Data protection: The EU institutions' battle over data processing vs. individual rights

by Paul de Hert and Vagelis Papakonstantinou

ABSTRACT

Data protection is a comparatively recent field of legislative activity, regulating a relatively recent human activity. The automated processing of personal data took place only after information technology allowed it to develop in the late 1960s, first in public and subsequently in private organisations. Consequently, when the first EU data protection law was enacted only a handful of countries had a data protection regulatory history of more than a decade. Another aspect important to bear in mind is the inherent cross-border character of personal data processing. Consequently, by definition supranational organisations matter when it comes to data protection. Given these two basic characteristics of data protection, 'policy change' in this field can be considered differently than in other sub-policies of the Area of Freedom, Security and Justice (AFSJ). This chapter investigates the role of EU institutions in the process of developing and changing EU data protection rules.

1. Introduction

Data protection is a comparatively recent field of legislative activity, regulating a relatively recent human activity. The automated processing of personal data took place only after information technology (i.e. the introduction of computers) allowed it to develop in the late 1960s, first in public and subsequently in private organisations. Until then, personal data processing was undertaken almost exclusively by public administrations in a manual and therefore slow and ineffective manner. Evidently, the widespread use of computers for

automatic processing of personal data occurred in countries that had the financial and educational level to support it. Consequently, when the first EU data protection law was enacted in the early nineties, only a handful of countries had a data protection regulatory history of more than a decade.

Another aspect important to bear in mind in the field of data protection is its inherent cross-border character. Personal data processing blatantly ignores national borders. Social networking websites, 'cloud' computing and the internet itself have made sure that data protection implementation at the national level alone is problematic for data subjects and data controllers alike. This cross-border characteristic unavoidably warrants international cooperation. *By definition* supranational organisations matter when it comes to data protection, exactly because national institutions alone can accomplish very little in terms of data protection (Pearce and Platten 1998).

Given these two basic characteristics of data protection, 'policy change' in this field can be considered differently than in other sub-policies of the Area of Freedom, Security and Justice (AFSJ). As already mentioned, most European states did not have the time to develop their own data protection policies in the first place. The few states that did faced substantial challenges implementing their national laws. They were quickly willing to elevate such policies to a level of decision-making beyond their national scope of influence. Whereas in the 1980s regulatory activities took place in parallel at national and supranational level, it proceeded thereafter almost exclusively at supranational level.

This chapter investigates the role of EU institutions in the process of developing and changing EU data protection rules. In the wake of 11 September 2001, the large-scale processing of data for security purposes became a priority for law enforcement authorities throughout

Europe—and the safeguarding of an individual's right to data protection a key concern for all those defending a rights-based approach. Security-oriented actors and those defending data protection interests have struggled to find compromise in the EU institutions, meaning that the core of the policy is still to be settled. Since the Treaty of Lisbon and the inclusion of data protection as a fundamental right, the necessity to solve the tension between large-scale data processing for security purposes and the right of individuals to data protection has become more pressing.

2. Overview of the degree of policy change in EU data protection

The first rules on data protection in Europe were outlined in the Council of Europe Convention 108. Its release in 1981 signalled an enthusiasm for the new regulatory field, especially when considering that data protection globally had a life span of no more than fifteen years. It also foretold of the resolve for its continued existence—indeed, countries such as the United Kingdom appeared reluctant at first and only participated in 1984. Finally, it perhaps revealed a naiveté towards the obstacles ahead—after all, Convention 108 was the only document regulating security-related personal data processing in Europe until 2008.

Convention 108 ultimately only marginally affected national law. By the early 1990s, the Commission had to intervene, since it felt that a lack of regulations impeded the Single Market project. The Commission's aim at the time was cautious: to achieve harmonisation among member states, at least with regard to commercial personal data processing. The 1995 Data Protection Directive (95/46/EC), whose introduction proved to be no small achievement, admittedly did not attempt to overturn already established member state practices and took years to implement across the EU. Yet, it ultimately constituted an influential regulatory text whose implementation changed data protection forever, both inside and outside the EU.

Within the 1995 Data Protection Directive-euphoric environment, the AFSJ was somehow left behind. The 11 September 2001 terrorist attacks and the attacks in European capitals that followed forcedly turned lawmakers' attention to it. In the wake of these events, policy was driven by crime prevention authorities' goal to improve the security-related processing of personal data. This 'security' rationale, however, has been persistently challenged by an individual's right to data protection.

2.1. The substantive dimension

2.1.1. The policy's rationale

When data protection entered the EU level with the 1995 Data Protection Directive, the prevailing rationale was clarified in its very first article: 'to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data', while, at the same time, not to 'restrict nor prohibit the free flow of personal data between member states'. At that time, however, data protection focused on private sector processing, only marginally affecting the personal data processing undertaken by security agencies at member state level.[1]

This changed in the wake of 11 September 2001, when western societies accepted some sacrifice of individual rights for the benefit of 'security'. A series of data protection instruments were released at EU level that, despite their 'data protection' label, ultimately served security-related data *processing* rather than data *protection* purposes. A common characteristic of these instruments is that they mention basic data protection principles and

[1] Article 3.2 of the Data Protection Directive explicitly excludes from its scope 'processing operations concerning public security, defense, State security […] and the activities of the State in areas of criminal law.' Although certain member states used the Data Protection Directive as an opportunity to also regulate security-related personal data processing within their territories, this did not constitute a general rule in the EU.

individual rights yet introduce such broad exemptions as to make them practically obsolete. Telling examples in this respect are the Passenger Name Record (PNR) agreements with the US and other third countries, or the Data Retention Directive (2006/24/EC)[2]. These cases show that crime prevention authorities have capitalized on the general public's expectation for an increased level of security to step up their activities at the EU level. Personal data processing has found its way into EU regulatory texts on data protection. This development has taken place 'bottom-up' (from member states to EU level) and has also affected member states that initially opposed large-scale data processing. In the years after 11 September 2001, the rationale of the policy area was clearly security-oriented.

