Opinion of the European Data Protection Supervisor on the future development of the area of freedom, security and justice

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Article 41(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1. The purpose of this Opinion is to contribute to the further development of the EU policies in the area of freedom, security and justice through fuller integration of privacy and data protection into the activities of all EU institutions. It responds to two communications adopted by the Commission on 11 March 2014 on the future of justice and home affairs,[3] the Resolution adopted by the European Parliament on 2 April 2014 reviewing the Stockholm Programme, and discussions in the Council, with a view to the conclusion by the European Council, for the first time, of strategic guidelines for legislative and operational planning in accordance with Article 68 TFEU.

2. This is a critical moment for the EU's role in justice and home affairs. We are approaching the end of the transitional period set out in the Lisbon Treaty after which the powers of the Commission to bring infringement proceedings and the powers of the European Court of Justice become fully applicable to EU laws on police and judicial

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] See below para [8] of this Opinion.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

cooperation in criminal matters.[4] Under the Treaty, the Charter for Fundamental Rights has assumed the status of primary law, and the Court of Justice has in recent judgments clarified the restrictions on the legislator's room for manoeuvre wherever a measure implies interference with those rights.[5]

3. Moreover, during the last five years concerns about privacy and data protection have arguably become more intense than ever before. In January 2012, the Commission proposed a package of legislative reforms of data protection in the EU.[6] Since June 2013 revelations of mass surveillance of individuals in the EU by US and other intelligence agencies have greatly damaged the trust in confidentiality of personal information. Most recently, the Court of Justice in April 2014 - in one of the two judgments just referred to - annulled the Data Retention Directive[7] due to its excessive interference with fundamental rights. Action at EU level on data protection has taken on a truly global significance, as attested for instance by the degree of international coverage and lobbying on the reform of the data protection framework, which led to around 4000 amendments submitted during first reading in the European Parliament[8].

4. The legal, technological and societal challenges for policymakers and legislators in the area of justice and home affairs are certain to intensify over the period to be covered by the strategic guidelines. Furthermore, the new guidelines by the European Council are an opportunity to state an intention to restore trust in the EU's capacity to protect individuals effectively. For that reason, we suggest that the European Council addresses explicitly the following themes in the new guidelines:

    a. the huge volumes of personal data processing that is required by many of the EU laws and policies in the area of freedom, security and justice;

    b. the fragility of any measure which fails to respect fundamental rights, as has been witnessed in the Data Retention Directive, but may also apply to other ongoing initiatives such as the 'smart borders' package,[9] and the various instruments relating to passenger name records;[10]

---

[4] The transitional provisions cease to apply on 1 December 2014; Article 10, Protocol 36 on transitional provisions, attached to the Lisbon Treaty.

[5] See in this context the judgments of the Court (Grand Chamber) of 9 November 2010 in *Schecke and Eifert* (Joined Cases C-92/09 and C-93/09) and in particular of 8 April 2014 in *Digital Rights Ireland and Seitlinger* (Joined cases C-293/12 and C-594/12). In the first case the Court also emphasised the need for the legislator to consider sufficiently less intrusive alternatives for a particular measure.

[6] COM(2012)11 final; COM(2012)10 final.

[7] Directive 2006/24/EC, OJ L 105/54.

[8] The first reading resulted in the European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading).

[99] See the EDPS Opinion of 18 July 2013 on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP).

[10] This includes an EU system for passenger name records (COM(2011) 32 final) and a possible proposal on the transfer of passenger data to third countries (http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_home_004_transfer_pnr_data_3rd_countries_en.pdf [accessed 3 June 2014]).

c. the importance of adopting as soon as possible a strong and modernised data protection framework in the EU, which should also be used as the compass for EU external policies; and

d. the need to integrate privacy and data protection considerations in the development of all new policies and legislation in the area of freedom, security and justice.

