BRIEFING

EU policies – Insights

European Parliament

Understanding EU data protection policy

SUMMARY

The datafication of everyday life and data scandals have made the protection of personal information an increasingly important social, legal and political matter for the EU. In recent years, awareness of data rights and enforcement expectations have both grown considerably.

The right to privacy and the right to protection of personal data are both enshrined in the Charter of Fundamental Rights of the EU and in the EU Treaties. The entry into force of the Lisbon Treaty in 2009 gave the Charter the same legal value as the Treaties and abolished the pillar structure, providing a stronger basis for a more effective and comprehensive EU data protection regime.

In 2012, the European Commission launched an ambitious reform to modernise the EU data protection framework. In 2016, the co-legislators adopted the EU's most prominent data protection legislation – the General Data Protection Regulation (GDPR) – and the Law Enforcement Directive. The framework overhaul also included adopting an updated Regulation on Data Protection in the EU institutions and reforming the e-Privacy Directive – still under negotiation between the co-legislators.

The European Parliament has played a key role in these reforms, both as co-legislator and author of own-initiative reports and resolutions seeking to guarantee a high level of data protection for EU citizens. The European Court of Justice plays a crucial role in developing the EU data protection framework through case law.

In the coming years, challenges in the area of data protection will include balancing the compliance and data needs of emerging technologies, equipping data protection authorities with sufficient resources to fulfil their tasks, combating child sexual abuse material online without compromising privacy, taming digital surveillance and further clarifying requirements of valid consent.

This is a further updated edition of a briefing of January 2022, which updated an earlier briefing *by Sofija Voronova, of May 2020.*

In this Briefing

EPRS | European Parliamentary Research Service

Author: Hendrik Mildebrath

Members' Research Service

PE 698.898 – January 2023

EN

Introduction

The volume of data being produced worldwide is growing rapidly. It is expected to grow from 33 zettabytes, i.e. 10^{21} bytes or one thousand billion gigabytes, in 2018, to 175 zettabytes in 2025. The daily number of clicks on e-commerce sites, social media platforms and other online services has helped create a shadow economy of data exposing human behaviour and preferences that are freely available to large commercial technology companies. Access to such data is power: behaviour or decisions can be manipulated for commercial purposes or political gains, often without the users' awareness or choice. The Facebook–Cambridge Analytica scandal revealed the extent to which the collection and profiling of personal data had fed algorithms affecting the outcome of democratic elections. Emerging, data-intensive technologies, such as artificial intelligence and the internet of things, further exacerbate concerns over rights violations. These developments have brought the relevance of data protection law and its reform to the fore in the public consciousness.

Public awareness

Heightened awareness of privacy breaches, increased use of online social networks, and a rise in the public exercise of data rights all indicate the growing relevance of data protection for EU citizens. An increasing number of EU individuals aged 16-74 use the internet at least weekly, (87 % in 2021). A 2021 Special Eurobarometer on Digital Rights and Principles revealed that the use and abuse of personal data ranks among the top three most worrying aspects of the widespread adoption of digital tools and the internet. According to a 2019 Special Eurobarometer survey on the GDPR, 78 % of respondents are either concerned or 'very concerned' about the control of their personal data provided online. Only 22 % of respondents who use the internet said that they always feel informed about the terms and conditions under which the personal data they provide online is collected and used. Conversely, the survey showed that 67 % of respondents know about the GDPR and that the number of those aware of the existence of a public authority responsible for protecting their personal data rights increased by 20 percentage points from 2015 to 2018. Respondents in Estonia, the Netherlands and the United Kingdom (UK) were most likely to have exercised their data rights, while respondents in Czechia and Slovenia were least likely to have exercised theirs. According to a 2019 expert group survey, requests to exercise data subjects' rights have increased in volume in both the private and the public sector and have become more wide ranging since the entry into force of the GDPR. Moreover, both the expert group survey and the EU Fundamental Rights Agency's (FRA) 2019 Fundamental rights report point to a significant increase in the number of complaints submitted to EU Member States' national data protection authorities (DPAs). Following complaints by individuals and organisations, several DPAs have launched actions against companies under the GDPR, including for lack of transparency, facial recognition, dating apps, transparency obligations, on location data, data breaches, children's data on Instagram, and WhatsApp.

