

Basic information	
1990/0287(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Directive	Procedure completed
Personal data protection Repealed by 2012/0011(COD) See also 1999/0153(COD) Subject 1.20.09 Protection of privacy and data protection	

Key players			
European Parliament	Committee responsible		Rapporteur
	JURI Legal Affairs, Citizens' Rights		MEDINA ORTEGA Manuel (PSE)
	Committee for opinion		Rapporteur for opinion
	ECON Economic and Monetary Affairs, Industrial Policy		HERMAN Fernand H.J. (PPE)
Council of the European Union	Council configuration		Meetings
	General Affairs		1827
	Economic and Financial Affairs ECOFIN		1828
	Competitiveness (Internal Market, Industry, Research and Space)		1769
	Competitiveness (Internal Market, Industry, Research and Space)		1815
	Budget		1866
	Research		1810

Key events			
Date	Event	Reference	Summary
24/09/1990	Legislative proposal published	COM(1990)0314 	Summary
12/10/1990	Committee referral announced in Parliament, 1st reading		
10/02/1992	Debate in Parliament		
		COM(1992)0422	Summary

15/10/1992	Modified legislative proposal published		
23/11/1993	Vote in committee, 1st reading		
16/06/1994	Debate in Council		Summary
01/12/1994	Debate in Council		
20/02/1995	Council position published	12003/3/1994	Summary
15/03/1995	Committee referral announced in Parliament, 2nd reading		
23/05/1995	Vote in committee, 2nd reading		Summary
23/05/1995	Committee recommendation tabled for plenary, 2nd reading	A4-0120/1995	
14/06/1995	Debate in Parliament		Summary
24/07/1995	Act approved by Council, 2nd reading		Summary
24/10/1995	Final act signed		
24/10/1995	End of procedure in Parliament		
23/11/1995	Final act published in Official Journal		

Technical information	
Procedure reference	1990/0287(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
Amendments and repeals	Repealed by 2012/0011(COD) See also 1999/0153(COD)
Legal basis	EC Treaty (before Amsterdam) E 100A EC Treaty (before Amsterdam) E 113
Stage reached in procedure	Procedure completed
Committee dossier	JURI/4/06427

Documentation gateway				
European Parliament				
Document type	Committee	Reference	Date	Summary
Text adopted by Parliament, 1st reading/single reading		T3-0140/1992 OJ C 094 13.04.1992, p. 0077-0198	11/03/1992	Summary
Committee final report tabled for plenary, 1st reading /single reading		A3-0364/1993 OJ C 342 20.12.1993, p. 0002	23/11/1993	
Text adopted by Parliament confirming position adopted at 1st reading		T3-0681/1993 OJ C 342 20.12.1993, p. 0015-0030	02/12/1993	Summary
Committee recommendation tabled for plenary, 2nd reading		A4-0120/1995 OJ C 166 03.07.1995, p. 0004	23/05/1995	
		T4-0296/1995		

Text adopted by Parliament, 2nd reading		OJ C 166 03.07.1995, p. 0080-0105	15/06/1995	Summary
Council of the EU				
Document type	Reference	Date	Summary	
Council position	12003/3/1994 OJ C 093 13.04.1995, p. 0001	20/02/1995	Summary	
European Commission				
Document type	Reference	Date	Summary	
Legislative proposal	COM(1990)0314 	24/09/1990	Summary	
Modified legislative proposal	COM(1992)0422  OJ C 311 27.11.1992, p. 0030	15/10/1992	Summary	
Reconsultation	COM(1993)0570 	10/11/1993		
Commission communication on Council's position	SEC(1995)0303 	24/02/1995		
Commission opinion on Parliament's position at 2nd reading	COM(1995)0375 	18/07/1995		
Follow-up document	COM(2003)0265 	15/05/2003	Summary	
Follow-up document	COM(2007)0087 	07/03/2007	Summary	
Follow-up document	C(2009)3200	12/05/2009		
Follow-up document	SEC(2009)0585 	12/05/2009		
Follow-up document	C(2010)0593	05/02/2010		
Commission document (COM)	COM(2015)0566 	06/11/2015		
Follow-up document	COM(2018)0860 	19/12/2018	Summary	
Follow-up document	SWD(2018)0497 	20/12/2018		
Follow-up document	COM(2019)0495 	23/10/2019	Summary	
Follow-up document	SWD(2019)0390 	24/10/2019	Summary	
Other institutions and bodies				
Institution/body	Document type	Reference	Date	Summary

EESC	Economic and Social Committee: opinion, report	CES0569/1991 OJ C 159 17.06.1991, p. 0038	24/04/1991	Summary
EU	Implementing legislative act	32004D0535 OJ L 235 06.07.2004, p. 0011-0022	14/05/2004	Summary
EU	Implementing legislative act	32006D0253 OJ L 091 29.03.2006, p. 0049-0060	06/09/2005	Summary
EDPS	Document attached to the procedure	52007XX1027(01) OJ C 255 27.10.2007, p. 0001	02/05/2007	Summary

Additional information		
Source	Document	Date
European Commission	EUR-Lex	

Final act
Directive 1995/0046 OJ L 281 23.11.1995, p. 0031 Summary

Personal data protection

1990/0287(COD) - 24/04/1991

Personal data protection

1990/0287(COD) - 15/06/1995 - Text adopted by Parliament, 2nd reading

The European Parliament adopted the recommendation for second reading by Mr MEDINA ORTEGA. Since the amendments tabled by the Commission following the EP's opinion at first reading had been included in the common position, the adopted report only incorporated some minor amendments to the Council's common position: - the right of access to data for persons should not adversely affect trade secrets; - "controller" should mean the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determined the purposes and means of the processing of personal data; - Member States could provide for exemptions or derogations for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they were necessary to reconcile the right to privacy with the rules governing freedom of expression.

