CONSEJO GENERAL DEL PODER JUDICIAL
ESCUELA JUDICIAL

ejtn

Red Europea de Formación Judicial (REFJ)
European Judicial Training Network (EJTN)
Réseau Européen de Formation Judiciaire (REFJ

MODULE III

UNIT 9

The principle of availability: criminal records and the Prüm Convention

5th Edition

2013

AUTHORS

Fernando Martínez Pérez
Senior judge, Criminal Court nº 7, Seville

María Poza Cisneros
Senior judge, Murcia Provincial Court

Con el apoyo financiero del Programa de Justicia Penal de la Unión Europea
With the financial support from the Criminal Justice Programme of The European Union
Avec le soutien financier du Programme de Justice Pénale de l'Union Européenne

LEVEL 1: SUBJECT

SUMMARY

1. The principle of availability

1.1. Definition

In the **Hague Programme**[1], of the10th of May 2005, the European Council "reaffirms the priority it attaches to the development of an area of freedom, security and justice, responding to a central concern of the peoples of the States brought together in the Union". Its specific orientations are developed in four chapters, relating to strengthening freedom, security and justice and developing external relations. The second of these chapters ("Strengthening security") refers to improving the exchange of information, the prevention and combating of terrorism, police cooperation, management of crises within the European Union with cross-border effects, operational cooperation, crime prevention and, briefly, organised crime, corruption and the strategy on drugs. In relation to improving the exchange of information, a definition of the principle of availability is introduced, for the first time, as an innovative instrument for the cross-border exchange of law-enforcement information, the implementation of which is given a set date, the 1st of January 2008, in categorical terms.

The **principle of availability** is defined in the Hague Programme as that which enables, throughout the Union, a law enforcement officer in one Member State who requires information in order to perform his duties to obtain this information from another Member State: the law enforcement agency in the other Member State holding this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State.

The principle of availability guarantees that the Police from one Member State, in carrying out their investigative function, may obtain information from the Police of another MS.

The Hague Programme itself anticipates certain **minimum conditions** to which the proposals that the Commission was invited to submit would have to be adjusted, in order to implement the principle:

- The exchange may only take place in order to enable legal tasks to be

[1] Communication from the Commission to the Council and the European Parliament, of the 10th of May 2005, "The Hague Programme: ten priorities for the next five years. The Partnership for

performed.

- The integrity of the data to be exchanged must be guaranteed.
- The sources of information need to be protected and the confidentiality of the data, at all stages of the exchange, secured.
- Subsequently, common standards for access to the data and common technical standards must be applied.
- Supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured.
- Individuals must be protected from abuse of data and have the right to seek correction of incorrect data.

It was stipulated, likewise, that the methods of exchange of information should make full use of **new technology** and must be adapted to each type of information, where appropriate, through reciprocal access to, or interoperability of national databases, or direct (on-line) access, including for Europol, to existing central EU databases such as the SIS. New centralised European databases should only be created on the basis of studies that have shown the value they add.

The nomination and reaffirmation of the principle of availability, in the Hague Programme, was preceded by a **growing concern** to improve exchanges of information between law enforcement authorities, expressed in various Commission Communications[2]fuelled, as was already the case with the mutual recognition principle on the occasion of 9/11, by the terrorist attacks in Madrid in March 2004. In fact, ever since the Tampere European Council, in 1999, the aim had been to strengthen police, customs and judicial cooperation, and to develop a coordinated policy with regard to asylum, immigration and external border controls.

Previously, the main instruments that had been intended to respond to this now revived concern about the weaknesses of the exchange of police information were[3]:

- The Convention implementing the Schengen Agreement of June 1990. Its Article 39 envisaged the exchange of information between the police authorities that requested it, but does not oblige the Member States to reply.

European renewal in the field of Freedom, Security and Justice" (COM(2005) 184 final – Official Journal C 236 of 24.9.2005).

[2] Communication from the Commission to the European Parliament and the Council for "Enhancing police and customs co-operation in the European Union", of the 18th of May 2004 (COM 2004/376 final, not published in the O.J.) and Communication from the Commission to the Council and the European Parliament "Towards enhancing access to information by law enforcement agencies", of the 16th of June 2004 (COM 2004/429 final, not published in the O.J.).

- The Europol Convention of 1995 and its protocols. Pursuant to Article 2 the objective of Europol is to improve the efficacy of the corresponding services within Member States and cooperation between them, with a view to preventing and combating terrorism, and other serious forms of international and organised crime.
- The initiative of the Kingdom of Sweden for a Draft Framework Decision on simplifying the exchange of information and intelligence, that sought to improve on the mechanism established by the Schengen Convention, further harmonise the legal framework for the exchange of data and reduce response times and which would be crystallised in FD 2006/960/JHA.

In parallel, the Treaty that would be signed in Prüm, on the 27th of May 2005, by seven member States, with the intention of incorporating its provisions into the legal framework of the European Union within a maximum period of three years, was being drawn up. This Treaty, which we refer to in more detail below, sought enhanced cooperation that offered a better response, among others, to the needs of exchange of police information, orientated in particular towards combating terrorism, cross-border crime and illegal migration.

1.2. Transposition of the principle

The Council and Commission Action Plan implementing the HagueProgramme[4] confirmed the presentation of the proposal that would enable the legislative transposition of the principle of availability, accompanied by another proposal, on the protection of personal data. The first initiative, represented by the **Proposal for a Council Framework Decision, of the 12th October 2005**[5], on the exchange of information under the principle of availability, did not, however, prosper.

Sweden's initiative fared better, the origin from which it takes the name by which it is known, which would become **FD 2006/960/JHA of the 18th of December 2006**[6], considered, by some authors, as a first approach to implementing the principle of availability, going beyond the primitive bilateral stage and, even, what we could call "institutional stage", in which the improvement of information was entrusted to European agencies or structures such as Europol. The Framework Decision referred to "simplifying the exchange of information and intelligence between law enforcement

[3] According to the MS of the failed Proposal for a Council Framework Decision of the 12th of October 2005 referred to in the previous section.
[4] Adopted by the Justice and Home Affairs Council of the 2nd and 3rd of June 2005.
[5] COM/2005/0490 final.

authorities of the Member States of the European Union". What would become a recurring objective in this area was expressly introduced, among other things, in its Explanatory Memorandum: strike the right balance between two pressing needs -

- The effective and expeditious exchange of information and intelligence between the law enforcement authorities of the Member States, indispensable for the fight against cross-border crime.
- The protection of personal data, fundamental freedoms, human rights and individual liberties.

The basic idea inspiring the FD is the free flow of information and intelligence between law enforcement authorities. Within the broad definitions that it incorporates, with the aim of ensuring that free circulation is not hampered by differences in national organisation:

- "Competent law enforcement authority" is the national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies or units dealing especially with national security issues are not covered by the concept, which will be clarified, through a declaration that may be modified at any time, by each Member State.
- “Criminal Investigation” is the procedural stage within which measures are taken by competent law enforcement or judicial authorities, including Public Prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts. The Decision is not limited, therefore, to the preliminary stages and its interest , consequently, goes beyond the area of police cooperation.
- "Criminal intelligence operation" is the procedural stage, not yethaving reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.
- "Information and/or intelligence" is any type of information or data which is held by:
    - The law enforcement authorities, already defined.
    - Public authorities or private entities availableto law enforcement

[6] Published in O.J. L 386, of the 29th of December 2006, with a rectification in O.J. L 75 of the 15th of March 2007.

authorities without having to use coercive measures.

With regards to the distinction between "information" and "intelligence", the authors take the view that criminal intelligence is the product resulting from the collection, processing, integration, analysis, evaluation and integration of the information available and its task is to establish the criminal patterns typical of organisations and companies engaged in perpetrating crimes: modus operandi, structures, members, resources and causes, among other relevant aspects.

With respect to its scope of application, the FD imposes on the Member States the obligation to:

- Ensure that the information and/or intelligence may be provided at the request of the competent law enforcement authority that conducts a criminal investigation or criminal intelligence operation, without subordinating it to stricter conditions than those applicable at national level.
- Request, when in accordance with national law judicial authorisation is necessary in order to access the information in question or to exchange it, such authorisation through the law enforcement authority of the addressed State, which will have to grant or refuse it by applying the same criteria as it would apply in a purely internal case.

In the request, the purpose for which the information or intelligence is requested must be explained, and the connection between the purpose and the person who is the subject of the information and intelligence, and short time limits are established, depending on the urgency, from 8 hours to 14 days, with the obligation to communicate the reasons for delay.