Legal framework

Historical developments

A right to protection of personal information or data is not a recent phenomenon in Europe. After World War II, the 1948 Universal Declaration of Human Rights included a right to freedom from 'arbitrary interference with ... privacy, family, home or correspondence', while the 1950 European Convention on Human Rights included a right to respect for private and family life. In 1970, the German *Land* of Hessen introduced the first law in Europe to specifically address protection of personal data. Sweden introduced the first national data protection laws in 1973, followed by Germany in 1977 and France in 1978. These laws were introduced both in response to surveillance regimes imposed by the state (Germany) and as an expression of a strong privacy culture (France and Sweden). In May 1975, the European Parliament adopted a resolution on the rights of individuals to data protection, stating that protection of these rights was a Member State responsibility. The 1980s saw attempts to approximate the growing number of national personal

data protection laws through adoption of Organisation for Economic Co-operation and Development (OECD) guidelines in 1980 and a Council of Europe convention in 1981. The latter, referred to as Convention 108, was the first binding international instrument to protect individuals against potential rights abuses arising in the course of data processing. It was signed by all Council of Europe members (including all EU Member States), and by Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay, and was updated by Protocol CETS No 223 in October 2018. In 1995, the Data Protection Directive 95/46/EC (DPD) became the first and main EU legal instrument protecting personal data prior to the GDPR. The DPD aimed at improving the internal market and addressing fundamental rights protection gaps in Member State laws.

Data protection reforms

In 2012, the Commission proposed a data protection reform package that included a reform of the DPD (giving birth to the GDPR) and a draft directive on data processing for law enforcement purposes (hereafter referred to as the Law Enforcement Directive). The Commission considered an overhaul of the rules to be necessary for achieving a greater degree of harmonisation (estimated at the time to save approximately €2.3 billion a year for companies in administrative burdens alone), and for ensuring that the right to personal data protection could be upheld in 'today's new challenging digital environment'. The GDPR (Regulation 2016/679) entered into force on 24 May 2016, but did not fully apply until 25 May 2018, giving businesses, organisations and public authorities two years to meet their new obligations. The Law Enforcement Directive 2016/680 entered into effect in May 2016, with a similar two-year timeframe for implementation; it had to be transposed into national laws by 6 May 2018. In January 2017, the Commission launched proposals for a regulation on data protection in the EU institutions and a regulation on e-privacy, focusing on electronic communications. Negotiations on data protection in the institutions have concluded; Regulation 2018/1725 entered into force in November 2018, while negotiations on the e-privacy reform are still ongoing.

Controllers and processors

The GDPR refers to the businesses, organisations and other entities collecting or processing data as 'controllers' or 'processors'. **Controllers** determine the purposes and means for processing, while **processors** process the personal data on behalf of the controllers**.** Controllers and processors without an establishment in the EU must designate a representative within EU territory.

Two or more controllers can be involved in determining the means of processing, and are referred to as **'joint controllers'**. Despite Case C-40/17 *Fashion ID* confirming that a website featuring a Facebook 'Like' button can be a joint controller with Facebook, confusion has persisted over the delineation of responsibilities between joint controllers. The Council of the EU has called on the DPAs and the European Data Protection Board (EDPB) to clarify these rules. On 2 September 2020, the EDPB adopted guidelines on these concepts, which were further updated in July 2021.

General Data Protection Regulation

The GDPR is arguably the most high-profile and well-known EU legal instrument on data protection. Given its history, it is considered an 'evolution, rather than a revolution' in EU data protection legislation.

Principles. The GDPR is a **technologically neutral** legal instrument, as the same rules apply to companies and organisation regardless of the techniques used to collect or process data; CJEU case law has affirmed this interpretation. It is an **omnibus** regulation, as it is not sector specific, though other sector-specific rules do exist for law enforcement and electronic communications. Academics also consider the GDPR a **risk-based regulation**, where the achievement of its policy objectives (i.e. free movement of data and fundamental-rights protection) is sought by targeting the regulation of activities that pose the highest risks to attaining those objectives.

Scope. According to Article 3 GDPR, the rules apply to companies established in the Union and to companies not established in the EU, which are processing data of EU data subjects in connection with behavioural monitoring or certain commercial activities in the Union. Protection extends to EU residents, i.e. both EU citizens and non-citizens who are resident in the EU. Only **personal data** fall

within the scope of GDPR protection. Data are considered 'personal' when they can directly or indirectly allow identification of a natural person, such as through a name, an identity (ID) number or location data. The CJEU has classified an IP address and written answers submitted by a candidate in an exam as personal data.

Lawful grounds for processing data. To be subject to GDPR obligations, the processing of personal data does not necessarily have to be performed with automated means, and can include collecting, recording, organising, storing, using, consulting, making available, or erasing data.

Processing can only be carried out on the basis of one of **six specified legal grounds** in Article 6 of the GDPR. These are i) 'freely given, specific, informed and unambiguous' consent of the data subject (i.e. the person whose data is being processed), ii) performance of a contract, iii) compliance with a legal obligation, iv) protection of the 'vital interests' of the data subject, v) performance of a task in the public interest, or vi) legitimate interests that override the fundamental rights of the data subject. The processing of particularly sensitive data, such as race, political opinions, religious beliefs, trade union membership or biometric data, is generally prohibited by the GDPR, but its Article 9(2) sets out some exceptions (explicit consent of the data subject, protection of vital interests of the data subject, data made public by the data subject, substantial public interest, etc.).

Data rights. Chapter III of the GDPR sets out data subjects' rights, including the right: to know what data a company has collected about them if they request them (right of access); to have wrong information corrected; and to request the deletion of any data not required to be kept for specific reasons, such as public interest (the right to be forgotten, also known as the right to erasure); to limit the controllers' uses of their data; the newly introduced right to data portability; and the right not to be subject to automated individual decision-making.

New obligations for companies include notification of a personal data breach to controllers and DPAs within 72 hours, and the designation of a data protection officer whose tasks include advising the controller and processor and cooperating with the relevant DPA. On 14 December 2021, the European Data Protection Board (EDPB) adopted its final guidelines on examples of personal data breach notifications.

The **DPAs** (also referred to as supervisory authorities) are independent public authorities responsible for supervising and monitoring the application of data protection laws in their territory. Their powers, tasks and responsibilities are set out in full in Chapter VI Section 2 of the GDPR, which expanded these powers considerably. Consequently, the DPAs' **new powers** include investigative powers for unannounced inspections (Article 58(1)) and the powers to fine a company up to 4 % of their total worldwide annual turnover for certain infringements (Articles 82 and 83). The DPAs provide expert advice on data protection issues and handle complaints regarding breaches of the GDPR or other relevant legislation. The 1995 Data Protection Directive introduced a decentralised enforcement system requiring that each Member State have its own DPA(s), which the GDPR maintains. The GDPR establishes a 'one stop shop mechanism' allowing companies to deal with a single DPA in cross-border data protection cases. This will usually be the DPA of the Member State where the company in question has its main or only establishment in the EU.

The **EDPB**. The GDPR establishes a new European Data Protection Board (EDPB) to replace the Article 29 Working Party (AW29) as the independent legal body bringing together representatives of all Member State DPAs and the European Data Protection Supervisor (EDPS). The EDPB's key responsibilities include adopting binding decisions on certain matters, advising the Commission on third-country data transfer agreements and issuing own-initiative or requested reports on best practices for the consistent application of the GDPR.

Remedies. Data subjects can lodge a complaint against a controller or a processor, or can mandate a not-for-profit body or organisation to lodge the complaint on their behalf. Complaints can also be lodged against a DPA where it fails to handle a complaint or inform the data subject about the progress of their complaint within three months of it being lodged. Compensation is available for

individuals who have suffered material or non-material damage. Article 80(2) of the GDPR, in conjunction with national legislation, allows non-governmental organisations (NGOs) to pursue **collective rights actions** without requiring a direct mandate by individuals. According to a non-binding opinion of Advocate General Richard de la Tour, Article 80(2) of the GDPR does not preclude Member States from empowering associations to plead objective breaches of data protection law without their being a need to claim the existence of actual cases affecting named individuals. Civil society and consumer organisations consider these provisions particularly important for making GDPR protection a 'reality for individuals' and for contributing to the development of harmonised jurisprudence and implementation of the GDPR. Representative actions so far have included complaints to DPAs, requests for injunctions and claims for compensation in court.

Data processing for law enforcement purposes

The Law Enforcement Directive or LED (Directive 2016/680) applies fully from 6 May 2018. It belongs to the same data protection reform package as the GDPR and aims to protect personal data when it is processed by Member State police or law enforcement and criminal justice authorities, and to improve cooperation in the fight against terrorism and cross-border crime. The directive covers both personal data-processing at domestic level and cross-border sharing of personal data between Member States. **Obligations for governments** include establishing time limits for the erasure of personal data or arranging for a regular review of the need to store such data. **Rights of individuals** include the right to have certain information made available to them by law enforcement authorities, including the name and contact details of the controller and the reasons for which their data are being processed, as well as the right to request access to and correction or deletion of their personal data. The Commission identified 10 legal acts that require further alignment with the LED and has tabled the first legislative initiatives. In July 2022 the Commission adopted a first report on the application and functioning of the LED assessing Member States' transposition efforts. Overall, it considered that the LED had been transposed in a satisfactory manner and that it was too early to revise it. It also noted several outstanding issues and offered some guidelines.