Personal data protection

1990/0287(COD) - 14/05/2004 - Implementing legislative act

PURPOSE : to establish the level of protection for PNR data transferred from the Community concerning flights to or from the United States, pursuant to Directive 95/46/EC.

LEGISLATIVE ACT : Commission Decision 2004/535/CE on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection

CONTENT : Pursuant to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.

In the framework of air transport, the 'Passenger Name Record' (PNR) is a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking and participating airlines.

It should be noted that the Council has adopted Decision 2004/496/EC on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. (Please refer to CNS/2004/0064.) This Decision was adopted in the context of the fight against terrorism.

The United States Bureau of Customs and Border Protection (CBP) of the Department of Homeland Security (DHS) requires each carrier, operating passenger flights in foreign air transportation to or from the United States, to provide it with electronic access to PNR to the extent that PNR is collected and contained in the air carrier's automated reservation system.

This Decision provides that for the purposes of Article 25(2) of Directive 95/46/EC, the United States' Bureau of Customs and Border Protection (CBP) is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with the Undertakings set out in the Annex. The Decision aims to establish a framework of rules for data to be transferred.

The transfer of data by EU airlines will be governed by certain "Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP)". The standards by which CBP will process passengers' PNR data on the basis of United States legislation and the Undertakings cover the basic principles necessary for an adequate level of protection for natural persons:

- As regards the purpose limitation principle, air passengers' personal data contained in the PNR transferred to CBP will be processed for a specific purpose and subsequently used or further communicated only in so far as this is not incompatible with the purpose of the transfer. In particular, PNR data will be used strictly for purposes of preventing and combating terrorism and related crimes; other serious crimes, including organised crime, that are transnational in nature; and flight from warrants or custody for those crimes.

- As regards the data quality and proportionality principle, which need to be considered in relation to the important public interest grounds for which PNR data are transferred, PNR data provided to CBP will not subsequently be changed by it. A maximum of 34 PNR data categories will be transferred and the United States authorities will consult the Commission before adding any new requirements. Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels. As a general rule, PNR will be deleted after a maximum of three years and six months, with exceptions for data that have been accessed for specific investigations, or otherwise manually accessed.

- As regards the transparency principle, CBP will provide information to travellers as to the purpose of the transfer and processing, and the identity of the data controller in the third country, as well as other information.

- As regards the security principle, technical and organisational security measures are taken by CBP which are appropriate to the risks presented by the processing.

It should be noted that the rights of access and rectification are recognised, in that the data subject may request a copy of PNR data and rectification of inaccurate data.

Onward transfers will be made to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes that correspond to those set out in the statement of purpose limitation. Transfers may also be made for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks, or in any criminal judicial proceedings or as otherwise required by law. Receiving agencies are bound by the express terms of disclosure to use the data only for those purposes and may not transfer the data onwards without the agreement of CBP.

The competent authorities in Member States may exercise their existing powers to suspend data flows to CBP in order to protect individuals with regard to the processing of their personal data in certain cases.

The Decision will expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Article 31(2) of Directive 95/46/EC.

ENTRY INTO FORCE: Member States shall take all the measures necessary to comply with the Decision within four months of the date of its notification.

Personal data protection

1990/0287(COD) - 20/02/1995 - Council position

The Council was in agreement with the approach adopted in the Commission's amended proposal. The amendments which were accepted by the Commission and incorporated in the modified proposal were adopted in the common position, and mainly comprise: - General approach: . the formal distinction between the requirements of the public and private sectors has been abandoned; . protection should not depend solely on the compilation of files containing personal data; a wider approach should be adopted which covers all the uses to which the data could be put; . data processing systems should serve the citizens; - Definitions: . the definition of personal data was clarified; . the data-collection phase and the different forms of data communication were included in the definition of the processing method; . definitions were introduced for third parties and subcontractors; - Data quality: . the purpose which the data will serve should be established before collection commences; . a derogation was introduced to the principle of the maximum duration for which data may be stored, which is laid down as a function of the purposes of the processing, in respect of data which is held for historical, statistical or scientific purposes; - Special processing categories: . data processing which is undertaken by non-profitmaking organizations involved in political, religious and trade-union activities, etc., would be entitled to a special derogation when the data in question were of a sensitive nature and came under the prohibition on all processing; . greater flexibility for the processing of data relating to criminal offences and prosecutions; . Member States would determine the conditions under which a national identification number or any other identifier of general application may be processed; - individual rights were specified and reinforced as follows: . the right to be kept informed was extended to include the origin of the data; . the right of access should be provided without restraint; . the right of objection would be exercisable at any time, particularly with regard to processing for canvassing purposes; . the rights of appeal, which were to be provided by the Member States, were extended; . the requirement was introduced

