



Paris, 19 November 2020

POLITICAL OPINION

on the European policy on data and Europe's digital sovereignty

The Senate European Affairs Committee,

Having regard to the Treaty on the Functioning of the European Union, in particular Article 16,

Having regard to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, 2000/C 364/01,

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector,

Having regard to Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, in particular Articles 2, 4, 24 to 43 and 44 to 50,

Having regard to Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA,

Having regard to Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union,

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013,

Having regard to Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information,

Having regard to Decision 2010/87/EU of the Commission of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended,

Having regard to Judgment C-311/18 of the Court of Justice of the European Union of 16 July 2020 (*Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*),

Having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 6 May 2015 entitled "A Digital Single Market Strategy for Europe", SWD(2015) 100,

Having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 10 January 2017 entitled "Building a European Data Economy", COM(2017) 9 final,

Having regard to the Communication from the Commission to the European Parliament and the Council of 24 January 2018 entitled "Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018", COM(2018) 43 final,

Having regard to the Communication from the Commission to the European Parliament and the Council of 29 May 2019 entitled "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union", COM(2019) 250 final,

Having regard to the Communication from the Commission to the European Parliament and the Council of 24 July 2019 entitled "Data protection rules as a trust-enabler in the EU and beyond – taking stock", COM(2019) 374 final,

Having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2020 entitled "A European strategy for data", COM(2020) 66 final,

Having regard to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 February 2020 entitled "Shaping Europe's digital future", COM(2020) 67 final,

Having regard to the Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions of 27 May 2020 entitled "Europe's moment: Repair and Prepare for the Next Generation", COM(2020) 456 final,

Having regard to the Communication from the Commission to the European Parliament and the Council of 24 June 2020 entitled "Way forward on aligning the former third pillar acquis with data protection rules", COM(2020) 262 final,

Having regard to the Communication from the Commission to the European Parliament and the Council of 24 June 2020 entitled "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation", COM(2020) 264 final,

Having regard to the recommendations 01/2020 of the European Data Protection Board on the measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data guaranteed by EU regulations, adopted on 10 November 2020,

Having regard to the recommendations 02/2020 of the European Data Protection Board on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020,

Having regard to the new draft standard contractual clauses published and submitted for consultation by the European Commission on 13 November 2020,

Having regard to the Senate's European resolution no. 122 (2015-2015) for a global, proactive and ambitious European digital strategy, adopted on 30 June 2015,

Having regard to the Senate's European resolution no. 131 (2016-2017) for a reform of the conditions for using the protective measures provided for in the regulation (EC) no. 1/2003 of the Council on the implementation of the rules on competition, adopted on 8 September 2017,

Having regard to the Senate's European resolution no. 122 (2019-2020) on modernising Europe's policy on competition, adopted on 20 July 2020,

Having regard to the Senate's information report "*L'Union européenne, colonie du monde numérique ?*" (no. 443, 2012-2013) - 20 March 2013 - by Ms Catherine Morin-Desailly, produced on behalf of the European Affairs Committee,

Having regard to the information report "*L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*" (no. 696, 2013-2014) - 8 July 2014 - by Ms Catherine Morin-Desailly, produced on behalf of the joint fact-finding mission on the Internet's global governance,

Having regard to the Senate's report "*Le devoir de souveraineté numérique*" (no. 7, 2019-2020) - 1 October 2019 - by Mr Gérard Longuet, produced on behalf of the committee of inquiry on digital sovereignty,

Having regard to the information report "*Moderniser la politique européenne de concurrence*" (no. 603, 2019-2020) - 8 July 2020 - by Messrs Alain Chatillon and Olivier Henno, produced on behalf of the European Affairs Committee and the Economic Affairs Committee,

Whereas data is central to the digital transformation, and data-driven innovation can provide considerable benefits in meeting major social and environmental challenges and transforming public action, including in the exercise of governments' sovereign powers,

Whereas the rapid growth in the amount of data produced each year around the world, estimated at 175 zettabytes in 2025, will continue to accelerate, driven in particular by the growing use of connected objects,

Whereas the data economy in the European Union is estimated to be worth €829 billion by 2025, more than double the amount in 2018,

Whereas personal data, in the same way as non-personal data, is a major strategic economic issue,

Whereas, also, the use of personal data, especially when they are related, for example, to racial and ethnic origin, political opinions, religious or philosophical convictions, union membership, or sexuality or sexual orientation, but also when they are of a socio-economic or behavioural nature, makes phenomena of interference in democratic processes possible,

Whereas, consequently, the control of data and its use, in particular via artificial intelligence technologies, represents a major economic and democratic issue,

Whereas the General Data Protection Regulation (GDPR) has already inspired many legislative adaptations in third countries in various regions around the world,

Whereas it is essential that European States ensure that neither third countries nor outside groups can access their strategic and sensitive data, personal or otherwise,

Whereas Article 4 of Regulation (EU) 2018/1807 of the European Parliament and the Council of 14 November 2018 establishing a framework for the free flow of non-personal data in the European Union sets out the principle of a free flow of this data within the European Economic Area, but, as it stands, there are no specific provisions on the hosting or processing of non-personal data abroad or by non-European-law companies,

