ARTICLE 29 DATA PROTECTION WORKING PARTY

819/14/EN
WP 215

Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes

Adopted on 10 April 2014

Executive Summary

Since the summer of 2013, several international media outlets have reported widely on surveillance activities from intelligence services, both in the United States and in the European Union based on documents primarily provided by Edward Snowden. The revelations have sparked an international debate on the consequences of such large-scale surveillance for citizens' privacy. The way intelligence services make use of data on our day-to-day communications as well as the content of those communications underlines the need to set limits to the scale of surveillance.

The right to privacy and to the protection of personal data is a fundamental right enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human rights and the European Union Charter on Fundamental Rights. It follows that respecting the rule of law necessarily implies that this right is afforded the highest possible level of protection.

From its analysis, the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society.

This is why the Working Party recommends several measures in order for the rule of law to be guaranteed and respected.

First, the Working Party calls for more transparency on how surveillance programmes work. Being transparent contributes to enhancing and restoring trust between citizens and governments and private entities. Such transparency includes better information to individuals when access to data has been given to intelligence services. In order to better inform individuals on the consequences the use of online and offline electronic communication services may have as well as how they can better protect themselves, the Working Party intends to organise a conference on surveillance in the second half of 2014 bringing together all relevant stakeholders.

In addition, the Working Party strongly advocates for more meaningful oversight of surveillance activities. Effective and independent supervision on the intelligence services, including on processing of personal data, is key to ensure that no abuse of these programmes will take place. Therefore, the Working Party considers that an effective and independent supervision of intelligence services implies a genuine involvement of the data protection authorities.

The Working Party further recommends enforcing the existing obligations of EU Member States and of Parties to the ECHR to protect the rights of respect for private life and to protection of one's personal data. Moreover the Working Party recalls that controllers subject to EU jurisdiction shall comply with existing applicable EU data protection legislation. The Working Party furthermore recalls that data protection authorities may suspend data flows and

should decide according to their national competence if sanctions are in order in a specific situation.

Neither Safe Harbor, nor Standard Contractual Clauses, nor BCRs could serve as a legal basis to justify the transfer of personal data to a third country authority for the purpose of massive and indiscriminate surveillance. In fact, the exceptions included in these instruments are limited in scope and should be interpreted restrictively. They should never be implemented to the detriment of the level of protection guaranteed by EU rules and instruments governing transfers.

The Working Party urges the EU institutions to finalise the negotiations on the data protection reform package. It welcomes in particular the proposal of the European Parliament for a new article 43a, providing for mandatory information to individuals when access to data has been given to a public authority in the last twelve months. Being transparent about these practices will greatly enhance trust.

Furthermore, the Working Party considers that the scope of the national security exemption should be clarified in order to give legal certainty regarding the scope of application of EU law. To date, no clear definition of the concept of national security has been adopted by the European legislator, nor is the case law of the European courts conclusive.

Finally, the Working Party recommends the quick start of negotiations on an international agreement to grant adequate data protection safeguards to individuals when intelligence activities are carried out. The Working Party also supports the development of a global instrument providing for enforceable, high level privacy and data protection principles.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of

24 October 19951,

Having regard to Articles 29 and 30(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

Since the summer of 2013, several international media outlets have reported widely on electronic surveillance activities from intelligence services, both in the United States (US), in the European Union (EU), and further across the globe, primarily based on documents provided by Edward Snowden. The revelations have sparked an international debate on the consequences of such large-scale electronic surveillance for citizens' privacy. Also, questions have been raised as to how far intelligence services should be legally allowed to go, both in collection and use of information on our daily lives. This opinion contain the results of the legal analyses of the data protection authorities in the EU, united in the Article 29 Working Party (the Working Party), of the implications of electronic surveillance programmes for the protection of the fundamental right to data protection and privacy.

The main task of data protection authorities is to protect the fundamental right to data protection for all individuals and ensure the relevant provisions in law are respected by data controllers. However, with regard to intelligence services, many data protection authorities have only limited or even no supervisory powers. For their supervision, including on the processing of personal data, other arrangements have been made by the Member States. The Working Party has therefore made an inventarisation of the various arrangements in the EU for supervision over the intelligence services, which is included in this opinion.