that those responsible for the processing operation would be held accountable for any illicit processing; . penalties were also to be imposed on those responsible for processing who were operating in the public sector; - notification of processing and prior checks: . the notification procedure was made more selective; Member States were offered the possibility of simplifying the procedure and of being exempt from the obligation to provide notification when the processing did not infringe individual rights and freedoms or when the processing was carried out by organizations engaged in political, religious or trade-union activities, etc.; . the principle was adopted that the controlling authority should conduct prior checks when carrying out processing which involved specific risks to individual rights and freedoms; . the public were offered the opportunity to consult the register of notified processing, which is kept by the controlling authority; - codes of conduct: . to encourage the drawing up of codes of conduct at both national and European level; the controlling authorities, the Working Party and the persons concerned could be involved in the drawing-up of these codes; - the Working Party on the protection of individuals with regard to the processing of personal data would be given the following tasks: . advising on the implementation of national provisions adopted pursuant to the Directive; . advising on the level of protection provided in the Community and in third countries; . submitting recommendations on its own initiative. . the Commission would draw up and publish a report informing the Working Party of the actions taken in response to its recommendations; this report would be submitted to Parliament and the Council. The Council also introduced the following amendments to its common position: - definitions: . a definition was introduced for the recipient of the processing data - data held in manual filing systems: . in order to help implement the Directive in Member States where manually-filed data have not yet been covered, a transitional period of 12 years was to be provided for the application of certain measures contained in the Directive; - national law applying: . the criterion of the place of domicile of the body controlling the processing was confirmed; . clarifications were made in respect of the security obligations of the subcontractor and the responsibilities of the controlling authorities for processing operations carried out in their territory; - special categories of processing: . exceptions to the measures prohibiting the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or concerning health or sex life, were included in order to cover the requirements of the medical and employment sectors; . derogations on grounds of major public interest, and derogations relating to offences, criminal convictions and security measures, were to be notified to the Commission; - freedom of expression: . the processing of personal data for journalistic purposes was included in the scope of the Directive; - processing of data for statistical, historical or scientific purposes: . scientific research and statistics were cited as areas in which major public interest could justify derogations from the prohibition on processing data of a sensitive nature; - processing transparency: . greater flexibility was given to the obligations under which information on the processing of personal data was to be provided to the individuals concerned; . Member States were to ensure that the processing operations were given proper publicity; - notification and prior checks: . derogations and/or simplifications could be applied when an official was appointed by the body responsible for processing who would ensure that the processing operations were not likely to infringe individual rights and freedoms; . prior checks could be carried out on processing operations which involved specific risks with regard to individual rights and freedoms; these checks would be undertaken either by the controlling authority or by the appointed official acting in cooperation with the controlling authority; - third countries: . confirmation of the principle of an adequate level of protection in third countries to which the data were transferred, and the obligation for Member States to ensure that this protection was provided; - controlling authority: . routine consultation of the controlling authorities would be introduced when drawing up statutory or administrative measures at national level; the powers of intervention of the controlling authorities were clarified. - The Council limited the powers of enforcement solely to the area of data transfer to third countries and retained procedure III a) in respect of the committee assisting the Commission in this field; - the deadline for the transposition of the Directive was increased to three years with effect from its date of adoption.

Personal data protection

1990/0287(COD) - 02/05/2007 - Document attached to the procedure

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive.

On 7 March 2007, the aforementioned Communication was sent by the Commission to the EDPS. In accordance with Article 41 of Regulation (EC) No 45/2001, the EDPS presents this opinion.

The Communication reiterates the importance of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data as a milestone in the protection of personal data and discusses the Directive and its implementation. The central conclusion of the Communication is that the Directive should not be amended. The implementation of the Directive should be further improved by means of other policy instruments, most of them with a non binding nature.

The EDPS shares the central conclusion of the Commission that **the Directive should not be amended in the short term**. The points of departure for the EDPS are as follows: (i) in the short term, energy is best spent on improvements in the implementation of the Directive; (ii) in the longer term, changes of the Directive seem unavoidable; and (iii) a clear date for a review to prepare proposals leading to such changes should already be set now. Such a date would give a clear incentive to start the thinking about future changes already now.

According to the EDPS, the **main elements for future change** include:

- no need for new principles, but a clear need for other administrative arrangements;
- the wide scope of data protection law applicable to all use of personal data should not change;
- data protection law should allow a balanced approach in concrete cases and should also allow data protection authorities to set priorities;
- the system should fully apply to the use of personal data for law enforcement purposes, although appropriate additional measures may be necessary to deal with special problems in this area.

Moreover, the EDPS suggests that the Commission specify: (i) a timeline for the activities of Chapter III of the Communication; (ii) a deadline for a subsequent report on the application of the Directive; (iii) terms of reference to measure the realisation of the activities foreseen; and (iv) indications on the way to proceed in the longer term.

The EDPS regrets that the **perspective of global privacy and jurisdiction** plays a limited role in the Communication and asks for practical solutions that reconcile the need for protection of the European data subjects with the territorial limitations of the European Union and its Member States, such as:

(i) the further development of a Global Framework for data protection; (ii) the further development of the special regime for transfer of data to third countries; (iii) international agreements on jurisdiction or similar agreements with third countries; and (iv) investing in mechanisms for global compliance, such as the use of binding corporate rules by multinational companies. The EDPS invites the Commission to start developing a vision on this perspective, together with most relevant stakeholders.