Data protection in the EU institutions

Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union's institutions, bodies, offices and agencies and on the free movement of such data updates the data protection rules for data processing by EU institutions and bodies, to align them with the provisions of the GDPR and the Law Enforcement Directive. This regulation also establishes the formal duties of the EDPS, the authority responsible for ensuring the effective protection of individuals' rights when their personal data is processed by or on behalf of EU institutions and bodies (Articles 52(1) and 52(3) of the regulation). The other tasks of the EDPS are set out in Article 57 of the regulation and include promoting public awareness of the risks, rules, and rights in relation to processing, particularly for activities involving children, and monitoring the development of technologies that have an impact on personal data protection.

e-Privacy legislation

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the **e-Privacy Directive**) aims at harmonising national provisions and providing specific rules for electronic communications services. Unlike the GDPR, the e-Privacy Directive applies to the data of both natural and legal persons (i.e. individuals and companies), and applies specifically to the data processed in connection with the provision of electronic communications services. In January 2017, the European Commission tabled a proposal for a regulation on privacy and electronic communications to replace the e-Privacy Directive. The proposed regulation aims to achieve greater harmonisation, define clearer rules for tracking technologies, such as cookies, and expand the scope of the current directive to include internet-based communications services that do not rely on traditional networks (OTT services). While the Parliament adopted its position in October 2017, the discussions in Council were stalled for

approximately four years. After several redrafts, the Member States agreed on a mandate for negotiation with the European Parliament and trilogues began on 20 May 2021. In contrast to the Parliament's position, the Council (arguably) proposes to broaden exceptions to the general prohibition on processing electronic communications data, to expand the grounds for the collection of information from end users' terminal equipment, and to legitimise the practice of making access to websites conditional on consent or payment (cookie walls). While industry trade associations welcome the Council's position, civil rights organisations urge the European Parliament to push back and ensure a high level of privacy and confidentiality. The EDPB considers that the Council position risks lowering the protection standard below the pre-existing standard under the e-Privacy Directive. The German Federal Commissioner for Data Protection and Freedom of Information was 'stunned' by the 'severe interferences with citizens' fundamental rights' and warned that several 'red lines in the area of data protection would be crossed'. There have been reports that the Commission may withdraw the proposal, but the Commission has not shown intentions to this effect.

Data protection outside the EU

EU data protection rules apply to the European Economic Area (EEA), which includes all EU Member States plus Iceland, Liechtenstein and Norway. When personal data are transferred outside the EEA, safeguards in Chapter V of the GDPR must be fulfilled to ensure that protection travels with the data.

Data transfers

Adequacy decisions. Article 45 of the GDPR regulates the most convenient mechanism to transfer data to third countries outside the European Economic Area (EEA). Where the European Commission, by means of an implementing decision on data adequacy, recognises that a foreign country's level of data protection is essentially equivalent to that of the EU, economic operators may conveniently transfer data to the importing entity located in a third country. The adoption of an adequacy decision requires: a proposal from the Commission; a non-binding opinion from the EDPB; approval from Member State representatives and the final adoption of the decision by the Commission. The Parliament and the Council can, at any time, request the Commission to maintain, amend or withdraw an adequacy decision, whenever they perceive the Commission to have exceeded its implementing powers. Adequacy decisions are to be reviewed at least every four years. The Commission is currently preparing the evaluation of existing adequacy decisions.

So far, the Commission has approved adequacy decisions for Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK, under the GDPR and the LED, and Uruguay. The Commission has referred to adequacy decisions as '**digital diplomacy**', considering them a means for exporting EU data protection values and standards worldwide. Data exchanges in the law enforcement sector are covered by the Law Enforcement Directive.

Alternative transfer tools. Adequacy decisions are not the only means for transferring personal data outside the EEA. Other GDPR tools include binding corporate rules, standard data protection clauses adopted by the Commission, and approved codes of conduct and certification mechanisms for processors and controllers. The Council has noted that these tools sometimes 'better meet the needs of individual controllers and processors in a specific sector'.

Privacy Shield framework. On 16 July 2020, the CJEU derailed EU-United States personal data transfers, by invalidating the US adequacy decision, the keystone of the broader Privacy Shield framework. Contrary to the Commission, the Court held that the USA does not provide

Data protection and Brexit

To sustain the flow of personal data between the EU and the UK, the Commission adopted two UK adequacy decisions following the UK's withdrawal from the EU. The draft adequacy decision was already heavily criticised by Parliament and commentators. The UK currently aims to develop separate and independent pro-tech data policies. If these diverge significantly from EU standards and lower the overall level of protection, the Commission may repeal, amend or suspend the UK adequacy decisions, which could be costly for both the EU and UK economies.

for an adequate level of data protection on account of invasive US surveillance programmes. While companies may resort to alternative transfer mechanisms, the ruling exacerbated the legal uncertainties and costs associated with these tools. Most notably, businesses would need to compensate the shortfall in US data protection with additional legal, technical and/or organisational safeguards. The EU-US negotiators are in the process of setting up a follow-up framework, the EU-US Data Privacy Framework. The US components of the framework have met with serious criticism from civil society organisations. The Commission expressed optimism about the US framework, has published a positive draft adequacy decision and has launched the formal adoption procedure.