This rationale has been challenged in recent years. Police and other crime-prevention agencies were increasingly asked to abide by data protection rules. This concept is still contested by its addressees: although data protection rules restrict the use of collected sets of personal data, security agencies often find it inconceivable that their crime-prevention practices are examined under this light. Information technology afforded new techniques and concepts to security agencies—including, among others, profiling, data mining, and data matching. This essentially involves the intensive and extensive processing of large sets of data to which law enforcement officials have been granted access. However, the shift from single-file, manual processing of (suspected) criminal records to the automated generalized processing of practically millions of (unsuspecting) individuals' records has brought the issue of data protection regulations to the forefront of the AFSJ (Custers 2012).

[2] The Directive aims to harmonize the national provisions of member states concerning the obligations of electronic communications service and network providers with respect to the retention of certain data that they generate or process. It aims, to ensure that the data is available for the purpose of the investigation, detection, and prosecution of 'serious crime' (as defined by each member state in its national law).

The Treaty of Lisbon includes a single, separate individual right to data protection (Article 16 TFEU). This is an important development, and marks the first major milestone since the first data protection acts appeared in Europe in the early 1970s.[3] The inclusion of this right implies that the AFSJ sub-policies will have to abide with extended data protection regulations, regardless of their special needs and circumstances. Although there is still space for exemptions in favour of security-related processing, the article may empower actors that favour a stronger emphasis on the individual's right to data protection. Triggered by Paragraph 2 of Article 16 TFEU, the EP and the Council have started since early 2012 to negotiate the draft Police and Criminal Justice Data Protection Directive (European Commission 2012a), which aims to deliver more comprehensive data protection rules for police and judicial authorities. It will change the way that personal data processing is conducted for security-related purposes in the AFSJ and is likely to accentuate a shift of the policy's rationale towards a more rights-based approach.

2.1.2. The depth of change: From a piecemeal to a comprehensive approach

When the EU started to develop data protection policies for justice and home affairs in the early 2000s, the split of the AFSJ across the first and third pillars was a serious obstacle. Security-related processing fell under the third pillar, with unanimous decision-making and Council, rather than Commission, involvement. This time period was therefore characterized by a reluctant and cautious EU role in data protection, where instruments of dubious

[3] The right to data protection was originally (and probably still is in the public perception) intrinsically connected to the right to privacy. Over the years it became clear that the right to data protection could be both broader and more specific than the right to privacy, thus justifying its eventual autonomy from its origins (Rodota 2009). This development occurred at supranational level, first in the EU Charter of Fundamental Human Rights of 2000 that was subsequently included in the Lisbon Treaty.

legitimacy[4], uncertain legal status[5], or effectiveness[6] were introduced with much difficulty, but, admittedly, admirable persistence and resilience by the EU institutions (in particular the Council) that sponsored them.

The result was a patchwork of data protection rules found in regulatory texts of varying legal status and binding power (O'Neill 2010). In addition to the Schengen, Europol and Eurojust agreements, JHA-related data protection regulations are also found in the PNR agreements, in the EU-PNR Directive currently under negotiation, in the Prüm Treaty and elsewhere. Each of these instruments was introduced without much attention either to the basic data protection principles (as set in the 1995 Data Protection Directive) or to any other related regulatory text already in effect. On the contrary, most of them attempted to establish a separate data protection system. The established AFSJ mechanisms in the EU to-date (Schengen, Europol, Eurojust) operate their own data protection offices and rules and have hardly any obligation to cooperate cross-institutionally, either at EU or member state level (Boehm 2012: 258).

Only in 2008 did the Council make a first attempt to overcome this piecemeal approach by adopting the 2008 Framework Decision. This Decision was meant to be the basic data protection text in the AFSJ field, following the example of the 1995 Data Protection Directive, which covered all other personal data processing fields. This, however, turned out to be an optimistic aim: policy differences among member states reduced the 2008

[4] For instance, the first EU-US Passenger Name Record Agreement that was annulled by the European Court of Justice.
[5] For instance, the Treaty of Prüm, which was adopted by only some member states outside the EU regulatory edifice. From the beginning, however, the treaty was open for other member states to access. Its main elements have been incorporated in the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.
[6] For instance, the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (the '2008 Framework Decision').

Framework Decision to an instrument ultimately regulating only trans-border (among member states) data flows. In addition, it expressly refrained from affecting both the existing AFSJ data protection mechanism (Schengen, Europol, Eurojust or, for the same purposes, any other instrument already in effect) and any bilateral agreement. The 2008 Framework Decision, therefore, constituted a lost chance for integration and harmonisation in the field. Yet it indicated the direction of future development: despite its failure, the need to harmonize personal data processing practices for security purposes was acknowledged (De Hert and Papakonstantinou 2009).