Nevertheless, certain nuances, limits and prohibitions are introduced:

- The obligation to collect and store information, with the aim of providing it to the law enforcement authority of another Member State, is not imposed on Member States. It is thus a matter of facilitating access to "existing" information, already available to the addressed State.
- The obligation to provide information and intelligence, to be used as evidence before the judicial authority, is not imposed on Member States, nor does it give any right to use such information or intelligence for this purpose, although it may be used for this purpose, with the consent of the Member State that has provided the information and/or intelligence, employing, where necessary, the instruments for judicial cooperation, except in the event that the State addressed had already provided its consent for the use of the information transmitted as evidence.

- The Member State receiving the request is not obliged to obtain any information or intelligence by means of coercive measures, defined according to its internal legislation.
- It is not possible to transmit information and/or intelligence to a Member State where this has been obtained from another Member State or from a third country, subject to the rule of speciality, save where the State that provided it authorises such transmission.
- It is prohibited to request more information than proves necessary to detect, prevent and investigate a crime.
- Strict rules are imposed on data protection and the confidentiality of the information and/or intelligence classified as confidential that is provided.
- Reasons are established to withhold information or intelligence.
    - Optional reasons
        - Where for factual reasons it is assumed that the provision:
            - Would harm essential national security interests of the addressedMember State, or
            - would jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals, or
            - would clearly be disproportionate or irrelevant in terms of thepurposes for which it has been requested.
        - Where the request pertains to an offence punishable by aterm of imprisonment of one year or less under the law of theaddressed Member State.
    - Imperative reasons: Where the competent judicial authority has not authorised access to and the exchange of the requested information.

The legislative transposition of the principle of availability can be found in:

- FD 2006/960/JHA (“Swedish initiative”).
- The Prüm Treaty
- Decision 2008/615/JHA

individuals held in civil registries, many of which are issues that had already been addressed by the Prüm Treaty. The Committee of Article 36 of the TEU (also known as CATS), as a Council working group, charged with the task of coordinating the working groups competent in the field of the third pillar, entrusted the implementation of this object of study to the Multidisciplinary Group on Organised Crime (MDG).

In parallel, as we have mentioned, the incorporation of the **Prüm Treaty** into the Community legal framework was prepared. The initiative for this purpose was dated the 15th of January 2007[7] and was finally crystallised in **Decisions 2008/615/JHA and J2008/616/JHA**, of the 23rd of June, representing the convergence of intentions to "Communitise" the Prüm Treaty, as announced by its signatories, and the demands for the legal articulation of the principle of availability incorporated into the Hague Programme, as recognised in the Explanatory Memorandum of the first of the aforementioned Decisions, "discovering" in the Treaty the contents that would enable the substantive requirements of the Programme to be fulfilled within the established deadlines. We will address these legislative instruments in independent sections below.

On the other hand, the five-year Hague programme having concluded in 2009, the Stockholm Programme (2009-2014), within a new political and legal context, coinciding with the entry into force of the Lisbon Treaty, announced new developments within the principle of availability that, in part, inspire the Community strategy in relation to information on criminal records, which is, however, already governed by the principle of mutual recognition, advancing, conceptually, in the final section, towards the subject of the next Module.

2. The Prüm Treaty

2.1. Origin, nature and scope of application.

On the 27th of May 2005 seven Member States of the EU (Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria) signed, in the German city of Prüm, the treaty bearing the same name "on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration", which sets out different measures for improving police cooperation and, by extension, judicial cooperation.

The **precedents** of this initiative are to be found in the Schengen Agreement of 1985 and the Implementing Convention of 1990, known as "Schengen I" and Schengen II", to such an extent that the Treaty in question is also known, evidently inappropriately, as Schengen III or Schengen Plus. Initially, it was only promoted by Germany, Belgium and Luxembourg, as a path to enhanced cooperation, which the other four States joined. It is open for **accession** by any member State and, subsequently, Bulgaria, Estonia, Finland, Hungary, Romania, Slovakia and Slovenia joined. Greece, Italy, Portugal and Sweden have communicated their desire to accede

[7] Published in the O.J. of the 28th of March 2007.

to the Convention to the European Council. Through specific agreements and in relation to the Decisions that have incorporated part of their projections into the legal framework of the European Union, Norway and Iceland participate in some of them. On the 5th of December 2006, the Technical Implementing Agreement to the Prüm Convention, envisaged in Article 44 of the Prüm Treaty, was signed.

From its inception, it has been clear that its transposition into the EU legal framework is inherent within the Treaty. Its legal nature, however, is that of a **traditional treaty** that lays down the basis for government cooperation outside the Community framework set up for police and judicial cooperation, within the context of the area of freedom, security and justice. It has been classified as an instrument of **"real-false reinforced cooperation"** (ZILLER):

- "False" reinforced cooperation, from a formal point of view, as the number of States that initially signed is less than the eight required, at that time, in the EU Treaty.
- "Real" reinforced cooperation, from a material point of view, as its content corresponds with one of the objectives of Article 29 of the EU Treaty, "preventing and combating crime, organised or otherwise, in particular terrorism".

In effect, the **objective** of the Prüm Treaty, which has a pioneering approach, is that of intensifying, in an area in which persons may move freely, cooperation between Member States in combating terrorism, cross-border crime and illegal migration, three objectives that are also to be found in the Hague Programme. In matters of terrorism, for example, the coincidence in developing possibilities of offering unsolicited information stands out, thereby confirming, on a general level, parallel development, at Community level and in the Treaty, of various issues, which generated considerable controversy.

Whilst reference to the principle of availability is not made explicitly, fulfilling this objective of maximum cooperation, especially in these three areas, is linked, from the first introductory paragraphs, to the instrument of a "better exchange of information". This objective is linked to the intention to incorporate the Treaty regime into the legal framework of the European Union, in order to achieve an overall improvement at this level, creating the necessary legal and technical foundations to attain this end. All of this "with respect for fundamental rights, as proclaimed in the Charter on Fundamental Rights of the European Union, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the common constitutional traditions of the

participating States", and anticipating the concern for the guarantee of an adequate level of the protection of personal data by the recipient party, parallel to the announcement of other agreements that enable the automated consultation of information in other databases.

Objective of the Prüm Treaty - more intense cooperation in the fight against:

- Terrorism.
- Cross-border crime.
- Illegal migration.

With respect to its **relation with Community Law and with other legislative instruments**, the Treaty provides for:

- The implementation of an initiative to transpose its provisions into the legal framework of the European Union within a maximum period of three years from its entry into force.
- Periodical reporting by the Contracting Parties, jointly, to the Council of the European Union and the European Commission, on progress in cooperation.
- The enforcement of its provisions, subject to compatibility with European Union law.
- Not affecting the rights and obligations contained in other existing bilateral or multilateral conventions, with the Contracting Parties retaining the power to apply them in their mutual relations, although with the preponderance, in the event of conflict, of the provisions of the Treaty.

The Treaty is structured into eight chapters:

I. General aspects.
II. DNA profiles, fingerprinting and other data.
III. Measures for the prevention of terrorist attacks.
IV. Measures to combat illegal migration.
V. Other forms of cooperation.
VI. General provisions.
VII. General provisions on data protection.
VIII. Provisions for implementation and final provisions.

2.2. Content

2.2.1. Automated access to national files.

The Treaty, in Chapter II, Articles 2 to 15, refers to three types of national files, allowing the authorities of the other States Parties immediate access to the information contained in the same, through reference data and via contact points. The three files contemplated refer to the following data:

2.2.1.1. DNA profiles.

- Establishment of national DNA analysis files.
    - The Parties commit themselves to the creation and maintenance of national DNA files for the investigation of criminal offences (not for prevention, as contemplated for other less-sensitive data).
    - Processing of data stored in those files, under this Treaty, shall be carried out in compliance with the national law applicable to each type of processing, notwithstanding the remaining provisions of the Treaty itself.
    - The Parties shall ensure the availability of reference data related to the information contained in such files. This data, however, shall only include DNA profiles established from the non-coding portion of DNA and a reference, without incorporating any data via which the individual in question could be directly identified. Nevertheless, the so-called "untraceables" or reference data not traceable to any individual must be recognisable as such.
    - Each Party shall specify the national DNA analysis files to which Articles 2 to 6 are applicable and the conditions for automated searching.