This Opinion does not address scenarios related to cable bound interception of personal data. At this stage, the Working Party has insufficient information available about this alleged situation to assess the applicable legal regime, even in a hypothetical manner.

2. Metadata

To assess the scope of the possible infringement of data protection rules, it first needs to be clear what we are dealing with. Government officials refer oftentimes to the collection of metadata, implying this is less serious than the collection of content. That is not a correct assumption. Metadata are all data about a communication taking place, except for the content of the conversation. They may include the phone number or IP address of the person placing a call or sending an e-mail, time and location information, the subject, the addressee, etc. Its analysis may reveal sensitive data about persons, for example because certain information

numbers for medical or religious centres are dialed. As stated by the European Court of Human Rights already in the Malone case[1], the processing of metadata, in this case 'metering', "is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts […] to an interference with a right guaranteed by Article 8." The Court has maintained this position throughout the years.

It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do.[2] They are easy to aggregate and analyse because of their structured nature. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours. This is not the case for the conversations, which can take place in any form or language. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits and behaviours.

According to Article 2(a) Directive 95/46/EC, personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly". A similar definition is given in article 2(a) of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Therefore, unlike in other countries, in Europe metadata are personal data and should be protected.[3]

In the recent judgment in the data retention cases, the Court of Justice of the European Union confirmed that "[telecommunications] data, taken as a whole, may allow very precise conclusion to be drawn concerning the private lives of the persons whose data has been retained".[4] And finally in that judgment the Court found "that the obligation to retain for a certain period, data relating to a person's private life and to his communications, constitutes in itself an interference with the right guaranteed by Article 7 of the Charter. Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right. […] The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"[5]

[1] ECHR, Malone v. UK, 2 August 1984

[2] ACLU v. Clapper, Case No. 13-3994 (WHP) – Written declaration of professor Edward W. Felten before the United States District Court for the Southern District of New York

[3] This is a long standing interpretation of data protection law. In its Opinion 4/2007 on the concept of personal data, the Working Party has already stated that also "in cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be 'identifiable' because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others".

[4] See ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014, §27

[5] See ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014, §34, 35 and 37

3. Key points

The Snowden revelations have been a hard wake-up call for many. Never before the existence of so many different surveillance programmes run by intelligence services and able to collect data about virtually everyone, had been disclosed. Some cases have emerged before, but now for the first time extensive evidence about their pervasiveness has been brought into the debate. The way intelligence services make use of data on our day-to-day communications as well as the content of those communications underlines the need to set limits on the scale of surveillance.

Even those who are careful about how they run their online lives can currently not protect themselves against mass surveillance programmes. And given the many legal, technical and practical challenges, also data protection authorities around the world cannot provide a satisfactory protection. Change is therefore in order.

In the following chapters the Article 29 Working Party analyses the mass data collection by intelligence services in the light of their surveillance programmes. From a legal perspective, a distinction needs to be made between surveillance programmes run by intelligence services of the Member States and those carried out by intelligence services of third countries making use of data of EU citizens.

Surveillance programmes run by the EU Member States will in general not be subject to EU law, following the national security exemption written into the European treaties, as well as – following this decision of the contracting Member States – several EU regulations and directives, including the EU data protection directive 95/46/EC. That does not mean however such programmes are only subject to national law. The analysis of the WP29 shows, that even though EU law in general and the data protection directive in particular do not apply, the data protection principles[6] following the European Convention on Human Rights and Council of Europe Convention 108 on the protection of personal data will for the most part still need to be respected by the intelligence services in order to lawfully perform their duties. These principles are oftentimes also included in the national constitutions of the Member States. Under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality set out in these data protection principles. Limitations to fundamental rights have to be interpreted restrictively, following case law from the European Court of Human Rights (ECtHR)[7] and the Court of Justice of the European Union (ECJ)[8]. This includes the need for all intrusions to be necessary and proportionate in relation to the purpose to be achieved. Also, it should be kept in mind that there is no automatic presumption that the national security argument used by a national authority exists and is valid. This has to be demonstrated.

[6] The main data protection principles are: fair and lawful processing, purpose limitation, necessity and proportionality, accuracy, transparency, respect for the rights of individuals and adequate data security.