Whereas a significant share of data produced in Europe by public and private actors are currently hosted and processed in third countries, particularly in the United States; whereas, also, even when these data are hosted and processed within Europe by extra-European companies, the existence of extraterritorial legislation such as the United States *Cloud Act* threatens the confidentiality of this data,

Whereas the Covid-19 health crisis has highlighted the dependency of European economic actors and European States on non-European, especially American but also Asian, digital actors for data collection, storage and processing capabilities, among others, due to a deficit in the European offering of infrastructure, software and platforms to make use of the data,

Whereas the modest size of European digital players compared to these extra-European actors do not allow them to be competitive on the European or global market nor to offer a service capacity comparable to their competitors,

On reinforcing European data protection

Underscores the dual threat to European States and the European Union represented, in terms of strategic autonomy, by the rivalry among government actors, for example through the existence of extraterritorial legislation such as the *Cloud Act*, on the one hand, and, on the other hand, the dominance of American and, to a lesser extent, Chinese private actors susceptible of competing with States in their sovereign functions given the considerable amount of data they hold,

Welcomes the European Union's growing awareness of the importance of digital sovereignty issues and the urgency of taking action,

Welcomes the Commission's recent initiatives, in particular the announcement of a body of legislation seeking to create a European area of non-personal data to guarantee optimal circulation and use of this data within the European Economic Area to support innovation and growth while ensuring the security of this data in a framework based on trust and equality,

Recalls that this legislative framework must be constituted without prejudice to the respect for pre-existing European legislation in terms of data protection, in particular personal data and data protected by business secrecy,

Will be attentive to the concrete arrangements for implementing these principles in the draft legislative texts that will be published by the Commission in the coming weeks,

Considers it essential to implement mechanisms in these texts that seek to effectively ensure compliance with European data protection standards by all actors, European or otherwise and irrespective of their location, susceptible of hosting and/or processing data, including data transferred for technical reasons,

Advocates a differentiated approach according to the degree of sensitivity of the data under consideration, taking into account their nature and the risk incurred, in the extension of existing European regulations, in particular Article 4 of Regulation (EU) 2018/1807 of the European Parliament and the Council of 14 November 2018 establishing a framework for the free flow of non-personal data in the European Union; underscores the need for a study coordinated at the European level of the scope of strategic data,

Calls for particular vigilance with regard to the personal and non-personal data necessary for States and European institutions to exercise their powers and sovereignty,

Requests the full and complete application of the provisions of the GDPR concerning the transfer of personal data to third countries; invites Member States and economic actors to not ignore the risks to personal data protection in these third countries, and to take all the organisational and/or technical measures necessary without delay to ensure that the guarantees provided in the GDPR are fully applied,

Calls for the full, complete, attentive application of the special protective dispositions on sensitive data, including when these result from the combination of personal data not categorised as "sensitive",

Underscores the need for economic actors to have clear and stable rules on the transfer of both personal and non-personal data to third countries,

Requests that computing service providers to both individuals and companies be required to be fully transparent about where the data entrusted to them are stored and processed as well as the purposes of this processing, and about the legislations to which they are subject,

On implementing a European strategy to support the European digital ecosystem

Considers it vital to promote greater awareness both among economic actors and the wider public of the strategic value of personal and non-personal data,

Calls for a reinforcement of the European digital ecosystem and for the implementation of a proactive industrial policy on the issue,

Recalls that Europe has all the necessary strengths, in particular in terms of human resources and training, to not just overcome its delay over the medium- and long-term in terms of data storage and hosting in strategic sectors but to also take full advantage of current and upcoming waves of innovation regarding the use of data (artificial intelligence, augmented reality, etc.),

Regrets the chronic under-investment in Europe in digital technologies over the past few decades; welcomes, however, the fact that 20% of the funds provided in the European stimulus plan being adopted are intended for the digitisation of the economy,

Calls, nevertheless, for greater vigilance in selecting the recipients of these funds to support, as a priority, the development and growth of European companies that fully respect European data protection regulations,

Welcomes the Franco-German Gaia-X initiative as well as the joint declaration of Member States supporting the European cloud initiative of 15 October 2020, wishes for the interactions between the two projects to be clarified, highlights the need to protect European cloud users from any exposure to legislation or practices allowing for improper access to their data while maintaining a maximum amount of openness to non-European actors,

Calls for special attention to be paid to interoperability and data portability to avoid lock-in effects within the cloud, encourage innovation, foster competition and allow for new players to emerge,

Desires the implementation of an important project of common European interest (IPCEI) in the cloud sector,

Requests, in general, that the Commission reconsider European rules of competition, particularly in terms of State aid, and ensure that practices in public contracts allow European small and medium enterprises (SMEs) to effectively access them in order to create the conditions for an innovative and competitive European digital ecosystem to emerge,

Calls on the European Union to continue and intensify its "data diplomacy" policy both towards international partners and within international bodies to spread standards in terms of data collection, processing and use.