to be ambitious about ensuring good privacy. The DPA shall work towards a fairer balance of power between on the one hand the private individual, and commercial actors and the public sector on the other.
      1) Large commercial companies and governmental agencies have large amounts of data about individuals. It is difficult for each individual to have control over their own information. The DPA will work purposefully to strengthen the principles of privacy and rights of the individual. This is going to be accomplished by:
         - Prioritizing principal cases that will contribute to change the balance of power towards the private individuals.
         - Actively enforce regulations to ensure better compliance among actors with a business model that in particular challenges privacy.

- Collaborating with other authorities and relevant organizations to strengthen the individual's rights nationally and internationally.
- Actively influence political processes and legislative work that provide guidelines for the use of personal data in the private and public sectors.
- Actively participate in the debate on surveillance in society and protect important principles of the European Convention on Human Rights and the Norwegian Constitution.

2) The DPA will work to promote privacy-friendly digitization, innovation and development. The usages of big data can contribute to solving a variety of challenges that our society is facing. At the same time, the use of big data also challenges the fundamental rights of privacy. Creating solutions that enable the usage of big data, while minimizing privacy disadvantages for the individual, will be even more important in the future. The DPA will try to accomplish this by:

- Making the data-intensive commercial players accountable in developing and implementing methods that safeguard privacy
- Encouraging relevant authorities to allocate more funding for research on privacy-promoting technologies
- Promoting the use of privacy by design and enforcing breaches of non-compliance
- Helping to increase the expertise in privacy impact assessments
- Working to ensure that privacy is part of the **ordering expertise(?)** in public and private sector
- Working actively for universities and colleges to incorporate privacy in all relevant education

3) The DPA shall work to ensure that companies become competent, understand the importance of good privacy and comply with the regulations. The new privacy regulation places more of the responsibility of protecting the private data on businesses. In order for them to uphold this responsibility and comply with the regulations, the companies must have sufficient expertise. They need to understand how and why privacy is important to both

the business itself and the individuals they have information about. The DPA will try to accomplish this by:

- Highlighting privacy as a valuable asset for businesses.
- Actively collaborating with business to ensure good knowledge and compliance in different sectors.
- Influencing key players to take upon themselves to develop sector-specific privacy needs.
- Encouraging the development and use of self-regulatory mechanisms such as industry norms, standardization and certification.
- Providing good guidance and tools that help businesses comply with the regulations.
- Ensuring that businesses safeguard the rights of those about which they have retained data and ensure that the business has a simple procedure for complaints.
- Ensuring that businesses that are obliged to create a DPO do so and that such officers have expertise and an understanding of their role.

4) To a greater extent that before, the DPA shall help individuals safeguard their own privacy. It is important that each individual can easily find information about their rights and be able to use them in practice. The DPA will try to accomplish this by:

- Highlighting the value of privacy for the individual and society as a whole.
- Developing guidance materials and self-help tools to help individuals safeguard their rights.
- Influencing businesses and industries to develop good solutions that help individuals to safeguard their rights
- Advocating to strengthen education about privacy and digital skills in schools.

5) The DPA shall influence and take the leadership in some selected international processes to promote better protection of personal privacy. It is important that the Norwegian DPA takes an active role in international work. The DPA will try to accomplish this by:

- Actively participating in European and international forums and projects to influence decisions and practice on the regulations affecting the privacy of Norwegian citizens.
- Taking a leading role in the Nordic co-operation.
- Using our national work (guides, investigations, decisions) to create added value internationally.
- Gaining expertise and learning from what is happening internationally.

6) The DPA must be a competent and forward-looking authority. The DPA shall be a knowledge-based workplace with high ceilings and a good working environment.

- **National Strategy for AI:** Section two includes some information relevant to data protection strategies. The relevant portions are summarized below:
  - The Norwegian Government will facilitate the sharing of data within and across industries and sectors. The Government has a goal of facilitating the sharing of data from the public sector so that business, academia and civil society can use the data in new ways.
    - However, data containing personal data, which is exempt from public disclosure or subject to a duty of confidentiality, shall not be made available unless there are special grounds for doing so. Examples of open data from the public sector are weather data from the Norwegian Meteorological Institute and traffic information from the Norwegian Public Roads Administration. The use of personal data for the development of KI raises a number of issues that must be addressed before sharing or using such data.
  - Principles of Data Sharing: Specific strategies for sharing data have been developed in the following sectors: culture, research and education, government spending, transport and transport and maps and real estate (geodata).
    - The government has put forward a separate strategy for making available and sharing research data. The strategy establishes three basic principles for publicly funded research data in Norway:
      - Research data should be as open as possible and as closed as necessary.
      - Research data should be handled and organized so that the values in the data can be utilized to the best possible extent.
      - Decisions on archiving and organizing research data must be made in the research communities.