- Automated searching of DNA profiles
    - Parties shall allow access to the reference data in their DNA analysis files, through the national contact points. Authorised access allows for automated searching by comparing profiles, for individual cases and in compliance with the searching Contracting Party's national law.
    - Should an automated search show that a DNA profile supplied matches a DNA profile stored in the file held by the recipient party, the requesting contact point shall receive automated notification of the hit and the reference. If no match can be found, automated notification of this shall be afforded. The system responds, therefore, to the “hit/no hit” model.
- Automated comparison of DNA profiles, for the purpose of comparing the DNA profiles of their untraceables with all DNA profiles from other national DNA

analysis files' reference data. This is obviously aimed at reducing the number of untraceables. Thus, if a match has been found, it shall be communicated without delay to the other Party's national contact point. Transmission for this purpose will only take place where provided for under the requesting Party's national law.

- Collection of cellular material and supply of DNA profiles. Where there is no DNA profile available for a particular individual located within a requested Party's territory, the Party addressed shall provide legal assistance by collecting and examining cellular material from that individual and by supplying the DNA profile obtained, if the three following requisites concur:
    - With respect to the requesting Party:
        - Communication of the purpose for which the profile is required.
        - Presentation of an investigation warrant or statement issued by thecompetent authority, showing that the requirements for collecting and examining cellular material would be fulfilled if the individual concerned were present within the requesting Contracting Party's territory.
    - With respect to the addressed Party's law, fulfilment of the requirements for these actions in accordance with their national legislation.

2.2.1.2. Fingerprinting data.

- The Parties shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offences. Unlike the previous case, it is assumed that all the States already possess such files.
- This data, however, shall only include fingerprinting data and a reference, without including any data via which the individual in question can be directly identified. Nevertheless, the so-called "untraceables" or reference data not traceable to any individual must be recognisable as such.
- Automated searching of fingerprinting data, with a system similar to that envisaged for the DNA profiles, also through national contact points. Firm matching of fingerprinting data with reference data held by the Contracting Party in charge of the file shall be carried out by the requesting national contact point on the basis of the automated communication of the reference data required for a clear match.
- If in the course of the automated search, a match between fingerprinting data is

verified, the supply of any other available personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the addressed Contracting Party.

2.2.1.3. **Vehicle registration data.**

In compliance with the national law of the Contracting Party that carries out a search, for broader purposes than the prevention and investigation of criminal offences and what is called, apparently in alternative terms "investigation of offences coming within the jurisdiction of the courts or the public prosecution service in the searching State", and prevention of threats to security and public order, through national contact points, automated searches may be conducted within the national vehicle registration data, in many States the responsibility of non-police authorities, in specific cases and always in relation to a complete vehicle identification number or a full registration number:

- Data relating to owners or operators.
- Data relating to vehicles.
- and with respect to a complete vehicle identification number or a full registration number, searches may be conducted of data relating to owners or operators and data relating to vehicles.

2.2.1.4. **Other information**

In addition to the three preceding specific categories, supply of data is envisaged, also through national contact points, for the purpose of **preventing** criminal offences and maintaining public order and security for **major events with a cross-border dimension, in particular for sporting events[8] or European Councilmeetings**:

- Transmission of non-personal data, upon request or on the initiative of the supplying party.
- Transmission of personal data, for the same purposes, if any final convictions or other circumstances give reason to believe that the individuals in question will commit criminal offences at the event or pose a threat to public order and security, insofar as the transmission of such data is permitted under the supplying Contracting Party's national law, also upon request or on its own initiative. This data may be processed only for the established purposes and for

[8] In this regard, refer to, for example, Decision 2002/348/JHA and the Council Resolutions of the 6th of December 2001 and the 17th of November 2003.

the specific event for which they were supplied and are to be deleted without delay once the purposes that justified the transmission have been achieved or are no longer achievable or, in any event, within a maximum period of one year.

2.2.2. Measures for the prevention of terrorist attacks.

2.2.2.1. **Transmission of information:**

Through national contact points, with a view to the prevention of terrorist attacks, in specific cases, in compliance with national law and with the possibility of imposing conditions on the receiving authority concerning the use of the data and without the need for a prior request, personal data and certain information (names, surnames, date and place of birth, and a description of the facts that justify the investigation) may be transmitted, insofar as such data proves necessary where certain events justify the assumption that the individuals in question will commit criminal offences, in accordance with the stipulations of the specific Community legislation on combating terrorism[9].

2.2.2.2. **Deployment of security escorts in flights.**

Their deployment, in accordance with specific international legislation[10], on flights of aircraft registered therein, is to be decided by each Contracting Party. The security escorts in flights referred to in the Treaty shall be police officers or other suitably trained officials responsible for maintaining security on board aircraft. Before a Contracting Party deploys security escorts, its relevant national contact point must give notice in writing of their deployment, at least three days before the flight in question and containing the minimum information specified in the annex to the Treaty. In the event of imminent danger, such notice must be given without any further delay, before the aircraft lands.

The Contracting Parties shall, upon request, grant security escorts in flights deployed by other Contracting Parties general permission to carry arms, ammunition and other equipment on flights to or from airports in Contracting Parties. Such permission shall cover the carrying of arms and ammunition on board aircraft and, subject to paragraph 2, in restricted-access security areas at an airport in the Contracting Party in question. The carrying of arms and ammunition shall be subject to the following conditions:

---

[9] Articles 1 to 3 of Framework Decision 2002/475/JI of the Council of the European Union, of the 13th of June 2002, on combating terrorism.

[10] International Chicago Convention of the 7th of December 1944, on international civil aviation, and its annexes, in particular Annex no. 17, and the documents implementing it, and, with

1. Those carrying arms and ammunition may not disembark with them from aircraft at airports or enter restricted-access security areas at an airport in another Contracting Party, unless escorted by a representative of its competent national authority.
2. The arms and ammunition carried must, immediately upon disembarking from the aircraft, under escort, be deposited for supervised safekeeping in a place designated by the competent national authority.

2.2.3. Measures to combat illegal migration.

The Treaty, to this end, envisages two techniques for police cooperation:

2.2.3.1. **Sending documentation advisors**

These advisors shall be sent to States regarded as source or transit countries for illegal migration. Amongst their functions, attention should be drawn to the following:

- Advising and training Contracting Parties' representatives abroad on passport and visa matters, particularly detection of false or manipulated documents.
- Advising and training carriers on their obligations under the specific legislation[11], and on the detection of false or manipulated documents and to have knowledge of existing provisions on immigration.
- Advising and training the host country's border control authorities and institutions.

2.2.3.2. **Support in cases of repatriation.**

Support is envisaged, under Community legislation[12], for organising joint flights for removals, from the territory of two or more Member States, of third-country nationals whose expulsion has been ordered, and in cases of transit for the purposes of repatriation by air. A Contracting Party may, where necessary, repatriate an individual via another Contracting Party's territory. The Contracting Party that's territory is to be traversed for the repatriation will decide and act in accordance with its national law.

2.2.4. Other forms of cooperation

2.2.4.1. Joint patrols and other forms of joint intervention.

In order to anticipate threats to security and public order and for the prevention of criminal offences, the competent authorities of theContracting Parties may organise

---

respect to the aircraft commander's powers, the Tokyo Convention of the 14th of September 1963, on offences and certain other acts committed on board aircraft.

[11] Convention implementing the Schengen Agreement of the 14th of June 1985 on the gradual abolition of checks at common borders, and Annex 9 of the Chicago Convention of the 7th of December 1944, on international civil aviation

[12] Decision of the Council of the European Union 2004/573/EC of the 29th of April 2004 and Directive 2003/110/EC of the Council of the European Union, of the 25th of November 2003.

joint patrols and other joint operations in which designated officers or other officials (hereinafter referred to as "officers") participate in operations within a Contracting Party's territory, without limiting themselves exclusively to the border area. Each Contracting Party may, as a host State, in compliance with its own national law, with the consent of the State of origin, confer sovereign powers on other Contracting Parties' officers involved in joint operations or, insofar as the host State's law permits, allow other Contracting Parties' officers to exercise their sovereign powers in accordance with thelaws of the State of origin. In any event, such sovereign powers may be exercised only under the guidance and, as a rule, in the presence of officers from the host State.

In Chapter VI, general provisions are established on the carrying of arms, ammunition and equipment allowed by the officers from a Contracting Party who are in the territory of another Contracting Party within the context of a joint operation. The arms, ammunition and equipment may be used only in legitimate defence, except where there is express authorisation allowing use other than in legitimate defence.