5. Having contributed to a similar exercise five years ago, we offer in this Opinion to work with the EU institutions in improving the quality of legislation from a data protection perspective, as part of a new template for cooperation.[11]

2. INSTITUTIONAL PERSPECTIVES ON THE FUTURE OF THE AREA OF FREEDOM, SECURITY AND JUSTICE

6. 'The Stockholm Programme - An Open and Secure Europe Serving and Protecting Citizens' ('the Stockholm Programme'),[12] adopted under conclusions of the European Council on 10/11 December 2009, was the third successive multi-annual statement of intent in the area of justice and home affairs.[13] It was informed by a communication of the Commission in June 2009 entitled 'An area of freedom, security and justice serving the citizen'. The EDPS Opinion published on 13 July 2009 acknowledged the emphasis placed by the Commission on the protection of fundamental rights, and in particular the protection of personal data in the context of EU action on citizenship, justice, security, asylum and immigration. Specifically, we welcomed the call for a comprehensive data protection scheme covering all areas of EU competence and the reaffirmation of basic principles such as purpose limitation. The Commission envisaged developing a 'European information model' and an 'EU Information Management Strategy', which as we hoped would properly reflect these principles and best practices.

7. On 19 and 20 December 2013, the European Council, in line with its function under Article 68 TFEU, announced its intention - for the first time under the current treaties - to define 'strategic guidelines for further legislative and operational planning in the area of freedom, security and justice ("post-Stockholm")'.[14]

8. On 11 March 2014, two communications from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions were adopted addressing these issues: the first communication, 'The Justice Agenda for 2020: Strengthening Trust, Mobility and Growth within the Union'[15] was organised according to the concepts of 'consolidation' of existing measures through, for example, more judicial training, 'codification' of civil and commercial laws,

[11] See on this approach more in general the 2014 EDPS policy paper "The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience", published on the EDPS website. .
[12] OJ 2010, C 115/01.
[13] COM(2009) 262 final.
[14] EUCO 217/13. While previous multi-annual programmes have applied for five year periods which by and large coincide with the mandates of colleges of Commissioners and European Parliamentary terms, the timescale for the envisaged set of strategic guidelines is unclear. The Council has discussed the option of aligning the new guidelines with the current seven-year multiannual financial framework 2014-2020.
[15] COM(2014) 144 final.

consumer rights and criminal laws, and identifying measures to 'complement' mutual trust, economic growth and citizenship rights. The second communication, 'An Open and secure Europe: making it happen',[16] contained more subject-specific suggestions on legal migration, such as coordinating assessments on labour migration, on irregular migration, on amending the EU visa code, on asylum – such as mutual recognition of decisions – and on security such as new laws on firearms control and international treaties on passenger name records. It would appear that the Commission, unlike the Parliament and the Council, no longer sees merit in a single, coherent vision on the future of the area of freedom, security and justice.

9. The European Parliament on 2 April 2014 adopted a resolution on the Stockholm Programme.[17] The resolution included calls for the European Council to implement a 'European Digital Habeas Corpus' on fundamental rights, for speeding up accession to the European Convention on Human Rights, for the Parliament to have a central role in evaluating and defining internal security policies in a new Internal Security Strategy from 2014, and for a 'future-oriented vision of how to shape and optimise law enforcement data sharing in the EU while guaranteeing fundamental rights , including a robust level of data protection'. More generally, the Parliament called for 'closer cooperation and better information-sharing between the European institutions and agencies and the Member States [in order to] improve the creation and implementation of policy', and argued that 'improving the quality of EU legislation […] requires a joint effort by the Member States and the European institutions'.

10. The Council has in the meantime held a series of discussions on the future of justice and home affairs, which will also be a subject of the newly elected European Parliament's deliberations. Like the Commission, the Council has tended towards broad political priority setting rather than the detailed programming of the last 10 years, consolidation or simplification of existing measures rather than new legislation, and evidence-based approaches based on impact assessments.

3. DATA PROTECTION AND THE STOCKHOLM PROGRAMME

Persisting urgency for a comprehensive and robust framework

11. Since the adoption of the Stockholm Programme, the EU has taken considerable steps to strengthen fundamental rights, in particular the rights to privacy and data protection. The Charter became legally binding with the entry into force of the Lisbon Treaty, and there is a requirement under Article 16 TFEU for the EU to set down data protection rules applicable to all activities falling within the scope of EU law. The adoption of a new and comprehensive legal framework for data protection is particularly acute. The key milestones for data protection during the period of implementation of the Stockholm Programme have been the Commission proposals of January 2012 for reforming the data protection framework and the legislative resolution in March 2014 on the reform by the European Parliament. It is regrettable that progress has been slower at Council level, and the EDPS continues to urge all parties to move towards agreement as soon as possible.

[16] COM(2014) 154 final.

[17] European Parliament resolution of 2 April 2014 on the mid-term review of the Stockholm Programme (2013/2024(INI)).