        - The Government uses the following principles for sharing data from the business community:
            - Voluntary data sharing is preferable, especially where the actors have common interests in sharing data.
            - The authorities can facilitate the sharing of data that the business itself does not see the value of sharing, where such sharing increases social benefits.
            - Sharing of data may be required if necessary, for example, in the interest of the community.
            - Data must be shared so that individuals and businesses have control over their own data. Privacy, security and business interests must be taken care of.
    - Consent:
        - Data containing personal data is covered by the Personal Data Act. The principle of purpose limitation means that the purpose for the processing of personal data must be clearly stated and determined when the information is collected. This is essential for the individual to be able to control their information and make an informed choice about consent to data processing. The development and use of artificial intelligence often requires many different types of personal information - information that in some cases is actually collected for other purposes. In addition, the handling of data, such as health data, may be covered by other regulations, such as the Health Register Act.

- ***COVID-19 Materials:*** Coronavirus and privacy (in Norwegian)

A.10 Sweden

- ***Materials:***
    - Strategic Plan 2019 - 2020 (Swedish)
    - Audits for 2019 - 2020 (Swedish)
    - Consent Review Extension (Swedish)
- ***Summary:***
    - **Mission & Priorities:** The DPA's Strategic plan will be updated annually. The current version, published in March 2019, stipulates the general plan for 2019-2020. Their overall mission is "to achieve as great an effect as possible in the protection of personal data and to ensure that good practices are observed in credit reporting and debt collection activities"
        - ***Sector Focuses:*** the Swedish DPA will focus its priorities on the following areas:

- **(1)** The Healthcare Sector: The focus will be on the basic structures of the processing of data such as responsibility, transparency for patients, and protection of data from unauthorized access and unauthorized sharing.
    - In addition, the DPA will focus on the legal need for large data collections.
- **(2)** The School System: Here, the focus will be on the legal need to process data, whether there are structures to protect the data from unauthorized access and sharing, and the use of technology such as camera surveillance and face recognition.
- **(3)** The Judiciary System: The personal data processing of the judiciary system relates to privacy-sensitive information that affects many people.
    - The judicial system has been given new obligations via brottsdatalagen" (Swedish Criminal Data Act(?)), supplementary regulations in various areas, and "lagen om passageraruppgifter i brottsbekämpningen" (law enforcement access to passenger data for crime fighting (?)).
    - The focus of supervision will be on how the competent authorities live up to their new obligations, but also on the authorities' use of technology.
- **(4)** The Processing of employees' personal data by employers: The focus will mainly be on employers' monitoring of employees. The supervision will include questions about basic principles, legal basis, and information to the employees (the people who are recorded).
- **(5)** Cellphone's operating systems: The focus will be on the basic principles of the dataskyddförordningen (Data Protection Regulation), such as legality, correct usage, and transparency. This will be accomplished by reviewing the legal basis for data processing and by reviewing the information that is provided to users in connection with the collection of personal data.
- **(6)** Retail: The retailer's handling of personal data in customer reward programs affects many people, and the information can be private and sensitive. Retail involves extensive amounts of data and includes legal issues where clarification is needed. Here, the legal basis for processing should be

examined, particularly with respect to the legal basis for profiling.
        - **(7)** Payment services providers: Payment intermediaries' collection of customers' purchase history concerns many people and large amounts of personal data. There is a need to clarify specific legal issues such as, for example, the purpose of processing and deselecting(?) personal data.
        - **(8)** The Visa information system (VIS): is a system in which a comprehensive exchange of visa data is exchanged between EU member states. According to the VIS Regulation, the system must be inspected every four years. The last time the Data Inspectorate inspected the system was 2015.
        - **(9)** The debt collectors: An overall goal for the DPA's activities regarding debt collection is to achieve as great an effect as possible regarding the compliance with the Swedish debt collection laws and to see that best practices are observed in debt collection activities.
            - Therefore, supervision will be aimed at debt collection companies that have cases concerning a large number of debtors.
    - ***Legal Focuses:***
        - **(1)** Role of the DPO: Who is receiving the rights to process personal data, and in the processing of this data, who is also gaining access to it?
        - **(2)** Lawful basis for consent: There is a need for the requirements stated in the GDPR to be specified so everyone can understand and follow them, especially with respect to voluntariness, delineation of categories of information collected, and the scope of consent.
        - **(3)** Boundary between the Swedish Payment Services Act and credit reporting activities: This concerns new services that may affect a large number of people and that involve personal data of a privacy-sensitive nature. There is a need to clarify when the GDPR and the Credit Disclosure Act's provisions apply.

- **Additional Information:** In 2019, facial recognition will be examined. Other technology uses may also be subject to supervision such as machine learning, automated decisions, profiling and blockchain.

- ***COVID-19 Materials:*** Coronavirus and personal data (in Swedish)

A.11 Ireland

- ***Materials:***
  - Consultation Document & corresponding blog post
    - The Irish Data Protection Commission (DPC) is preparing its new Regulatory Strategy for 2020-2025. To develop their new strategy, the DPC is holding two rounds of open public consultation. The first round of consultation is on the DPC's Target Outcomes. The DPC's analysis in this first round is goal oriented: it centers on identifying what the DPC wants to achieve as a regulator rather than on what is required of them by law.
- ***Summary:*** For a more in-depth summary, click here.
  - **Priorities:** Each of the below outcomes builds on those preceding it, and the DPC strives to make progress on each outcome simultaneously.
    - ***(1) Data Protection rights and obligations are regulated consistently.*** There are three different aspects to consistent regulation:
      - (a) Consistency with how complaints, inquiries, and other matters are handled while accounting for the different contexts for those cases. The DPC has worked to apply the GDPR consistently so that people and organizations know what to expect procedurally, even while substantive legal aspects are still in development.
      - (b) Consistency with how the DPC supervises and enforces the GDPR relative to other EEA supervisory authorities.
      - (c) The availability of consistently high data protection standards for people in countries both within and outside of the EEA.
    - ***(2) There is clarity and certainty in how data protection law is applied.*** The DPC identifies clarity and certainty in how data protection law is applied as a target outcome because the GDPR, which is principles-based, does not have set legal requirements for specific contexts or technologies.
      - This creates a particular need for the GDPR to be interpreted carefully every time it is applied to those specific contexts or technologies.
      - Careful interpretation would provide stability for organizations and people, and increase the likelihood of compliance.
      - The DPC expresses particular interest in helping organizations that want to comply but are not sure how to go about doing so.

- ***(3) Organizations operate and innovate in an accountable, compliant, ethical and fair way in their processing of personal data.*** The DPC states that organizations must take accountability for how they process personal data by following the fundamental principles for personal data protection under the GDPR. (For the principles, see page 30 of the consultation document)
    - The DPC's job is to supervise how organizations take accountability for meeting these principles, which makes their regulatory approach different from regulators that supervise economic activity and from whom organizations must seek preapproval.
    - The DPC uses a multi-pronged approach to supervision, which ranges from "raising awareness to influencing to advising to authorizing to monitoring to investigating to enforcing to prosecuting."
    - As part of the activities that the DPC undertakes to effectuate this target outcome, it prioritizes the development of guidance for micro, small and medium sized enterprises by ensuring that the guidance is as practical and clear as possible.
        - This way, organizations generally don't require external advice on their compliance and accountability once they follow DPC guidelines.
- ***(4) As many people as possible understand and have control over how their personal data is used.*** The DPC is motivated by their core purpose of safeguarding data protection rights for individuals. As part of the DPC's responsibility of protecting those rights, it aims to provide as many people as possible with useful information on their rights.
    - The DPC may do so by providing support with immediate advice for people who contact them directly.
    - Other times, the DPC may contact an organization directly when someone has raised an issue.
    - To achieve as much as possible for as many people as possible, the DPC will balance their work on individual complaints with their work on issues that can affect millions of people.
- ***(5) Children are specifically protected.*** The DPC is especially passionate about safeguarding the rights of vulnerable people and most particularly the rights of children. In addition to being a vulnerable class of people, the negative impact of not meeting a

child's data protection rights can have a long-term effect into adulthood.

- The DPC will take particular care in defining the specific protections required to safeguard the data protection rights of children, and will provide guidance for people and organizations.
- The DPC also aims to initiate and actively promote the development of codes of conduct on the processing of children's personal data.

- ***COVID-19 Materials:*** Data Protection and COVID-19