[7] See ECtHR, Delcourt, 17 January 1970, and Klass, 6 September 1978

[8] See ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014 where the Court has held that the retention of traffic data "without any differentiation, limitation or exception" constitutes "a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" (§§57 jo. 65).

The Working Party stresses it is the responsibility of the Member States´ governments to comply with all their national and international obligations, including the International Covenant on Civil and Political Rights Failing to do so not only infringes upon the fundamental rights of their citizens, but also damages the trust of society in the rule of law.

For surveillance programmes run by third countries, the situation is more complex. Where data is collected, either directly from a source within the EU or after a transfer to the said third country (or another third country for that matter), EU law may still be applicable to the disclosures made under the surveillance programmes. In fact, the national security exemption referred to above only applies to the national security of an EU Member State, and not to the national security of a third country. Of course, situations may occur where the national security interest of a third country coincides with that of a Member State and where joint surveillance operations may be warranted. Also here, the public authorities involved in the surveillance need to be able to demonstrate why and how the national security interests coincide and thus exclude the application of EU law.

All conditions for international transfers of personal data set out in directive 95/46/EC need to be respected: this means above all that the recipient ensures an adequate level of protection and that transfers need to be in line with the original purpose for which the data were collected. Transfers must also comply with the need to have the appropriate legal basis for a fair and lawful processing.

None of the instruments available that can be used as an alternative basis to transfer personal data to countries that have not been found adequate (Safe Harbor, Standard Contractual Clauses and BCRs) allow for third country public authorities for the purpose of indiscriminate, massive surveillance to gain access to personal data transferred on the basis of these instruments. In fact, the exceptions included in these instruments are limited in scope and should be interpreted restrictively (i.e. to be used in specific cases and for specific investigations). Since the adequacy instruments are primarily intended to offer protection to personal data originating in the EU, they should never be implemented to the detriment of the level of protection guaranteed by EU rules and instruments governing transfers. The Working Party furthermore stresses that under the data protection directive the current assessment of the level of data protection in third countries in general does not cover the processing of data for law enforcement or surveillance purposes.

Also companies need to be aware that they may be acting in breach of European law if intelligence services of third countries gain access to the data of European citizens stored on their servers or comply with an order to hand over personal data on a large scale. In that regard, companies may find themselves in a difficult position in deciding whether they comply with the order to supply personal data on a large scale or not: in either case they are likely to be in breach of European or third country law. Enforcement action against these companies in particular should not be excluded in situations where data controllers have willingly and knowingly cooperated with intelligence services to give them access to their data. Companies do need to be as transparent as possible and ensure that data subjects are aware that once their personal data are transferred to non-adequate third countries on the basis of the instruments available for such transfers, they might be subject to surveillance or access

rights by third country public authorities, as far as such exceptions are provided for by the instruments mentioned above. The main focus is however to find an effective solution at the political level. An international agreement providing safeguards could ensure that intelligence services respect fundamental rights.

In order to ensure that intelligence services indeed do respect the limits imposed on surveillance programmes, meaningful oversight mechanisms need to be implemented in the laws of all Member States. This should include fully independent checks on data processing operations by an independent body as well as effective enforcement powers. Next to effective and robust parliamentary scrutiny, this could be done by a data protection authority or another suitable independent body, depending on the oversight arrangements adopted by the Member State. If the oversight were to be carried out by another body, the Working Party encourages regular contacts between this body and the national data protection authority to ensure a coherent and consistent application of the data protection principles.

It should be stressed that oversight mechanisms do not only need to exist on paper, but also have to be applied consistently. The Snowden revelations have shown that even though on paper many checks and balances are in place, including judicial review of intended data collection schemes, the effectiveness of the way the safeguards have been implemented remains doubtful. If safeguards against unwarranted access are not applicable to all surveillance programmes nor apply to all individuals, they do not add up to what the Working Party would consider to be meaningful oversight.