The end of the pillar system brought about by the Lisbon Treaty not only strengthens the role of supranational EU institutions in all AFSJ sub-policies but also the objective of developing a more comprehensive approach towards data protection. The draft Police and Criminal Justice Directive that was released in early 2012 to regulate security-related processing, together with a Regulation for all other personal data processing (European Commission 2012b), offers a preview of things to come.

Thus far, the field of data protection has been characterized more by a process of *policy development* than *policy change* at EU level. This does not imply that EU rules have not triggered any change. The effect of these rules has been substantial on the scope and nature of data protection at the member state level. A case in point has been the Data Retention Directive (2006/24/EC). Although adopted as a first pillar instrument, it has served security-related purposes, namely to make certain electronic communications data available to security agencies. Its adoption at the EU level meant that data retention found its way into the legislation of all member states, despite the fact that several member states and their supreme courts bitterly contested both the directive's lawfulness and effectiveness (including Cyprus, Germany, Bulgaria and Romania).

Another example of an issue that was newly regulated at EU level before it became relevant to all member states was 'profiling'. At the beginning, profiling was a marginal practice among some member states that attracted much criticism due to its manifold rights-infringement risks. Still, the mechanism of profiling found its way into a variety of isolated personal data processing texts and is now formally acknowledged in the draft Police and Criminal Justice Directive (González Fuster et al. 2010). Once it is formally introduced, profiling will become a widely-used type of personal data processing among all member states.

In both instances of data retention and profiling, the idea of establishing EU rules was put forward by member states that had such rules already at the national level.[7] In consequence, these member states ensured that their policies found a European-wide relevance. These rules, however, never ended up as an exact copy of existing national models but were quite different after years of debates and negotiations.

2.2. The functional dimension

2.2.1. The form of European integration

The field of data protection is mainly governed by 'hard' law (directives, framework decisions and, potentially, regulations). During the past decade, the EU adopted these laws at an unprecedented pace, although it refrained from constructing a hierarchical, coherent system. At least one—at times even more than one—legislative proposals have preoccupied

[7] With regard to data retention, several member states had already expanded the permitted uses of electronic communications data afforded by the ePrivacy Directive that concerned billing issues to include security processing as well.

the EU every year since 2001. This marks an astonishing contrast to non-security related data protection; the 1995 Data Protection Directive has remained in effect more or less unchanged and unaided by any other formal instruments (save for the electronic communications sector) until today. As shown earlier, the (hard) laws in the AFSJ were released in a rather *ad hoc* manner. The 2008 Framework Decision was the only harmonization effort, which, however, failed to achieve its stated objectives. Within this hectic environment, little space or care was left for 'soft law'. 'Soft law' thrived under the 1995 Data Protection Directive environment, but not under the AFSJ data protection field.

Still, the policy field has contributed to member states strengthening their operational cooperation. The data protection rules developed at the EU level often required member states to install new administrative mechanisms at the national level. The national Data Protection Authorities, by now regular participants in the EU data protection scene, are the result of the 1995 Data Protection Directive. A chapter in this directive outlined in great detail their characteristics and powers. In consequence, all data protection instruments that followed the 1995 Directive provided member states with the option to vest the relevant powers upon these agencies. This has been the case for the most part with Schengen, Europol or Eurojust mechanisms as well as with the 2008 Framework Decision.

In some cases, however, EU data protection regulations have resulted (or will result) in the establishment of more specialized data protection units within the public administration of member states. The Passenger Information Units (PIUs) to be included in the EU-PNR Directive will be an example, once the directive is formally adopted. In this case, EU law does not only state the general rules and objectives but also prescribes the very administrative mechanism by which these rules are to be implemented.

2.2.2. The type of European integration

The type of integration established by the aforementioned regulatory patchwork in AFSJ personal data processing inevitably varies, following the particulars of each separate regulatory field. The Schengen mechanism is in operation only among the member states that participate in the border-free project. These states have achieved a high level of integration in terms of their data protection scheme (De Hert et al. 2008). The same can be said with regard to the Europol and Eurojust data protection mechanisms (Boehm 2012: 175ff). These three cooperation frameworks have allowed the participating members to gain substantial knowledge on overcoming implementation problems both at the EU and member state level. Their specialized data protection systems follow different sets of general rules, thus warranting a strong level of harmonisation. Overall, however, these cooperation frameworks fall under the category of 'negative' integration: the removal of national barriers when it comes to law enforcement activities—more specifically, the removal of barriers for law enforcement authorities of other member states to access national (police and judicial-related) databases.

'Positive' integration—the harmonisation of common regulatory standards and the creation of common EU policies—is more difficult to establish when it comes to data protection in the AFSJ field. The 2008 Framework Decision was supposed to harmonise member states' practices in relation to data processing, yet its scope was purposefully limited to trans-border data flows and it did not touch upon already existing data protection regulations (both at EU and at member state level). Given its short period of existence (even by late 2013 a substantial number of Member States had not yet incorporated it into their national laws), it did not have enough time to fully develop its potential. Even if it had done so, it is very unlikely that its vague wording would have contributed to the harmonisation of personal data processing

practices in the AFSJ field among member states. It was a typical case of 'weak' integration that provided member states with flexibility and discretion.

The only very clear case of 'positive' integration in the field is the Data Retention Directive. This is only if, of course, the law is removed from its first pillar origins and placed in the AFSJ context; a step the European Court of Justice (ECJ) refused to take (Breyer 2005). The law has achieved a harmonised regulatory framework in data retention valid throughout the EU. However, as mentioned, the supreme courts of several EU member states found the disclosure of telecommunications data unlawful in national constitutional law. The law also faced strong opposition from data protection proponents all over Europe. This opposition contributed to problems applying the law in practice, which, in turn, reduced the overall level of harmonisation. Therefore, if one looks at the actual application, the level of integration appears to be at best medium, if not weak.

