BRIEFING

EU policies - Insights

Understanding EU data protection policy

SUMMARY

The near-ubiquity of data in the lives of ordinary people, along with its exponential growth in generation rate and potential misuse, has made the protection of personal information an increasingly important social, legal and political matter for the EU. In recent years, both awareness of data rights and expectations for EU action in this area have 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 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 data protection regime in the EU.

In 2012, the European Commission launched an ambitious reform to modernise the EU data protection framework. It resulted in the adoption in 2016 of the main EU data protection legislative instrument – the General Data Protection Regulation (GDPR) – and the Law Enforcement Directive. The framework overhaul also included adopting an updated Regulation on Data Processing in the EU Institutions and reforming the ePrivacy Directive, pending in the Council since September 2017.

The European Parliament has played a major role in passing these reforms, both as co-legislator and author of own-initiative reports and resolutions seeking to guarantee a high level of data protection to EU citizens. Last but not least, the European Court of Justice has also played an important part in building the EU data protection framework, with several landmark judgments delivered in recent years.

In the coming years, potential challenges to the data protection framework include the question of how to adapt the GDPR to emerging technologies such as artificial intelligence, facial recognition technology and the Internet of Things. Potential fragmentation issues include differing Member State interpretations of consent for data processing, while compliance burdens for SMEs and insufficient resources for data protection authorities may present challenges for enforcement. The European Commission is expected to address these issues in its upcoming evaluation of the GDPR.

In this Briefing

EPRS | European Parliamentary Research Service

Author: Sofija Voronova with Anna Nichols
Members' Research Service

PE 651.923 – May 2020

EN

State of play

The volume of data being produced worldwide is growing rapidly. The daily number of clicks on e-commerce sites, social media platforms and other online services has helped create a huge 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 outcomes, 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.

Concerns regarding potential rights violations by emerging technologies are unlikely to be allayed any time soon. Artificial intelligence, which relies on the mass collection of data to operate, poses fundamental challenges to privacy and personal data protection, as well as a discrimination risk. Facial recognition technology, which allows to swiftly identify an individual via their biometric data, is currently in use by the police forces of at least 10 Member States. The Internet of Things is expected to generate massive amounts of new data that can be transmitted between connected devices and machines without human intervention. Most recently, governments have adopted exceptional emergency measures including the use of digital technologies, in an attempt to map, monitor and flatten the Covid-19 curve.

To address these issues, the EU has taken a 'human-centric' approach to technological development; this approach has found expression, among others, in the adoption of the General Data Protection Regulation (GDPR) and in the active role the Court of Justice of the EU (CJEU) has assumed in defending the rights of individuals. All these issues, which directly affect people's everyday lives, have brought the relevance of data protection law and its reform to the fore in public consciousness.

Public awareness

According to the 2019 Special Eurobarometer survey on the GDPR, 84 % of respondents use the internet, with 75 % of respondents using it daily – an increase of 15 percentage points since 2015. 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. The survey furthermore found that 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. On the other hand, the survey showed that 67 % of respondents know about the GDPR and that the number of persons 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 were the most likely to have exercised their data rights, while respondents in Czechia and Slovenia were the 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 such complaints by individuals and organisations, several DPAs have launched actions against companies under the GDPR, including for forced consent, dating apps, transparency obligations, and data breaches.

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 be free 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 the 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 the protection of these rights was a responsibility of the Member States.

The 1980s saw attempts to approximate the growing number of national laws on personal data protection through the adoption of 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 of the 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 for personal data protection prior to the GDPR. The DPD aimed to improve the functioning of the internal market and address the gaps in Member State legislation on the protection of fundamental rights.

Treaty basis

Article 16(1) of the Treaty on the Functioning of the EU (TFEU) establishes the right to protection of personal data. Articles 7 and 8 of the Charter of Fundamental Rights of the EU provide for a right to privacy and a right to protection of personal data respectively. Compliance with these rules shall be subject to control or oversight by an independent authority. Article 47 of the Charter provides for a right to an effective remedy where the rights under Articles 7 and 8 have been violated. Following the entry into force of the Lisbon Treaty, rights enshrined in the Charter have enjoyed the same legal status as those enshrined in the Treaties (Article 6(1) TEU). The European Convention on Human Rights also provides for a right to respect for private and family life in its Article 8. Under Article 52(3) of the Charter, corresponding Charter and Convention rights have the same meaning and scope.

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 implement 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.

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(2) of the GDPR, this regulation's rules apply to companies regardless of whether or not the data processing takes place in the EU; this is sometimes referred to as 'extraterritoriality'. Protection extends to EU residents, i.e. both EU citizens and non-citizens who are resident in the EU. Only **personal data** falls within the scope of GDPR protection. Data are considered 'personal' when it can directly or indirectly allow to identify a natural person, such as through a name, an 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.

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 its 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.

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 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 the rights of the data subjects, including the right to know what data a company has collected about them if they request them (right of access); the right to have wrong information corrected; and the right 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); the right to request from the controller to restrict the processing 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 the 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.

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 dawn raids (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). 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, 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.

EDPB. The GDPR establishes a new European Data Protection Board (EDPB) to replace the Article 29 Working Party as the independent legal body bringing together representatives of all Member State DPAs and the European Data Protection Supervisor (EDPS). Key responsibilities of the EDPB 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 allows NGOs to pursue **collective rights actions** without requiring a direct mandate by 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 (Directive 2016/680) applied 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. It 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 the 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. In its 2020 work programme, the Commission announced a non-legislative initiative on aligning relevant EU law enforcement rules with regard to data protection in the second quarter of 2020.

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 institutions, bodies, offices and agencies and on the free movement of such data updates the data protection rules for data processing by the EU institutions and bodies, in order to keep them in line 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.

ePrivacy legislation

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the **ePrivacy Directive**) intends to harmonise national provisions and provide specific rules for electronic communications services. Unlike the GDPR, the ePrivacy 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 Commission tabled a proposal for a regulation on privacy and electronic communications to replace the ePrivacy 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).

Despite the Parliament having adopted its position in October 2017, progress on the proposal is currently blocked in the Council. The Council Working Party on Telecommunications and Information Society (WP TELE) published several redrafts of the proposal, but no compromise was found before the end of the Finnish Presidency of the Council in December 2019. The incumbent Croatian Presidency has stated that it would continue discussions on the proposal, but has not committed to finalising discussions before the end of its term in June 2020. Outstanding issues include the ePrivacy Directive's relationship with the GDPR, the grounds for processing, the protection of terminal equipment, cookies, and the possibility for different national bodies to be responsible for implementation. Newer issues that have arisen since the initial talks concern the way in which the new regulation would take into account the latest developments in new technologies, such as the Internet of Things, how it would handle the question of processing data for the purposes of preventing child abuse imagery and/or other serious crimes, and how it would interact with 'any potential solution' on data retention.

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, certain safeguards must be fulfilled in order to ensure that protection travels with the data. The Commission has referred to these international agreements as '**digital diplomacy**', considering them a means for exporting EU data protection values and standards worldwide.

Data transfers

Adequacy decisions. Article 45 of the GDPR regulates the transfer of personal data from the EU to a third country or international organisation, stipulating that the Commission decides whether the third party provides an 'adequate' level of protection for the transferred data. Such a decision allows the data to be transferred freely with no further safeguards or checks. The adoption of an adequacy decision requires: a proposal from the Commission; an 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 the transfer 'exceeds the implementing powers provided for in the regulation'. Adequacy decisions are to be reviewed at least every four years.

The Commission has so far approved adequacy decisions for Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States (limited to the Privacy Shield framework), while talks are ongoing with South Korea. Data exchanges in the law enforcement sector are not covered by this provision, but are governed 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'.

Data protection and Brexit

According to the UK Information Commissioner's Office, the GDPR will continue to apply in the UK until the end of 2020. After this transition period, transfer rules for third countries will apply to data transfers from the EEA to the UK.

Privacy Shield framework. The EU-US Privacy Shield (which replaced the earlier Safe Harbour scheme invalidated by the CJEU) applies to certified US companies and organisations engaged in personal data transfers between the EU and the US. For personal data to be transferred to these entities, they must be on the Privacy Shield list, which is maintained and published by the US Department of Commerce, and uphold commitments such as displaying their privacy policy on their website, complying with data protection rules in the onward transfer of personal data, and being subject to oversight by EU and US authorities. The Privacy Shield has applied since 21 August 2016 and is reviewed annually. The 2019 review sets out concrete steps for improving the practical implementation of the agreement.

Data protection worldwide

The GDPR has been praised 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 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:

- **Scrutiny of Commission decisions**. The 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 the above-mentioned 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**. The 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 US and Australia. It will similarly be involved in any agreement with Japan; in February 2020 the Council authorised the Commission to begin negotiations. The Parliament had a particularly pivotal 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, in order 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's work in the **2019-2024 term** is expected to focus on monitoring the implementation of data protection legislation and continuing the scrutiny of rights implications in upcoming reforms. One of the Parliament's main tasks will be to conduct negotiations with the Council on the draft e-privacy regulation, once the latter adopts its position on this complex file.

The role of the CJEU

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.