4. Supervision of intelligence services

While other entities have conducted expert analysis over the past year of the oversight arrangements for the security and intelligence services of third countries, fewer expert analyses have emerged about the national intelligence services in each EU Member State. To get a clearer picture of the various arrangements in Europe for supervision over the national intelligence services, the Working Party has issued a questionnaire to all data protection authorities (including two non-EU observers), to find out about their national supervision practice in this regard.[9]

There are two issues worthy of analysis in particular:

1. The existence of comprehensive oversight in the legal framework for national security and intelligence services;

2. The role (or absence of role) of the national data protection supervisory authority in that framework.

The Working Party herewith also responds to the request of Vice President Reding of the European Commission to analyse what the role of data protection authorities could be.[10]

[9] The answers to the questionnaire were provided by 27 EU national data protection authorities, the sub-national data protection authority of Saxony (Germany) and the non-EU data protection authorities from Switzerland and Serbia.
[10] Letter from Vice President Reding to the Chair of the Article 29 Working Party, 30 August 2013.

4.1. Overview of the applicable national oversight mechanisms

The surveillance activities discussed in this Opinion and the appended Working Document are mainly carried out by the intelligence services in the light of their task to protect national security. A wide diversity of oversight models exists, depending on the national legal traditions and structures dedicated to national security arrangements. In 26 of 27 Member States that provided information in response to the questionnaire[11], intelligence services exist and operate on the basis of laws specifying their competences, structure, and responsibilities. In one Member State there are no intelligence services and the security function of the State is carried out by a national police force.[12]

Most respondents report the existence of between one and three security and intelligence authorities at national level. In general there is a division of tasks between internal national security threats and external (foreign) national security threats, which leads as well to different responsibilities, civilian (Ministry of Interior or Justice) and military (Ministry of Defence). In three States, the different structures are integrated so as to form a system of protection that directly reports to the Head of the Government (eg Prime Minister).

The processing of personal data is based on a law at Member State's level and the supervision is based either in the general data protection law (further referred to as 'GDPL') or one or more special laws regulating the processing of personal data by one or more intelligence services.

4.2. The role of the national data protection supervisory authority

It becomes clear from assessing the relevant national legislation that the GDPL in many countries does not apply to the activities of intelligence services and the data protection authority has a limited or in some cases non-existent supervisory role. Often, a specific data protection regime is provided for in law, but it does not necessarily include dedicated oversight from the data protection authority.

In the two other non-EU countries who kindly contributed to the questionnaire[13] processing of personal data by the intelligence services is regulated by the GDPL. They are subject to oversight by the national data protection authority based on provisions of the GDPL.

The GDPL, when applicable, generally provides for a number of exemptions (derogations to one or more principles) for the processing of personal data by intelligence services. These exemptions routinely refer to the basic duties of data controllers and the data subject rights.[14] The limitations may concern restriction to the right to be informed and the right of access by the data subject, which is in general to be exercised through the data protection authority.

[11] Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.
[12] Ireland.
[13] Serbia (one civil service, two military services), Switzerland (one civilian, one military)
[14] E.g. Belgium, Bulgaria, Cyprus, Germany, Hungary, Greece. For some Member States information on exemptions could not be established.

As to supervision of the data processing, in four Member States only it seems that the national general data protections laws (or law establishing general data protection supervisory bodies) provide for in principle the same supervisory powers over the intelligence services as over any other data controller. [15] In thirteen Member States the data protection authority supervision competence includes the national security and intelligence services within scope, but in some cases special rules or procedures apply to the supervision of intelligence or intelligence services, including the possibility to impose sanctions.[16] In nine Member States the data protection authority has no supervisory powers over the intelligence services acting as data controllers.[17]

Only in Sweden and Slovenia is full supervision by the data protection authority over compliance with the applicable data protection obligations in place. Where some other national data protection authorities have powers over the intelligence services, they check compliance with the applicable GDPL and deal with complaints and the exercise of the right of access by the individual concerned. They also have the power to investigate cases either on their own initiative or at the request of a third party and make in situ inspections. Some limitations to these powers may be in place in certain Member States, for example imposing compliance with special security rules when investigation cases to take account of State secrecy requirements.

4.3. The role of other independent oversight mechanisms

Twenty Member States declared that the law provides for parliamentary oversight and/or control over the activities of intelligence services alongside the competences of the data protection authorities for the data processing[18], and specific internal systems of scrutiny.[19] However, different understandings of parliamentary control seem to be in place in the Member States, few of which may be considered to entail having an actual body responsible for the oversight of data protection (including assessing a data subject's rights and compliance with the provisions of both GDPL and specific legislation).[20]

Existing oversight schemes are extremely diverse, comprising as follows:

- A parliamentary committee which may have the broad task of supervising intelligence and security authorities in general, or a particular intelligence services.