The data protection field is also characterized by the possibility of member states to implement higher data protection standards, if they wish to do so (see, for instance, Article 1(5) of the 2008 Framework Decision). Although this option is no longer included in the draft Police and Criminal Justice Directive, at least as released in early 2012, the choice offered by the law (a directive rather than a regulation, as for non-ASFJ personal data processing) indicate member states' persisting preference to retain a certain level of flexibility. In these cases of 'weak' integration, member states can maintain quite distinct national laws, if considered necessary. It is likely that AFSJ personal data processing will need more time to come to the point that 'first-pillar data processing' and the 1995 Data Protection Directive have already reached: the realization that harmonisation and 'strong' integration is only possible through common rules that avoid vague wording.

Table 10.1 Overview of policy change/stability in the area of EU data protection

	Pre-Lisbon Treaty (until 2009)	**Post-Lisbon Treaty (after 2009)**
Substantive dimension		
Rationale	Data processing for law enforcement authorities	Increasing emphasis on individual's rights to data protection within data processing
	Security	***Security vs. right-based***
Depth	Piecemeal approach	Attempt to create coherent framework
	No clear core	***Settling policy core***
Functional dimension		
Form of integration	Emphasis on directives and framework decisions	Emphasis on directives and regulations
	Hard law	***Hard law***
Type of integration	Positive and negative integration across first and third pillar	Advances towards positive integration
	Mixed	***Mixed***

3. The role of EU institutions in the area of data protection

EU institutions have always held a central role in data protection developments in the AFSJ field and their contribution is only expected to increase in importance in the future. However,

this ought not to be interpreted as evidence of a conflict-free environment of mutual goal-setting and decision-making; in fact, quite the contrary is true. The various EU institutions involved in data protection within the AFSJ field do not have a common agenda nor do they operate in harmony. Political expediencies and constraints, institutional ambitions and power-struggles have affected data protection developments in the AFSJ field more frequently than one would like to admit. This section underlines the different positions and power-struggles of the EU institutional actors in respect to data protection matters.

3.1. Institutional dynamics before the Treaty of Lisbon

A characteristic perhaps unique to EU data protection refers to the multitude of actors involved in one way or another in the decision-making process. Apart from the expected EU institutions—the Parliament, the Commission, the Council, and the Court of Justice of the European Union (CJEU)—, the Article 29 Data Protection Working Party, the European Data Protection Supervisor (EDPS), as well as the separate data protection units of Schengen, Europol and Eurojust form a large mosaic of contributors to the data protection policy process. Despite the fact that only a few have formal rule-making powers, the influence of actors that have either an established and important presence or direct access to the public ought not to be underestimated.

In the pre-Lisbon environment, the 'war on terror' that followed the 11 September 2001 terrorist attacks on the United States led to a clear division between those willing to sacrifice a level of data protection (or, for the same purposes, other individual rights) for increased security within the EU and those with pro-data protection stances. The Council has traditionally been considered a pro-processing actor, willing to sacrifice some data protection to the needs of law enforcement agencies. Its central role in decision-making before Lisbon

allowed it to lay the path for data protection in third-pillar matters. Its primary contributions during that period were the 2008 Framework Decision and the PNR Agreements with the US, Canada, and Australia. Despite the shortcomings of these contributions in data protection standards, one ought to bear in mind two basic impediments in the Council's rule-making process. First, the principle of unanimity that forced lawmakers to accept the will of the minorities or risk ending with no rules at all. Second, the fact that data protection work was entrusted to the Council's permanent committees, such as the Council's Multidisciplinary Group on organised crime (MDG) comprised of police officers and Ministry of Justice officials with little connection to, or interest in, data protection matters.

In addition, the Council, whose composition by definition reflects political preferences at the member state level, was internally divided across several lines. The practice of policing differs substantially in Europe and is strongly defined by distinct national cultures and historical experience. First, while certain member states were actively involved in the 'war against terror' and even witnessed terrorist attacks on their soil, many did not face a direct terrorism problem. Consequently, not all member states were equally eager to allow for more space for personal data processing by their law enforcement agencies. Second, member states also displayed major cultural differences towards the importance of data protection and the ability of national authorities to access and process personal information. For instance, Germany, Austria, Hungary, and Greece have always proved more reluctant than other countries to facilitate access to personal information, such as the UK (Monar 2010: 146). Third, the importance of the sophistication of police methods and general information technology processing capacity ought also not to be overlooked: some member states operate and process automatically vast amounts of personal information on a daily basis, whereas others are less developed from this point of view (De Pauw et al. 2011).

The emphasis on data processing was supported by other actors such as Eurojust, Europol, and Schengen; although not vested with law-making powers, these well-established organisms have permanent data protection mechanisms embedded in structures that have been in operation for years and are generally considered of fundamental importance to the EU. Consequently, their opinions, whenever expressed, are taken seriously by other law-making EU bodies; a fact that can be, for instance, witnessed in their exclusion from any general data protection rule (such as the 2008 Framework Decision or the draft Police and Criminal Justice Directive, at least in its 2012 draft).

While member states and operational agencies tended to promote far-reaching access of law enforcement authorities to personal data, several actors openly opposed low data protection standards. The EP bitterly contested its exclusion from the relevant decision-making arenas ever since the first data protection AFSJ instruments made their appearance. It consistently charged the Council and the Commission of inadequately protecting individual rights, sacrificing data protection to enable increased security-related processing. Whenever possible, it successfully challenged these instruments in front of the European Court of Justice, as was the case with the first PNR Agreement with the US. It also never failed to intervene in new regulatory initiatives, presenting its point of view that for the most part supported data protection purposes. However, before the Treaty of Lisbon, its role was at best of a consulting nature; the substance of its work carried out mostly under its LIBE Committee (Ripoll Servent 2009). It is exactly the composition of the Parliament, with complex political parties and alliances not exactly reflecting national politics, together with the fact that EP elections are of a different character than national elections, which probably best explain its persistent pro-data protection standpoint.

The EP was generally supported by the Article 29 Working Party and the EDPS. Since its establishment in 2001, the EDPS has become an important participant in the EU data protection process. Although not vested with formal rule-making powers, the EDPS benefits mostly from two factors: first, the fact that its office must be consulted and invited to participate in the decision-making process; second, that its office is a 'visible' organ that has direct access to the public—adding political value to its opinions and interventions (De Hert and Papakonstantinou 2014). On the other hand, the Article 29 Working Party has expanded its role over the years and issued opinions on AFSJ regulatory instruments as well. The Article 29 Working Party reflects the opinions of national Data Protection Authorities, providing important feedback from the authorities in charge of implementation.

While the position of the EP and the Council was relatively stable and clear, the position of the Commission is more difficult to interpret. Whereas under the first pillar it was a clear promoter of data protection issues that encroached on the Single Market, on AFSJ matters it was viewed with suspicion by data protection proponents—considering that it produced texts of questionable data protection value (the Data Retention Directive, the 2008 Framework Decision) and submitted to what were considered excessive requests by the US, for instance with regard to PNR processing. However, what has to be taken into account is that first, the internal organisation of the Commission changed the locus of authority from the 'Internal Market' Directorate General to the 'Justice, Liberty, and Security' DG (currently, DG Justice). This was a manifest shift from market- to AFSJ-related issues which, in turn, affected the tone of the regulatory texts released during that period. Second, under consultation, the central role of the Council made it necessary for the Commission to reach compromised solutions and establish a personal data processing system that worked and was acceptable among member states.

Finally, given that the ECJ did not have the power to enter the AFSJ field, help was requested and frequently granted from the European Court of Human Rights (ECtHR), applying an as-of-yet non-EU instrument. The few relevant ECJ (now, CJEU) decisions served mostly to add even more complexity in the field.[8] In comparison, the Strasbourg court provided individuals with a more welcoming forum to bring their claims. By interpreting Article 8 of the European Convention on Human Rights (ECHR) in the broadest way possible, the ECtHR issued important case law over the years on the personal data processing of law enforcement agencies.

3.2. Institutional dynamics after the Treaty of Lisbon

Although events such as 11 September 2001 raised awareness of the role of data processing and its relevance for data protection issues, practical limits were soon evident in the procedural structure and the treaty limitations imposed by the third pillar. That is why formal institutional change in data protection in the AFSJ field, introduced through the ratification of the Treaty of Lisbon, presented a way out of this regulatory dead-end. Given the necessary period to adapt to the new Lisbon environment, the major changes to the procedures and substantive content are still pending. However, three main areas with potentially far-reaching effects can already be identified.

First, the entry into effect of the Treaty of Lisbon changed the formal decision-making rules in AFSJ data protection. Essentially, the EP has been officially brought into the process that was once the prerogative of the Council and the Commission. This sudden shift already has

[8] For instance, the court interpreted a difference between the data collected by airlines and then accessed by law enforcement agencies (as in the PNR agreement) – which were considered to be security-related – and electronic communications data collected by providers and then accessed by security agencies (as in the Data Retention Directive) – which was considered not to be security-related.

observable results. For instance, the batch of PNR Agreements with third countries has been revised at the EP's request. Also, in view of the role of the EP as a co-legislator, the older EU-PNR regulatory drafts were abandoned and a new draft directive has been released by the Commission. The EP also actively participates in the EU data protection recast process. Given the full involvement of the EP and its past commitment to high data protection standards, it will be particularly interesting to observe whether it will ultimately insist on supporting the data protection purposes. Or, if political expediency will change the Commission's point of view now that, unlike the recent past, it has to make decisions and contribute to an operating security personal data processing model in the EU—as was the case of the Data Retention Directive (Ripoll Servent 2009; 2013). Equally, it may be that the Council and the Commission water-down their regulatory initiatives, in order to appease the data protection concerns of the EP.

Second, a further structural change of potentially equal gravity is expected in the near future in the AFSJ data protection field when the EU joins the ECHR. At that time, the case law of the ECtHR, which has long elaborated upon security-related personal data processing and acted as the last recourse to individuals who felt their data protection rights had been infringed, will become binding within the EU and will have to be incorporated into the EU regulatory structure. This is expected to bring fundamental changes to AFSJ data protection regulations that cannot be properly assessed or even foreseen at this time. Finally, the wider remit of the CJEU may lead to a new wave of rulings seeking to define the new individual rights inserted in the Treaty of Lisbon. The CJEU may prove to be a key arena where further battles between data processing and data protection are fought—particularly now that individuals can also appeal to it.

The Treaty of Lisbon has thus been a watershed for data protection matters; it has widened the participation of the EP in decision-making and abolished the previous division between first and third-pillar matters. While the latter has far-reaching consequences, particularly in relation to the role of the European courts, it can also lead to a more direct confrontation between the principle of data protection and the increasing attention paid by all institutions—the EP included—to data processing matters and the need to ensure the security of EU citizens.

4. Case-study: The case of PNR processing

The term 'Passenger Name Record' (PNR) denotes the travel record for a person, as used by airline and travel agency databases. Before 11 September 2001, PNR data were not systematically collected. Afterwards, however, in the belief that the processing of PNR data could contribute to the prevention of terrorism, US authorities started asking international air carriers for access to passenger data, which also had to increase in accuracy and quantity. As the request seemed to contradict EU airlines' data protection obligations concerning the personal data they possessed, air carriers were faced with the dilemma of which law to break. At that point, the Commission, rather than individual member states whose air carriers were affected, decided to intervene and entered negotiations with the US in 2003 in order to resolve the PNR matter centrally—i.e. for all member states. The Commission assumed that PNR processing constituted commercial processing—whose legal basis fell under first-pillar rules and allowed for the Commission's direct intervention (Papakonstantinou and De Hert 2009).

On February 2004, the Council authorised the Commission to negotiate such an agreement with the US, and issued a series of negotiating guidelines. The first PNR Agreement was thus signed on 28 May 2004. However, a couple of months after it was concluded, on 27 July 2004, the EP filed two actions with ECJ against the Council's and Commission's Decisions,

upon which the first PNR Agreement was based (Argomaniz 2009; Occhipinti 2010). The (then newly established) European Data Protection Supervisor intervened in support of the EP in both cases. The Court reached its decision two years later, on 30 May 2006.[9] It did not go into the substance of the EP's claims because it found that the first PNR Agreement did not pertain to commercial communications but rather to security matters. Hence, its legal basis could not be the 1995 Data Protection Directive that only applies on first pillar processing. It therefore annulled the Council decision—upon which the PNR Agreement was concluded—in effect, also annulling the PNR.

Negotiations for conclusion of the second PNR Agreement began on July 2006, this time led by the Council. The Council authorised 'the Presidency, assisted as appropriate by the Commission' to open the relevant negotiations with the US; negotiations between American and EU officials, which included the Finnish and German Presidencies assisted by the Commission, went on for the second half of 2006 and the first half of 2007. The second PNR Agreement entered into force on 29 June 2007 (Council Decision 2007/551/CFSP/JHA). Data protection concerns were raised on various accounts, both by data protection proponents and the EP (Papakonstantinou and De Hert 2009), which regretted that 'EU negotiations with the US took no account of Directive 2004/82 [on the obligation of carriers to communicate passenger data] nor of EU PNR agreements with Australia and Canada, that ensure higher standards of protection of personal data' (European Parliament 2007).

The actual entry into force of the Lisbon Treaty proved to be a catalyst, at least with regard to the EP (Koesters et al. 2010). Exercising its newly acquired powers, it asked for an overhaul

[9] Joint Cases C-317/04 and C-318/04, 30.05.2006.

of the whole PNR scene. At its request, the Commission and the US initialised in 2011 a new draft agreement on the transfer and use of Passenger Name Records, which ultimately constituted the third EU-US PNR Agreement. However, the end result—voted on 19 April 2012 by the majority of its members (409 for, 226 against, thirty-three abstentions)—was hardly different from that of 2007. It left data protection proponents dissatisfied and lamenting that the EP, once in a decision-making position, repealed its resolutions of 2010 (Digital Civil Rights in Europe 2012; European Association for the Defense of Human Rights (AEDH) 2012). A similar episode occurred with the new EU-Australia PNR Agreement, voted by the EP on 27 October 2011 with an even wider majority (463 for, ninety-six against, eleven abstentions) (Digital Civil Rights in Europe 2011).

The above serves to demonstrate that the EP, the body most favoured by procedural changes after the ratification of the Lisbon Treaty, once vested with decision-making powers, abandoned its previous resolutions against past PNR agreements with third countries and accepted similar solutions to those already in place. Therefore, it is important to examine what happened and why the position of the EP shifted so substantially during the EU-US PNR negotiations. In comparison with the previous PNR agreements, one of the main changes concerned the voting majorities inside the EP. Before the 2009 elections, the liberals and left-wing groups had generally formed a winning coalition with very high data protection standards. However, the new majorities in the chamber shifted towards the centre-right and conservative groups– which were able to tip the balance towards more security-oriented policy alternatives. In the PNR vote of April 2012, the winning majority was formed mainly by the European People's Party (EPP) and the European Conservatives and Reformists group (ECR). They were supported by half of the Socialist and Democrats (S&D) and even some liberals—which had led the EP delegation during negotiations. This shows how salient and controversial the vote was; it split the former left-wing coalition and underlined important

differences in national circumstances. For instance, the Danish MEPs generally voted in favour because they already had a bilateral PNR agreement with the US, while the Romanians thought that their support would lead towards obtaining a visa waiver to travel to the US (European Parliament 2012c).

There were other reasons proffered to support the agreement. For one, many MEPs feared that if the EP failed to give its consent, the US would prefer bilateral agreements with twenty-seven member states or that the 2007 Agreement would apply again, leaving EU citizens in an even worse situation. Some were also interested in the side-effects of the agreement, since it offered some reciprocity in the shape of intelligence leads and information that could be transmitted to EU authorities—effectively covering a gap in the security systems of EU member states, which do not (yet) have the capacity to process PNR data.

However, these shifts in the composition of the EP and the potential detriments of a 'no' vote are not enough to understand why some groups, such as the socialists and liberals, were split on an issue that had been previously characterised by its capacity to repeatedly unite the left-wing side of the EP. Reading the (exceptionally long and heated) debates that took place before and after the vote, it is clear that various elements served to delegitimise the 'no' vote (European Parliament 2012c). Several discursive practices were used in order to reframe the policy alternatives of the PNR framework. First, there were various attempts to present the 2012 Agreement as the only possible solution. The Commission repeatedly demonstrated its discursive entrepreneurship skills by framing the policy alternatives available to member states in order to avoid separate, bilateral, agreements with the US. Its strategy was aimed at seeking the approval of member states so as to legitimise its role as lead negotiator. However, as a result, there was a generalised feeling that there were no other available alternatives. The rapporteur remarked that 'the European Commission has insufficiently explored alternative,

less intrusive measures, for example the use of API or ESTA data for the identification of suspects' (European Parliament 2012a: 9).

The lack of alternatives and the seeming impossibility of reopening negotiations with the US were presented to MEPs as an unavoidable fact and for which the EP should take responsibility. The new powers of consent acquired with the Treaty of Lisbon seem to have produced a change in the behaviour of the EP; the acquisition of more decision-making powers in international agreements rendered its traditional confrontational behaviour less legitimate. Droutsas (S&D) came to the same interpretation by stating that 'the European Parliament rightly wants a more substantial role in negotiations on international treaties brokered by the Union and, as the European Parliament, we should have that role in the future. However, we must demonstrate that we have responsibilities, as the European Parliament, and that we know how to assume those responsibilities' (European Parliament 2012c). Interestingly, recourse to the CJEU appeared also less appealing; with some Members of Parliament 'reluctant to outsource political decision-making to the courts (…) the House should take its own responsibility' (in't Veld in European Parliament 2012c).

There was also a clear shift in the discursive interpretations on how to best protect EU citizens. The Greens, communists, and some sections of socialist and liberal groups maintained that the most legitimate way to protect citizens was to ensure that their absolute right to data protection would not be subjected to security considerations (see minority opinion in European Parliament 2012b: 8). They considered that the agreement would set a precedent for future PNR negotiations that could prove particularly problematic with countries seen as more 'challenging'—such as China, Russia or Saudi Arabia (Albrecht, in't Veld, and Tavares in European Parliament 2012c). On the other hand, a growing number of socialists and liberals supported the more security-oriented stances of the right-wing groups

that considered it necessary to prioritise the safety of citizens from the effects of serious crime, even at the expense of the level of protection of their personal data. The latter interpretation was amplified by the commitment of these groups to the success of transatlantic relationships; they deemed that healthy cooperation with the US on security matters would further benefit EU citizens and ensure their safety.

Table 10.2. Explaining the adoption of the 2012 PNR Agreement

Factors altering actors' opportunity structure	
Formal changes to the structural context.	Introduction of the consent procedure; EP elections.
Altered exogenous preferences.	Domestic implications of a 'no' vote for some EP national delegations.
Factors altering actors' beliefs and norms	
Shift in social practices.	Increased sense of shared responsibility between EU institutions and towards US.
Re-framing of policy debates and policy solutions.	Recourse to CJEU framed as a less legitimate option.
Mechanisms leading to policy change	
Bargaining.	Coalition-building (coalition of centre-right political groups across EU institutions).
Redefinition of beliefs and norms.	Discursive entrepreneurship ('Security' of EU citizens framed as more legitimate goal than data protection).

5. Conclusion

Data protection is a relatively recent field of law that has, from its beginnings, relied upon international co-operation in order to achieve its objectives. EU institutions have done much more than only enhance co-operation among member states; since the release of the Data Protection Directive in the early 1990s they set the pace and the substantive rules for data protection in Europe. After a period of relative neglect, the terrorist attacks in Europe and elsewhere made personal data processing an integral part of crime-prevention policies. The last decade has witnessed an unprecedented release of EU regulations on personal data processing in the AFSJ.

This process was neither structured nor unquestioned, particularly in the pre-Lisbon era. In fact, regulations were established according to time constraints and political expedience by the EU institutions that had the power and motivation to do so. This was first and foremost the work of the Council, which led the policy-making process in the AFSJ, putting emphasis on data processing for security-related purposes rather than on data protection. The laws resulting from this period were frequently and sometimes successfully challenged by other EU institutions. In particular, the EP brought cases to the ECJ, which addressed the relevant issues with resolve but not always with clarity. Much has changed and is expected to further change through the ratification of the Lisbon Treaty. The empowerment of the EP has constituted a decisive structural change: in past discussions, the EP demonstrated a fervent pro-data protection profile; nevertheless, once in power, this profile has been watered-down and subjected to political necessity.

The case study on the EU-US PNR illustrates how the impact of institutional change was not so much seen in terms of policy outcomes but rather on the level of inter-institutional

interactions. The 2007 Agreement negotiated and ratified by the Council had met fierce opposition from the EP on the grounds that it would contravene European data protection laws. Upon the insistence of the EP, the EU entered into new negotiations with the US. However, after two years of intense and difficult discussions, the substance of the 2012 Agreement was not substantially different from the previous one. The EP's U-turn was the product of a combination of factors. A new composition of actors—mainly the political majorities inside the EP—made a centre-right-led coalition easier and also served to give more force to a new interpretation of the EP's responsibility towards EU citizens that prioritised their security at the expense of their right to data protection. At the same time, the structural changes introduced by the Treaty of Lisbon amplified the EP's feeling of responsibility—both towards its own citizens but also towards the US and the other EU institutions involved in negotiations.

If the EU-US PNR Agreement proves to be an indication of the EP's future stand on this matter, data protection proponents' enthusiasm over the inclusion of the EP in the law-making process may prove to be premature. At the same time, the imminent accession of the EU to the ECHR and particularly the case law of the Court in Luxembourg may lead to changes both to the procedures and substance of the EU's structural environment that might turn out to have far-reaching implications for the EU data protection policies.

References

Argomaniz, J. (2009) '"When the EU is the "Norm-taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms', *Journal of European Integration* 31(1): 119–36.

Boehm, F. (2012) *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-Level*, Heidelberg: Springer.

Breyer, P. (2005) 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR', *European Law Journal* 11(3): 365–75.

Custers, B. (2012) 'Technology in Policing: Experiences, Obstacles and Police Needs', *Computer Law & Security Review,* 28(1): 62–8.

De Hert, P. and Papakonstantinou, V. (2014) 'The EDPS as a Unique Stakeholder in the European Data Protection Landscape, Fulfilling the Explicit and Non-explicit Expectations', in: H. Hijmans and H. Kranenborg (eds.) *Data Protection anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014),* Brussels: Intersentia, 237-252.

De Hert, P., and Papakonstantinou, V. (2009), 'The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters - A Modest Achievement However Not the Improvement Some Have Hoped For', *Computer Law & Security Review,* 25(5): 403–14.

De Hert, P., Papakonstantinou, V., and Riehle, C. (2008) 'Data Protection in the Third Pillar. Cautious Pessimism', in: M. Maik (ed.) *Crime, Rights and the EU : the Future of Police and Judicial Cooperation*, London: Justice, 121–94.

De Pauw, E., Ponsaers, P., van der Vijver, K., Bruggeman, W., and Deelman, P. (2011) 'Technology-Led Policing', *Journal of Police Studies*, 3(20).

European Commission (2012a): 'Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data', COM(2012)10 final, 25 January 2012.

European Commission (2012b): 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)', COM(2012)11 final, 25 January 2012.

European Council Decision (2007): 'Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)', *Official Journal of the European Union*, 4 August 2007.

Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)

European Parliament (2007): 'Resolution of 12 July 2007 on the PNR Agreement with the United States', P6_TA(2007)0347, 12 July 2007.

European Parliament (2012a): ‘Draft Recommendation on the Draft Council Decision on the Conclusion of the 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’, PE480.773v01-00, 1 February 2012.

European Parliament (2012b): ‘Recommendation on the Draft Council Decision on the Conclusion of the 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’, PE480.773v02-00, 3 April 2012.

European Parliament (2012c): ‘Debates - Thursday, 19 April 2012 - EU-US PNR’, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0099&language=EN, accessed 2 April 2013.

González Fuster, G., Gutwirth, S., and Ellyne, E. (2010) ‘Profiling in the European Union: A High-Risk Practice’, *CEPS INEX Policy Brief* [online paper], http://www.ceps.eu/book/profiling-european-union-high-risk-practice, accessed 2 April 2013.

Koesters, J., Lachenmaier, A., van Bergen, J., Wagner, N., Winter, M., and Wirtz, A. (2010) ‘Who Cares About Strasbourg? The Role of the European Parliament in the PNR Agreements’, *Maastricht European Studies Papers 1(1)* [online paper], http://www.fdcw.unimaas.nl/mesp/Papers%20%282006%29/MESP_Koesters%20et%20al.%20_2010_.%20Role%20of%20EP%20in%20PNR%20Agreements_PUBLICATION.pdf, accessed 2 April 2013.

Monar, J. (2010) ‘The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic View and Its Implications’, *European Foreign Affairs Review* 15(2): 143–51.

O'Neill, M. (2010) 'The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar', *Journal of Contemporary European Research* 6(2): 211–35.

Occhipinti, J. D. (2010) 'Partner or Pushover? EU Relations with the US on Internal Security', in: D. S. Hamilton (ed.) *Shoulder to Shoulder: Forging a Strategic US-EU Partnership*, Washington D.C.: Johns Hopkins University Centre for Transatlantic Relations, 121–38.

Papakonstantinou, V., and de Hert, P. (2009) 'The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic', *Common Market Law Review* 46(3): 885–919.

Pearce, G., and Platten, N. (1998) 'Achieving Personal Data Protection in the European Union', *Journal of Common Market Studies* 36(4): 529–47.

Ripoll Servent, A. (2009) 'Setting Priorities: Functional and Substantive Dimensions of Irregular Immigration and Data Protection Under Co-decision', *Journal of Contemporary European Research* 5(2): 225–42.

Ripoll Servent, A. (2013) 'Holding the European Parliament Responsible: Policy Shift in the Data Retention Directive from Consultation to Codecision', *Journal of European Public Policy* 20(7): 972-987.

Rodota, S. (2009) 'Data Protection as a Fundamental Right', in: S. Gutwirth, Y. Poullet, P. de Hert, C.de Terwangne, and *S.* Nouwt (eds.) *Reinventing Data Protection?*, Dordrecht: Springer, 77–82.