2.2.4.2. **Border crossing.**

In urgent situations, which are defined by the Treaty, officers from one Contracting Party may, without another Contracting Party's prior consent, cross the border between the two so that, within an area of the other Contracting Party's territory close to the border, in compliance with the host State's national law, they can take any provisional measures necessary to avert imminent danger to the life or physical integrity of individuals, notifying the host State without delay. The host State shall also without delay take the necessary measures to avert the danger and take charge of the operation. The officers crossing the border may operate in the host State only until the host State has taken the necessary measures to avert the danger, and shall be required to follow the host State's instructions.

Consequently, progress is made with respect to the "hot pursuit" envisaged in Schengen[13], limited to the pursuit of criminals in the territory of the other State in cases of *flagrante delicto* and only where immediate communication with the host State was not possible.

2.2.4.3. Assistance in connection with major events, disasters and serious accidents.

The Contracting Parties' competent authorities shall provide one another with mutual assistance, in compliance with national law, in connection with mass gatherings

[13] Art. 41 of the Implementing Convention of the 19th of June 1990 of the Schengen Agreement of the 14th of June 1985.

and similar major events,disasters and serious accidents, by notifying one another as promptly as possible, and providing coordination and assistance, at the request of the Contracting Party within whose territory the situation has arisen, by means of dispatching officers, specialists and advisors and supplying equipment.

2.2.4.4. Cooperation upon request.

In search of a closing clause, the Treaty envisaged that the Contracting Parties' competent authorities shall provide one another with assistance, upon request, within the scope of their powers and in compliance with their own national law. Furthermore, in order to strengthen border cooperation techniques that were being implemented through the creation of police and customs cooperation centres on the actual borders, measures are envisaged, in no particular order, consisting in:

- Identifying owners and operators of vehicles and providing information on drivers, masters and captains of vehicles, vessels and aircraft, in so far as not already provided for in the provisions on automated searching of registration data.
- Supplying information on driving licences, navigation licences and similar permits.
- Ascertaining individuals' whereabouts and place of residence.
- Checking on residence permits.
- Ascertaining the identity of telephone subscribers and subscribers to other telecommunications services, where publicly accessible.
- Establishing the identity of individuals.
- Investigating the origin of items such as arms, motor vehicles and vessels (enquiries via trade channels).
- Supplying data from police databases and police records and supplying information from official records accessible to the public.
- Issuing urgent alerts concerning arms and explosives and alerts concerning currency counterfeiting and securities fraud.
- Supplying information on practical implementation of cross-border surveillance, cross-border hot pursuit and controlled deliveries.
- Ascertaining an individual's willingness to make a statement.

2.2.5. Provisions on the protection of personal data.

Although the sincerity of the concerns and, above all, the effectiveness of the proposed guarantee, are questionable and have been discussed, ever since its first "recitals" the Prüm Treaty has put forward, in an apparently obvious way that we have already referred to, that the Parties consider themselves "with respect for fundamental

rights" and that they are "conscious in particular that the transmission of personal data to another Contracting Party requires that the receiving Contracting Party must guarantee an adequate level of data protection. Notwithstanding the announcement of other agreements on the subject, the Treaty incorporates into Chapter VII (Articles 33 to 41) provisions related to data protection, which will be applied to the data that are transmitted or have been transmitted in accordance with the Treaty.

The continuous references in the Treaty to national law (Arts. 2.1, 4.1, 5, 6.1, 10, 14, etc.) has raised problems of interpretation, as specific conventional protective rules will coexist, on two levels, incorporated into the treaty itself and into national law, in which both state and Community laws will be integrated, which, at that time, were in the development stage[14].

2.2.5.1. Definitions

For the purposes of the Treaty, certain authentic definitions are offered:

- **Processing of personal data**: Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment,combination, blocking, erasure or destruction of data. Processing within the meaning of this Convention shall also include communicating whether or not a hit exists;
- **Automated searching**: Direct access to the automated files of another body where the response to the search procedure is fully automated.
- **Marking:** The marking of stored personal data without the aim of limitingtheir processing in future;
- **Blocking** shall mean the marking of stored personal data with the aim of limiting their processing in future.

2.2.5.2. Level of data protection.

Each Contracting Party shall guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention of the 28th of January 1981 for the protection of Individuals with regard to automatic processing of personal data and the Additional Protocol of the 8th of November 2001 and in doing so, shall take account of Recommendation No R (87) 15 of the Committee

[14] Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters and on the exchange of information under the principle of availability COM (2005) 475 and COM (2005) 490. The latter, as we mentioned in another section, failed.

of Ministers of the Council of Europe to the Member States regulating the use of personal data in the police sector, of the 17th of September 1987, even where data are not processed automatically.

2.2.5.3. **Principle of a link to the purpose and other limits to data use and processing.**

- Use of data: Processing of the personal data by the receiving Party shall be permitted solely for the purposes for which they have been supplied in accordance with this Treaty; processing for other purposes shall be permitted solely with the prior authorisation of the Party administering the file and subject only to the national law of the receiving Party. Such authorisation may be granted provided that processing for such other purposes is permitted under the national law of the Contracting Party administering the file.
- Data processing: The processing of data transmitted in automated searching for DNA profiles and fingerprints and automated comparison of profiles and data by the Contracting Party performing the search or the comparison is also restricted to certain purposes, basically, those that it was transmitted for (verifying matches, preparation of administrative or judicial assistance or registration envisaged in the Treaty).
- The use of vehicle data are also subject to restrictions, which are limited, moreover, to the procedure that gave rise to the search.
- Personal data transmitted may only be processed by the authorities and courts with responsibility for a task in furtherance of the aims set out in the Treaty. The Treaty specifies that data may be supplied to other entities only with the prior authorisation of the supplying Party and in compliance with the national law of the receiving Party.

2.2.5.4. **Guarantees of accuracy, current relevance and storage time of data.**

- **Accuracy and current relevance:** The Contracting Parties must ensure the accuracy and current relevance of personal data. If it is verified, even ex officio, that incorrect data or data which should not have been supplied have been supplied, this must be notified without delay to the receiving Party or Parties, which must correct or delete the data. Data, the accuracy of which the data subject contests and the accuracy or inaccuracy of which cannot be established must be marked at the request of the individual in question, in accordance with

the national law of the Contracting Parties. The mark may only be removed, subject to national law, with the permission of the data subject or based on a decision of the competent court or the independent dataprotection authority.

- **Storage time of data**: Notwithstanding the immediate cancellation of data that should not have been transmitted or received, data that has been sent and received lawfully are also subject to storage time limits, when they are no longer necessary for the purpose for which they were supplied or following the expiry of the maximum period for keeping data laid down in the national law of the supplying Contracting Party, where the supplying body informed the receiving body of those maximum periods at the time of supplying the data.
- **Blocking**: It is an alternative to the deletion of data, ordered in compliance with national law, where there is reason to believe that deletion would prejudice the interests of the individual in question. Blocked data may be supplied or used solely for the purpose for which the data was not deleted.

2.2.5.5. **Technical and organisational measures to ensure data protection and data security**.

The obligation to ensure that personal data is effectively protected against accidental or unauthorised destruction, accidental loss,unauthorised access, unauthorised or accidental alteration and unauthorised disclosure is imposed, with reference to an implementation agreement to specify details but with set minimum standards.

2.2.5.6. Documentation and registration

The Parties take on obligations of comprehensive documentation and recording of searches and transmissions, protection against improper use and the legal control of transmission and reception is regulated, which is the responsibility of the competent independent body for the supervision of data protection in each party.

2.2.5.7. Rights of the individuals concerned

The rights of the individuals concerned to information, rectification, cancellation and compensation, where appropriate, for damages are regulated.

THE BALANCE OF PRÜM	
SECURITY	FREEDOM
Automated access to national files (DNA, fingerprints, vehicles).	Protection of personal data
Measures for the prevention of terrorist attacks (information, security escorts in flights).	
Measures for the prevention of disturbances at major cross-border events (sport, European Council meetings).	
Measures against illegal migration.	
Other measures (joint patrols, border crossing, advisors and border centres).	

3. The partial incorporation of the Treaty of Prüm into the legal framework of the European Union

3.1. Decision 2008/615/JHA

As we know, the Prüm Treaty, in spite of its "bastard" origins for orthodox Europeanism, was created with a "Community spirit". In its very first Article, it announces:

"Within three years at most following entry into force of this Convention, on the basis of an assessment of experience of its implementation, an initiative shall be submitted, in consultation with or on a proposal from the European Commission, in compliance with the provisions of the Treaty on European Union and the Treaty establishing the European Community, with the aim of incorporating the provisions of this Convention into the legalframework of the European Union".

In a "fortunate coincidence", with an almost simultaneous expiry date, the Hague Programme gave the 1st of January 2008 as the date from which the cross-border exchange of police information should be governed by the principle of availability.