On **law enforcement**, the EDPS has the following suggestions to the Commission:

- further reflection on the implications of the involvement of private companies in law enforcement activities;
- preserve the *effet utile* of Article 13 of the Directive, possibly by proposing legislation aiming at harmonizing the conditions and the safeguards for using the exemptions of Article 13.

Full implementation of the Directive means: (i) that it be ensured that the Member States fully comply with their obligations under European law; and (ii) that other, non binding tools, that could be instrumental to a high and harmonised level of data protection be fully used. The EDPS asks from the Commission to clearly indicate how it will use the different instruments.

In relation to those **instruments**:

- in certain cases, specific legislative action at EU level may be necessary;
- the Commission is encouraged to pursue a better implementation of the Directive through infringement procedures;
- the Commission is invited to use the instrument of an interpretative communication for the following issues: (i) the concept of personal data; (ii) the definition of the role of data controller or data processor; (iii) the determination of applicable law; (iv) the purpose limitation principle and incompatible use; and (v) legal grounds for processing, especially with regard to unambiguous consent and balance of interests;
- non binding instruments include instruments building on the concept of 'privacy by design';
- for longer term also: (i) class actions; (ii) actions initiated by legal persons whose activities are designed to protect the interests of certain categories of persons; (iii) obligations for data controllers to notify security breaches to data subjects; and (iv) provisions facilitating the use of privacy seals or third-party privacy audits in a trans-national setting.

Lastly, the EDPS invites the Commission to present a paper to the Working Party giving clear indications on the division of roles between them.

Personal data protection

1990/0287(COD) - 15/05/2003 - Follow-up document

The European Commission submitted a first report on the implementation of Directive 95/46/EC and the identification of the actions necessary to address the main problems that had emerged. The Commission considered that results of the public review which had preceded the preparation of this report on balance militated against proposing modifications to the directive at this stage. In the course of the consultations conducted, few contributors had advocated the modification of the directive. The most notable exception had been the detailed proposals for amendments submitted jointly by Austria, Sweden, Finland and the UK. These proposals for amendments concerned only a small number of provisions (notably Article 4 which determined the applicable law, Article 8 on sensitive data, Article 12 on the right of access, Article 18 on notification and Articles 25 and 26 on transfers to third countries), leaving most of the provisions and all of the principles of the directive untouched. The Commission, along with a large majority of the Member States, believed that the following general considerations made it unwise to make proposals to amend this directive in the immediate future: - Experience with the implementation of the directive was so far very limited. Only a few Member States had implemented the directive on time. Most Member States had only notified implementing measures to the Commission in 2000 and 2001, and Ireland had still not notified its recent implementation. Important implementing legislation was still pending in some Member States; - Many of the difficulties that had been identified during the review could be addressed and resolved without amending the directive. In some cases, where problems were caused by incorrect implementation of the directive, they had to be solved by specific modifications of Member State law. In others, the margins of manoeuvre allowed by the directive permitted closer cooperation among supervisory authorities to achieve the convergence necessary to overcome difficulties arising from practices that diverged too widely from Member State to Member State; - Where amendments had been proposed by stakeholders, the aim was often the reduction of compliance burdens for data controllers. While the Commission espoused this end, it believed that many of the proposals would also involve a reduction in the level of protection provided for. The Commission believed that any changes that might in due course be considered should aim to maintain the same level of protection. The Commission considered that some of the issues that had emerged needed to be further analysed and could need in due course to be the subject of a proposal to revise the directive. The Commission's attention would continue to be focussed in particular on areas where Community law was clearly being breached and on areas where divergent interpretations and/or practices were causing difficulties in the Internal Market. The Commission also considered as a priority the harmonious application of the rules relating to the transfer of data to third countries, with a view to facilitating legitimate transfers and avoiding unnecessary barriers or complexities. The Commission encouraged citizens to make use of the rights conferred by the legislation and data controllers to take all necessary steps to guarantee compliance with the legislation. The Commission would make proposals for further follow-up towards the end of 2004, by which time both the Commission and the Member States would have the benefit of considerably more experience than at present with the implementation of the directive.

Personal data protection

1990/0287(COD) - 06/09/2005 - Implementing legislative act

ACT : Commission Decision 2006/253/EC on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency.

CONTENT : Pursuant to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.

In the framework of air transport, the 'Passenger Name Record' (PNR) is a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking and participating airlines.

The Decision provides that for the purposes of Article 25(2) of Directive 95/46/EC, the Canadian Customs Border Services Agency (CBSA) is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights bound for Canada in accordance with the Commitments set out in the Annex. The competent authorities in Member States may exercise their existing powers to suspend data flows to the CBSA in order to protect individuals with regard to the processing of their personal data in the following cases:

- where a competent Canadian authority has determined that the CBSA is in breach of the applicable standards of protection; or
- where there is a substantial likelihood that the standards of protection set out in the Annex are being infringed, there are reasonable grounds for believing that the CBSA is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the CBSA with notice and an opportunity to respond.

Suspension shall cease as soon as the standards of protection are assured and the competent authorities of the Member States concerned are notified.

Member States shall take all the measures necessary to comply with the Decision within four months of the date of its notification.

The Decision will expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Article 31(2) of Directive 95/46/EC.