- The parliamentary oversight and / or control is in place alongside other (non-data protection authority) independent supervisory bodies. Existing formats of parliamentary control take the form of a parliamentary ombudsman, parliamentary delegation or a parliamentary commission.

[15] Bulgaria, Hungary, Slovenia, Sweden.
[16] Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Luxembourg, Poland, Sweden.
[17] Czech Republic, Denmark, Malta, Netherlands, Portugal, Romania, Slovakia, Spain, United Kingdom
[18] For example, in Finland the Parliamentary Ombudsman is responsible alongside the data protection authority; but his competencies are based on the dedicated law for the security and intelligence services.
[19] The twenty Member States referred to: Austria, Bulgaria, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Luxembourg, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, United Kingdom.
[20] The opinion does not analyse information on managerial (ministerial) and general political control provided by several contributing states.

- A parliamentary committee is the only supervisory authority outside the executive power structure. The tasks of the parliament here are formulated either in rather a general way, or so that access to open cases is not provided for.

- The oversight is vested in a special authority exclusively. However, the competence can be created by the data protection legislation but there is also a reported incidence of this authority being regulated by soft-law until recently.

- Specialised judicial control is in place alongside the general parliamentary oversight.

- A mixed executive and parliamentary control is in place alongside the general data protection authority, where the chair of the dedicated Commission is a judge and other members are from different political parties in Parliament past and present. Procedures exist for consultation with the data protection authority.

- Inspiration for improving elements of oversight can also be gained from those systems, where a special body was created specially dedicated to data protection oversight of the intelligence services: the Data Supervising Commission, composed of three public prosecutors, nominated by the General Public Prosecutor which supervises the intelligence services alongside with the parliamentary Supervising Council.

- While cases can be brought to the data protection authority to test whether national security is involved, once this involvement is established it must refer the case to two independent Commissioners with independent judicial oversight of national intelligence services and the role of the Secretary of State in granting warrants for conducting covert surveillance. Supporting these is a dedicated Tribunal for data subject redress.

- Dedicated law provides for the co-operation between the special oversight body and the general data protection authority: an independent Legal Protection Commissioner must give authorisation if the intelligence or intelligence services wish to conduct certain operations (e.g. undercover investigations, video surveillance of specific persons). The Legal Protection Commission is further obliged to lodge a complaint with the data protection authority if he is of the opinion that rights under the GDPL have been infringed.

The data protection authority has the power to supervise intelligence services with some limitations, but a special parliamentary body is responsible for oversight on the interception of communication and dealing with complaints. Members of the respective committee are appointed by the Parliamentary Control Committee. The chairperson must have the qualification to hold judicial office.

5. Recommendations

A. More transparency

1. More transparency is needed on how the programmes work and what the supervisors do and decide

The Working Party considers it important that Member States are transparent to the greatest extent possible about their involvement in intelligence data collection and sharing programmes, preferably in public, but if necessary at least with their national parliaments and the competent supervisory authorities. Data protection authorities are recommended to share their expertise at national level in order to restore the balance between national security interests and the fundamental right of respect for the private life of individuals.

Some form of general reporting on surveillance activities should be in place, also in line with the transparency obligation that lies on Member States following the ECtHR.[21] Every interference with fundamental rights has to be foreseeable and therefore these programmes have to be based in clear, specific and accessible legislation. The national data protection authorities are invited to bring this position to the attention of their respective governments.

2. More transparency by data controllers

Companies do need to be as transparent as possible and ensure that data subjects are aware that once their personal data are transferred to non-adequate third countries on the basis of the instruments available for such transfers, they might be subject to surveillance or access rights by third country public authorities, as far as such exceptions are provided for by these instruments. The Working Party is aware that controllers might be ordered to refrain from informing the data subject of the order it has received from a public authority. It welcomes recent efforts to provide the data subject with better and more information about the requests it receives and encourages the companies to continue to improve the information policies.

3. Maximising public awareness

Data subjects need to be aware of the consequences the use of online and offline electronic communication services may have as well as how they can better protect themselves. This is a shared responsibility of data protection authorities, other public authorities, companies as well as civil society. To this end, the Working Party intends to organise a conference in the second half of 2014 bringing together all stakeholders to discuss a possible approach.