The data-retention saga

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 and Watson*), 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. Following these judgments, and while other court cases are still pending at the time of writing, Member States did not respond in a uniform way. Several kept their domestic data retention regimes, while others annulled existing laws and replaced them by new ones in an attempt to comply with the CJEU requirements of proportionality and targeted retention. At present, only a couple of Member States do not have a data retention regime in place. Member States regard this patchwork of national laws as thwarting law enforcement cooperation; the situation has given rise to still unresolved debates on the need for reintroducing EU-wide legislation.

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 decision of the CJEU 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 October 2015, in Case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), the CJEU struck down the agreement for data transfers between the EU and the US due to a lack of safeguards for European citizens' data

protection in US domestic law, and prompted a renegotiation on how the personal data of EU citizens are transferred to the US. 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).

A number of key decisions are expected in 2020. The validity of the EU-US Privacy Shield may come under CJEU scrutiny again in the upcoming Case C-311/18 (*Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems - 'Schrems II'*). The final judgment is expected on 16 July, but commentary on the Advocate General's opinion suggests that several important deficiencies identified, such as its voluntary basis and block on Parliament scrutiny, raise doubts as to whether the CJEU will uphold the Privacy Shield.

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 occur, particularly in cross-border cases, many positive effects of the GDPR will remain invisible, some complex and controversial issues have already arisen.

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 of their personal data is properly addressed.

Artificial Intelligence (AI), for which there is currently no agreed legal definition at EU level, is defined by the Commission as 'systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals'. Certain types of AI, such as machine-learning, are particularly reliant on huge 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 data quality is poor and produces biased or discriminatory results.

Facial Recognition Technology (FRT) relies on particularly sensitive biometric data for its application, and its use is already limited under Article 9 of the GDPR. FRT is particularly susceptible to privacy violations, through unauthorised access and use of biometric data; indeed, you can throw away your phone, but not your face. The Commission and the Fundamental Rights Agency (FRA) have warned against FRT being 'deployed haphazardly' or made interoperable with other IT systems. The use of FRT by law enforcement authorities for security or crime-fighting purposes also calls into question the proportionality of its use; Germany and the UK have both had active national debates on this.

The Internet of Things (IoT) generates huge amounts of new, non-personal data with a potential that the Commission is keen to exploit. While non-personal data do not have to be processed under GDPR rules, some academics remark that businesses have struggled to harness their potential, particularly where non-personal data are de-anonymised, i.e. converted into personal data, and consequently needs to be made GDPR compliant. Connected cars or virtual assistants may not be functional enough to allow individuals to control or access their personal data, while usage patterns from smart meters can identify individuals, their periods of holidays and religious practices. There are also concerns regarding surveillance and data collection happening without the awareness of the users, particularly when done in their homes or in proximity to children.

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. The EDPS Tech Dispatches provide a preliminary

assessment of the possible impacts of privacy and data protection posed by new technologies, while the EDPB 2019-2020 work programme includes plans to release guidelines on the use of new technologies.

- **Automated decision-making and explainability**. Article 22 of the GDPR and Article 11 of the Law Enforcement Directive provide that data subjects cannot be subject to decisions based solely on automated processing.
- **Artificial intelligence**. **T**he 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 is expected to be followed by a series of legislative initiatives in late 2020.
- **Facial Recognition Technology**. The Commission has affirmed the need to better define processing, and to establish accuracy criteria in surveillance depending on system use and risk level.
- **Data subject awareness**. Directive 2019/2161 on better enforcement and modernisation of EU consumer protection grants consumers the express right to receive pre-contractual information and the confirmation that a 14-day right of withdrawal will apply to 'free' digital service contracts. These contracts are particularly pertinent from a data protection point of view, as they include cases where consumers must provide personal data to the service provider in order to access the service, a model used by many social media companies.

Resources for data protection authorities

In line with Member States' enforcement responsibilities, DPAs have seen their role increase considerably. To this end, they have been conferred investigative and sanctions powers and enabled to step up their cross-border cooperation through the establishment of specific mechanisms. While the first 'big' investigations into data protection violations are ongoing in several Member States, in January 2019, CNIL, the French DPA, already handed down a €50 million fine to Google for a data rights violation, the heaviest such fine imposed so far.

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 with the Member States. Article 42(4) of the GDPR requires Member States to provide their DPAs with the 'human, technical and financial resources, premises and infrastructure necessary for the effective performance' of their tasks. It should be noted at this point that when performing their tasks, DPAs cannot impose costs on the data subjects. During the initial drafting process with regard to the DPAs, the EPDS and the AW29 cited 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's entry into force, the LIBE committee, the EPDB, the Multilevel Stakeholder Group and the Council have alerted the Commission about this issue. The EDPB noted that 'almost none' of the 17 DPAs included in their report received the requested amount of budgetary increases in 2019.

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, in order to mitigate resource constraints.
- **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 Commission funding**. Some funding for national DPAs is provided in the Rights, equality and citizenship (REC) programme, which aims to contribute to 'the further development of an areas where equality and the rights of persons ... are promoted, protected and effectively implemented'.