Personal data protection

1990/0287(COD) - 24/10/1995 - Final act

OBJECTIVE: to facilitate the free movement of data within the Community by ensuring a high level of protection for individuals in relation to the processing of personal data.

COMMUNITY MEASURE: European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

SUBSTANCE:

- The directive establishes the common basic rules for the protection of individuals in relation to personal data;
- A high level of protection is guaranteed through the obligations imposed on those responsible for processing data (public authorities, enterprises, agencies, etc.) and through the rights conferred on individuals whose data is the subject of processing;
- The obligations imposed on those responsible for processing relate to the quality of the data, insofar as processing must have an explicit and legitimate purpose, security and notification to an independent supervisory authority, which must be created by the Member States;
- The directive covers in general the collection, adaptation, use, interconnection and erasure of personal data;
- Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life;
- Member States shall provide for exemptions or derogations for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression;
- The data subject has the right to be informed of the processing being carried out and the data being used, to request that the data be rectified if it is incorrect and to object to the processing;
- The directive also relates to the confidentiality and security of processing. It covers both the private and public sectors, with the exception of the provisions concerning the CFSP, cooperation on justice and home affairs, public safety, and national defence and security.

Deadline for the transposal of the directive into national legislation: 24 October 1998.

Personal data protection

1990/0287(COD) - 24/07/1995

After agreeing to the amendments made by the European Parliament at second reading, the Council unanimously (with the United Kingdom abstaining) adopted the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Member States have three years in which to transpose the Directive into their national legislation. The Danish delegation made the following statement to explain how it had voted: ' Denmark can accept the European Parliament's amendments to the Directive and can therefore agree to the definitive adoption of the Directive by the Council. Denmark nevertheless regrets that it has not proved possible to reach the consensus needed within the

Council for the European Parliament to be informed of the content of the statements entered in the minutes. Denmark considers that the request made by the President of the European Parliament to the President of the Council (General Affairs) revealed the need to bring to a swift conclusion the current discussions on the publication of the statements entered in the minutes in the interests of greater transparency of the work of the Council'.

Personal data protection

1990/0287(COD) - 11/03/1992 - Text adopted by Parliament, 1st reading/single reading

Personal data protection

1990/0287(COD) - 02/12/1993

In its first reading under the codecision procedure, the European Parliament confirmed its vote of 11 March 1992.

Personal data protection

1990/0287(COD) - 16/06/1994

Personal data protection

1990/0287(COD) - 07/03/2007 - Follow-up document

The Commission's first report on the implementation of Directive 95/46/EC (please refer to the summary of 15/05/2003) contained a Work Programme for better implementation of the data protection

Directive. This Communication examines the work conducted under this programme, assesses the present situation, and outlines the prospects for the future as a condition for success in a number of policy areas in the light of Article 8 of the European Charter of Fundamental Rights, recognising an autonomous right to the protection of personal data.

The Commission considers that the Directive lays down a general legal framework that is **substantially appropriate and technologically neutral**. The harmonised set of rules ensuring a high standard of protection for personal data throughout the EU has brought considerable benefits for citizens, business and authorities. It protects individuals against general surveillance or undue discrimination on the basis of the information others hold on them. The trust of consumers that personal details they provide in their transactions will not be misused is a condition for the development of e-commerce. Business operate and administrations cooperate throughout the Community without fearing that their international activities be disrupted because personal data they need to exchange are not protected at the origin or the destination.

The Commission details the work that has been carried out under 10 action areas since the publication of the first report. This includes a "structured dialogue" with Member States on national transposition, and a detailed analysis of national legislation and discussions with national authorities aimed at bringing national legislation fully in line with the requirements of the Directive.

Overview of implementation of the Directive: the Commission states that **implementation has improved**. All Member States have now transposed the Directive. On the whole, national transposition covers all the main provisions along the lines of the Directive. The actions undertaken under the Work Programme have been positive and have substantially contributed to improving the implementation of the Directive throughout the Community. The decisive involvement of the national data protection supervisory authorities through their participation in the Working Party has played a major role. However, some countries have **not yet properly implemented** the Directive. One concern is respect for the requirement that data protection supervisory authorities act in complete independence and are endowed with sufficient powers and resources to exercise their tasks. These authorities are key building blocks in the system of protection conceived by the Directive, and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation.

In some case divergences arise within the margin of manoeuvre of the Directive. However, a study shows that despite some divergences, the Directive has been implemented with modest costs for firms.

No evidence is found among the complaints received by the Commission that national divergences within the limits of the Directive may actually obstruct the proper functioning of the internal market or limit the free flow of data on grounds of a lack or inadequacy of protection in the country of origin or destination. Nor do constraints within their country of establishment distort competition between private operators. The Directive is therefore fulfilling its objectives: to secure the free flow of personal data within the internal market while ensuring a high level of protection in the Community. The Commission goes on to state that the legal solutions provided by the Directive, beyond achieving harmonisation, are themselves appropriate to the issues at stake. It considers the **requirements imposed by public interests**, such as the International Agreement with the US to address the use of passengers' PNR data and states its commitment to respecting the Charter of Fundamental Rights in all its proposals.

The way ahead: the Commission intends to pursue a policy characterized by the following elements:

- the Directive should not be amended, since the Data Protection Directive constitutes a general legal framework which fulfils its original objectives by constituting a sufficient guarantee for the functioning of the Internal Market while ensuring a high level of protection;
- the Commission will pursue proper implementation of its provisions at national and international level.

- it will produce an **interpretative communication** on some provisions. The problems identified in implementing particular provisions of the Directive that may lead to formal infringement procedures correspond to an understanding by the Commission about the meaning of the provisions in the Directive and about the correct way to implement them, taking into account the case law, as well as the interpretation work conducted by the Working Party. Such ideas will be clearly set forth in an interpretative communication;

- the Commission encourages all actors involved to endeavour to reduce national divergences. Different activities will be conducted for this purpose. The Work Programme will continue and the Working Party should improve its contribution to harmonising practice. The Commission will consider the **challenges of new technologies**. Where a particular technology is found to consistently pose questions as regards the application of the data protection principles, and its widespread use or potential intrusiveness is considered to justify more stringent measures, the Commission could propose sector-specific legislation at EU level in order to apply those principles to the specific requirements of the technology in question.

- the Commission considers the task of providing a coherent response to the demand for public interest uses, especially for security. In striking the important balance between measures to ensure security and protect nonnegotiable fundamental rights, the Commission makes sure that it protects personal data as guaranteed by Article 8 of the Charter of Fundamental Rights. The EU works with external partners also. In particular the EU and USA have a continuous transatlantic dialogue to discuss information sharing and the protection of personal data for law enforcement purposes. The Commission will consider the implementation of the Directive once again upon conclusion of the measures laid out in this Communication.

Lastly, it will continue to monitor the implementation of the Directive, work with all stakeholders to further reduce national divergences, and study the need for sector-specific legislation to apply data protection principles to new technologies and to satisfy public security needs.

Personal data protection

1990/0287(COD) - 15/10/1992 - Modified legislative proposal

The Commission had introduced several fundamental amendments to its text, following the EP opinion: - As regards the approach to protection, first, it had dropped the formal distinction between the rules applying in the public sector and the rules applying in the private sector; secondly, it had expanded the provisions on the selective procedures for notification to the supervisory authority and on codes of conduct. It was thus made clearer that the protection provided must be the same whatever the sector in question. - As regards concepts and definitions, the Commission had concurred with Parliament's wish to include the collection of data under the definition of processing of personal data. In addition, whilst the Commission had not completely eliminated the concept of a 'file', as Parliament had requested, it had clarified its meaning in order to define the scope of the directive, where processing was not automated, as covering only personal data which were entered or intended for entry in files. Lastly, a definition of the third party to whom personal data are disclosed was introduced. - The scope had also been modified: processing carried out by non-profit-making organisations was no longer excluded, but could be the subject of exemptions from the obligation to notify; processing carried out for purposes of journalism must, rather than simply may, be subject to exemptions; processing that involved no particular danger, carried out for example to satisfy a legal obligation, could similarly be subject to an exemption from the obligation to notify. - The provisions on protection against rules being circumvented in the course of transfers of data to non-Community countries had been strengthened. - Lastly, the proposal had been restructured in order to take account of the dropping of the formal distinction between the public and private sectors.

Personal data protection

1990/0287(COD) - 24/09/1990 - Legislative proposal

Personal data protection

1990/0287(COD) - 19/12/2018 - Follow-up document

The Commission presents its second annual review of the functioning of the EU-U.S. Privacy Shield.

The [EU-U.S. Privacy Shield Decision](#) was adopted on 12 July 2016. It ensures an adequate level of protection for personal data that has been transferred from the EU to organisations in the U.S. The Decision provides for an annual evaluation of all aspects of the functioning of the framework. The first annual review took place in 2017, with the Commission concluding that the U.S. continued to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the U.S. At the same time, the Commission made ten recommendations to improve the Privacy Shield framework in order to ensure that the guarantees and safeguards provided therein continued to function as intended.

This report concludes the second annual review of the functioning of the Privacy Shield and is based on information gathered from relevant stakeholders (in particular Privacy Shield-certified companies, and non-governmental organisations active in the field of digital rights and privacy), as well as from the relevant U.S. authorities involved in the implementation of the framework. The review took place in the context of the challenges to data privacy that are increasingly global in nature, as exemplified by the Facebook / Cambridge Analytica case. The report states that both sides stressed the need for vigorous enforcement actions by the EU's Data Protection Authority and the U.S. Federal Trade Commission.

Findings

Commercial aspects: this relates to questions concerning the administration, oversight and enforcement of the obligations applying to certified companies. The Commission notes that in line with its recommendations from the first annual review, the Department of Commerce has further strengthened the certification process and introduced new oversight procedures, including: (i) a new process that requires first-time applicants to delay

public representations regarding their Privacy Shield participation until their certification review is finalised by the Department of Commerce; (ii) new mechanisms to detect potential compliance issues, such as random spot-checks (at the time of the annual review, such spot checks had been performed on about 100 organisations) and the monitoring of public reports about the privacy practices of Privacy Shield participants; (iii) a quarterly review of companies that have been identified as more likely to make false claims and a system for image and text searches on the internet.

Since the first annual review, the Department of Commerce has referred more than 50 cases to the Federal Trade Commission, which in turn took enforcement action in those cases where the referral as such was not sufficient in order to make the company concerned come into compliance.

With respect to enforcement, the Commission noted that the Federal Trade Commission recently issued administrative subpoenas to request information from a number of Privacy

Shield participants. Although the Commission considers that the Federal Trade Commission's more proactive approach to compliance monitoring is an important development, it regrets that at this stage it was not possible for to provide further information on its recent investigations and will closely monitor any further developments in this regard.

Access and use of personal data by U.S. public authorities

The reauthorisation of Section 702 of the Foreign Intelligence Surveillance Act at the beginning of 2018. While the reauthorisation did not lead to the incorporation of the protections of Presidential Policy Directive 28 into the Act, as the Commission wanted, neither did it restrict any of the safeguards contained in the Act which were in place when the Privacy Shield decision was adopted. Moreover, the amendments did not expand the powers of the U.S. Intelligence Community to acquire foreign intelligence information by targeting non-U.S. persons under Section 702. Instead, the Amendments Reauthorization Act of 2017 introduced some limited additional privacy safeguards, for instance in the area of transparency.

The Privacy and Civil Liberties Oversight Board: new members of the Board have been appointed which restores the Board's quorum. The Board's report of 16 October 2018 confirms that Presidential Policy Directive 28 is fully applied across the intelligence community, which has adopted detailed rules on the implementation of that Directive and have changed their practices in order to bring them in line with the requirements of Presidential Policy Directive 28.

Conclusions

On the basis of the findings, the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States. In particular, the steps taken to implement the Commission's recommendations following the first annual review have improved several aspects of the practical functioning of the framework in order to ensure that the level of protection of natural persons guaranteed by the adequacy decision is not undermined.

However, the report notes that although the Commission had recommended the swift appointment of the ***Privacy Shield Ombudsperson***, the position of Under-Secretary in the State Department to whom the office of the Ombudsperson has been assigned had not yet been filled by a permanent appointment at the time of the report.

Accordingly, the Commission reiterates its call on the U.S. administration to confirm its political commitment to the Ombudsperson mechanism by appointing a permanent Privacy Shield Ombudsperson as a matter of priority. The Ombudsperson mechanism is an important element of the Privacy Shield framework and, while the acting Ombudsperson continues to carry out the relevant functions, the absence of a permanent appointee is highly unsatisfactory. The Commission expects the U.S. government to identify a nominee to fill the Ombudsperson position on a permanent basis by 28 February 2019.

Personal data protection

1990/0287(COD) - 23/10/2019 - Follow-up document

The Commission presents its report on the third annual review of the functioning of the EU-U.S. Privacy Shield.

In its third year of operation, the Privacy Shield, which at the time of the annual review meeting had more than 5000 participating companies, has moved from the inception phase to a more operational phase. Covering both commercial aspects and issues relating to government access to personal data, the third annual review focused on the experience and lessons learnt from the practical application of the framework.

Main findings

Commercial aspects

In light of the findings of last year's annual review, the Commission's assessment of the commercial aspects focused notably on the progress made by the Department of Commerce on:

- Re-certification process

With respect to the re-certification process, it emerged at the third annual review that as a regular practice, at the expiration of the (re)certification period, if a company has not yet completed the re-certification process, the Department of Commerce, following an internal procedure, grants to the company a "grace period" of a significant length. During this period (for approximately 3.5 months, or, in some instances and depending on when the Department of Commerce detects that the re-certification process was not completed, even a longer period of time), the company remains on the Privacy Shield "active" list. For as long as a company is listed as participating in the Privacy Shield, the obligations under the framework remain binding and fully enforceable. However such a long period in which a company's recertification due date has lapsed while the company continues to be listed

as active Privacy Shield participant reduces the transparency and readability of the Privacy Shield list for both businesses and individuals in the EU. It also does not incentivise participating companies to rigorously comply with the annual re-certification requirement.

- Effectiveness of the "spot-checks"

With respect to proactive checks of companies' compliance with the Privacy Shield requirements, the Department of Commerce introduced in April 2019 a system in which it checks 30 companies each month. The Commission welcomes that the Department of Commerce is carrying out proactive compliance spot-checks on a regular basis and in a systematic manner. However, it notes that these spot-checks tend to be limited to formal requirements such as the lack of response from designated points of contact or the inaccessibility of a company's privacy policy online. Compliance with these spot-checks are crucial for the continuity of the Privacy Shield and should be subject to strict monitoring and enforcement by the U.S. authorities.

- Tools to detect false claims

The Department of Commerce had continued to conduct searches on a quarterly basis, which has led to the detection of a significant number of cases of false claims, which in some instances were also referred to the Federal Trade Commission. However, these searches have so far only been aimed at companies that had in some way already been certified or applied for certification under the Privacy Shield (but, for example, were not re-certified). It is important that they also target companies that have never applied for certification under the Privacy Shield. From all kinds of false claims, the false claims from companies that never applied for certification are potentially the most harmful.

- Progress and outcome of Federal Trade Commission enforcement actions regarding violations of the Privacy Shield

The Commission noted that since last year, the Federal Trade Commission concluded seven enforcement actions related to Privacy Shield violations, including as a result of the announced ex officio sweeps. All seven cases concerned false claims of participation in the framework. The Commission welcomes the enforcement action taken by the Federal Trade Commission in the third year of operation of the Privacy Shield. However, the Commission would have expected a more vigorous approach regarding enforcement action on substantive violations of the Privacy Shield Principles.

Access and use of personal data by U.S. public authorities

The third annual review was, first of all, aimed at confirming that all the limitations and safeguards that the adequacy decision relies on remain in place. In addition, the third annual review provided an opportunity to look at new developments and to further clarify certain aspects of the legal framework, as well as the different oversight mechanisms and the possibilities for redress, in particular with respect to the handling and resolution of complaints by the Ombudsperson.

Conclusion

The information gathered in the context of the third annual review confirms the Commission's findings in the adequacy decision, both with regard to the commercial aspects of the framework and with regard to aspects relating to access to personal data transferred under the Privacy Shield by public authorities. In this respect, the Commission noted a number of improvements in the functioning of the framework as well as appointments to key oversight bodies.

However, in light of some issues that emerged from the day-to-day experience or became more relevant in the context of the practical implementation of the framework, the Commission concludes that a number of concrete steps need to be taken to better ensure the effective functioning of the Privacy Shield in practice:

- The Department of Commerce should shorten the different time periods that are granted to companies for completing the re-certification process. A period of maximum 30 days in total would seem reasonable to allow companies sufficient time for re-certification, including for rectifying any issue identified in the re-certification process, while at the same time ensuring the effectiveness of this process. If at the end of this period the re-certification is not completed, the Department of Commerce should send out the warning letter without further delay.
- In the context of its spot-check procedure, the Department of Commerce should assess companies' compliance with the Accountability for Onward Transfers Principle, including by making use of the possibility provided by the Privacy Shield to request a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company for the purposes of onward transfer.
- As a matter of priority, the Department of Commerce should develop tools for detecting false claims of participation in the Privacy Shield from companies that have never applied for certification, and use these tools in a regular and systematic manner.
- The Federal Trade Commission should, as a matter of priority, find ways to share meaningful information on ongoing investigations with the Commission, as well as with EU Data Protection Authorities that also have enforcement responsibilities under the Privacy Shield.
- The EU Data Protection Authorities, the Department of Commerce and the Federal Trade Commission should develop common guidance on the definition and treatment of human resources data in the coming months.

Lastly, the Commission will continue to follow closely the ongoing debate about federal privacy legislation in the U.S. A comprehensive approach to privacy and data protection would increase the convergence between the EU and the U.S. systems and this would strengthen the foundations on which the Privacy Shield framework has been developed.

Personal data protection

This Commission staff working document accompanies the report from the Commission on the third annual review of the functioning of the EU-U.S. Privacy Shield.

It presents the findings of the Commission services on the implementation and enforcement of the EU-U.S. Privacy Shield framework in its third year of operation.

Commercial aspects

The Commission assessed the concrete functioning of the administration, oversight and enforcement of the Privacy Shield process. The third annual review focused notably on the recertification process, compliance monitoring and enforcement.

The (re)-certification process

At the time of the review meetings, just over 5000 companies were certified under the Privacy Shield. After three years of operation, the Privacy Shield has therefore more participating companies than its predecessor, the Safe Harbor arrangement. The majority (more than 70%) of Privacy Shield certified companies are Small and Medium-sized enterprises (SMEs). The success of the Privacy Shield is also reflected in the current re-certification rate of 89%.

The Commission services welcome that the Department of Commerce (DoC) continuously reviews the (re)-certification process and amends it to address issues as they arise.

Monitoring and supervision by the Department of Commerce

The Commission services welcome that the DoC is carrying out proactive compliance spot-checks on a regular basis and in a systematic manner, which is important for improving the overall compliance with the framework. Whereas the spot-checks should continue to be done regularly and in a systematic manner, compliance with these requirements is thus crucial for the continuity of the Privacy Shield and should be subject to strict monitoring and enforcement by the U.S. authorities.

False claims

The DoC detected 669 cases of false claims of participation since the last review in October 2018. In all these cases, the DoC sent certified warning letters to the companies concerned. In most cases, companies completed their (re)-certification further to these warning letters.

The Commission services regret that the DoC does currently not have appropriate tools at its disposal to more effectively identify false claims of participation in the framework by companies that have never applied for certification.

Enforcement by the Federal Trade Commission (FTC)

Seven enforcement actions related to Privacy Shield violations were concluded. All seven cases concerned false claims of participation in the framework. The Commission services would have expected a more vigorous approach regarding enforcement action on substantive violations of the Privacy Shield Principles.

More generally, the Commission services note that it has been an important year for the FTC's enforcement actions in the area of privacy. In particular, two major settlements were reached for alleged violations of the Children's Online Privacy Protection Rule ("COPPA"). The first case resolved the charges against YouTube to have illegally collected personal information from children without their parents' consent. As a result of this settlement, YouTube (and its parent company Google) agreed on a \$170 million penalty.

The second case, settled with a penalty of \$5.7 million, concerned the FTC's allegations against the Video Social Networking App Musical.ly (known as TikTok) for having illegally collected personal information from children without parental consent.

Access and use of personal data

The Commission services welcome clarifications, which confirm the Commission's findings in the adequacy decision that the collection of foreign intelligence information under Section 702 the Foreign Intelligence Surveillance Act (FISA) is targeted through the use of selectors and that the choice of selectors is governed by law, subject to independent judicial and legislative oversight.