BRIEFING

Requested by the LIBE committee

European Parliament

Personal data protection achievements during the legislative term 2014-2019: the role of the European Parliament

Protection of personal data and respect for private life are important fundamental rights in the European Union.

Considerable progress was made in safeguarding privacy during the legislative term 2014-2019 – most importantly, new EU data protection rules strengthening citizens' rights and simplifying the rules for companies in the digital age took effect in May 2018.

The European Parliament has always insisted on the need to strike a balance between enhancing security and safeguarding human rights, including data protection and privacy.

In Parliament, the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) is responsible for legislation in the area of the protection of natural persons with regard to the processing of personal data, according to Parliament's Rules of Procedure.

Main legislative instruments on data protection

1. EU Treaties

Article 16 of the **Treaty on the Functioning of the European Union** (TFEU) stipulates that everyone has the right to protection of personal data concerning them. It specifies that Parliament and the Council lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

Compliance with these rules is subject to monitoring by independent authorities.

Articles 7 and 8 of the **Charter of Fundamental Rights of the European Union** provide the basis for the respect for private and family life and the protection of personal data.

Policy Department for Citizens' Rights and Constitutional Affairs
Author: Kristiina Milt
Directorate-General for Internal Policies
PE 608.870- April 2019

EN

2. International Conventions

2.1 The Council of Europe Convention for the **Protection of Individuals with regard to Automatic Processing of Personal Data** (ETS No 108) of 28 January 1981. This Convention is the first binding international instrument protecting the individual against abuses which may accompany the collection and processing of personal data. It sets out the right of individuals to protect their personal data and, at the same time, seeks to regulate the transfrontier flow of personal data.

Under the consent procedure, Parliament adopted its legislative resolution of 12 March 2019 on the draft Council Decision authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Council can now authorise Member States to ratify the amending protocol.

The amending Protocol aims to widen the scope, increase the level of data protection afforded under Convention 108, as well as improving its effectiveness. The modernised Convention (i.e. Convention 108 modified by the amending Protocol) will cover all types of data processing under the jurisdiction of the Parties, in both the public and private sectors, as well as national security.

2.2 Article 8 of the Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms (**European Convention on Human Rights** (ECHR)) establishes the right to respect for private and family life: 'Everyone has the right to respect for his private and family life, his home and his correspondence.'

Main EU legislative acts on data protection

1. General Data Protection Regulation (GDPR)

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 (General Data Protection Regulation), entered into force in May 2018. The GDPR applies to the European Economic Area (EEA), which includes all EU countries plus Iceland, Liechtenstein and Norway.

The rules aim to protect all EU citizens from privacy and data breaches in an increasingly data-driven world, while creating a clearer and more consistent framework for businesses, and a more robust and clear set of rights for data subjects. The rights enjoyed by citizens include clear, affirmative and freely given consent for their data to be processed and the right to receive clear and understandable information about it; the rights of access, rectification, deletion and restriction; the right to be forgotten: the right to ask for his/her data to be deleted; the right to transfer data to another service provider or data portability (e.g. when switching from one social network to another); and the right to know when data has been hacked. These rules apply to all companies operating in the EU, even if these companies are based outside of the EU, provided they offer services or goods in the Union or monitor the behaviour of data subjects in the Union. Furthermore, strong enforcement powers are conferred on the data protection authorities, enabling them to impose corrective measures, such as warnings and orders, or impose fines on firms that break the rules.

2. Data Protection Law Enforcement Directive

Directive (EU) 2016/680 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 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, entered into force in May 2018.

The directive protects citizens' fundamental right to data protection whenever personal data is used by Member States' law enforcement authorities for law enforcement purposes, either at domestic level or when data is shared between the Member States. It ensures that the personal data of victims, witnesses, and suspects of crime are duly protected, and facilitates cross-border cooperation in the fight against crime and terrorism. Independent national public authorities are endowed with effective powers to monitor and enforce compliance with the rules and to ensure the protection of data subjects' rights.

3. Directive on privacy and electronic communications

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 (Directive on privacy and electronic communications) was modified by Directive 2009/136/EC of 25 November 2009.

The ePrivacy Directive sets out rules to ensure the confidentiality of electronic communications content and traffic data sent by means of publicly available electronic communications services, security in the processing of personal data, and the notification of personal data breaches. It states that the placing of cookies or other similar devices in the data subject's terminal equipment to gain access to information stored without the consent of the individual is unlawful. It also bans unsolicited communications where the user has not given his/her consent.

The new proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) is currently under consideration. The new proposal would apply to the EEA.