Data protection worldwide

The GDPR has been praised and criticised for its **standard-setting** role and has been used as a model for law reform worldwide. Several countries and regions have taken inspiration from the GDPR when adopting their national legislation, while some multinationals have opted to use the GDPR as their global standard of operation. However, such legislation may still differ significantly from the GDPR in practice, particularly where legal traditions differ or where economic priorities inform the drafting.

The role of the European Parliament

During its **2014-2019 term**, the European Parliament played a key role in reforming data protection law and policy in the EU, in many different ways:

- **Legislative procedures**. Parliament has continuously advocated a high level of data protection in the abovementioned legislative procedures concerning, for instance, the GDPR, the Directive on the use of passenger name records (PNR) and the pending e-Privacy Regulation. The Belgian Constitutional Court, the Cologne District Court and the Wiesbaden Administrative Court (joined cases C-215/20 and C-222/20) referred cases to the CJEU concerning the PNR Directive for a preliminary ruling. In a first judgment of 21 June 2022, the Court ruled that the directive is valid, but needs to be interpreted strictly so as not to undermine its validity. For more information, see the critical position of the EDPB and a commentator.
- **Scrutiny of Commission decisions**. Parliament actively followed Commission negotiations on adequacy decisions, adopting resolutions on transatlantic data flows (2016), on protection afforded by the EU-US Privacy Shield (2017 and 2018), as well as on the adequacy of personal data protection afforded by Japan. In its 2018 resolution, it raised multiple concerns, including on the misuse of Facebook users' data, and called for the suspension of the Privacy Shield until the US authorities complied fully with EU data protection legislation.
- **Approval of international agreements**. Parliament was involved in the approval process of other international agreements, including the EU-US Data Protection Umbrella Agreement, and the EU's Passenger Name Record (PNR) agreements with the USA and Australia. It will similarly be involved in any PNR agreement with Japan; in February 2020, the Council authorised the Commission to begin negotiations. Parliament played a crucial role in the **EU-Canada PNR Agreement**, where it sought a CJEU opinion before giving its consent under Article 218 TFEU. The CJEU found that the agreement interfered with fundamental rights to data protection and privacy, going beyond what could be justified for fighting terrorism. This prompted the Council to launch new negotiations with Canada, which began in June 2018 and are ongoing.
- **Hearings**. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) organised several hearings with industry stakeholders and experts on key data protection issues, such as trade agreements and data flows, a new EU-US Privacy Shield post-Schrems, fundamental rights implications on big data and the e-privacy reform. Most notably, the LIBE committee held a three-part hearing in 2018 on the use of Facebook user data by Cambridge Analytica in elections, which focused on mapping the case, consequences and policy solutions and remedies, following a Parliament Conference of Presidents meeting with Facebook CEO Mark Zuckerberg. Zuckerberg also provided a set of written answers to the outstanding questions from his meeting with the Parliament's leaders. In October 2018, the Parliament adopted a resolution on the use

of Facebook users' data by Cambridge Analytica, urging Member States to engage with online platforms to increase awareness and transparency regarding elections.

- **Sector-specific Parliament resolutions** addressed data protection in specific sectors, especially those related to digital technologies, to ensure consistency with the more general framework. The resolutions addressed, among other things, civil law rules on robotics, big data, blockchain, European industrial policy on artificial intelligence and robotics, online platforms and the digital single market, a digital trade strategy and cybercrime.

The Parliament has continued to promote a high level of data protection and privacy during the **2019-2024 term**. It ensured the inclusion of privacy-preserving safeguards in the regulation, temporarily exempting the scanning of internet-based communications for online child sexual abuse from certain e-Privacy requirements. The Parliament also adopted two resolutions cautioning against the lenient assessment of US and UK data adequacy. Two previous Parliament resolutions, of February 2020 and June 2020, on the negotiations for a post-Brexit EU–UK Trade and Cooperation Agreement, raise concerns regarding the UK's level of data protection. In a resolution of March 2021, on the Commission's GDPR evaluation report, Parliament pointed out various lacunae in implementation. In a November 2020 resolution, the Parliament called on the Commission to launch infringement proceedings against Member States who did not repeal or align their data retention laws with CJEU case law, invalidating the Data Retention Directive (see box on the data retention issue). Furthermore, it emphasised that all initiatives announced in the data strategy should be consistent with the EU data protection and privacy *acquis*. Finally, Parliament also held a number of hearings, concerning, for instance, AI and the data strategy, common values and fundamental rights issues in the European digital strategy, and the pending data governance act.

The role of the Court of Justice of the EU

The Court of Justice of the EU (CJEU) can be considered to have played an active role in shaping the standards for data protection rights in the EU. Since 2014, its decisions have emphasised the importance of firmly upholding data protection and privacy rights as an intrinsic feature of EU democracies. One of the first landmark cases in this regard was the CJEU's ruling in Case C-131/12 (*Google Spain*), where it affirmed the existence of a 'right to be forgotten' for EU citizens, namely that they have a right to request search engines such as Google to take down links to personal information when this information is 'inadequate, irrelevant or no longer relevant'. This right has since been enshrined in Article 17 of the GDPR.

More recently, the CJEU has had to address cases dealing with the scope of EU data protection rules. In Case C-507/17 (*Google* v *CNIL*), the CJEU limited the geographical scope of the 'right to be forgotten' under the GDPR, by deciding that a search engine is not necessarily required to implement GDPR obligations on all its versions worldwide. This decision was criticised for being inconsistent with other recent case law, where no territorial limitation was stipulated for Facebook's obligation to remove or block illegal content online under the 2000/31 e-Commerce Directive.

Another important recent CJEU decision concerns the concept of consent: in Case C-673/17, the CJEU ruled that consent must be actively given, and that 'silence, pre-ticked boxes or inactivity' do not constitute legally valid consent.

The CJEU also played an important part in framing the rules on international transfers of EU citizens' data. In July 2020, in Case-311/18 (Schrems II), and October 2015, in Case C-362/14 (Schrems I), the CJEU struck down the agreements for data transfers between the EU and the USA, due to a lack of safeguards for European citizens' data protection in US domestic law, and prompted a renegotiation on supplementary safeguards. Similarly, Opinion 1/2015 invalidated the Canada-EU PNR Agreement because of necessity and proportionality issues (see the section on the role of the Parliament).

The data retention issue

The Data Retention Directive (2006/24/EC) was adopted in 2006 to create an EU-wide scheme for the retention of personal data generated or processed by electronic communication services providers, in order to make it available when investigating and prosecuting crimes. It took several years before Member States transposed the directive into national law. In 2014, the CJEU struck down the directive in Case C-293/12 (*Digital Rights Ireland*), on the basis that the 'mass, indiscriminate' storage of personal data permitted by the directive constituted a disproportionate interference with privacy rights. The CJEU followed this approach in Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige*), clarifying however that 'targeted retention of traffic and location data for the purpose of fighting crimes' may be permitted, if the retention is limited to what is strictly necessary. By two Grand Chamber judgments of 6 October 2020, in *Privacy International* and *La Quadrature du Net*, the Court confirmed and nuanced the case law in *Tele2 Sverige* and further clarified the requirements for data retention and the scope of national competences for national security under Article 4(2) TFEU. In his opinion of 18 November 2021, Advocate General Campos Sánchez-Bordona indicated a certain irritation with the reluctance of national courts to apply CJEU principles and request further preliminary rulings on data retention. While other court cases are still pending at the time of writing, Member States did not respond to *Tele2 Sverige* a uniform way, and despite further clarifications, the situation remains heterogeneous at the national level. Several Member States kept their domestic data retention regimes, while others annulled existing laws and replaced them with new ones, in an attempt to comply with the CJEU requirements of proportionality and targeted retention. Member States regard this patchwork of national laws as thwarting law enforcement cooperation; the situation has given rise to still unresolved debate on the need to reintroduce EU-wide legislation. (For the most recent and possible future developments, see section on 'Taming digital surveillance' under 'Challenges for the future'.)

Challenges for the future

According to the Commission, 'strong data protection rules are not a luxury, but a necessity'. While experts have cautioned that the GDPR is still in the early stages of its application and that until more DPA decisions and court proceedings take place, particularly in cross-border cases, many positive effects of the GDPR will remain invisible, some complex and controversial issues have already arisen.

Compliance and data needs of emerging technologies

The Parliament and the Commission have stressed that the full potential of data as a social good cannot be unlocked until citizens' lack of trust in technology and their sense of a loss of control over personal data is properly addressed. The Commission perceives data protection as a 'trust-enabler'. The following emerging technologies exhibit features or data needs that may conflict with EU data protection and privacy. Devices may consist of one or more of these technologies.

Artificial intelligence (AI), for which there is currently no agreed legal definition at EU level, is defined by Article 3(1) of the draft AI act as '... software that is developed with ... specific techniques and approaches listed in Annex 1 and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with'. Certain types of AI, such as machine-learning, are reliant on vast amounts of data to feed into decision-making algorithms. While this use of data is not a problem per se, rights violations may occur where AI is used for commercial or political manipulation, where data subjects are not informed of how their data are being used, where decisions made about an individual cannot be explained, or where poor data quality produces biased or discriminatory results. Concerns regarding AI data needs are polarising the debate on (de)regulating AI training data.

Facial Recognition Technology (FRT) raises a number of data protection concerns. These systems rely on particularly sensitive biometric data, which is subject to strict requirements under Article 9 of the GDPR. The Commission and the Fundamental Rights Agency (FRA) have warned against deploying FRT 'haphazardly', or making it interoperable with other IT systems. The use of FRT by law enforcement authorities for security or crime-fighting purposes also calls the proportionality of its use into question. Parliament called for a ban on police use of facial recognition technology in public places, as well as on private facial recognition databases.

The internet of things (IoT) generates vast amounts of data, with a potential that the Commission is keen to exploit. Although sensor and machine data may qualify as purely non-personal data outside the GDPR's scope, operators of IoT devices deployed in social environments may find it challenging to generate data that precludes the identification of data subjects and therefore may be freely processed. For instance, usage patterns from smart meters can identify individuals, their holiday periods and observance of religious practices. There are also concerns regarding inconspicuous and ubiquitous surveillance and data collection, particularly when done in data subjects' homes or in proximity to children. Conversely, connected cars or virtual assistants may not be functional enough to allow individuals to exercise their data subjects' rights. The EDPB and EDPS have also repeatedly raised concerns regarding the interplay and alignment of pending tech regulation with the EU data protection *acquis*.

Possible ways forward:

- **Clarification**. The Council, the FRA and the Parliament have called on the Commission to clarify how the GDPR applies to new technologies such as artificial intelligence. The EDPS Tech Dispatches offered a preliminary assessment, and the EDPB plans to release guidelines.
- **Automated decision-making**. Article 22 of the GDPR and Article 11 of the Law Enforcement Directive provide that data subjects may only be subject to decisions based solely on automated processing under strict conditions.
- **Artificial intelligence and facial recognition technology**. The Parliament emphasises the importance of designing a policy framework that encourages the development of 'all kinds of AI' beyond deep-learning systems, which need a particularly large amount of data. A Commission White Paper on Artificial Intelligence was delivered in February 2020, and in April 2021, it unveiled a draft regulatory framework on artificial intelligence. Among other things, the Commission's draft framework would introduce new rules for **facial recognition technologies** and differentiate them according to risks associated with their usage, i.e. 'high-risk' or 'low-risk'.

Equipping data protection authorities with sufficient resources

In line with Member States' enforcement responsibilities, the DPAs' role has grown considerably. They have been given investigative and sanctions powers and enabled to step up their cross-border cooperation through specific mechanisms. The 'biggest' fines for data protection violations in Member States include: the National Commission for Data Protection (*Commission Nationale pour la Protection des Données* – CNPD), the Luxembourg DPA, imposing a fine of €746 million on Amazon in July 2021, which Amazon is currently appealing. In September and November 2022, the Irish Data Protection Commission (DPC) fined Meta Platforms Ireland Limited €405 million and €265 million over the public disclosure of children's data and data scraping practices. The DPC is reportedly finalising further fines against Meta. The DPAs' powers, and responsibilities have been increased in response to the growing number of requests they have to address. The onus of providing resources for data protection enforcement rests on the Member States, under Article 42(4) of the GDPR. The DPAs cannot impose costs on the data subjects. During the initial drafting process on the DPAs, the EPDS and the AW29 cited the risks posed by insufficient resources, including a lack of capacity to address 'what matters', and DPAs acting as 'an impediment to rather than an enabler of innovation and growth'. Since the GDPR entered into force, the LIBE committee, the EPDB, the Multilevel Stakeholder Group and the Council have alerted the Commission to concerns over resource constraints. Most recently, the Irish Council for Civil Liberties and Access Now welcomed the overall increase in fines imposed, but deplored persisting enforcement deficits and divergences in DPAs' enforcement practices. In a 2021 EDPB data compilation exercise, conducted at the request of the LIBE committee, the vast majority of supervisory authorities explicitly stated that they did not have sufficient resources to carry out their tasks.

Possible ways forward:

- **Member State responsibility**. The Commission has called for Member States to allocate sufficient resources to their DPAs. It has also recommended a pooling of efforts, such as joint investigations, on issues affecting more than one Member State.
- **Infringement action**. The Commission has confirmed it is prepared to take infringement action against Member States that fail to comply with their resource obligations.
- **Addressing the issue of limited funding**. From 2016 to 2020, the Commission funded projects on the implementation of the GDPR worth almost €6.3 million, under the rights, equality and citizenship (REC) programme, some of which were carried out by DPAs. As part of the equality, rights and gender equality strand of the 2021-2027 citizens, equality and values programme (CERV), the EU earmarked funding for projects that tackle challenges related to the protection of personal data, as well as to support the stakeholder dialogue in this area.

Communications control

With the adoption of Regulation (EU) 2021/1232, the co-legislators temporarily enabled internet-based communications services ('providers') to scan communication and traffic data for child sexual abuse material. It covers the processing of images, videos, and text data, but not of audio communications. The regulation is without prejudice to the applicability of GDPR, under which the lawfulness and proportionality of such detection practices remain uncertain. The regulation will expire on 3 August 2024. On 11 May 2022 the Commission tabled a proposal containing permanent rules to replace the interim regulation. Unlike the interim regulation, the new proposal would, amongst other things, i) follow a system of risk mitigation obligations and detection orders, ii) act as a legal basis under the GDPR, and iii) apply to hosting services. Various child protection organisations and industry stakeholders have welcomed the proposal. 118 civil society groups have called on the EU to withdraw the CSA Regulation and to pursue alternative measures that are more likely to be effective, sustainable and fully respect EU fundamental rights. 65 individuals and organisations have raised concerns over the incompatibility of this proposal with end-to-end encryption. The joint opinion of the EDPB and EDPS is largely critical. The German Federal Government has, reportedly, raised 61 critical questions to the Commission and the German Federal Parliamentary Research Service issued a negative assessment of the proposal.

Possible ways forward:

- **Legislative action fails**. If Parliament and the Council do not find an agreement, the interim regulation will expire on 3 August 2024. Voluntary detection of child sexual abuse material will become subject to serious compliance risks (beyond persisting concerns under the GDPR).
- **Compromise legislation**. Like with the interim regulation, Parliament and Council may well agree on a compromise text. Depending on the Parliament's and Council's mandates and their priorities, the outcome may reflect variations of Commission and stakeholder suggestions.
- **Legal actions**. Patrick Breyer MEP is suing Meta/Facebook for scanning his private chats.

Clarifying requirements of valid consent

Differing derogations, implementations and interpretations of the GDPR present challenges for GDPR compliance. Where Member States exercised their discretion, such as concerning consent given by minors and consent for health data, they inadvertently produced fragmentation in the GDPR framework. Large digital companies have also been criticised for relying on designs that discourage users from choosing more privacy-friendly settings and for forcing users' consent. Recently, Parliament deplored that 'the implementation of valid consent continues to be compromised by the use of dark patterns, pervasive tracking and other unethical practices'.

Possible ways forward:

- **Consent code for minors**. The Council has suggested drafting a sector-specific code addressing children's data, in accordance with Article 40 of the GDPR.

- **Guidelines**. Under the EDPB guidelines, consent is an appropriate legal basis for processing only if the data subject is offered 'a genuine choice' to accept or decline the terms offered and can decline the terms without detriment.
- **Administrative or legal actions**. In May 2018, NOYB – initiated by digital rights activist Max Schrems – filed complaints over 'forced consent' with DPAs in five Member States against Facebook, Google, WhatsApp and Instagram. France's highest administrative court rejected Google's appeal against the €50 million fine imposed by the CNIL, France's DPA. In August 2021, NOYB filed complaints against cookie paywalls on German and Austrian news websites.
- **Voluntary commitments**. Reportedly, European Commissioner Didier Reynders 'stressed the intention to explore voluntary commitments to find an easier way to ask for consent that is not based on a false choice between giving consent or losing one's time [...]'.

Taming electronic surveillance

The debate on a new EU-wide data retention regime, in line with standards set by the CJEU, has intensified in recent years. In June 2019, the Council adopted conclusions on data retention for fighting crime, tasking the Commission with a study 'on possible solutions for retaining data, including the consideration of a future legislative initiative'. Contrary to the Juncker Commission, the von der Leyen Commission seems more open to putting forward a new proposal. However, any legislative or non-legislative initiative must be in line with CJEU case law, according to which there can be no 'mass, general and indiscriminate' data retention. While the European Council insists on the need for data retention, Parliament has called on the Commission to launch infringement proceedings against Member States that have not repealed or aligned their data retention laws with CJEU case law. The Commission has apparently begun seeking Member States' views on a way forward, with regulatory intervention a plausible option.

The Pegasus revelations and the Encrochat investigations in 2021 signify a rise in hacking by law enforcement bodies, or 'government hacking'. The Pegasus revelations spiralled into an EU wide spyware scandal, revealing that Member State authorities had potentially instrumentalised commercial spyware against political rivals. In contrast, the infiltration by law enforcement authorities of the encrypted phone network Encrochat – widely used by criminals – has been portrayed as 'an example of good practice'. Nevertheless, defence lawyers across Europe have challenged evidence and convictions claiming flawed investigations, violations of cross-border evidence-sharing rules and insufficient disclosure of evidence. Besides this, the use of AI and biometric surveillance technology, such as facial recognition technology, is growing and the co-legislators are considering safeguards in the proposed AI act. Similarly, commercial surveillance is coming under scrutiny.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2023.

Photo credits: © vchalup / Adobe Stock.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)