The future of data protection and privacy
How the European Parliament is responding to citizens' expectations

SUMMARY

During the Conference on the Future of Europe (CoFoE), many citizens seized the opportunity to express their vision for the future of EU data protection and privacy. This briefing examines the European Parliament's activities in the context of these expectations.

The Conference on the Future of Europe provided European citizens with the opportunity to have their say on what the EU does and how it works for them, through a multilingual digital platform and four European Citizens' Panels. The panels provided a forum for a (post-)stratified random sample of European citizens to reflect on the future of Europe and to recommend improvements. This briefing draws on recommendations shared in Panel 1 (Stronger economy, social justice and jobs/Education, culture, youth and sport/Digital transformation), Panel 2 (European democracy/values, rights, rule of law and security), and via the multilingual digital platform (topic clusters: Digital transformation, and Values and rights, rule of law, security).

Overall, citizens call for a high level of data protection and stringent implementation. They recommend measures promoting industry compliance, increasing citizens' control over data, and limiting the monitoring, profiling and manipulation of citizens by private and public actors. As this briefing demonstrates, Parliament has largely kept pace with citizens' concerns by taking initiatives in areas where citizens participating in the Conference panels and through the platform identified a need for action during their discussions. However, citizens indicate irritation with industry's haphazard implementation of their data protection and privacy expectations. This highlights EU citizens' perception that compliance (and enforcement), or even certain aspects of the data acquis, are insufficient.

This is the fifth in a series of briefings discussing citizens' expectations and recommendations expressed in the course of the Conference on the Future of Europe as well as corresponding European Parliament activities.
The Conference on the Future of Europe (CoFoE) has provided citizens with a forum to debate their visions for the future of Europe, including on data protection and privacy. As a key component, a multilingual digital platform allowed citizens to contribute and debate ideas through posts, endorsements, comments and events. Kantar Public analysed the outcomes in a final report. Four European Citizens’ Panels were organised on different topics, with the aim of fostering discussion among participants. A random selection of approximately 200 citizens per panel, representing the EU’s sociological diversity, discussed issues within each Panel’s theme. After agreeing collective recommendations, these were delivered to the Conference Plenary and made publicly available.

Citizens’ recommendations in the area of data protection and privacy reveal five core expectation clusters. Citizens demand: (i) increased control over data; (ii) enhanced protection of minors; (iii) restrictions on surveillance, profiling and manipulation; (iv) enhanced compliance and enforcement; and (v) the promotion of privacy awareness and literacy.

The prominent position of data protection and privacy among citizens’ recommendations and suggestions collected during the exercise attest to their high relevance to EU citizens. An increasing number of individuals aged 16-74 years use the internet at least weekly, (86% in 2021). A 2021 Special Eurobarometer 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, 78% of respondents are either ‘concerned’ or ‘very concerned’ about the use of their personal data online. In the EU, personal data and privacy are principally protected by the Charter of Fundamental Rights, the General Data Protection Regulation 2016/679 (GDPR), the Law Enforcement Directive 2016/680 and the e-Privacy Directive 2002/58/EC.

Parliament has promoted the adoption of a high level of data protection and privacy in legislative acts including the General Data Protection Regulation, the Directive on the use of passenger name records (PNR) and the (pending) e-Privacy Regulation. Conversely, certain groups of Members of the European Parliament advocate more lenient data protection rules. In March 2021, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) rejected amendments urging the Commission to ‘present plans for a more comprehensive revision’ of the GDPR after studying any ‘unintentional obstacles it may have created to the development of technologies’.

Citizens’ expectations and Parliament’s responses

Increase data subjects' control over data

Ensure genuine choice over data processing

Citizens repeatedly call for genuine choice and control over how their data are used. They strongly object to providers making access to products and services conditional on consent or payment (cookie-walls), the lack of options to reject all non-essential data processing, and the complexity of terms and conditions, privacy notices, and pre-formulated declarations of consent. They recommend:

- introducing ‘standardised privacy policies and easily understandable, concise and user-friendly consent forms’;
- promoting the use of visual aids for consent requests;
- ‘forbidding entities to limit their services more than necessary if there is no consent to optional data processing’;
- ‘avoiding default consent to re-use and resell ... data’;
- mandating a ‘do not sell my personal information’ option on websites;
- introducing privacy/GDPR compliance scores for websites; and
- ensuring that refusing ‘the collection of personal data should be made at least as easy as accepting it’, for instance by mandating an option to decline all (non-essential) processing.
According to the European Data Protection Board (EDPB) guidelines, consent is only an appropriate legal 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. Recital 32 of the GDPR clarifies that silence, pre-ticked boxes or inactivity do not constitute consent. In Case C-673/17 Planet49, the Court of Justice of the European Union (CJEU) clarified that this rationale also applies under the e-Privacy Directive. Recital 42 of the GDPR stipulates that a pre-formulated declaration of consent should be provided in an intelligible and easily accessible form, using clear and plain language and should not contain unfair terms. Where controllers use dark patterns to collect consent or make the provision of services conditional on the data subjects’ consent, this consent would (arguably) be invalid and the data processing unlawful. Concealing intentions behind legalistic wording ('legalese') and obscure pop-ups/cookie banners, may also conflict with the GDPR’s consent requirements. Under Articles 21(5) and 25 GDPR, automated objections to data collection through 'do not track' browser controls that signals users' preferences must be respected. While individuals do not enjoy a dedicated right to opt out of data sales under the GDPR, they may opt out of processing for marketing purposes and withdraw consent for processing operations.

Considering electronic communication services are often used to communicate private and sensitive information, and metadata allow detection of inferences, EU lawmakers put e-privacy rules in place that aim at ensuring confidentiality. Anyone intending to track individuals by storing cookies in the terminal equipment of a subscriber or user must, as a rule, obtain prior consent. According to the EDPB, if the information stored in the end-users’ device constitutes personal data, Article 5(3) of the e-Privacy Directive shall take precedence over Article 6 of the GDPR with regards to the activity of storing or gaining access to this information. [...] [Notwithstanding,] subsequent processing of personal data including personal data obtained by cookies must ... have a legal basis under ... the GDPR in order to be lawful.' Stakeholders, academics, and supervisors disagree on the interpretation of design requirements for cookiebanners. France’s data protection authority (DPA), the Commission nationale de l'informatique et des libertés (CNIL), recently updated its GDPR developer’s guide, highlighting provisions on third-party cookies, other tracers and audience measurement technologies, while the EDPB recently set up a cookie banner taskforce. However, even where the advertising industry resorts to other tracking technologies instead of cookies, data protection and privacy must be respected. With the incorporation of the European Electronic Communication Code (EECC) into national law through transposition or interpretation ('indirect effect of directives'), interpersonal communication services, including webmail, messaging services and internet telephony, became subject to all e-privacy rules from 21 December 2020 at the latest. In principle, webmail services and interpersonal communication services will need to obtain prior consent to scan emails or use traffic and location data for the purpose of targeted advertising. In its 2017 position on the e-privacy regulation, Parliament proposed to ban cookie-walls, mandate do-not-track pre-sets in browsers and smartphones, and subject offline tracking to consent requirements. Subsequently, the EDPB raised concerns about the Council’s position.

Civil society, government agencies, supervisors and the European Parliament have repeatedly criticised companies for relying on designs that discourage users from opting for privacy-friendly settings and for forcing users’ consent. In May 2018, digital rights activists the NOYB – European Centre for Digital Rights filed complaints regarding ‘forced consent’ with DPAs in five Member States, against Facebook, Google, WhatsApp and Instagram. France’s Conseil d’État, the highest administrative court, upheld the €50 million penalty imposed by CNIL on Google. In August 2021, NOYB filed complaints against cookie paywalls on German and Austrian news websites.

While consent requests traditionally take the form of pop-ups, innovative solutions provide users with a one-stop dashboard to manage consent and data (consent management systems and personal information management systems). These systems must be developed with a view to the preconditions and parameters laid down in the GDPR, e-Privacy transposition acts, and the data governance act. The German Federal Ministry of Justice, the German Federal Ministry for Economic
Affairs and Climate Action and the Federation of German Consumer Organisations commissioned studies to clarify the complex interplay of legislation and to survey best-practices.

Parliament advocated genuine choice and data subjects’ autonomy during negotiations on the GDPR and e-Privacy Directive, and continues to take a privacy-friendly position in negotiations over the e-privacy regulation. Recently, Parliament criticised that ‘the implementation of valid consent continues to be compromised by the use of dark patterns, pervasive tracking and other unethical practices’. Consequently, it called ‘for the empowerment of consumers so that they can make informed decisions on the privacy implications of using new technologies and to ensure fair and transparent processing by providing easy-to-use options to give and withdraw consent to the processing of their personal data as provided for by the GDPR’.

Promote data control technologies

Besides transparent consent management, citizens seek tools from trusted intermediaries that help them control their personal data and exercise their data rights. Specifically, citizens suggest:

- providing data wallets that pool data about data subjects and their behaviour, allowing data subjects to monitor how their data are being used and shared, and to restrict or permit their usage. Others specify that data-re-users should submit any inferred data to a data pool and that login credentials could serve as a ‘single-sign-on’ to other websites and services. Others would prohibit the storing of data in providers’ databases altogether and ensure that data re-use takes place in the data subject’s processing environment.

- providing an e-mail address as a public service, since inboxes contain vast amounts of sensitive data and an address is required for basic services including banking, public services and healthcare. This could also function as a digital identity.

- providing one-stop applications (apps) through which data subjects could exercise a right to erase centrally.

Civil society organisations, researchers and commercial intermediaries are developing privacy-enhancing technologies (PETs), transparency-enhancing technologies (TETs), data rights automation apps, personal information management systems (PIMS) and other intermediation services. To promote these developments and unlock the potential of data while preserving EU rights and values, EU lawmakers aim to put a data governance act in place. As the first of a set of measures announced in the European Commission’s strategy for data, the proposed act is designed to facilitate voluntary data-sharing across the EU and between sectors, by strengthening mechanisms that increase data availability and foster trust in intermediaries. Specifically, it lays down: (i) conditions under which public authorities may allow the re-use of data that are subject to the rights of others; (ii) a compulsory notification and supervisory framework for providers facilitating the sharing of data; (iii) a framework for voluntary registration of data altruism organisations that facilitate the sharing of data for altruistic purposes; and (iv) a European data innovation board (EDIB) to ease the exchange of national practices and promote standardisation and interoperability. The proposed voluntary registration and labelling framework (regarding data altruism organisations), as well as the compulsory notification and supervisory regime (for data intermediation services), are meant to enhance trust in data organisations’ operations and thereby stimulate data-sharing at data-holder level. Stakeholders have expressed doubts regarding the conduciveness of these frameworks and concerns over excessive compliance burdens. Besides setting up a data governance framework, EU lawmakers aim to update the digital identity framework. As the call for papers for the 2022 Annual Privacy Forum demonstrates, the Commission is supporting research on PETs.

Parliament has asked the Commission to unlock the potential of the data economy in several resolutions, including in January and March 2016. After the publication of the Commission proposal, Parliament expressed its support for ‘the creation of a data governance framework ..., with a view to enhancing the flow and re-use of ... personal data that is fully GDPR-compliant’. Subsequently, Parliament welcomed the classification and certification of intermediaries, supported the EU-wide approach to data altruism and encouraged the Commission to facilitate a data-sharing culture and
voluntary data-sharing schemes, whilst advocating for compliance with consumer and data protection rights. During interinstitutional negotiations, Parliament favoured a prescriptive and detailed regulation, whereas the Council took a moderate approach, leaving public authorities and data intermediation services with more room for manoeuvre.

Bolster protection of minors

In its Recommendation 8, Citizens' Panel 2 suggests clear and strict rules are imposed on the processing of data relating to minors, ‘including consent rules, age verification and control by legal guardians’. The panel also recommends introducing in the GDPR ‘a special category for sensitive minors’ data (e.g. criminal record, health information, nudity), so that minors are protected from any form of abuse and discrimination'.

The GDPR contains specific provisions ensuring a child-oriented approach to data processing, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data (Recital 38 of the GDPR). Special protection is warranted in light of possible immaturity and vulnerabilities, and takes account of the development stages. Under Article 8(1) GDPR, a child reaches the age of consent at 16 years old, but Member States may provide for a lower age that is not below 13 years. Parliament regretted that Member States fixed disparate ages of consent and called on the Commission and the Member States to assess the impact of this fragmentation on children’s activities and on their protection online. Where a child has not reached the age of consent, processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. In its guidelines on consent, the European Data Protection Board (EDPB) provides clarifications on children's consent and parental responsibility and recommends practical solutions for verifying the age of users ('age-verification measures') and the parental responsibility. Under Article 9(1) GDPR, the processing of special categories of data, including data concerning health or a natural person’s sex life are prohibited, unless the exceptions in Article 9(2) GDPR apply. While the legal bases for sensitive data resemble those for the processing of ordinary data, they are stricter, particularly where children are involved. Article 10 GDPR specifies that controllers may process data relating to criminal convictions and offences based on the legal bases for ordinary data, but that it ‘shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’.

To accommodate the use of automated technology to detect online child sexual abuse, the co-legislators recently adopted a regulation that would temporarily exempt such practices from certain provisions of the e-Privacy Directive. Parliament ensured that privacy-preserving safeguards were included. Referring to a negative legal opinion, Patrick Breyer (Greens/EFA, Germany) announced plans to take legal action against the adopted regulation. The Commission aims to replace this temporary regulation by 3 August 2024 at the latest, with a more prescriptive long-term legislation. According to the European Digital Rights advocacy group, a recently leaked Regulatory Scrutiny Board opinion on the unpublished proposal for ‘legislation to effectively tackle child sexual abuse’ shows strong concerns regarding the legislative proposal.

Restrict surveillance, profiling and manipulation

Citizens are particularly concerned about preventing a ‘surveillance state’, curbing surveillance capitalism and prohibiting biometric mass surveillance in the EU. Specifically, they recommend:

- curbing state collection of data, not least to prevent chilling effects;
- respecting Court of Justice rulings on data retention and surveillance;
- intervening against the collection of data and control of the digital world through big tech companies;
- strictly regulating ‘use of biometric technologies … to avoid undue interference with fundamental rights' and prohibiting ‘indiscriminate or arbitrarily-targeted uses of biometrics’.
Restricting the surveillance state

Alongside the Pegasus revelations and European Commission reports on Member State views on how to frame a possible new EU law on data retention, citizens are raising concern about government surveillance. The Data Retention Directive (2006/24/EC) was adopted in 2006 to create an EU-wide scheme for the retention of data generated or processed by electronic communication services providers, 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. In subsequent case law, the CJEU clarified conditions under which data retention would be permitted and distinguished national competences more precisely, among other things. However, Member States did not respond in a uniform way – some repealing, and others upholding, recasting, or amending their domestic data retention regimes. As civil society continues to challenge national data retention regimes, Advocate General Manuel Campos Sánchez-Bordona indicated a certain irritation with the reluctance of national courts to apply CJEU principles, in his opinion of 18 November 2021. Debate on the need to reintroduce EU-wide legislation has consequently intensified. Most recently, the European Council insisted on the need for data retention and the Commission appears more open to considering a possible way forward. Parliament called on the Commission to launch infringement proceedings against Member States that have not repealed or aligned their data retention laws to CJEU case law. Parliament had already pointed out the risks arising for fundamental rights from the use of big data technologies by law-enforcement agencies in 2017.

As Pegasus revelations gain momentum, implicating EU Member States, one of the most high-profile spying scandals of recent years has come to Europe. The Canadian interdisciplinary laboratory Citizen Lab first discovered traces of Pegasus spyware in 2015, but it was only in 2021 that the scandal broke on a global level through a joint effort by Citizen Lab, Amnesty International, Forbidden Stories and 17 media organisations. Reports revealed that authoritarian and democratic governments around the world used Pegasus to spy on journalists, lawyers, activists, politicians, and high-ranking state officials. Investigators link the spyware to human rights harms including intimidation, harassment, detention, and murder. Pegasus was developed by the NSO Group and is designed to breach mobile phones and extract data stored or processed by the target system, including text messages, call interceptions, passwords, locations, microphone and camera recordings, and information from apps. In the EU, media organisations have uncovered extensive use of Pegasus spyware by the Hungarian and Polish governments against opposition figures and government critics. This raises fundamental concerns at several levels of the EU legal order, over data protection and privacy, freedom of expression, freedom of the press, freedom of association, redress mechanisms, and democratic processes and institutions. Individuals and authorities are sounding out redress and enforcement options against such abusive surveillance practices, including as individual litigation, formal complaints, infringement procedures and sanctions mechanisms for qualified rule of law deficiencies. Reportedly, Germany and Spain may also use Pegasus, and Cypriot and Bulgarian authorities may have authorised exports to third countries. Parliament has set up a committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware. Parliament adopted a resolution condemning the use of Pegasus surveillance software by Hungarian and Polish state entities and urging the Commission to draw up a list of illicit surveillance software and to keep this list updated. In their mission report following a three-day visit to Hungary, Members of the Committee on Civil Liberties, Justice and Home Affairs concluded that ‘the Pegasus case ... shed light on increased surveillance by the state against activists, journalists and lawyers’. Members of the European Parliament have discussed the Pegasus scandal on at least six different occasions. (See forthcoming EPRS study on the Pegasus-scandal.)

Recently, the EU obligation to take fingerprints and store them on EU identity cards was challenged.
Restricting surveillance capitalism

As manufacturers and operators increasingly design and deploy smart applications and machines, citizens raise concerns on their implications for individuals' dignity, autonomy and privacy. Such smart technologies collect vast amounts of data on individuals and their behaviour for systems designed to serve the interests of their shareholders. Data may feed into biased choice architectures, targeted advertisements, data monetisation or even non-compliant trade in data. Where developers or operators seek to increase profit or influence, they may opt for intrusive profiling and manipulative choice architectures or risk violations of fundamental rights including through error- or discrimination-prone algorithms. Constant monitoring may have chilling effects and alter human behaviour, whereas the predetermination of human behaviour through responsive environments may exceed the bounds of legal persuasion and amount to illegal manipulation. Risks of algorithmic discrimination and errors are inherent to AI-powered profiling and decision-making, which may form part of such responsive environments. Additionally, the inscrutability of AI black boxes hampers effective redress. To mitigate these risks, EU law applies a number of levers.

According to the GDPR’s core principles, processing of personal data must be lawful, fair and transparent; follow a specific, explicit and legitimate purpose; and comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability. The need to anticipate a legitimate purpose, which (in principle) determines the scope of data processing, as well as the data minimisation principle, help to prevent excessive data collection and hidden/unauthorised re-use. The Article 29 Working Party (Art. 29 WP) clarified that ‘it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing and advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering’. Consequently, controllers need to respect consent requirements under the GDPR and e-Privacy transposition acts. It appears doubtful whether pre-formulated declarations consenting to the processing of personal data to personalise a manipulative choice architecture, would pass the fairness test under the Unfair Contract Terms Directive (UCTD) in conjunction with Recital 42 GDPR. Similarly, the processing itself may prove unfair within the meaning of Article 5(1)(a) GDPR. The GDPR imposes additional requirements for automated decision-making and profiling, as well as the processing of sensitive data. Article 22(1) of the GDPR gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or affects them in a similarly significant manner. In accordance with the GDPR’s data protection by design and by default principle, controllers and processors must design their processing operations in a manner that is compliant with the GDPR from the outset. The fairness and accuracy principle further safeguard the data subject against algorithmic discrimination and error-prone algorithms. Depending on a broad or narrow interpretation, transparency requirements ensure that controllers provide data subjects with actionable information. Transparency presents the logical first step to obtaining redress.

Besides data protection and privacy, the Unfair Commercial Practices Directive (UCPD) prohibits certain unfair commercial practices. Practices are unfair if they are listed in Annex I, qualify as misleading or aggressive practices, or contravene professional diligence and are likely to materially distort the economic behaviour of the average consumer. According to one commentator, the
Article 5(2) UCPD general clause is fit to rein in manipulative practices. Some argue that price differentiation among consumers and behavioural manipulation may cause competitive harm and qualify as abuse of dominance under Article 102 TFEU, thereby violating EU competition law. According to the sector-specific Audiovisual Media Services Directive (AVMSD), audiovisual commercial communications must not use subliminal techniques (Article 9(1)(b) AVMSD). The Commission guidance on the interpretation and application of the UCPD and Annex 1.5 of the Commission study on advertising and marketing practices contain further details on the EU legal framework for commercial practices and advertisement.

To mitigate risks posed by AI systems to health, safety and fundamental rights, the Commission proposes an artificial intelligence act (AI act). The Commission suggests a risk-based approach that i) prohibits AI ‘practices’ entailing unacceptable risks, ii) subjects high-risk AI systems and practices to strict conditions including an ex-ante conformity assessment, and iii) mandates transparency obligations for AI systems with limited risks. The manipulation through subliminal techniques and the exploitation of vulnerabilities would be prohibited where such practices cause or are likely to cause physical or psychological harm (as opposed to economic harm). While certain AI systems qualify as ‘high-risk’ based on their technical functionality and intended use, it appears unlikely that manipulative AI systems causing economic harm would be covered systematically. Researchers have called for the prohibition of such manipulative AI systems, including when operators deploy them in a non-subliminal manner. Additionally, a wider range of biometric surveillance systems and practices (see next section for details), as well as employee monitoring, would be subject to additional requirements. Researchers suggest adding ‘total surveillance’ and ‘infringement on mental privacy and integrity as prohibited AI practices’.

On 15 December 2020, the Commission tabled its digital services act proposal (DSA), which ‘seeks to foster responsible and diligent behaviour by providers of intermediary services to ensure a safe online environment, which allows Union citizens and other parties to freely exercise their fundamental rights, in particular the freedom of expression and information’. To this end, it enumerates liability exemptions for intermediary services providers for third-party information they transmit or store, and imposes asymmetric due diligence obligations, concerning content moderation, recommender systems, online advertising and algorithmic systems, among other things. Online platforms would need to provide advertisement recipients with meaningful information, including on why the individual was targeted. ‘Very large platforms’ (VLOPs, with more than 45 million users), would need to conduct risk assessments of the fundamental right implications of ‘content moderation systems, recommender systems and systems for selecting and displaying advertisement’ and mitigate risks where necessary (Articles 26 and 27, DSA). Additionally, VLOPs would need to set out the main parameters used in their recommender systems in their terms and conditions. In its position of 20 January 2022, Parliament proposed more options for tracking free advertising, a ban on using minors’ data for targeted ads, and prohibition of deceiving or nudging techniques to influence users’ behaviour through ‘dark patterns’. Council and Parliament reached a provisional agreement on the text in April 2022.

Throughout 2020, Parliament repeatedly signalled awareness of risks of data misuse and behavioural manipulation associated with increasing digitalisation and the dissemination of new technologies. Parliament noted that new techniques for the collection and processing of personal data for the purposes of behavioural prediction and manipulation have an increasing impact on fundamental rights, and encouraged the effective application of EU data protection law and privacy law. It underlined the need to avoid any use that might lead to inadmissible direct or indirect coercion, threaten to undermine psychological autonomy and mental health, or lead to unjustified surveillance, deception or inadmissible manipulation. Ahead of the DSA proposal, Parliament stressed that consumers’ and users’ fundamental rights should be protected from harmful online business models, including those conducting digital advertising, as well as from behavioural manipulation and discriminatory practices. The Internal Market and Consumer Protection (IMCO)
Committee requested a study on online advertising and held a hearing on the risks of the use of dark patterns for consumers and the digital single market.

Restricting biometric technologies

As biometric surveillance systems spread, civil society is raising awareness of their intrusive nature and advocating a ban on mass biometric surveillance. Besides posing risks to fundamental rights to privacy, data protection and non-discrimination, they may interfere with children’s and elderly people's rights, the freedoms of expression, assembly and association, and others. 'As the context of their processing could create significant risks to the fundamental rights and freedoms', the processing of biometric data is subject to additional requirements under the GDPR (Article 9 and Recital 51) and the Law Enforcement Directive (LED, Article 10 and Recital 37). Like the GDPR, the LED also contains special provisions on the use of automated decision-making (Article 11).

Under the proposed AI act, Biometric systems are not regulated equally, but rather disparately depending on their risk classification, which depends on their design and application. The circulation and use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is prohibited, unless strict conditions are satisfied. Several forms of biometric systems, such as those used for 'real-time' and 'post' remote biometric identification, or those used by public authorities to detect individuals' emotional states, qualify as 'high-risk' AI systems and are subject to strict conditions, including an ex-ante conformity assessment. These conditions are not mutually exclusive and apply cumulatively where the biometric technique satisfies the criteria that give rise to the respective legal conditions. In principle, users of emotion recognition and biometric categorisation systems must inform concerned individuals about the operation of these systems. For high-risk AI systems intended to be used for 'real-time' and 'post-' remote biometric identification of natural persons, special record-keeping and human oversight rules would apply. In their joint opinion, the EDPB and European Data Protection Supervisor (EDPS) called for a complete ban on biometric identification in publicly accessible spaces. To ensure regulation of next-generation biometric systems, researchers recommend covering systems relying on 'biometrics-based' data. Additionally, they suggest recognising a new category of 'restricted AI applications'. The regulation of facial recognition technologies is one of the most contentious issues (see a September 2021 EPRS publication).

Parliament has called for limits to the use of facial recognition in the EU on several occasions. It highlighted that the use of biometric data gathered in public areas for remote identification purposes (such as facial recognition) bears particular risks for fundamental rights and stressed that such technology should only be used by Member States' public authorities for substantial public interest purposes. Parliament also invited the Commission to consider a moratorium on the use of these facial recognition systems in public spaces by public authorities and on education and healthcare premises. It also called for a moratorium on the deployment of facial recognition systems for law enforcement purposes that have an identification function, unless strictly used for the purpose of identification of victims of crime, until compliant technical standards are established, as well as calling for a ban on the use of private facial recognition databases in law enforcement.

Enhance compliance and enforcement

Citizens criticise a lack of compliance and enforcement and recommend measures to improve the situation. Specifically, they suggest:

- reinforcing strict and uniform enforcement of the existing EU data acquis;
- setting up a pan-EU agency 'that would have to clearly define intrusive behaviour ... and create guidelines and mechanisms for how citizens can opt-out and revoke data, especially from third parties. It must have a mandate to identify and sanction fraudsters and non-compliant organisations'.


imposing a licensing obligation as a precondition for processing personal data. This authorisation should be suspended or revoked after two consecutive violations (to be defined), and immediately after a serious violation.

creating an 'EU certification system that would reflect compliance with the GDPR ... This certificate would be mandatory and visible on websites and platforms.'

Enhanced enforcement of existing EU data protection acquis

The GDPR provides for individual, collective and public data protection enforcement instruments. Individuals may seek to enforce their rights, including claiming compensation for material and non-material damages, through legal actions under the GDPR or Member State law. EU countries have set up national DPAs to supervise and monitor the application of data protection laws in their territory (Article 57 GDPR). Additionally, the GDPR established the EDPB as a replacement for the Art. 29 WP, gathering representatives of all Member State DPAs and the 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 (Article 70 GDPR).

National supervisory authorities may launch compliance investigations ex officio or upon complaint. They are equipped with investigative, corrective, authorisation and advisory powers (Articles 58 and 83 GDPR). Most prominently, supervisory authorities may impose fines of up to €20 million, or 4 % of the party at fault’s total worldwide turnover (Article 58(2)(i) and 83(5) GDPR).

The GDPR establishes a 'one stop shop mechanism' allowing companies to deal with one single DPA in cross-border data protection cases. The mechanism is designed to: ensure the GDPR is consistently applied; provide legal certainty; reduce the administrative burden for organisations; and make it simpler for individuals to exercise their rights from their home base.

Since the GDPR’s entry into force, the LIBE committee, the EPDB, the Multilevel Stakeholder Group and the Council have alerted the Commission to concerns over resource constraints. 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 receive sufficient resources to carry out their tasks. In a March 2021 resolution, Parliament: 1) urged DPAs 'to speed up the resolution of cases, and to use the full range of possibilities under the GDPR, particularly if there are systematic and persistent breaches, including with gainful interest and a large number of affected data subjects'; ii) called on 'Member States ... to comply with their legal obligation under Article 52(4) to allocate sufficient funds to their DPAs to allow them to carry out their work in the best way possible and to ensure a European level playing field for the enforcement of the GDPR'; and iii) called on 'the Commission to evaluate the possibility of obliging large multinational technology companies to pay for their own oversight through the introduction of an EU digital tax'.

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 DPA’s enforcement practices. Divergent practices also signify shortcomings in the one-stop-mechanism. Parliament expressed great concern over the functioning of this mechanism, particularly regarding the role of the Irish and Luxembourg DPAs. It is ‘particularly concerned that the Irish data protection authority generally closes most cases with a settlement instead of a sanction and that cases referred to Ireland in 2018 have not even reached the stage of a draft decision pursuant to Article 60(3) of the GDPR’. It pointed out that the success of the ‘one-stop shop-mechanism’ is contingent on the time and effort that DPAs can dedicate to the handling of and cooperation on individual cross-border cases in the EDPB. Consequently, ‘the lack of political will and resources has immediate consequences on the extent to which this mechanism can function properly’. Conversely, Irish Commissioner for Data Protection, Helen Dixon, shines a light on the challenges DPAs face in her correspondence with the LIBE committee. In a May 2021 resolution, Parliament called on the Commission to start infringement procedures against Ireland for not properly enforcing the GDPR.
Introduce a compulsory licensing or certification scheme

The International Organization for Standardization (ISO) provides a universal definition of certification as 'the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements'. While certification may be mandated by law, it is voluntary under the GDPR (Article 42(3) GDPR), meaning the data controller or processor may freely decide to submit to the certification procedure. The acknowledgement of compliance (certification) by a non-partisan instance (certification body) serves to inspire consumer trust and confidence in business-to-business relationships. In practice, an accredited certification body, such as a supervisory authority or third party, would assess the controller's or processor's activities for compliance with approved certification criteria. Upon successful completion of the procedure, the certification body would issue a statement of GDPR conformity (certification) and potentially grant the use of a logo or symbol (seal or mark). According to Article 42 GDPR, Member States, the supervisory authorities, the Board and the Commission should encourage the establishment of data protection certification mechanisms and of data protection seals and marks.

The voluntary nature of certification does not mean that it is without legal consequences. Once a controller or processor successfully concludes the certification process, a contractual relationship between the certification body and the controller or processor is established. Accredited monitoring and certification bodies may sanction infringements against certification schemes in accordance with contractual sanction policies. Supervisory authorities must be informed about violations, not least to enable them to exercise their supervisory powers where violations of the certification scheme simultaneously present an infringement of the GDPR. Certification does not reduce the controller or the processor's responsibility for compliance with the GDPR and is without prejudice to the tasks and powers of the supervisory authorities (Articles 42(4) and 43(1) GDPR). However, certification does relax the burden of proof for compliance (e.g. Articles 24(3), 25(3), 28(5) or 32(3) GDPR) and serves as an attenuating circumstance in the face of fines (Article 83(2)(j) GDPR).

Promote privacy awareness and literacy

Citizens' Panel 1 recommends that communication around the GDPR is improved. According to a 2019 Special Eurobarometer survey on the GDPR (fieldwork 2019), more than two thirds (67%) of respondents have heard of the GDPR, although there is a fairly even split between those who have heard of it and know what it is (36%) and those who have heard of it but don’t know exactly what it is (31%). Almost two thirds (65%) have heard of the right to access their data, while 61% have heard of the right to correct their data if it is wrong. Almost 6 in 10 (57%) respondents indicate they have heard about the existence of a public authority in their country that is responsible for protecting their rights regarding their personal data. One in five have heard of this and know which public authority is responsible, while 37% have heard of it, but do not know which authority is responsible.

Supervisory authorities are tasked with promoting awareness and understanding of the GDPR (Article 57(1)(b) and (d), as well as Recital 132 GDPR). Recently, the EDPB released guidelines on the right of access for public consultation. The GDPR obliges controllers to inform data subjects of their rights and to facilitate the exercise of such rights (Article 12-14 GDPR). Further transparency obligations (arguably) ensure that controllers provide data subjects with actionable information to enable legal redress. Within the sphere of controllers and processors, data protection officers shall raise awareness and train staff involved in processing operations (Article 39(1)(b) GDPR). 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. Under 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.

Parliament recently raised concerns that some companies continually fail to provide concise, transparent, intelligible and easily accessible information to data subjects, using clear and plain language and that properly functioning data subject access mechanisms are not widely available.
Commission called on the EDPB and DPAs ‘to adopt further guidelines which are practical, easily understandable, and which provide clear answers and avoid ambiguities on issues related to the application of the GDPR, for example on ... data subject rights...’. On consumer protection, EU lawmakers set an example by mandating an online entry point where consumers can access updated information about their EU consumerrights in a clear, understandable and easily accessible manner.

Summary table

<table>
<thead>
<tr>
<th>Citizens’ expectations</th>
<th>Citizens’ policy recommendations</th>
<th>Related Parliament activities</th>
<th>Parliament and citizens aligned on policy problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced data subject control over data</td>
<td>- ensure genuine choice by design</td>
<td>- enacted strict consent rules under the GDPR and e-Privacy Directive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- promote data control technologies</td>
<td>- adopted the data governance act</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- provide clearer and stricter rules on the processing of minors’ data</td>
<td>- advocates for genuine choice design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- introduce a special category for sensitive minors’ data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced protection of minors</td>
<td>- restrict public actor collection of data</td>
<td>- enacted and negotiating several laws restricting state surveillance, surveillance capitalism and certain biometric data processing</td>
<td>- Article 3 Regulation 2021/1232</td>
</tr>
<tr>
<td></td>
<td>- restrict big tech company collection of data and control of the digital world</td>
<td>- called for infringement procedures against Member States with non-compliant data retention rules</td>
<td>- Article 3(5) Regulation 2019/1157</td>
</tr>
<tr>
<td></td>
<td>- restrict biometric technologies</td>
<td>- set up a committee of inquiry to investigate the Pegasus scandal</td>
<td>- compulsory or voluntary certification</td>
</tr>
<tr>
<td>Tamed surveillance, profiling and manipulation</td>
<td>- enforce EU data protection acquis</td>
<td>- called for action against forms of biometric surveillance</td>
<td>- pan-EU agency with enforcement power</td>
</tr>
<tr>
<td></td>
<td>- impose compulsory data protection certification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- set up a pan-EU agency with enforcement powers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced compliance and enforcement</td>
<td>- better explain the GDPR and improve communication around it</td>
<td>- enacted information and awareness-raising obligations in the GDPR and flagged shortcomings in their implementation</td>
<td></td>
</tr>
<tr>
<td>Promoted privacy awareness and literacy</td>
<td>- enacted GDPR enforcement instruments, a one-stop-shop mechanism, and a voluntary certification scheme</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- urged dissuasive, uniform, and swift enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- called for increased funding for DPAs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- called for an infringement procedure against Ireland for insufficient enforcement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Author’s own elaboration based on sources referenced in the text.

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.


Photo credits: © vectorwin / Adobe Stock

eprs@ep.europa.eu (contact)

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

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

http://epthinktank.eu (blog)