This proposal seeks to update the legal framework and aims to reinforce trust and security in the digital single market. The draft regulation also aligns the rules for electronic communications services with the new world-class standards of the GDPR. It would apply to new providers or electronic communications services (Over-the-Top communications services (OTTs), such as telephony and communications over the internet, chat messaging services, etc.).

The LIBE Committee adopted its report on the ePrivacy proposal and the mandate for negotiation in October 2017. Parliament then voted to approve the decision to enter into interinstitutional negotiations on 26 October 2017. Parliament is waiting for the Council to conclude its work in order to start the trilogues. Please see the procedure file in the Legislative Observatory for more details.

4. Regulation on processing of personal data by the Union institutions and bodies

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC entered into force on 11 December 2018. The Regulation applies to the EEA.

The Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies, and rules relating to the free movement of personal data between them or to other recipients established in the Union. The Regulation protects the fundamental rights and freedoms of natural persons and, in particular, their

right to the protection of personal data. The European Data Protection Supervisor monitors the application of the provisions of this Regulation to all processing operations carried out by a Union institution or body.

Articles on data protection in sector-specific legislative acts

In addition to the main legislative acts on data protection alluded to above, specific articles on data protection are also stipulated in the sector-specific legislative acts, such as:

- Article 13: protection of personal data, in Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;
- Chapter VI: data protection safeguards, in Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol);
- Chapter VIII: data protection, in Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO').

The EU's main international arrangements on data transfers

1. Commercial data transfers: Adequacy Decisions

The Commission[1] has the power to determine, on the basis of Article 45 of the GDPR whether a country outside the EU offers an adequate level of data protection, whether on the basis of its domestic legislation or of the international commitments it has entered into.

The adoption of an adequacy decision involves a proposal from the Commission; an opinion of the European Data Protection Board; approval from a committee of representatives of EU countries; and the adoption of the decision by the Commission.

At any time, Parliament and the Council may request that the Commission maintain, amend or withdraw the adequacy decision on the grounds that its enactment exceeds the implementing powers provided for in the Regulation.

The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to the third country in question without any further safeguards being necessary. In other words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

The Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

Adequacy talks are ongoing with South Korea.

[1] Please see the European Commission's website: Adequacy of the protection of personal data in non-EU countries, last accessed 13 March 2019.

These adequacy decisions do not cover data exchanges in the law enforcement sector, which are governed by the Data Protection Law Enforcement Directive (Article 36). For the special arrangements concerning exchanges of data in this field, please see the Passenger Name Record (PNR) and Terrorist Financing Tracking Programme (TFTP) agreements below.

From the outset, the LIBE Committee has followed negotiations on the adequacy decisions closely and will continue to scrutinise their implementation.

In particular, during the current legislative term, Parliament has adopted several resolutions on transatlantic data flows:

- its resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens;
- its resolution of 26 May 2016 on transatlantic data flows;
- its resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield;
- its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield;
- its resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection.

In all of these resolutions, Parliament raised several concerns regarding transatlantic data flows. In its most recent resolution of 25 October 2018, Parliament regretted that the deadline of 1 September 2018 for the US to be fully compliant with the Privacy Shield had not been met and considered, therefore, that the Commission had failed to act in accordance with Article 45(5) of the GDPR. It went on to urge the Commission to suspend the Privacy Shield until the US authorities comply with its terms.

The adoption procedure for the adequacy decision concerning Japan was launched on 5 September 2018. Parliament's resolution of 13 December 2018 on the adequacy of the protection of personal data afforded by Japan called on the Commission to provide further evidence and explanations regarding the concerns expressed in the resolution, in order to demonstrate that the Japanese data protection legal framework ensures an adequate level of protection that is essentially equivalent to that of the European data protection legal framework. Parliament expressed its belief that this adequacy decision could, furthermore, send out a strong signal to countries around the world that convergence with the EU's high data protection standards offers very tangible results; and stressed, in this regard, the importance of this adequacy decision as a precedent for future partnerships with other countries that have adopted modern data protection laws. Following this, the Commission adopted its implementing decision of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information.

2. EU-US Umbrella Agreement

Parliament has been involved in the approval, under the consent procedure, of the Agreement between the US and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, known as the 'Umbrella Agreement'. The aim of this agreement is to ensure a high level of protection of personal information transferred in the framework of transatlantic cooperation for law enforcement purposes, namely in the fight against terrorism and organised crime. The agreement complements existing and future EU-US and Member State-US agreements between law enforcement authorities. It is not in itself a legal instrument for any transfer of personal information to the US but it supplements, where necessary,

data protection safeguards in existing and future data transfer agreements or national provisions authorising such transfers.

Following the adoption of the Judicial Redress Act by the US Congress in February 2016 giving EU citizens the right to seek judicial redress in the US, the agreement was signed by the Commission and the US authorities on 2 June 2016.

Parliament gave its consent in its legislative resolution of 1 December 2016 on the draft Council decision on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.

Parliament's consent was followed by Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion of the Agreement, and the Agreement itself was published on 10 December 2016.

3. EU-US, EU-Australia and EU-Canada passenger name record (PNR) agreements

The EU has signed bilateral passenger name record (PNR) agreements with the United States, Australia and Canada. PNR data is information provided by passengers when they book flight tickets and when checking in for flights, as well as data collected by air carriers for their own commercial purposes. PNR data can be used by law enforcement authorities to fight serious crime and terrorism. The transfer of PNR data from the EU to third countries can only be done through a bilateral agreement that provides for a high level of personal data protection.

The current Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security entered into force on 1 June 2012.

The current Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service entered into force on 1 June 2012.

The Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data was published on 21 March 2006. It expired in September 2009. The Commission, on the basis of Council directives, negotiated a new draft agreement with Canada on PNR. On 18 July 2013, it adopted a proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data and a proposal for a Council decision on the signature of the Agreement. The Agreement was signed on 25 June 2014. The Council asked for Parliament to give its consent to it on 8 July 2014.

Before voting on the envisaged new EU-Canada Agreement, Parliament decided to seek an opinion of the Court of Justice of the European Union (CJEU), as provided for under Article 218(1) of the TFEU, in its resolution of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data.

Following this, on 26 July 2017 in its Opinion 1/15 the CJEU found that the PNR agreement could not be concluded in its current form because several of its provisions were incompatible with fundamental rights recognised by the EU. Specifically, Articles 7, 8, 21 and 52(1) of the Charter of Fundamental Rights of the European Union. In sum, the CJEU believed that the transfer of PNR data from the EU to Canada, and the rules laid down in the envisaged agreement on the retention of data, its use and its possible subsequent transfer to Canadian, European or foreign public authorities

entailed interference with the fundamental right to respect for private life. Similarly, the envisaged agreement entailed interference with the fundamental right to the protection of personal data.

Subsequent to this opinion, on 18 October 2017 the Commission adopted a recommendation for a Council Decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime 'in line with the requirements laid down by the Court's Opinion' and with an amended title. Further to the Council Decision of December 2017, new PNR negotiations with Canada were launched in June 2018. Negotiations are ongoing.

On 11 April 2018, the Article 29 Data Protection Working Party released a letter to the Commission stating that the Court's analysis could have an implicit effect on other PNR agreements.

Please see the procedure file in the Legislative Observatory for more details on the ongoing EU-Canada PNR Agreement.

4. EU-US Terrorist Finance Tracking Programme (TFTP)

The EU has signed a bilateral agreement with the US on the processing and transfer of financial messaging data from the EU to the US for the purposes of the terrorist finance tracking programme.

Council Decision (2010/412/EU) of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program entered into force on the day of its adoption.

In its resolution of 9 July 2015 on the European Agenda on Security, Parliament recalled the crucial importance of tracking and disrupting financial flows, including non-Swift financial flows, in combating terrorist networks and organised crime groups, and welcomed the efforts undertaken to ensure a fair and balanced participation in the Terrorist Finance Tracking Programme (TFTP).

In its resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, Parliament expressed disappointment that the Commission had disregarded its clear call for the suspension of the TFTP agreement, given that no clear information had been given to clarify whether SWIFT data could have been accessed outside TFTP by any other US government body, and noted that it intended to take this into account when considering giving consent to future international agreements.

Addressing data protection aspects in sector-specific resolutions

Several Parliament resolutions on different policy areas also address personal data protection in order to ensure consistency with general Union data protection law and the protection of privacy in those specific sectors. The most relevant resolutions are:

- its resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics;
- its resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement;
- its resolution of 13 December 2018 on Blockchain: a forward-looking trade policy;
- its resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics.

EU Data Protection Supervisory Authorities

1. European Data Protection Supervisor (EDPS)

The EDPS is an independent supervisory authority that ensures that the EU institutions and bodies meet their obligations with regard to data protection. The primary duties of the EDPS are supervision, consultation and cooperation.

The EDPS is established in the Regulation on processing of personal data by the Union institutions and bodies.

2. European Data Protection Board (EDPB)

The EDPB, formerly the Article 29 Working Party, has the status of an EU body with legal personality and is provided with an independent secretariat. The EDPB brings together the EU's national supervisory authorities, the EDPS and the Commission. The EDPB has extensive powers to settle disputes between national supervisory authorities and to give advice and guidance on key concepts of the GDPR and the Data Protection Law Enforcement Directive.