[21] Also see European Court of Human Rights, Case no. 48135/06 – *Youth Initiative for Human Rights v Serbia* (25 June 2013), p.6

B. More meaningful oversight

1. Maintain a coherent legal system for the intelligence services, including rules on data protection

The Snowden revelations have made clear the intelligence services in the European Union Member States process large amounts of personal data on a daily basis. These data are also shared with other services in- and outside the EU. The Working Party considers it is important that the Member States have a coherent legal framework for the intelligence services including rules on data processing in compliance with the data protection principles as laid down in European and international law. The rights of the data subject need to be guaranteed to the maximal possible extent, while preserving the public interest at stake.

The Working Party furthermore recommends the national legal framework to contain clear rules on the cooperation and exchange of personal data with law enforcement authorities for preventing, combating and prosecuting crimes, including on the transfer of such data to authorities in other EU Member States and in third countries.

2. Ensure effective oversight on the intelligence services

In the national legal framework on the intelligence services, specific attention should be paid to the oversight mechanisms in place. Appropriate, independent and effective oversight is of the highest importance in a democratic society. The Working Party therefore considers the following good practices from the various oversight mechanisms currently in place in the Member States should be part of the oversight mechanisms in all Member States. The national data protection authorities are urged to bring these elements into the national debate on intelligence services oversight:

- Strong internal checks for compliance with the national legal framework in order to ensure accountability and transparency;

- Effective parliamentary scrutiny in line with national parliamentary traditions. National data protection authorities should encourage parliaments already having supervisory powers over the intelligence services to actively carry out these tasks;

- Effective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself, having power to access data and other relevant documentation on a regular basis and on its own initiative (ex officio), as well as an obligation to inspect following complaints. Prior approval of the intelligence services to be supervised must not be required;

C. Effective application of current law

1. Enforce the existing obligations of EU Member States and of Contracting Parties to the ECHR to protect the rights of respect for private life and data protection

All Member States are Parties to the European Convention of Human Rights. Thus, they have to comply with the conditions Article 7 and 8 ECHR set for their own surveillance

programmes. Their obligations do not end there. Article 1 ECHR also obliges the Parties to secure everyone within their jurisdiction the rights and freedoms provided in the Convention. In both scenarios, EU Member States, as well as any Party to the ECHR, can be brought before the ECtHR for a violation of European legal subjects' right to respect for private life.

2. Controllers subject to EU jurisdiction shall comply with applicable EU data protection legislation

Data controllers established in the EU or making use of equipment in a Member State must respect their obligations under EU law, even where the law of other countries where they operate contradicts EU law. In this regard, data protection authorities cannot ignore the fact that data transfers can occur in contravention of EU law. The Working Party therefore recalls that data protection authorities may suspend, according to the terms set by EU and national data protection provisions, data flows foreseen in the transfer instruments where there is a substantial likelihood that the data protection principles are being violated and that continuing transfers would create an imminent risk of grave harm to the data subject. National data protection authorities should decide according to their national competence if sanctions are in order in a specific situation.

D. Improve the protection on European level

1. Adoption of the data protection reform package

In order to offer strong data protection in Europe, the finalisation of the negotiations on the data protection reform package is of the utmost importance. Not only does the new General Data Protection Regulation and the Police and Justice Data Protection Directive aim for better data protection for individuals. Also, they are designed to clarify their scope of application and give more enforcement powers to data protection authorities. Especially the option to impose (financial) penalties – as a final resort – should ensure more leverage towards data controllers. The Working Party welcomes the proposal of the European Parliament to provide for mandatory information to individuals when access to data has been given to a public authority in the last twelve months. Being transparent about these practices will greatly enhance trust. The Working Party therefore urges the Council and the European Parliament to stick to their agreed timetable[22] and ensure both instruments can be adopted in the course of 2014.

2. Clarify the scope of the national security exemption

There is currently no common understanding of what is meant by national security. No clear definition has been adopted by the European legislator, nor is the case law of the European courts conclusive. However, the exemption must not be extended to the processing of personal data for purposes for which they cannot legally be used.