12. The ambitious proposal to replace the central piece of existing legislation on data protection, Directive 95/46/EC, with a directly applicable regulation – the 'General Data Protection Regulation'– promises to strengthen individual rights, to increase accountability of data controllers, to reinforce national supervision of compliance and to provide greater legal certainty for businesses.

13. Directive 95/46/EC does not apply to the activities of the State in areas of criminal law (Article 3(2)) and it provides for Member States the possibility to restrict the rights and obligations where necessary to safeguard, among other things, 'the prevention, investigation, detection and prosecution of criminal offences' (Article 13(1)). Data processing in the framework of police and judicial cooperation in criminal matters can have a particularly high impact on an individual's life. The current instrument however, Council Framework Decision 2008/977/JHA, only covers cross-border data processing and allows wide discretion to Member States in how principles are applied. The proposed directive replacing Framework Decision 2008/977/JHA would apply to domestic processing, though without affecting or improving the various existing rules contained in police and judicial cooperation instruments.

14. The EDPS has consequently expressed regret that the Commission missed a unique opportunity to propose a single comprehensive framework with a high level of protection.[18] If the legislator insists on a separate instrument for police and judicial cooperation, then the proposed directive must offer a level of protection equivalent to that in the proposed regulation. Evident gaps between the two instruments, such as the lack of clarity on responsibilities where there is a mix of actors and purposes in data processing, must be addressed.

First efforts to evaluate

15. In home affairs, the Commission presented in December 2012 a 'European Information Exchange Model', as the information management strategy promised by the Stockholm programme.[19] This document, which contained the conclusion that neither new EU-level law enforcement databases, nor new EU information exchange instruments were needed, represented a welcome first step in the full evaluation of effectiveness of the use of data in the fight against crime which EDPS has long called for.

16. Overall, however, data protection standards in justice and home affairs activities remain a patchwork which in the words of the European Parliament is 'complicated and scattered, leading to inefficient use of the instruments available and to inadequate democratic oversight and accountability at EU level'.[20]

Specific measures

17. The need for strict and specific conditions for disclosure of personal data from private parties to law enforcement authorities has been clearly underlined by the CJEU in its

[18] Opinion of the EDPS on the data protection reform package, 7 March 2012.
[19] COM(2012) 735 final.
[20] Paragraph 66, Resolution 2013/2024(INI)).

judgment on the Data Retention Directive.[21] However, as was for instance illustrated by the agreement with the United States on the Terrorist Finance Tracking Programme, there is a tendency to grant law enforcement authorities access to personal data held by the private sector. This was one of the main reasons for the European Parliament's rejection of the first agreement with the United States.[22] Furthermore, there is a more general tendency - see for instance the Eurodac Regulation, the proposals for passenger name records and the smart borders package, to grant law enforcement authorities access to personal data of individuals that have been collected for other purposes.[23]

18. We have consistently raised concerns about these proposals. Resistance to initiatives in this area reflects heightened public sensitivity to measures which potentially interfere with fundamental rights - the European Parliament's rejection of Anti-Counterfeiting Trade Agreement is an analogous high-profile case from outside the area of freedom, security and justice - which has become all the more acute in the wake of the National Security Agency revelations in 2013. MEPs also repeatedly criticised the Data Retention Directive before its eventual annulment by the CJEU. National laws on data retention are now susceptible to challenge on the grounds of lack of proportionality and sufficient safeguards as outlined by the Court.

4. THE AREA OF FREEDOM, SECURITY AND JUSTICE AND DATA PROTECTION: RISKS AND OPPORTUNITIES

Strategic evaluation of need for gathering and processing of personal data

19. Revelations in the last year concerning mass surveillance programmes have evoked in the most dramatic and tangible way the urgency of addressing the interests of individuals, not simply as consumers of online services but as citizens with the fundamental rights to privacy and to the protection of personal data. A harmonised and relevant data protection framework reflects both the core values and the economic mission of the EU, and like overall justice policy should be viewed as 'a support for economic recovery, growth and structural reforms'[24] Data protection can play a key role in demonstrating the added value of an EU approach within the area of freedom, security and justice.

20. The EDPS has called on the Commission to assess the interference with fundamental rights in light of technological changes, the developments relating to IT large-scale systems and the growing use of data initially collected for purposes not related to the combat of crime, as well as on the effectiveness for public security of the current tendency to a widespread, systematic and proactive monitoring of non-suspected individuals and its real usefulness in the fight against crimes.[25]

---

[21] See footnote 5 above.
[22] See Commission Staff Working Paper, SEC(2011) 438 final.
[23] See e.g. the Opinions of the EDPS of 15 December 2010 on the establishment of 'EURODAC' for the comparison of fingerprints, Eurodac, and Opinion of 18 July 2013 on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP). .
[24] COM(2014) 144 final, p. 3.
[25] Opinion of the EDPS on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)' of 29 April 2013.

21. A number of measures and proposed measures which envisage the processing of personal data have been unsuccessful due to insufficient respect for the rights to privacy and to the protection of personal data which in turn, in our view, results from the lack of strategic and systematic evaluation of future needs and policy objectives. This should be done via the integration of data protection concerns in general impact assessments, consideration of whether goals could be achieved through better implementation of existing measures or through alternative less intrusive means[26] and strengthening data quality and data subject rights and redress.

22. The Commission intends to review and update the integrated border management strategy, with the possibility of 'integrated' systems and platforms. It further envisages a joint review by the Parliament, Commission and Member States of the Internal Security Strategy[27]. The Council for its part has discussed the need to explore a 'comprehensive inter-connectedness of information, communication and data systems' in the area of internal security. These exercises will provide an opportunity to evaluate home affairs policies, including initiatives like smart borders which have been under discussion for several years. The impact on data protection must be an integral part of that evaluation. As part of this, and in the light of the EP's call for a European Digital Habeas Corpus, the EU should gather views on mass surveillance[28], with particular reference to relevant CJEU judgments.

Understanding the real impact on citizens of specific measures

23. The Commission recognises the need to continue a citizen-centred approach to the area of freedom, security and justice. The Commission in its communications on the future of justice and home affairs, reflects the view of several Member States that the EU should consolidate progress so far, monitor and evaluate existing measures, rather than seek to adopt more legislation for the sake of it.[29] A citizen-centred approach which addresses the interests and fundamental rights of citizens would appear entirely sensible, especially given the difficult political and legal challenges to the EU's policy. Part of the overall policy objectives should always be to reduce interference with the right to privacy and to better ensure the protection of personal data.

24. However, as the recently published report from the Fundamental Rights Agency on judicial remedies has demonstrated, the ordinary citizen is hampered by lack of information and prohibitive costs from obtaining redress for illegal data processing.[30] Although the Commission notes that 'Close cooperation between national authorities or administrative bodies is particularly important for the effectiveness of certain EU rights,'[31] the new strategic guidelines must make it a priority to identify practical steps

[26] In line with the CJEU judgment in *Schecke and Eifert*, paragraphs 81 and 86.
[27] COM(2014) 154 final, p.9
[28] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), paragraphs 131-133.
[29] COM(2014) 144 final, pp.5-8; COM(2014) 154 final, p. 13.
[30] Fundamental Rights Agency, Access to data protection remedies in EU Member States, 2013.
[31] COM(2014) 144 final, p. 6.

which empower individuals to enforce the protection of their personal data. This would be in line with the Commission's call for 'complementary initiatives' which will 'facilitate citizens' lives'.

25. Impact assessments and evidence-based evaluation should address the real effect of measures which involve processing of personal data, in terms of number of people affected, risks of and safeguards against misuse of those data, and the remedies available to the individual data subject in the event of abuse. Implementation of measures and operational activities which depend heavily on data processing including those taking place under the EU policy cycle on Serious and Organised Crime should also take into account any instances or allegations of abuse, and training needs addressed.[32] An overall consideration here is the independence of national supervisory authorities, the importance of which has been reinforced by the CJEU in several recent judgments,[33] and how supervision can be coordinated as is currently the practice with Eurodac, Customs, VIS and SIS II.

Codification and standardisation: a chance to repair the patchwork

26. For the justice area, the Commission argues in favour of codification of existing laws, practices and case law in the areas of civil and commercial law, consumer rights law and criminal law, on the grounds that this would simplify, raise awareness and enhance mutual trust, and eliminate inconsistencies and conflicting rules of interpretation in the area of freedom, security and justice.[34] It is unclear what such a codification would entail. The EDPS has argued repeatedly for a more consistent standard for data protection in this area, rather than the current panoply of norms which militates against legal certainty for all concerned, whether competent authorities, industry or citizens. Any codification exercise ought to be extended to all instruments in the area of freedom, security and justice which have an impact on the right to personal data protection, whilst providing sufficient flexibility for legitimate public interests to be served.

27. On home affairs, the Commission refers to the role of the Schengen Information System in safeguarding security and free movement, and to the need to revise the Schengen Visa Code and to complete 'the world-wide roll out of the Visa Information System.' The Commission is considering an evaluation of the impact of a system 'based more on the assessment of individuals that [sic] on nationalities'.[35] A more calibrated approach to personal data processing such as occurs through VIS and SIS II is sensible. Among the CJEU's criticisms of Directive 2006/24/EC was that it did not require any relationship between the data and a threat to public security, and was not restricted to specific individuals, time periods and places where data processing was likely to assist in the prevention, detection or prosecution of serious crime.[36]

[32] COM(2014) 154 final, p. 9
[33] Judgments of the Court (Grand Chamber) of 9 March 2010 - *Commission v Germany* (Case C-518/07), of 16 October 2012 - *Commission v Austria* (Case C‑614/10) and of 8 April 2014 —*Commission v Hungary* (Case C-288/12).
[34] COM(2014) 144 final, pp.8-9.
[35] COM(2014) 154 final p. 6.
[36] *Digital Rights Ireland* paragraph 59.

28. A move towards individual risk assessment would presumably imply the gathering and analysis of information on certain individuals from multiple sources. As well as an implied need for mechanisms to monitor data quality, careful attention as part of the envisaged evaluation of such an approach would need to be paid to weighing the interference with those individuals' rights to privacy and to protection of personal data.[37] It will be essential to ensure clear and precise rules for such a policy change, setting out the responsibilities of data controllers especially if there is a possibility of subcontracting the collection of visa information.

Cooperation with the private sector

29. There is a clear emphasis in the Commission's communication on the role of the private sector in the implementation of home affairs aims. This includes multiple measures, including the proposed EU framework for processing passenger name record data, how to address access to and use of telecommunications data following the annulment of Directive 2006/24/EC, 'stepping up' cooperation on cybercrime through the European Cybercrime Centre, the proposed new anti-money laundering package, and cooperation between Europol and the private sector under a new Europol regulation.

30. Access by law enforcement authorities to personal data which has been collected for other purposes has raised major concerns. It is an exception to the purpose limitation principle, and therefore it must respect strict criteria under data protection law and Articles 7 and 8 of the Charter. This requires that policy objectives must be clearly defined and procedural precision and sufficient safeguards against abuse must be foreseen. The danger to the citizen of increased cooperation between private and public sector in law enforcement matters, combined with a dual framework, is a diminution in accountability and transparency. This is even more evident if the cooperation takes place on a voluntary basis. The identity of the data controller responsible for ensuring compliance must be clear, as must be the data protection rules which are applicable. There must be a more explicit legal basis for such cooperation and a clearly specified and legitimate purpose for data processing.

Third country cooperation

31. Both the Commission and the Council lay significant emphasis on interaction with third countries, such as on cybercrime and human trafficking. The Commission intends to assess the effectiveness of existing arrangements for law enforcement information exchange with third countries.[38] Meanwhile, it continues to work towards an EU-US Umbrella Agreement on privacy and data protection and redress mechanisms for EU

[37] On the risks of developing profiles on the basis of unknown and evolving assessment criteria, see Opinion of the EDPS of 25 March 2011 on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[38] COM(2014) 154 final, p.10.

citizens, and it is reviewing the agreement with Canada on provision of passenger name records.[39]

32. The EDPS supports the objective of concluding agreements which establish clear legal frameworks for those exchanges of data between law enforcement authorities which are necessary and provide stronger data protection safeguards. However, any obligations imposed by an international agreement cannot prejudice the principle that EU measures must respect fundamental rights which cannot be violated by excessive surveillance activities.[40] Agreements must not legitimise massive data transfers in a field - law enforcement - where the impact on individuals is particularly serious and where strict and reliable safeguards and guarantees are thus all the more needed, in particular preventing further processing for incompatible purposes, setting clear conditions for transfers to other authorities or third countries, and ensuring enforceable rights, including judicial redress mechanisms for data subjects in the EU. In cases where the national security exception is invoked, exceptions should be narrowly defined and with appropriate safeguards and limitations agreed.

Recommendations on how to integrate privacy and data protection considerations

33. For us, it is crucial that privacy and data protection considerations are fully integrated in the development of all new policies and legislation in the area of freedom, security and justice. Ways forward could in this context be:

- integrating data protection concerns in general impact assessments;
- assessing alternative less intrusive means to achieving policy objectives;[41]
- strengthening data quality and data subject rights and redress;
- evaluating the exchange of information against policy objectives;
- ensuring international agreements with third countries respect EU individuals' right to data protection.

5. TOWARDS A NEW TEMPLATE FOR COOPERATION

34. Over the coming years EU institutions will require a more sophisticated range of policymaking tools, ensuring that any measures in the area of freedom, security and justice which encroach on the rights to privacy and to data protection are proportionate to their aims, precise in their drafting and comprehensive in their safeguards against abuse. We recommend that references to these tools be mentioned in the European Council's strategic guidelines. In our Policy Paper 'The EDPS as an advisor to EU institutions on

[39] See Opinion of the EDPS on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 30 September 2013.
[40] See CJEU judgment in Joined Cases C-402/05 P and C-415/05 *P, Kadi and Al Barakaat International Foundation v./ Council and Commission*, 3 September 2008; see also European Parliament resolution 2013/2188(INI), paragraph 132.
[41] In accordance with CJEU judgment in *Schecke and Eifert*, paragraphs 81 and 86.

policy and legislation: building on ten years of experience'[42] we announced that we will develop a 'policy toolkit', including general guidance to the legislator in the form for instance of thematic or sectoral guidelines. The toolkit would be designed to help the institutions make informed decisions on the data protection impacts of new proposals, and could be particularly helpful in the area of freedom, security and justice.

35. We remain available to work with the institutions to devise a strategy and practical methodology for safeguarding data protection to enable the EU to meet legitimate objectives in more effective and efficient ways.[43] Sector-specific guidance could set out the practical steps in assessing legitimacy of purpose and proportionality and in identifying minimum safeguards. The purpose of these guidelines would be to provide sufficient guarantees to individuals whose data are processed against the risk of abuse and against any unlawful access and use.[44] The guidelines should also assist the quality of law-making at all stages where a proportionate interference with fundamental rights may be justified on grounds of legitimate public interest. This effort will take account of developing case law laying out criteria for assessing necessity and proportionality of a measure, and of course sufficient progress towards adoption of the revised data protection framework.

6. CONCLUSIONS AND RECOMMENDATIONS

36. The added value of the EU's action in the area of freedom, security and justice is frequently queried, especially by Member States. The benefit lies in ensuring a consistent approach, for example through designing proportionate interoperable systems which can be, at the same time, good for security and for data protection. The new strategic guidelines are in our view an excellent opportunity for the institutions to bank the lessons learned and develop a toolkit for remedying the often insufficient safeguards for the fundamental right to personal data protection.

37. The EU needs to demonstrate that it has learnt the lessons from the last five years, that it cannot adopt measures which, on close examination, interfere with fundamental rights and fail the tests of necessity and proportionality. As the Commission has reiterated many times, the Charter must now be the compass for EU policies and laws. The EDPS stands ready to assist in that process.

38. The new guidelines by the European Council are a good occasion for the Union to show its intention to restore trust in its capacity to effectively protect individuals. For that reason, we suggest that the European Council addresses explicitly the following themes in the new guidelines:

    a. the huge volumes of personal data processing that is required by many of the EU laws and policies in the area of freedom, security and justice;

[42] See note 11.
[43] The EDPS Policy Paper includes an offer to agree MoUs with each of the institutions to help improve quality of legislation.
[44] *Digital Rights Ireland*, paragraphs. 54, 60, 62, 65 and 67.

b. the fragility of any measure which fails to respect fundamental rights, as has been witnessed in the Data Retention Directive, but may also apply to other ongoing initiatives such as the 'smart borders' package, and the various instruments relating to passenger name records;

c. the importance of adopting as soon as possible a strong and modernised data protection framework in the EU, which should also be used as the compass for EU external policies; and

d. the need to integrate privacy and data protection considerations in the development of all new policies and legislation in the area of freedom, security and justice.

39. Ways forward to ensuring that privacy and data protection considerations are fully integrated in the development of all new policies and legislation in the area of freedom, security and justice could be:

- integrating data protection concerns in general impact assessments;
- assessing alternative less intrusive means to achieving policy objectives;
- strengthening data quality and data subject rights and redress;
- evaluating the exchange of information against policy objectives, and
- ensuring international agreements with third countries respect EU individuals' right to data protection.

Done in Brussels, 4 June 2014

(signed)

Peter HUSTINX