Costs for SMEs

While Recital 13 of the GDPR requires Member States to consider the specific needs of SMEs, the latter report that they are among the stakeholders that struggle the most in applying data protection rules. SMEs are particularly likely to require 'considerable resources' for GDPR implementation and do not find instruments, such as the certification mechanisms that are available to them, a 'financially attractive' means for compliance.

Possible ways forward

- **Institutional guidance**. While the EPDB has published detailed guidelines regarding data access requests, stakeholder submissions have indicated that smaller businesses and civil society organisations would welcome further guidance from the EDPB on what constitutes an 'unfounded or excessive request' and what are 'concrete, simple and user friendly tools to help them apply the guidelines in practice'.
- **Sector-specific codes**. The Council has suggested drafting sector-specific codes that would take account of the specific features of the various processing sectors and the specific needs of micro-, small and medium-sized enterprises.

Consent

Differing interpretations of consent have already presented issues for coherent GDPR implementation. Categories of consent where Member States have a margin of discretion, such as consent given by minors and consent for health data, have inadvertently produced fragmentation in the GDPR framework. Large digital companies have also been criticised for relying on specific designs to discourage users from choosing more privacy-friendly settings, or to force their consent.

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 only an appropriate lawful basis for processing if the data subject is offered 'a genuine choice' to accept or decline the terms offered and can decline the terms without detriment.
- **Legal action**. In May 2018, digital rights activists NOYB.eu filed complaints in five Member States against Facebook, Google, WhatsApp and Instagram, on the basis that they were forcing their users to consent to both their privacy policies and terms in full in order to keep using their services. Google has filed an appeal against the €50 million fine that the CNIL imposed on it; the appeal is currently under review by France's *Conseil d'État*.

Data retention

The debate on the possibility of establishing a new EU-wide data retention regime, in line with the standards set by the CJEU, has intensified in recent years. A dedicated Council Friends of the Presidency Working Party on data retention has been meeting regularly to examine the issue. In June 2019, the Council adopted conclusions on data retention for fighting crime, tasking the Commission with carrying out a study 'on possible solutions for retaining data, including the consideration of a future legislative initiative'. While the Juncker Commission did not wish to put forward a new proposal for EU legislation on the matter, the von der Leyen Commission seems ready to consider a possible way forward. However, any legislative or non-legislative initiative has to be in line with CJEU case law, according to which there can be no 'mass, general and indiscriminate' data retention, as confirmed by Advocate General Campos Sánchez-Bordona, in his recent opinions. The Parliament is closely following these developments, notably through regular questions to the Commission and the Council.

Outlook

In her July 2019 political guidelines, the European Commission President, Ursula von der Leyen, emphasised the need to balance the wide use of data with high standards with regard to privacy, security and ethics, quoting the GDPR as a global achievement.

Justice Commissioner Didier Reynders, responsible for GDPR implementation, enforcement and international promotion, has committed to ensuring that 'fundamental rights are fully protected in the digital age'. The Commission is required to submit a public report on the evaluation of the GDPR to the Parliament and the Council by 25 May 2020. The Council has asked the Commission to go beyond the two required chapters on data transfers and DPA cooperation, and include an 'overview' of the GDPR's implementation, including the challenges outlined above.

The European data strategy and White paper on AI, presented by the Commission in February 2020, set out the von der Leyen Commission's vision on data protection in the context of developing digital technologies. While the data strategy focuses mostly on non-personal data, it also aims to enhance data subjects' rights, such as the right to data portability with the help of decentralised technologies, such as blockchain, and to provide people with tools to control their data. The AI white paper identifies the areas in which artificial intelligence is already subject to data protection rules, while also suggesting possible adjustments to these legal frameworks in order to futureproof them; it furthermore focuses on the use of biometric data in facial recognition technology.

MAIN REFERENCES

Lynskey O., *The Foundations of EU Data Protection Law*, Oxford University Press, 2015.

Milt K., Personal data protection achievements during the legislative term 2014-2019: the role of the European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, April 2019.

Monteleone S., Reform of the e-Privacy Directive, EPRS, European Parliament, September 2017.

Montelone S., Rules for EU institutions' processing of personal data, EPRS, September 2018.

Monteleone S., The Privacy Shield: Update on state of play of the EU-US data transfer rules, EPRS, July 2018.

Monteleone S., Artificial intelligence, data protection and elections, EPRS, May 2019.

Madiega T., EU guidelines on ethics in artificial intelligence: Context and implementation, EPRS, September 2019.

Madiega T., European Court of Justice limits the territorial scope of the 'right to be forgotten', EPRS, October 2019.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

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

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

http://epthinktank.eu (blog)