Another part of the question that needs to be answered is to what extent an exemption focused on national security continues to reflect reality, now it appears the work of the intelligence

[22] http://euobserver.com/justice/122853

services is more than ever before intertwined with the work of law enforcement authorities and pursues several different purposes. Data is shared on a continuous and global basis, leaving aside the question which nation's security is to benefit from the analysis of these data. The Working Party therefore calls upon the Council, the Commission and the Parliament to come to an agreement in order to define the principle of national security and be conclusive as to what should be regarded as the exclusive domain of the Member States. When defining the principle of national security, due account shall be given to the reflections of the Working Party, including the ones made in this Opinion. The EU institutions are also urged to clarify in the data protection reform package that the protection of the national security of third countries alone cannot exclude the applicability of EU law.

E. International protection for EU residents

1. Insist on adequate safeguards for intelligence data sharing

Third countries´ public authorities in general, and intelligence services in particular, must not have direct access to private sector data processed in the EU. If they require access to such data in a specific case based on a reasonable suspicion, where applicable they need to make a request under international agreements, providing adequate data protection safeguards. As far as the sharing of intelligence information is concerned, Member States have to ensure that the national laws provide for a specific legal basis for such transfers as well as adequate safeguards for the protection of personal data. In the view of the Working Party, secret cooperation agreements between Member States and/or third countries do not meet the standard of the ECtHR for a clear and accessible legal basis.

2. Negotiate international agreements to grant adequate data protection safeguards

The idea of a so-called Umbrella agreement, currently negotiated between the US and the EU, is a step into a right direction. However, such an agreement is likely to have two shortcomings: it will exempt cases concerning national security, at least from an EU perspective, since it is negotiated as an agreement based on EU law only. Its structure suggests that it would only apply to data transferred between public authorities in the US and the EU, not to data collected by private entities. This is also what becomes clear from the report of the EU-US High Level Contact Group (HLCG) on information sharing and privacy and personal data protection[23], which forms the basis for the negotiations on the Umbrella agreement. The Working Party stresses that under the Umbrella agreement, the purpose for the processing of the transferred data should be the same both in the EU and the US. It would not be acceptable if data originating from EU law enforcement could subsequently be used by US intelligence for national security purposes, if such is not also possible in the EU.

Since the Umbrella Agreement will fall short in offering full protection to all citizens, what is needed is an international agreement providing adequate protection against indiscriminate surveillance. Also the current conflict of jurisdictions affecting part of the disclosed surveillance activities, could be mitigated if such an agreement sets clear limits to

[23] Council Document 15851/09, 23 November 2009

surveillance. However, this agreement would be directly linked to the national security exemption and thus fall outside the scope of EU law. Therefore, it is up to the Member States to start negotiations in a coordinated manner. Due account should be given to the clear identification of which of the surveillance activities described would indeed be covered by national security, and which are rather more related to law enforcement and foreign policy purposes, areas which would fall under Union law. This would trigger the possibility for EU institutions to participate more closely in case steps are taken in this direction.

This new agreement must not be a secret one. It must be published and should include obligations on the contracting parties on the necessary oversight of surveillance programmes, on transparency, on equal treatment of at least citizens of all Parties to the Agreement, on redress mechanisms and other data protection rights. Also, the involved Parties should be encouraged to ensure their parliaments are informed about the use and value of the concluded agreement on a regular basis.

3. Develop a global instrument protecting privacy and personal data

The Working Party supports the development of a global instrument providing for enforceable, high level privacy and data protection principles as agreed upon by the International Conference of Data Protection and Privacy Commissioners in their Madrid Declaration.[24] In this regard, the adoption of an additional protocol to Article 17 of the UN International Covenant on Civil and Political Rights could be considered. In such an international instrument, it must be ensured that the safeguards offered are applicable to all individuals concerned. It is also necessary to come to a general interpretation of the meaning of 'data processing', because there are large differences in the understanding worldwide.

The Working Party supports the initiative taken by the German government and the call from the International Conference of Data Protection and Privacy Commissioners.[25,26] Furthermore, the Working Party continues to support the accession of third countries to the Council of Europe's Convention 108.

[24] International Standards on the Protection of Personal Data and Privacy, adopted by the 31st International Conference of Data Protection and Privacy Commissioners in Madrid.
[25] http://www.bundesregierung.de/Content/EN/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.
[26] Resolution on anchoring data protection and the protection of privacy in international law, adopted during the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw.