EDPS

EUROPEAN DATA
PROTECTION SUPERVISOR

Shaping a Safer Digital Future

The EDPS Strategy 2020 - 2024

PDF/Volume_01 Catalogue: QT-04-20-366-EN-N ISBN: 978-92-9242-562-3 DOI: 10.2804/124494
PRINTED/Volume_01 Catalogue: QT-04-20-366-EN-C ISBN: 978-92-9242-560-9 DOI: 10.2804/290035
eBook/Volume_01 Catalogue: QT-04-20-366-EN-E ISBN: 978-92-9242-563-0 DOI: 10.2804/520028
Electronic Files/Volume_01 Catalogue: QT-04-20-366-EN-Q ISBN: 978-92-9242-561-6 DOI: 10.2804/112343

The EDPS Strategy 2020 - 2024

Shaping a Safer Digital Future

CONTENTS

Foresight

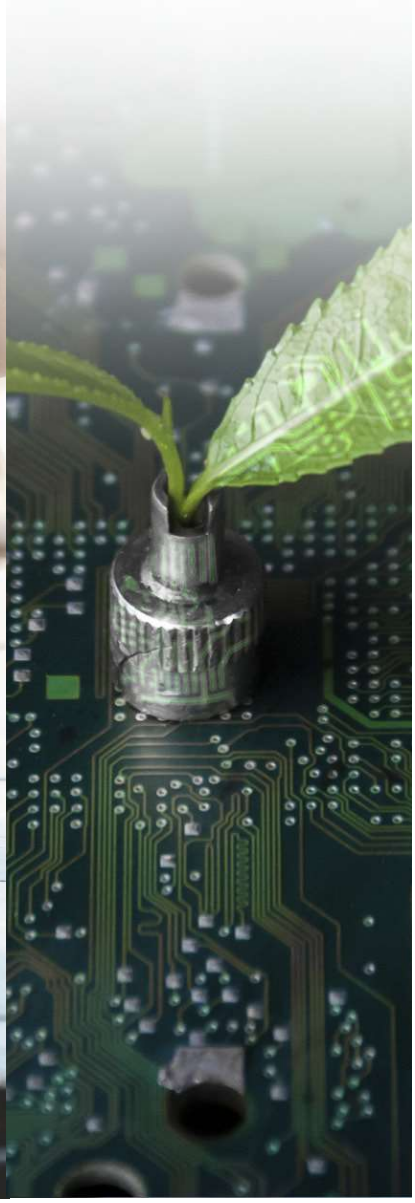
- Smart
- Trends

Action

- Tools
- Coherence

Solidarity

- Justice
- Sustainability



A new strategy for a new decade

Human rights should never be taken for granted. We must continuously work to defend and preserve them. In recent years, we have observed the fragility of the rule of law and other fundamental values in our democratic institutions that Europeans share with many other places in the world.

Bolstered by the Lisbon Treaty, which puts the EU Charter of Fundamental Rights on an equal footing with the Treaties, data protection has, in the last decade, become, a bulwark for most, if not for all democratic rights and freedoms. This is particularly important for those in a position of vulnerability, such as children and the elderly, patients or mentally ill person, asylum seekers or even employees under some circumstances of power imbalance.

Technological advances, occurring thanks to human ingenuity and ability to derive insights from experience, are, nowadays, particularly driven by personal data. The companies that have exploited these technologies have become the most valuable in the world, dominating not only their respective markets but also global information flows. Consumer choice is now very restricted and popular services have often not been designed in compliance with the EU legal framework in mind. Governments are also keen to exploit the technologies that promise innovation, efficiency and that are cost effective. At the same time, technologies designed to increase convenience and prosperity - from behavioural targeting to facial recognition - now enable authoritarian states to strengthen and export their self-serving model of surveillance, repression and censorship.

The first two decades of 21st century have also shown that digital technologies, contrary to prior expectations, have a large and increasing negative impact on natural resources, at the risk of becoming unsustainable at a time of growing environmental crisis.

The outbreak of the COVID-19 pandemic has substantially changed the circumstances in which the European Data Protection Supervisor (EDPS) was preparing its strategy and action plans. The health crisis has elevated the importance of the digital economy, as well as the need for effective guarantees concerning data protection and privacy. Communication networks, data and devices are employed today on a large scale, as part of our collective efforts to manage the crisis and restore the European economy and this will still be the case, for the months and years to come. Measures of

confinement and social distancing have greatly accelerated the pace of digital transformation. More than ever, society and the economy have come to rely on digital approaches for daily activities. The increased dependency on data and technology amplifies the pre-existing conditions of our digital ecosystem, including the concentration of market power, information asymmetries, disinformation, manipulation, data breaches and platform dominance.

The EU took a leap of courage, ambition and foresight when adopting the General Data Protection Regulation (GDPR) in 2016. This achievement followed years of intense negotiations. More than two years on, people are entitled to ask, what has changed and what will change in the years to come. Effective enforcement is an important element of any data protection framework. The enforcement regime of the GDPR marries the principles of proximity with the citizen, the independence of supervisory authorities and an obligation to cooperate constructively. Its experimental nature, between a central regulatory body and a loose grouping of national regulators, requires some adjustments. As European supervisory authorities, it is our responsibility to ensure that existing mechanisms are maximised so that the law is adequately and proportionally enforced.

Since the entry into application of the GDPR, all data protection authorities (DPAs) have started to take decisive actions in respect of controllers, large and small, who are found to have breached the rules. Despite limited resources, authorities represent the interests of individuals and their fundamental right to data protection, in the face of the largest companies in the world bound by procedural rules that often vary from Member State to Member State.

Although European Union institutions, bodies, offices and agencies are subject to the EDPR instead of the GDPR, both regulations pursue the same objectives and their principles are identical. As supervisory authorities, it is our collective responsibility to ensure that these laws are respected. Furthermore, the EDPS, as provider of the European Data Protection Board (EDPB) Secretariat, is committed to strengthen the cooperation of DPAs for high-profile enforcement cases.

We must continue to stake our claim as advocates for the fundamental rights to data protection and privacy, because it is the cornerstone of individual freedom and democracy. As the authority overseeing EU institutions and bodies (EUI), the EDPS has sought to challenge terms of service from powerful software providers that compromise the role of the EUI as controllers and the interests of citizens' right to data protection.

Europe must uphold its values in the digital world, but, as much as we need 'sovereignty', the EU also needs digital solidarity - making data work for all people across Europe's borders, especially for the most vulnerable. Digital solidarity would refuse to replicate the now tarnished and discredited business models of constant surveillance and targeting, which have been damaging the trust in the digital society. This means, engaging with the EU industrial policy to boost privacy enhancing technologies, designed in Europe and exported around the world. It is about using all the available tools, not just data protection enforcement, but also taxation and international trade, to foster a fairer and more sustainable digital Europe.

Most of all, we will use our role as supervisor, policy adviser and loyal partner of our fellow DPAs, to avoid the misuse of personal information and digital technologies. Our strategy sets out the way we intend to achieve this vision.

Wojciech Rafał Wiewiórowski

About us

Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

In order to protect and guarantee the rights to data protection and privacy, the processing of personal data is subject to control by an independent authority. The European Data Protection Supervisor (EDPS) is the European Union's independent data protection authority, tasked with ensuring that the institutions and bodies of the EU (EUI) embrace a strong data protection culture.

In accordance with Regulation (EU) 2018/1725[1] the EU as a policy making, legislating and judicial entity looks to the EDPS as an independent supervisor and impartial advisor on policies and proposed laws which might affect the rights to privacy and data protection. The EDPS performs these functions by establishing itself as a centre of excellence in the law, and in technology, insofar as it affects, or is affected by the processing of personal data.

We carry out our functions in close cooperation with fellow data protection authorities (DPAs) as part of the European Data Protection Board (EDPB), and aim to be as transparent as possible in our work serving the EU public interest. Under the General Data Protection Regulation (GDPR), the EDPS is also responsible for providing the secretariat to the EDPB.

Furthermore, the EDPS is also in charge of supervising the processing of personal data relating to activities at the EU's law enforcement agency, Europol and the EU's agency for judicial cooperation, Eurojust. The relevant legislation in this case is Regulation (EU) 2016/794, which applies to Europol and Regulation (EU) 2018/1725 and Regulation (EU) 2018/1727, which applies to Eurojust. A similar, specific data protection regime is in place for the European Public Prosecutor's Office (EPPO).

1 Whenever the provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union be interpreted homogeneously, in particular because the scheme of the EDPR Regulation should be understood as equivalent to the scheme of the GDPR; see recital 5 EDPR, referring to ECJ judgment of 9 March 2010, European Commission v Federal Republic of Germany, Case C-518/07, ECLI:EU:C:2010:125 paragraph 28.

CORE VALUES

Our approach to our tasks and the way in which we work with our stakeholders are guided by the following values and principles:

- **Impartiality** – working within the legislative and policy framework given to us, being independent and objective, finding the right balance between the interests at stake.
- **Integrity** – upholding the highest standards of behaviour and to always do what is right
- **Transparency** – explaining what we are doing and why, in clear language that is accessible to all.
- **Pragmatism** – understanding our stakeholders' needs and seeking solutions that work in a practical way.

The world around us

Global competition on standard-setting

The next 5 years could prove to be a global turning point for privacy and personal data protection. Most of the world will have a general data protection law, including the largest countries currently without one – India, Indonesia and, quite possibly, the United States. Most policy interventions addressing social, environmental and public health issues, will involve technology and data usage. Data protection will become relevant in almost every context. The Covid-19 crisis, which, initially, seemed to be a danger to such an evolution, has, instead, strengthened the call for the protection of individuals' privacy. This is especially the case when governments take measures to defend society and the economy against such an extraordinary threat.

At the same time, it becomes clear that some governments may try to attract its citizens with the vision of security, in exchange of granting public authorities the possibilities to intrude into the private sphere of citizens, to an extent that was not considered acceptable before.

We would be negligent if we failed to recognise that data protection is being tested in an unprecedented manner. There is a risk that the epidemiological surveillance (strictly necessary to fight against Covid-19) paves the way for greater calls concerning new forms of participatory and "under the skin" surveillance, for purposes other than public health.

Every day, people generate ever-increasing amounts of data through their digital activities. Its collection and reuse need to respect, first and foremost, the rights and interests of individuals, in line with European values and rules. With the GDPR, the EU has laid down a solid basis for a human-centric data economy by ensuring that individuals remain in control of their data. This has made the EU a source of inspiration for the protection of privacy in many countries worldwide.

The new decade will see the battle for industrial data, where Europe wants to play a leading role, while simultaneously redesigning some important internet protocols and standards currently in force. Business models relying on tracking, profiling and behavioural targeting are now under intense scrutiny. On occasions, models can become so invasive that public sector websites, including those of the EUI, sometimes (often unwittingly) permit the third-party tracking of visitors, without prior consent, in breach of applicable legal provisions. In response to the growing backlash against third-party cookies, there might be new methods of identifying individuals, posing new challenges to privacy and data protection.

Growing complexity in digital systems, together with tight corporate secrecy around automated decision-making, will push the user further away from how it works. Powerful controllers could retain the ability to target individuals, using personal data. While at the same time, masking or deleting explicit identifiers in those datasets in a way that makes it even harder for individuals to exercise their rights to information and access. On the other hand, edge computing could move data and services closer to users and provide new opportunities - but also risks - to improve privacy and security.

The first review of the GDPR takes place in 2020, with a particular focus on the rules for transfers of data outside the EU and the cooperation between DPAs. The EDPS, as a member of the EDPB, contributed to this reflection process and welcomes the fact that the European Commission has identified areas for improvement. The EU may have been the pioneer of such a regulation, but can no longer be regarded as the sole driver for data protection legislation. The success of the EU approach to data protection will, therefore, be constantly assessed.

Widespread surveillance

The deployment of biometric technology and various forms of facial and automatic recognition systems will have a profound impact on privacy and anonymity, as well as a chilling effect on lawful political protests and activism.

Public health management and research during the Covid-19 pandemic, increasingly relies on data and technology (e.g. contact-tracing applications for epidemiological surveillance and monitoring, AI-supported research for treatments). The extensive use of digital tools can further foster the development of innovative solutions, but also increases the potential risks for data protection and privacy, cybersecurity and human rights.

This challenges the rights of individuals, particularly when political will leads to the interoperability of resources and information systems, which sometime fail to communicate with each other.

Artificial Intelligence (AI) will be increasingly deployed in public services and criminal justice. Predictive policing and Legal Tech will become an everyday environment for law enforcement and judicial authorities, as well as other actors involved in litigations. Augmented/Virtual Reality (AR/VR) rolled out in entertainment, healthcare and retail settings, will generate highly sensitive data.

Security risks are growing. Machine-to-machine (M2M) communications are poised to expand, exponentially, in the next 5-10 years to the extent that the mere notion of M2M may replace the older Peer-to-peer (P2P) notion. The Internet of Things (IoT) will be enabled by 5G and, gradually, 6G technology. The proliferation of devices and data raises almost unlimited privacy and data protection concerns, extending the risk surface for criminal and state-sponsored hacking to gain access to protected information, disrupt services and extort money. Industrial control networks within the energy, telecommunications, water, and transport sectors will be potential targets. Targeted offensive cyber operations will increase and often go undetected.

In a period of growing environmental emergency, natural disasters will increase and backups of mission-critical applications will have to be ready for recovery and transfer to other locations, and more often than not, to other cloud servers. Election security will be of critical importance for democracies.

Post-Covid-19 world

Increased digitalisation - accelerated by the Covid-19 crisis - means an increase in data collection, not just on patients or consumers, but also in the context of education, work and social life. The current crisis will continue to affect all individuals, but it will hit vulnerable groups the hardest. The severe economic impact of the crisis might turn up the pressure on organisations to maximise their efficiency, in ways, which may come at the expense of the rights and freedoms of individuals. Merging personal data from different sources, reusing the digital traces we generate on a daily basis, can potentially lead to the blurring of boundaries and, ultimately, freedom. We remain convinced, however, that the GDPR provides for a solid legal framework guiding us through this process.

The new reality will require the data protection community to continuously engage with the process of reaching a fair balance between the need to ensure public health and the protection of privacy and personal data. At the same time, it will require the data protection community to actively contribute to the debate on facilitating the use of personal data for the public good. We will need to be both rigorous and creative. Continuously stand ready to offer tangible advice on issues and technologies that can help save lives, working in close connection with all competent oversight authorities and, in case of data processing in the health care sector, with public health authorities.

Digital solidarity means ensuring that data and technology works for all people in Europe and especially for those who are the most vulnerable. We need to make sure that the "new normal" does not give way to the permanent erosion of rights we have fought so long and hard to promote. EU data protection norms need to be part of the EU's road to recovery. At the core of the right to the protection of personal data, is the value of human dignity and control that the concerned person has over their personal data as the enabler of a free (not pre-determined or unduly influenced) life in society.

Sovereignty

Many parts of the world, including China, Russia and India, have taken measures to control the infrastructure and data generated in their jurisdictions, with rules on local data storage, restrictions on foreign inward investments and acquisitions of local companies.

We do not support the creation of artificial geographical borders, but we do have a preference for data being processed by entities sharing European values, including privacy and data protection. The EDPS is interested in policy initiatives to achieve 'digital sovereignty', where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values. At the same time, we are committed to overcome the detrimental vendor's lock-in syndrome in EUI.

Strategy pillars

Our strategy describes how we intend to carry out our statutory functions and deploy the resources available to address these challenges. There are three pillars to the strategy, each reflecting our values.

Foresight

Our commitment to being a smart institution that takes the long-term view of trends in data protection and the legal, societal and technological context.

Action

Proactively develop tools for EUI to be world leaders in data protection. To promote coherence in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden sharing and common approach.

Solidarity

Our belief is that justice requires privacy to be safeguarded for everyone, in all EU policies, while sustainability should be the driver for data processing in the public interest.

Our objectives: what we aim to achieve by the end of 2024

The strategic objectives under the three pillars express what we intend to achieve by 2024. A number of strategic initiatives will support the achievement of those objectives. We will take more actions than can be described in this strategy; all of these will appear in our Annual Management Plan for each year of this mandate. This strategy is a live, iterative document. It will be kept under regular review as a reference point for our staff and stakeholders.

1. Foresight

EDPS to be a recognised and respected centre of expertise that helps understand the impact of the design, evolution, risks and deployment of digital technology on the fundamental rights to privacy and data protection.

1.1 Smart →

We want to be a smart administration in a smart EUI environment

Knowledge is an essential asset for the EDPS to effectively support strategic objectives. However, we do not want to be a centre of excellence in a way that does not benefit the outside world. We want to share knowledge, expertise and contribute to the smart administration of the EUI environment.

Our aim is to use the best expertise and latest sustainable technology, to look after our people, promote diversity in all its forms, as well as being transparent and inclusive towards our stakeholders.

Hence, this part of the strategy is dedicated to outline the specific actions for this mandate.

To this extent, we will:

- Carefully monitor jurisprudence, pursue our interventions in cases before the Court of Justice of the European Union (CJEU).
- Make an inventory of the measures introduced by EUI during the Covid-19 crisis. Distinguishing those that have naturally developed from the measures that were only accelerated due to extraordinary circumstances. The latter should be recognised as temporary and discarded when the crisis is over.
- Plan a simple and short online training module for all new EUI staff and propose that this becomes compulsory. We will equip Data Protection Officers (DPOs) with the tools they need and help build a 'satellite' network of data protection experts.
- Organise evidence-based discussions on intrusive, emerging or hypothetical practices, such as eHealth, biometric technologies and automatic recognition systems, quantum computing, edge computing and blockchain.
- Engage with experts from the public health community in the EU and other international organisations, to better understand the needs for

epidemiological surveillance and accurately measure the efficiency and purpose of the tools being developed with regard to personal data protection (e.g. by developing together practical guidance on data protection by design).

- Continue to facilitate discussions between data protection experts, regulators and the research community, including ethics boards, to ensure that data protection enhances the efforts of genuine scientific research.

- Collaborate more closely with academia and independent researchers by setting up a research visitor programme, hosting events and supporting summer academies in close cooperation with the EDPB and other DPAs. We will encourage and facilitate more exchanges between our staff and DPAs and between DPAs themselves.

- Publish case law digests concerning data protection and privacy at EU level.

- Keep exchanging information and best practices with international organisations and interlocutors in third countries.

- To study and prioritise the impacts of data processing practices on individuals and groups, especially those in vulnerable situations, such as refugees and children.

- Invest in knowledge management to ensure the highest quality of our work and to recruit a diverse, inter-disciplinary and talented workforce.

1.2 Trends →

We want to know what is going on and what is going to happen

The EDPS places strategic importance on integrating the technological dimension of data protection into our work. As a data protection supervisory authority, we must closely examine both the potential risks and opportunities offered by these advances, understand the possibilities of new technologies and, at the same time, encourage the integration of data protection by design and data protection by default in the innovation process.

We aim to explain in a simple way the interaction between these trends, and to include data protection in the new EU skills agenda. In our work with the EDPB, as well as an advisor to the EUI, we focus on areas where the interests of data protection interacts with technology and other areas of law, including competition law, consumer law, finance and payment services.

The EDPS is uniquely positioned to monitor developments in the Areas of Freedom, Security and Justice (AFSJ). This is particularly emphasised through our role as supervisory authority of Europol, Eurojust, EPPO, Frontex, EASO[2] or eu-LISA[3].

2 EASO : European Asylum Support Office

3 The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

- We will actively follow the evolution of data processing practices and technology that may have an impact on privacy and data protection. We will continue to issue reports on emerging technology issues. Moreover, we will promote the understanding of what is the 'state of the art' of a specific technology, such as anonymisation, encryption, and network security.

- Where the European Commission proposes measures with data protection implications, we will continue to provide legal advice regarding compliance with the EU Charter and the principles of data protection set out in applicable legislation.

- We will focus on the potential impact of technology-driven policy, as recently demonstrated in our opinions on the European Commission's "White paper on Artificial Intelligence: A European approach to excellence and trust", and the European Commission's Communication on "A European strategy for data".

- Where EUI intend to deploy new technologies, we will systematically request them to clearly explain the impact of these technologies and their risks on individuals and groups.

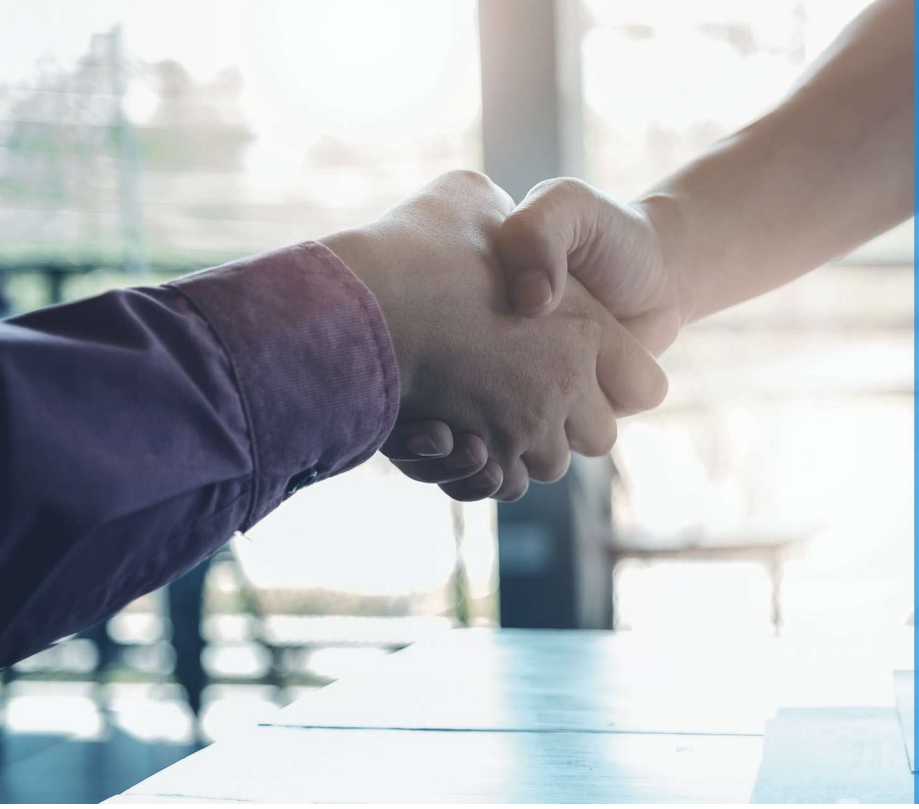
- We will alert EUI and the public when digital technology is deployed in a way that does not respect the essence of the fundamental rights of personal data protection, privacy and other rights and freedoms enshrined in the EU Charter of Fundamental Rights.

- We strive to do this in close collaboration with the European Commission, other EUI and agencies active in related areas, such as the Fundamental Rights Agency (FRA) or the European Agency for Cybersecurity (ENISA), via updated Memoranda of Understanding (MoU).

- We will build on existing initiatives such as the Internet Privacy Engineering Network (IPEN) and consolidate the network for technology expertise among data protection authorities in Europe. We aim to develop core knowledge on how essential and emerging technologies work. This will include talking to innovators in the private sector.

- We will invest special attention to the development of eHealth services at EU level.

- We will develop a consistent and targeted communications strategy with various stakeholders to address the COVID-19 pandemic's newest developments and data protection issues. In 2022, we will host a conference on how to safeguard individuals' rights in a world that will, hopefully, be recovering from this current crisis.