The EDPB is established in the GDPR.

Tools to support the evidence-based policies

1. Meetings with experts

Parliament has held numerous meetings, hearings, interparliamentary committee meetings and conferences on various aspects of personal data protection. The following main meetings on this topic permitted Members to hear from experts and to hold discussions on the key issues:

- Appointment of the European Data Protection Supervisor and the Assistant Supervisor on 20 October 2014;
- Hearing on Trade agreements and data flows: Safeguarding the EU data protection standards on 16 June 2015;
- High level conference on Protecting online privacy by enhancing IT security on 8 December 2015;
- Hearing on The new EU-US Privacy Shield for commercial transfers of EU personal data to the US on 17 March 2016;
- Hearing on the Fundamental Rights Implications on Big Data on 8 December 2016;
- Hearing on the e-Privacy reform on 11 April 2017;
- Interparliamentary Committee meeting on The Implementation of the Data Protection package – At the eve of its application on 15 May 2018;
- Meeting with Mark Zuckerberg at the European Parliament on 22 May 2018;
- Hearing on the Facebook/Cambridge Analytica Case – Part 1: Use of Facebook users' data by Cambridge Analytica and impact on data protection – Mapping the case on 4 June 2018;
- Hearing on the Facebook/Cambridge Analytica Case – Part 2: Use of Facebook users' data by Cambridge Analytica and impact on data protection – Consequences on 25 June 2018;
- Hearing on the Facebook/Cambridge Analytica Case – Part 3: Use of Facebook users' data by Cambridge Analytica and impact on data protection – Policy solutions and remedies on 2 July 2018.

2. Ad hoc delegations

Parliament organises various ad hoc delegations to obtain first-hand information from the relevant countries or organisations. In the field of personal data protection, it has proved a very useful tool to enable the LIBE Committee to follow the negotiations on the adequacy decisions and their implementation. In the current legislative term, the LIBE Committee organised such ad hoc delegations to Japan in October 2017, to South Korea in October 2018 and several ad hoc delegations to the US in 2015, 2016, 2017 and 2018.

3. Supporting analyses

Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, and the European Parliamentary Research Service, have commissioned several analyses at the request of the LIBE Committee to support the work of Parliament in the field of personal data protection. The main studies produced during the current parliamentary term are as follows:

- The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area, published in November 2014;
- The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, published in May 2015;
- A Comparison between US and EU Data Protection Legislation for Law Enforcement, published in September 2015;
- Big Data and Smart Devices and Their Impact on Privacy, published in September 2015;
- An Assessment of the Commission's Proposal on Privacy and Electronic Communications, published in May 2017;
- Assessment of the impact of specific aspects of the new model of governance and accountability of data protection by Union institutions and bodies proposed by the European Commission, published in September 2017;
- The future EU-UK relationship: options in the field of the protection of personal data for general processing activities and for processing for law enforcement purposes, published in August 2018.

Conclusions

Parliament has played a key role in shaping EU legislation in the field of personal data protection by making protecting privacy into a political priority. An almost complete overhaul of the EU personal data protection rules has taken place during the current legislative term. Parliament has been working on the data protection reform on an equal footing with the Council under the ordinary legislative procedure. Parliament has also concluded its work on the only remaining significant piece of the puzzle, the new Regulation on Privacy and Electronic Communications, and is impatiently waiting for the Council to conclude its work, in order to start the negotiations.

During the current legislative term, Parliament has also considerably stepped up its involvment in supervising the international arrangements on data transfers. Whether via the consent procedure or own-initiative reports, Parliament has made sure its voice has been heard. Moreover, it did not shy away from seeking an opinion of the CJEU, as provided for under Article 218(1) of the TFEU, resulting in the Court sharing Parliament's legitimate concerns. In addition, the LIBE Committee has been actively monitoring the negotiations on and implementation of the agreements via several ad hoc delegations to the relevant third countries.

Having made sure that the EU data protection rules were properly put in place, Parliament's role will probably now shift more towards monitoring the implementation of the legislation.

In sum, considerable progress has been made in relation to safeguarding privacy during the legislative term 2014-2019 – most importantly, the new EU data protection rules strengthening citizens' rights and simplifying the rules for companies in the digital age took effect in May 2018.

Contact: poldep-citizens@europarl.europa.eu

This document is available on the Internet at: http://www.europarl.europa.eu/supporting-analyses

Print ISBN 978-92-846-4734-7 | doi: 10.2861/541540 | QA-03-19-249-EN-C
PDF ISBN 978-92-846-4733-0 | doi: 10.2861/666189 | QA-03-19-249-EN-N