2. Action

EDPS to support EUI to continue to lead by example in safeguarding digital rights and responsible data processing.

2.1 Tools →

We are going to use the tools we have and develop new ones

Privacy and data protection are cornerstones in any democratic society based on the rule of law and fundamental rights. Likewise, a free internet society depends on the design of technology. This is particularly relevant whenever the EU adopts laws and policies related to the processing of personal data, or when EUI process personal data.

Personal data have and will continue to play an important role in the fight against the COVID-19 pandemic. Our laws, such as the GDPR and the ePrivacy rules, allow for the processing of personal data for public health purposes, including in times of emergency. Data protection law is well-equipped to help support the public good, and do not represent an obstacle, in fighting the virus. It is certainly possible to build technological solutions, which are compliant with the legal data protection framework. Some recent application show that societies can take up technologies while upholding privacy and data protection rights. It remains paramount that EUI and Member States continue to actively engage with DPAs.

Certain processing activities are however, by their nature, highly risky, they may even violate the essence of fundamental rights and freedoms and should be suspended or stopped altogether, i.e. when broad internet content monitoring interferes with privacy and freedom online. Being a supervisory authority, we must be equipped to monitor and anticipate problems and quickly respond to operational situations, policy and legal questions. We recognise DPOs' of EUI as the emissaries of positive change in how data is handled.

The outsourcing of tasks by EUI to providers of communications services and digital tools is an operational reality, and often a necessity. This, however, creates risks for data protection and good administration, particularly where there are few or no viable alternatives to monopoly providers with questionable standards on privacy and transparency.

The EU and European public administrations have considerable leverage to bring about real change to business models which are not consistent with EU values, fundamental rights and data protection rules. This was

particularly relevant when an enforcement action was launched in 2019 concerning EUI contracts with software providers. There is now a renewed appetite for coordinated support to the European industry and for data to be processed according to our European values.

In this sense, our commitments are as follows, we will:

- Promote data protection by design and by default, to be implemented irrespective of the technology deployed or the political priorities.

- Develop effective oversight mechanisms, particularly on technologies and tools, when these are deployed in the common fight against COVID-19, to empower and not control, repress or stigmatise citizens.

- Contribute to developing strong oversight, audit and assessment capabilities for technologies and tools, which are increasingly "endemic" to our digital ecosystem (e.g., profiling, machine learning, AI). We will provide guidance on personal data processing using automated decision-making systems and AI.

- Support the idea of a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place.

- Reinforce the central role of the controller in relation to processors and sub-processors in EUI, both by raising awareness and, more formally, by providing advice on possible standard contractual clauses.

- Aim to minimise our reliance on monopoly providers of communications and software services, to avoid detrimental lock-in and work with other EUI and other public administrations in the EU so they can do the same. We will call on EUI and other public administrations in the EU to review their external contracts on digital products, software, services and technology to achieve compliance as required by EU data protection laws. We will explore how to deploy free and open source software and solutions.

- Review previous authorisations for transfers to third countries and adopt standard data protection clauses.

- Continuously assist EUI by demonstrating and developing bespoke privacy tools and solutions. This also involves giving advice when Data Protection Impact Assessments (DPIAs) are necessary.

- Publish standardised information about personal data breaches that are notified to us, including the types of organisations involved and the number of people affected.

- Use our enforcement powers to ensure EUI websites and mobile apps are complying with EU law, particularly in respect of third party tracking.

- Closely monitor the ongoing process that makes EU systems 'interoperable', with a particular focus on the access and processing of personal data (Europol, Frontex et al.), in collaboration with national supervisory authorities where needed, to ensure effective supervision.

- Launch, explore and explain, as a follow up to the 'Necessity Toolkit' and 'Guidelines on Proportionality', the concept of the 'essence' of the rights to privacy and data protection, based on the jurisprudence of the Court of Justice and growing scholarship in this area.

2.2 Coherence →

We do not protect data - we protect human beings

The GDPR is directly applicable throughout the EU. Nevertheless, it provides Member States with the possibility to further legislate their respective laws. This could compound the fragmentation of national approaches. The EDPB exists to check and avoid such fragmentation.

The EDPS has a unique dual role as a full member and provider of the EDPB's secretariat. We will exercise this role creatively, seeking to represent the wider EU interest, and contribute to the success of the EDPB, as well as ensuring the consistent application and enforcement of the GDPR and the Data Protection Law Enforcement Directive. We aim to develop with other DPAs a common set of tools.

The EU has not completed its updating of the data protection framework for the digital age. EU legal gaps remain, where specific data protection rules are either absent – for the processing of personal data by the Common Foreign and Security Policy (CFSP) mission as referred to in Articles 42(1), 43 and 44 TEU, or fragmented police and judicial cooperation in criminal matters, as well as Europol and EPPO. Such a situation undermines the possibility of achieving a consistent approach to protecting individual's personal data in the EU. We will interpret the applicable rules in the spirit of the EDPR, and we will apply the principles of the Regulation in areas where specific rules are missing.

We need up-to-date - but also technologically neutral - rules on the protection of confidentiality of electronic communications. Sustainable economic growth cannot be achieved through the infinite monetisation of people's private conversations or indiscriminate retention of all communications data.

Personal data supports privacy, as well as other rights and freedoms, such as freedom of expression and non-discrimination. We recognise the synergies between the enforcement of data protection and other rules applicable to the digital economy, especially concerning consumer and competition law, and will carry on our work to ensure that they are mutually reinforced.

EUI are already making use of new and emerging technologies. In the interest of a coherent approach throughout the EU, the EDPS recommends that any new EU regulatory framework, such as potential AI, will apply both to EU Member States and to EU institutions, offices, bodies and agencies.

Data protection and privacy are the foundations for democracy in a time of digitisation. To this end, we will:

- Continue to build the capacity of the EDPB, both as a member and as a provider of its secretariat, to ensure that, by 2025, the GDPR is recognised as a model for all democracies around the world - a formidable blueprint to strengthen the trust and respect in the digital society.

- Call for a stronger expression of genuine European solidarity, burden sharing and common approach to ensure the enforcement of our data protection rules. The EDPS supports the establishment of a Support Pool of Experts within the EDPB, which would assist DPAs dealing with resource-heavy and complex cases.

- Contribute to the review of Regulation (EU) 2018/1725, scheduled for April 2022, and make a strong case to address the gaps and discrepancies that continue to exist. In the meantime, the EDPS will interpret any specific rules in the spirit of Regulation (EU) 2018/1725.

- Closely monitor the use of new tools involving data analytics and artificial intelligence by Europol and other agencies in the AFSJ, in compliance with the mandate assigned to them by law, while promoting solutions to protect individuals' rights and freedoms.

- Call for a coherent approach regarding new EU regulatory frameworks on the use of new technologies so that EUI are subject to the same rules as those applied in EU Member States.

- Supervise EPPO as new actor in the criminal justice area, and especially its relations with Europol and Eurojust.

- Call for the adoption of the proposed ePrivacy Regulation, but not to the detriment of existing protections.

- Contribute to the establishment of the Digital Single Market where European rules on privacy and data protection, as well as competition law, are fully respected. We will also make sure that the rules on the access and use of data are fair, practical and clear.

- Develop European and international cooperation measures, and promote joint enforcement actions and active mutual assistance, by concluding - when necessary - Memoranda of Understanding with DPAs.

3. Solidarity

The EDPS promotes a positive vision of digitisation that enables us to value and respect all individuals. The full potential of data shall be dedicated to the good of society and with respect to human rights, dignity and the rule of law.

3.1 Justice →

We actively promote justice and the rule of law.

Solidarity, being aware of shared values, interests and objectives, is at the heart of the EU project. As an EU institution, the EDPS is committed to upholding the rule of law and democracy. As an independent data protection supervisory authority, we act in line with these values. When we believe that these are threatened, we speak up, and vigorously defend them. Likewise, we take action if the independence of other DPAs and the 'collective independence' of the EDPB are jeopardised.

When planning strategies on democracy and human rights, the EU should promote digital justice and privacy for all. Privacy and data protection can never be traded for access to essential services. Data protection is one of the last lines of defence for vulnerable individuals, such as migrants and asylum seekers approaching EU external borders. Although the EU has accumulated a patchwork of measures in the areas of police and judicial cooperation and border management, the legal framework remains fragmented, creating unnecessary discrepancies. This puts unwarranted constraints on the EDPS' supervisory and enforcement powers.

Fundamental rights are necessary because they protect those less likely to have the means to fully defend themselves. In the so-called gig economy, workers and consumers find themselves governed by algorithms that make decisions based on data collected about them, with limited ability to understand or challenge those decisions. Women, people of colour and those with disabilities are routinely discriminated against, and this is reinforced by the proliferation of algorithmic decision-making.

We recognise the need for individuals to have greater control over whether data about them is collected, and, if so, how and for what purpose their personal data is processed. Where the digital environment becomes more complex, responsibility falls on controllers and enforcers to avoid any data practices that harm the rights or interests of the individuals concerned. The burden of proof should not fall on those individuals to understand risks and take action.

In complex scenarios, 'consent' should not be relied upon because it indicates obvious power imbalances between the controller and the individual's rights to data protection. We are convinced that EU data protection legislation provides other lawful grounds for processing.

A misguided debate continues on the appropriateness of the concept of personal 'data ownership'. This is unlikely to be compatible with the Charter of Fundamental Rights and will not empower individuals in a digitised society. We believe data protection 'disrupts' the markets for personal data, where data as a commercial or political asset is monetised or used to manipulate people. DPAs acting collectively should be an agent for such positive changes.

In this context, we will actively:

- Stress that privacy and data protection are an integral part of the rule of law and can never be treated in isolation. We will take actions if the independence of other DPAs or the 'collective independence' of the EDPB are jeopardised.

- Advocate for the fundamental rights to data protection and privacy to be at the heart of the Conference on the Future of Europe. We will also support the efforts to integrate data protection considerations in the European Democracy Action Plan, as a safeguard for independent journalism, lawful dissent and political activism.

- Continue to enforce EUI compliance with the rules, to protect those who are in a position of weakness, such as minors or displaced persons near or at the EU's external border. Indeed, they have as much of a right to data protection and privacy as anyone else.

- Identify discrepancies in the standards of data protection within EU law in the Areas of Freedom, Security and Justice (AFSJ) and we will consistently enforce the rules.

- Encourage the European Commission to further harmonise the data protection rules on processing operational data (Chapter IX of the Regulation 2018/1725), including in the context of the Europol Regulation review

- Advise EU lawmakers to safeguard data protection and privacy in the New Pact on Migration and Asylum.

- Keep contributing to the European Commission's proposals related to combatting discrimination.

- Provide guidance to EUI on policies and measures (such as the Digital Services Act) that hold private companies accountable for manipulation and amplification serving private gain, but to avoid blanket monitoring and censorship of speech that inevitably interferes with the rights to privacy and data protection.

- Building on our experience with the Digital Clearinghouse and other fora, we will work with the EDPB, the European Commission and the relevant EUI to establish practical cooperation and joint enforcement between digital regulators on specific cases and learn lessons from the past.

- Actively contribute to the development of a common EU vision on digitisation and technology. For example, determining how AI can be used for humankind and re-engineered along the lines of EU

rights and values and alongside strict liability rules; so that manufacturers and controllers are held responsible for damage caused by defects in their products, even if the defect resulted from autonomous decisions after its entry on the market. In the interest of a coherent approach throughout the EU, the EDPS recommends that any new regulatory framework should apply to both EU Member States and EUI. Where EUI use AI, they should be subject to the same rules as those applied in EU Member States.

- Regularly engage in the debate on digital ethics, emphasising the need to not only comply with the law, but to also consider the effects of data processing by controllers in EUI and elsewhere, on individuals, groups and society; including shared values and the environment.

- Promote diversity in all discussions on data protection, including those we organise ourselves. We will ensure gender balanced representation among speakers and panellists in the

3.2 Sustainability →

We know there is only one world

Data processing and data protection have to go green.

The EDPS is a socially-responsible organisation. Our values are to treat people – our employees, the people whose activities we supervise, the individuals whose data is processed by EUI, our stakeholders - and the natural environment around us, with respect.

The ongoing development of AI and blockchain based technologies, as well as illegal tracking and profiling of individuals generate an increasing amount of dangerous waste, due to short-lived connected goods, combined with exponential carbon footprint emissions. This is a great source of concern in light of the EU Green Deal and data protection in this new decade.

Enforcing personal data minimization and responsible data processing can be part of the solution to help counteract these damaging trends. There should be competition on the most beneficial ways to use data, not on who can collect the most.

The redistribution of wealth and its practical application are bound to change with the continuous evolution of social norms, politics, and culture. As highlighted by the EDPS' Preliminary Opinion on scientific research and data protection, there is growing concern about how digitisation has contributed to the exponential growth in data generation; while also concentrating the control of the means for converting that data into valuable knowledge in the hands of a few powerful private companies. There are growing calls for regulated access across the EU to privately-held personal data for research purposes exclusively serving the public interest to improve health care, advance health research and address the climate crisis or growing social inequalities. While the Open Data Directive organises the access to public sector information to foster competition and economic innovation; access to privately held data by non-profit stakeholders to foster social and solidarity innovation and scientific research in the public interest deserves specific attention as well. Current barriers to such access reveals the need for a broader debate on a data redistribution policy for the digital age, to maximise societal benefits of data sharing initiatives, in compliance with the European fundamental rights framework.

To address these challenges, we will:

- Convey a deeper understanding of the impact of digitisation on our world.
- Encourage broader and long-term view of the future of data protection in a period of environmental crisis, growing inequalities and geopolitical tensions.
- Pay particular attention to our energy consumption, emissions due to the travelling of officials (missions), procurement and commuting to and from work, promoting telework.
- Engage in the debate on data sharing to advocate for a data redistribution policy for the digital age based on a rigorous proportionality tests and appropriate safeguards - including anonymisation and pseudonymisation - against misuse and unlawful access.

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

0100010101 1010101110010 0110111 01110000010010101100001011011100010000