It is not surprising that, in view of the coincidence of objectives that we have also referred to and taking advantage of the German Presidency, one of the four promoters of Prüm, in the informal meeting in Dresden, on the 15th and 16th of January 2007, presented an **initiative[15] to transpose the Prüm Treaty into the legal framework of the European Union**. This initiative was to bear fruit, not without misgivings[16], in spite of the initial support, in the Justice and Home Affairs Council's Agreement of the 15th of February 2007, in which it was stipulated that some parts of the Prüm Treaty were to be incorporated into the legal framework of the European Union, by means of a decision based on the Third Pillar, which would be Decision 2008/615/JHA, of the 23rd of June.

In its initial recitals, after a recapitulation in which, as well as the Prüm Treaty, mention was also made of the conclusions of the Tampere European Council, the Hague Programme and the aforementioned Council Framework Decision 2006/960/JHA, of the 18th of December 2006, it was concluded that the Prüm Treaty was the response to fulfil the Hague Programme on time. Likewise, the starting point was the conviction that, in particular, the improvement in the exchange of information is an objective that cannot be achieved satisfactorily by Member States alone, and thus the Decision was adopted in accordance with the principles of subsidiarity and proportionality.

In parallel, a declaration of respect for fundamental rights was incorporated, in particular the right to privacy and the right to protection of personal data, "to be guaranteed by special data protection arrangements, which should be tailored to the specific nature of different forms of data exchange. Such data protection provisions should take particular account of the specific nature of cross-border online access to databases. Since, with online access, it is not possible for the Member State administering the file to make any prior checks, a system ensuring post hoc monitoring should be in place". When it came to including provisions on data protection, the absence of a Framework Decision on data protection in the Third Pillar, that is, in the

[15] O.J. 28th of March 2007.

[16] See the working document of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament of the 10th of April 2007, Rapporteur: Fausto Correia.

area of police and judicial co-operation in criminal matters, was taken into account, specifying an identical minimum standard as that set by the Prüm Treaty[17].

The **objective** of the Decision, according to its Article 1, is to step up cross-border cooperation in the area of police and judicial cooperation in criminal matters (Title VI TEU), particularly the exchange of information between authorities responsible for the prevention and investigation of criminal offences. Its rules refer to **questions** already addressed by the Prüm Treaty.

- Conditions and procedure for the automated transfer of DNA profiles, fingerprinting data and certain national vehicle registration data.
- Conditions for the supply of data in connection with major events with a cross-border dimension, with new express mention of sport and European Council meetings.
- Conditions for the supply of information in order to prevent terrorist attacks.
- Conditions and procedure for stepping up cross-border police cooperation through various measures:
    - Patrols and other joint operations.
    - Assistance in connection with mass gatherings, disasters and serious accidents.
- Data protection.

The headings, like their legislative development, are very similar to those that we have examined in the section dedicated to the Prüm Treaty. The most significant differences affect the exclusion of the express regulation of "border crossing", the "deployment of security escorts in flights" and everything related to illegal migration.

With respect to the **legislative articulation** of the Treaty and the Decision for the Contracting Parties of the Treaty, in accordance with Article 35 of the Decision, the relevant provisions of the Decision shall be applied instead of the corresponding provisions contained in the Prüm Treaty. All the other provisions of the Prüm Treaty shall remain applicable between the Contracting Parties of the Treaty. In relation to other legal instruments, it is worth highlighting the declaration according to which the

[17] We recall that this standard was incorporated by the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, of the 28th of January 1981, and its additional Protocol of the 8th of November 2001, taking into account Recommendation No R (87) 15 of the 17th of September 1987 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, also where data are not processed automatically.

Decision does not affect existing agreements on legal aid or mutual recognition of court decisions.

3.2. Decision 2008/616/JHA

According to what was anticipated in the Prüm Treaty itself and given the high technical and legal complexity of many of the issues addressed therein, the Treaty was followed by an Agreement concerning administrative and technical implementation of the 5th of December 2006. In parallel and for the same reason, in compliance with the stipulations of Article 33 of Decision 2008/616/JHA, the Council, by a qualified majority and after consulting the Parliament, adopted the measures necessary for its implementation, in Decision 2008/616/JHA, of the same date of the 23rd of June 2008, accompanied by a substantial technical annex and with particular reference, as corresponds to its nature, to the automated exchange of DNA profiles, fingerprinting data and vehicle registration data.

4. The principle of availability in the Stockholm Programme

The progression of the European integration process in matters of justice and home affairs has, as key milestones, the creation of the Third Pillar in the Maastricht Treaty, in 1992, the restructuring carried out by the Amsterdam Treaty, in 1997, on incorporating into its objectives the development of an Area of Freedom, Security and Justice and the Extraordinary Tampere Council, in 1999, in which the operational bases for the realisation of this area are laid down[18] and it is affirmed that the principle of mutual recognition should become the cornerstone of judicial cooperation in both civil and criminal matters within the Union. The first multiannual programme known as the Tampere Programme originated from this Extraordinary Council. If, in conditions of "political consensus and momentum", the impact of the 9/11 attacks on its development was undeniable, the following Hague Programme was also drawn up, as we mentioned, at a special time, under the impact of the Madrid attacks of March 2004, which had prompted the Brussels Declaration of the 25th of March 2004 on Combating Terrorism. Upon the expiry of this second Programme, in 2009, the situation that had to be faced by what would be the Stockholm Programme was different.

[18] RODRÍGUEZ, J.M y SORROZA BLANCO, A., "El Espacio de Libertad, Seguridad y Justicia y la próxima Presidencia española de 2010. Parte 1ª: la implementación del Tratado de Lisboa y el Programa de Estocolmo". ARI nº 173/2009, Real Instituto Lecanto.

From a legal perspective, after the failure of the European constitutional project, doubts about the entry into force of the Lisbon Treaty on the 1st of December 2009 were allayed and, consequently, new opportunities opened up to continue making progress in matters of Justice and Home Affairs, with novelties such as the disappearance of the Pillars and the consequent overhaul of the legislative system, increasing the number of issues excluded from the requirement of unanimity, the recognition of the legal personality of the European Union or the strengthening of the Commission, with the power to initiate proceedings against Member States for non-compliance with Community law.

From a sociological and political perspective, the threat of international terrorism is perceived as more distant and simultaneously reduces the disposition to suffer a reduction in freedoms and make budgetary efforts, in pursuit of an objective that had set the European agenda in such matters during the last decade.

From a technological perspective, the possibilities of invasion of privacy and of unauthorised processing of personal data had grown exponentially in a decade marked by, among other things, the creation and expansion of social networks and the emergence of online business transactions.

Reading the Stockholm Programme[19] reveals, even from its title ("An open and secure Europe serving and protecting citizens"), that we have before us we are facing a new paradigm. By its adoption, the European Council considers that the priority for the coming years will be to focus on the interests and needs of citizens. The challenge will be to ensure respect for fundamental rights and freedoms and the integrity of individuals while guaranteeing security in Europe. In this sense, "It is of paramount importance that law enforcement measures, on the one hand, and measures to safeguard individual rights, the rule of law and international protection rules, on the other, go hand in hand in the same direction and are mutually reinforced".

With respect to the subject we are concerned with here, it is worth pointing out, as the order is significant, that the Stockholm Programme puts "promoting citizenship and fundamental rights" at the top of its priorities, making express reference to the protection of personal data. The reference to security ("A Europe that protects") has been relegated to fifth place in the list of priorities.

As regards the instruments identified to implement the priorities, on addressing the legislation the exercise in self-criticism is evident by appealing to the complete and

[19] Official Journal C 115 of 04/05/2010 p. 0001 – 0038

effective application, implementation and evaluation of existing instruments and by pointing out that the European Council " considers that the development of legislation in the area of freedom, security and justice is impressive, but it has shortcomings in terms of overlapping and a certain lack of coherence". The time has come to reorganise and, despite maintaining enhanced cooperation, to avoid, as far as possible, confusing legislative situations such as that generated by the parallel development of the Prüm Treaty and the Hague Programme.

And in the chapter dedicated to security, by requiring the Council and the Commission to design an internal security strategy, ideas are introduced, very present in Prüm, of encouraging the "reflection of a proactive and intelligence-led approach", of "the need for a horizontal and cross-cutting approach in order to be able to deal with complex crises or natural or man-made disasters". of "stringent cooperation between the Union agencies, including further improving their information exchange" or of an "integrated border management".

In another section of the same chapter, on upgrading the tools for the job, the Programme refers to managing the flow of information, expressly incorporating a mention of the principle of availability, which, it is affirmed "will continue to give important impetus to this work". Specifying this statement, the Programme insists on the recurring ideas of coherence and consolidation, also in developing information management and exchange, inviting the Council and the Commission to implement the Information Management Strategy for EU internal security, which includes a strong data protection regime and, in particular, inviting the Commission to assess the need for developing a European Information Exchange Model based on the evaluation of the current instruments, including the aforementioned Council Decisions 2008/615/JHA and 2008/616/JHA and Council Framework Decision 2006/960/JHA, to determine whether these instruments function as originally intended and meet the goals of the Information Management Strategy. This Strategy is based on:

- business-driven development (a development of information exchange and its tools that is driven by law enforcement needs),
- a strong data protection regime consistent with the strategy for protection of personal data referred to in Chapter 2,
- a well targeted data collection, both to protect fundamental rights of citizens and to avoid an information overflow for the competent authorities,
- guiding principles for a policy on the exchange of information with third

countries for law enforcement purposes,

- interoperability of IT systems ensuring full conformity with data protection and data security principles when developing such systems,
- a rationalisation of the different tools, including the adoption of a business plan for large IT systems,
- overall coordination, convergence and coherence.

Moreover, the European Council calls for the establishment of an administration, having the competence and capacity to develop technically and manage large-scale IT systems in the area of freedom, security and justice and puts forward initiatives with a view to setting up a Union Passenger Names Record (PNR) system.

The Stockholm Programme also emphasises the principle of availability, but stresses the compatibility needed with the protection of fundamental rights.
Recognition of the effects of foreign convictions = principle of mutual recognition

Another of the objectives set refers precisely to mobilising the necessary technological tools, adding immediately "while ensuring consistency with the strategy for protection of personal data", inviting, in particular, an improvement in the exchange of information with respect to criminal records, in terms that we will examine at the end of this subject. Within the same objective, the Commission is invited to:

- Make a feasibility study on the need for, and the added value of, setting up a European Police Records Index system (EPRIS) and to make a report to the Council in the course of 2012 on the issue.
- To reflect on how to further develop the use of existing databases for law enforcement purposes, while fully respecting data protection rules, so as to make full use of new technologies with a view to protecting citizens.
- Examine how best to promote the exchange of information between Member States' competent authorities on travelling violent offenders including those attending sporting events or large public gatherings.

On addressing the objective of developing effective policies in matters of security, emphasis is placed on the need for more effective European law enforcement cooperation. The change of orientation and priorities is evident when it is pointed out that focus should not only be placed on combating terrorism and organised crime, but also on the spread of cross-border crime that has a significant impact on the daily life of the citizens of the Union. The value of Europol is retrieved as a hub for information exchange between the law enforcement authorities of the Member States, a service

provider and a platform for law enforcement services. To this end, the Commission and, where appropriate, the Council and the High Representative of the Union for Foreign Affairs and Security Policy, are invited to:

- Examine how it could be ensured that Europol receives information from Member States law enforcement authorities.
- Examine how operational police cooperation could be stepped up, for example as regards incompatibility of communication systems and other equipment.
- Make a proposal to the Council and the European Parliament to adopt a decision on the modalities of cooperation, including on exchange of information between Union agencies, in particular Europol, Eurojust and Frontex, which ensures data protection and security,
- Develop ad hoc law enforcement cooperation at sporting events or large public gatherings.

Later, in relation to protection against serious and organised crime, it is emphasised that this objective would require systematic exchange of information. Worthy of note is the express mention, in the sub-section of economic crime and corruption, of further development of information exchange between the Financial Intelligence Units (FIUs), in the fight against money laundering, with the possibility that their analyses, within the framework of the European Information Management System, could feed a database on suspicious transactions, for example, within Europol, and of the mobilisation and coordination of sources of information to identify suspicious cash transactions.

In the light of the Stockholm Programme, an **Action Plan**, dated the 25th of November 2009[20] was established, stressing the **critical aspects of the principle of availability, which is mentioned repeatedly**. In implementing its envisaged creation of a comprehensive data protection scheme in the European Union, the 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[21] and 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)[22] were drawn up on the same date, the 25th of January 2012. These replaced Framework Decision

[20] Brussels, 20.4.2010 COM (2010) 171 final.
[21] Brussels, 25.1.2012. COM (2012) 10 final.

2008/977/JHA and Directive 95/46/EC. Likewise, on the subject we are concerned with, the Proposal for a Council Regulation on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (recast)[23] is being processed.

5. Criminal records

5.1. Introduction

The establishment of an area of freedom, security and justice requires, among other things:

- The efficient circulation of information between the relevant authorities of the Member States **on convictions** or disqualifications of Community and non-Community nationals residing in the territory of the Member States.
- The possibility of **consequences being attached tosuch convictions or disqualifications outside the territory** of the sentencing Member State[24].

The first of these objectives, concerning the mere exchange of information, evokes the postulates of the **principle of availability** that constitutes the main theme of this subject. In contrast, the second, more ambitious, objective already belongs more to the field of the **principle of mutual recognition** that we will address in the next Module.

Free circulation of information on convictions ≈ principle of availability Recognition of the effects of foreign convictions = principle of mutual recognition

This is not, as is well known, a recent concern. There have been numerous bilateral **conventions** that envisage mechanisms for the transmission of information on criminal records. Among the multilateral conventions, the European Convention on Mutual Assistance in Criminal Matters of the 20th of April 1959 (Arts. 13 and 22) envisaged expressly that each MS should communicate the conviction to the MS of which the convicted person is a national, annually, maintaining the communication via a central authority for this purpose (opposed to what is the general rule of direct communication), in Art. 6.8 of the 2000 Convention. Furthermore, this form of cooperation is usually understood to consist of the commitment to provide the broadest possible assistance that is common in conventional texts. On the other hand, some

[22] Brussels, 25.1.2012. COM (2012) 11 final.
[23] Brussels, 30.4.2012. COM(2012) 81 final

[24] The white paper on exchanges of information on convictions and the effect of such convictions in the European Union refers expressly to these two objectives. COM/2005/0010 final, of the 25th of January 2005.

international conventions, figuring prominently the Convention on the International Validity of Criminal Judgements, signed at the Hague on the 28th of May 1970, were already concerned with the more ambitious dimension of recognition of the effects of foreign convictions.

In **national Law** the effects of convictions handed down abroad are recognised, even, occasionally, in connection with certain forms of crime and this objective was to be found explicitly in the development of the conclusions of the Tampere Council in 2000.

And, nevertheless, even with these precedents, the objectives of free circulation and mutual recognition of convictions in the common judicial area faced serious **obstacles**.

With respect to the circulation of information, the first difficulty was determined by the profound differences between the different national systems of criminal records, regarding:

- The authority on which they depend.
- Content, as some only record the final judgments, while others also refer to legal persons.
- Access.
- Cancellation rules, in some cases automatic, in others at the request of one of the parties or, even, without the possibility of cancellation, etc.

As regards the exchange of information on convicting sentences, which was basically adapted to the mechanisms of the 1959 Convention, the defects detected concerned the breach of the obligation to send the information to the MS of nationality of the convicted individual, the absence of identification of the nationality of the convicted individual, the lack of resources at national level, the loss or modification of the information, the "filtering" of information by the MS of nationality of the convicted individual, the absence of requests for information, the submission of the few requests that were actually sent, the slow mechanism of the international request, without deadlines and with difficulties of comprehension, due to language problems and differences in systems, habitual in cooperation and, finally, as an additional factor or a result of the previous difficulties, the national judge limited, in virtually all cases, his or her enquiry to national criminal records.

In view of such obstacles and as preparation for the development, also in this matter, of the mutual recognition principle enshrined in Tampere and which would be continued in the Hague Programme, in January 2005 the White Paper on exchanges of

information on convictions and the effect of such convictions in the European Union[25] was presented. But, at the same time, the Programme of measures for implementation of the goals set at Tampere, which represent a real programmatic text[26] in relation to the principle of mutual recognition of final decisions in criminal matters, envisaged the adoption of one or more instruments establishing the principle that a judge in one Member State must be able to take account of final criminal judgments rendered by the courts in other Member States for the purposes of assessing the offender's criminal record, to establish whether he or she has re-offended and in order to determine the type of sentence applicable and the arrangements for enforcing it.

The first of these instruments was **Council Decision 2005/876/JHA, of the 21st of November 2005** on the exchange of information extracted from the criminal register, that did not in fact modify the content of the 1959 Convention, but rather determined that criminal records would be requested by the judicial authorities from its own central authority and this would obtain them directly, in the event of corresponding to interconnected registers (France, Germany, Spain and Belgium), or would request them from other judicial authorities via their central authorities. The central authority should send, at regular intervals, the criminal convictions of non-nationals to the Member State or States of the nationality concerned and permitted Member States to obtain, in accordance with national legislation, the previous convictions handed down against their own nationals in other Member States. Among the improvements, worthy of note are the use of forms annexed to the Decision or the setting of deadlines. In 2006 and 2007, the Commission presented an comprehensive legislative package consisting of three instruments:

- Council Framework Decision 2008/675/JHA obliging Member States to take account of previous convictions in new criminal proceedings.
- Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from criminal registers.
- Council Decision 2009/316/JHA establishing ECRIS as the technical means of exchanging information extracted from criminal registers.

[25] COM/2005/10 final, of the 25th of January 2005.
[26] The Communication to the Council and to the European Parliament , dated the 26th of July 2000, led to a Programme of measures (OJ C 12, 15.1.2001) for its implementation, presented by the Commission, where the orientations of the JHA Council in Marseilles are incorporated.

EXCHANGE OF INFORMATION ON CRIMINAL RECORDS		TAKING CONVICTIONS INTO ACCOUNT
FD 2009/315/JHA (repeals FD 2005/876/JHA) Deadline: 26.3.2012		FD 2008/675/JHA Deadline: 15.8.2010
FD 2009/316/JHA (ECRIS) Deadline: 7.4.2012		

5.2. Council Framework Decision 2008/675/JHA

This FD, of the 24th of July 2008[27], on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings, has as its objective determining the conditions under which, in the course of criminal proceedings in a Member State against a person, previous convictions handed down against the same person for different facts in other Member States, are taken into account. The dispositions should be substituted with the same objective of article 56 of the European Convention of the 28th of May 1970 on the international validity of criminal sentences, between the Member States that are also parties in the convention.

The **obligation** to take into account is imposed on the States insofar as previous national convictions are taken into account and equivalent legal effects are attached to these convictions as to previous national convictions, in accordance with national law. With regards the specific extension of this obligation:

- In a positive sense, it is specified that it will be applied at the pre-trial stage, at the trial stage itself and at the time of execution of the conviction, in particular with regard to:
  - provisional detention;
  - the definition of the offence;
  - the type and level of the sentence;
  - and the rules governing the execution of the decision.

[27] OJ L 220/32, of 15.8.08.

- In a negative sense:
    - Where, in the course of new criminal proceedings, a Member State takes into account previous convictions handed down in another Member State, this will not interfere with previous convictions, nor will it involve a revocation or review of such convictions (in contrast to what would occur had the previous conviction been a national one).
    - If the offence for which the new proceedings being conducted was committed before the previous conviction had been handed down or fully executed, States would not be required to apply their national rules on imposing sentences, where the application ofthose rules to foreign convictions would limit the judge in imposing a sentence in the new proceedings. However, other means are employed to ensure that previous convictions are borne in mind within the new process.

In spite of the fact that it is envisaged that information on convictions will be obtained "under applicable instruments on mutual legal assistance or on the exchange of information extracted from criminal registers", it is certain that Decisions 2009/315/JHA and 2009/316/JHA constitute instruments linked to the effectiveness of this taking into account, which may explain why the **transposition deadline**, of the 15th of August 2010, has been largely ignored.

5.3. Council Framework Decision 2009/315/JHA

FD The FD 2009/315/JHA, of the 26th of February 2009[28], on the organisation and content of the exchange of information extracted from criminal registers between Member States, repeals Decision 2005/876/JHA and complements, on the matter which constitutes its subject, the 1959 and 2000 Conventions, with their respective Protocols.

The Decision has as its **objective**:

- To define the ways in which a convicting Member State should transmit the information on the conviction to the Member State of the convicted individual's nationality.
- To define the obligations of the Member State of the convicted individual's nationality to store information on convictions.

[28] OJ L 93/23, of 7.4.2009.

- To define the procedures to be followed by the Member State of the convicted individual's nationality when replying to a request for information on its nationals.
- To lay down the framework for a computerised system ofexchange of information.

The following **obligations** are imposed on the **convicting Member State**:

- Guarantee the registration on the national criminal register of the nationality or nationalities of the convicted individual who is not a national.
- Inform the other Member States of any convictions handed down against the nationals of such other Member States.
- Inform the Member State of the convicted individual's nationality of the subsequent alteration or deletion of the recorded information on the conviction.
- Inform the Member State of the convicted individual's nationality, on the request of this Member State, and in relation to individual cases, a copy of the conviction and subsequent measures, or any other information necessary to enable it to consider whether they necessitate any measure at national level.

For its part, the **Member State of the convicted individual's nationality**, assumes the following **obligations**:

- To store the information received on any of its nationals for the purpose of subsequent retransmission.
- Alter or delete the information that was transmitted to it when informed of an alteration or deletion of the conditions of the conviction,
- Transmit, after any request, only use information which has been updated.

With regards to the **procedure of request** and reply, the request is made in accordance with the national law of the requesting State, so that it can have effects in legal proceedings of for any other purpose. The request may even be made by an individual, but only where the individual concerned is or has been a resident or a national of the requesting or requested Member State. All requests from a central authority shall be submitted using the form annexed to the FD.

With respect to the **reply**, the F.D. establishes different regimes depending on the reason for the request for information:

- request made within the context of criminal proceedings. Information on convictions will be transmitted:
    - Handed down in the Member State of the convicted individual's nationality and recorded in the corresponding register.
    - Handed down in other Member States and transmitted to it after the 26th of March 2012.
    - Transmitted before this date and recorded in the criminal register.
    - Handed down in non-EU Member States and subsequently transmitted to it and entered on the criminal register.
- A request for purposes other than criminal proceedings. The reply will be in accordance with its national law, with regard to the convictions handed down in the Member State of the convicted individual's nationality and the convictions handed down in third countries that have been transmitted to it and entered in the criminal register. With respect to information on the convictions handed down in another Member State, that have been transmitted to the Member State of the convicted individual's nationality, the central authority of the latter Member State, in accordance with its national law, will transmit to the requesting Member State the information which has been stored and the information which has been transmitted to that central authority before the 26th of March 2012, and has been entered in its criminal register (although it is possible that the convicting Member State, on transmitting the information to the Member State of the convicted individual's nationality, has prohibited the "retransmission" for purposes other than criminal proceedings, in which case it shall inform the requesting State that the request must be submitted to the convicting State).
- Request from a third country to the central authority of the Member State of the convicted individual's nationality: The Member State may only respond within the limits established for the transmission of information to Member States.

Different deadlines are established, depending on the type of request, either immediately or within a period not exceeding ten working days. If its objective is to have effects in legal proceedings or another State purpose the reply must be immediate, and within twenty working days from the date the request was received when the request is made by an individual.

The information, requests for information and replies will be made through the **Central Authority** or Central Authorities of the Member States.

The principle of connection is recognised for the purpose of the information, although exceptionally its use is allowed by the requesting Member State to prevent an immediate and serious threat to public security.

The **transposition deadline** of the Decision expired on the 26th of March 2012.

5.4. Council Decision 2009/3j16/JHA

The previous Framework Decision is supplemented by Council Decision 2009/316/JHA, of the 06 April 2009[29] on the establishment of the European Criminal Records Information System (ECRIS).

The system will enable the computerised interconnection of criminal registers, in order that the exchange of information between Member States take place in a uniform and simple way by computer transmission.

The objectives of this Decision are the following:

- To establish the general architecture for the computerised exchange of information extracted from criminal registers. ECRIS is a decentralised information technology system that is based on the criminal records databases of other Member States. It consists of interconnection software that enables the exchange of information between national databases and the existence of a common communication infrastructure, which initially will be the Trans European Services for Telematics between Administrations (S-TESTA) network.
- It also enables the creation of a standardised European format for transmission of information on convictions. In this sense, two reference tables with categories of crimes and categories of sanctions are employed, which should facilitate automatic transfer and enable mutual understanding of the information transmitted via a system of codes. The Member States must consult these tables when they transmit information on the crime that gave rise to the conviction and information on its content.

Member States should have taken the measures necessary to implement the ECRIS Decision by the 7th of April 2012.

[29] O.J. L 93/33, of 7.4.2009.

As regards future prospects, the Action Plan of the Stockholm Programme invited the Member States to implement ECRIS as soon as possible, and invited the Commission to assess whether the networking of criminal records makes it possible to prevent criminal offences from being committed (for example through checks on access to certain jobs, particularly those relating to children), and whether it is possible to extend the exchange of information on supervision measures and to propose, in addition to ECRIS, a register of third-country nationals who have been convicted by the courts of the Member States.

Fernando Martínez Pérez
María Poza Cisneros
1st of September 2012

LEVEL II: TO KNOW MORE

6. The principle of availability

6.1. Definition

- In the Communication from the Commission to the European Parliament and the Council "Enhancing police and customs cooperation in the European Union"[30], of the 18th of May 2004, the Commission reviews the measures and initiatives that have been adopted since the Amsterdam Treaty[31], in the field of police and customs cooperation, an essential element in maintaining an area of security justice. The Commission notes, as **factors that hinder police and customs cooperation**, the following:
  - The nature of the work of the Police.
  - The absence of a strategic approach.
  - The proliferation of non-binding texts.
  - Decision-making procedures in the Third Pillar.
  - Insufficient application of the legal instruments adopted by the Council.
  - The lack of research into police and customs cooperation.
  - The nature of the cooperation between police and customs.
  - Databases and communication systems.

As **areas where improvements were required**, the Commission identified the following:

- The nature of the work of the Police. The objective of raising awareness amongst national authorities was established, developing mutual trust, wherein the assignation of national contacts to oversee the exchange of information was held to be essential, the Member States being obliged to possess an electronic system designed for the fast and secure exchange of information and legal authorities, to employ the technical instruments that facilitate cooperation.
- A strategic approach. Having verified the lack of a strategic approach, it was acknowledged that the rule of unanimity within decision making hindered progress.

[30] COM/2004/376 final. Not published in the O.J.
[31] Entered into force on the 1th of May 1999.

- The proliferation of non-binding texts as a hindrance to cooperation within the Third Pillar. Agreement should be reached on measures that are effectively applied by all parties.
- Decision-making procedures in the Third Pillar. The need to decide by unanimity and the right of initiative shared between Member States and the Commission seriously hindered progress. It was envisaged that the European Constitution (which, as we know, failed to prosper) would afford considerable improvement to the decision-making process.
- The application of legal instruments. In the Laeken European Council32, stress was again placed on the need for the rapid transposition to national rights of the Decisions made by the European Union.
- Research into police and customs cooperation. Having verified that scientific research in this area is scant, a proposal to afford the necessary resources to increase research was issued.
- The nature of the cooperation between police and customs. The need to establish better coordination and communication was voiced.
- Databases and communication systems. Having cited the various existing databases and communication systems (Europol Information System, SIS...) the Commission pondered the interoperability of the various systems, proposing the study of three possible options: the unification of existing systems; maintaining independent systems, creating new systems, should the need arise; and research with subsequent harmonisation of the data format and access regulations with regards to the various systems.

- In the Commission Communication addressing the Council and the European Parliament of the 16th of June 2004, "Towards enhancing access to information by law enforcement agencies"[33], a proposal was made to have the Member States adopt an **information policy** aimed at:
  - - Affording law enforcement agencies and those charged with preventing crime and terrorism the appropriate and necessary information.
  - - Stimulating the production and employment, within the EU, of high-quality information on crime, on both strategic and operational levels.
  - - Establishing a climate of trust between the services in question, particularly via the protection of personal data.

[32] December, 2001.
[33] COM/2004/429 final. Not published in the O.J.

6.2. Transposition of the principle

- With regards to the suspicions aroused by the principle of availability and by the Treaty of Prüm itself, the reflections and recommendations of the European Data Protection Supervisor (EDPS) prove highly illustrative: **Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability34**. The opinion indicated that difficulties arise as a result of the context in which the principle, in itself fairly straightforward, is applied. Such difficulties are manifest in the following:
    - The heterogeneous organisation of the police and judiciary within Member States, with different controls and balances.
    - - The inclusion of various types of information (of a sensitive nature), such as DNA or fingerprints.
    - The different forms of access to the information in question employed by the competent authorities, even with the same Member State.
    - The difficulty of ensuring that information afforded by another Member State is correctly interpreted, given linguistic differences, differences between technical systems (interoperability) and differences between legal systems.
    - The need to include this principle within the existing extensive mosaic of legal provisions concerning the exchange of police and judicial information between the various countries.
- When referring to the Swedish initiative, which would ultimately give rise to Framework Decision 2006/960/JHA of the 18th of December 2006, the aforementioned Opinion draws attention to the manner in which it takes in all information and intelligence, even where held by individuals other than the competent police or judicial authorities. From the point of view of data protection, it was held to be positive that the proposal strictly limited itself to the processing of existing data and did not entail the creation of new databases, or even index data, although attention was drawn to the fact that a lack of index data could not be viewed in a positive light. Index data, where properly guaranteed, can facilitate selective investigation, which proves less invasive in terms of data of a sensitive nature. It also allows for

[34] Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final). Official Journal C 116 of the 17/05/2006, pp 0008-0017.

improved filtering of requests and a greater degree of supervision.

- With regards to the Treaty of Prüm, the Opinion referred to above indicates that the initiative that failed to prosper (proposal for a Council Framework Decision of the 12th of October 2005), adopts a different approach to the application of the principle of availability. In contrast to a general approach that does not establish specific regulations for the exchange of certain types of information, the approach of the Treaty of Prüm is gradual, "data field by data field". It is applied to specific types of information (DNA, fingerprints and data relating to vehicle registration records), establishing the obligation to take the precise nature of the data into consideration. However, in a clearly critical tone, the EDPS makes the following observations in relation to the Treaty of Prüm:
    - With regards to its origin: He advises, moreover holding it to be obvious, that "the EDPS does not endorse the process leading up to this Convention, outside the institutional framework of the European Union, and therefore without substantive involvement of the Commission. Moreover, this means no democratic control by the European Parliament and no judicial control by the Court of Justice and as a result there are less guarantees that all the (public) interests are equally balanced."
    - With regards to its "invasive" content: He also draws attention to the fact that "it is obvious that some elements of the Prüm Convention are clearly more intrusive to the data subject than the proposal for a Framework Decision on availability. The Convention necessarily leads to the establishment of new databases which in itself presents risks to the protection of personal data. In particular, criticism is levelled at the creation of new DNA databases and the increased gathering of DNA data. Moreover, it is not clear which type of data is to be included in DNA analysis files and the Treaty does not take the dynamic evolution of DNA profiles into consideration.
    - With regards to its "ambitious" approach: Whilst it remains a "data field-by-data field approach", it is held " preferable not to set up a system for a range of data, but to start with a more cautious approach that involves one type of data and to monitor to what extent the principle of availability can effectively support law enforcement, as well as the specific risks for the protection of personal data. Based on these experiences, the system could possibly be extended to other types of data and/or modified in order to be more effective," which would prove more respectful towards

the principle of proportionality.

- The Explanatory Memorandum of the **Proposal for a Framework Decision of the 12th of October 2005**[35], concerning the exchange of information under the principle of availability, which failed to prosper, makes reference to its motivation and objectives. Specifically, in reference to the general context, it identifies seven main impediments to making information available throughout the EU, with a view to facilitating and expediting the prevention, detection and investigation of crime:

    - Bilateral and multilateral agreements between Member States are geographically limited or fail to oblige Member States to afford information, whereby the exchange of data is dependent upon discretionary factors.
    - Existing forms of cooperation between police and judicial authorities generally require the intervention of national Europol units or central contacts. Direct exchange of information between authorities remains the exception.
    - There is no standardised procedure at EU level for requesting and obtaining information.
    - There is no efficient mechanism at EU level that enables us to ascertain whether or not additional information is available and where it is to be found.
    - Differences in the conditions of access to and the exchange of information and the variations between police, customs and judicial cooperation prevent the efficient exchange of information.
    - Differences in the level of protection hinder the exchange of confidential information.
    - There are no common standards for the control of the legal use of information obtained from another Member State and the possibilities of identifying the source and original purpose of the information are scant.

  The proposed Framework Decision, along with the proposed Framework Decision on data protection, was intended to overcome these impediments, to

[35] COM/2005/0490 final.

the point where, in order to avoid a weakening of the principle of availability, the provision of information could only be refused for the following motives:

- Where the results of an ongoing investigation would be compromised.
- The protection of a source of information or the physical integrity of an individual.
- The protection of the confidentiality of information, in all stages of processing.
- The protection of the fundamental rights and freedoms of the individuals whose data is being processed as a result of the Framework Decision.

- The Commission Communication addressing the European Parliament and the Council offering an "Overview of information management in the area of freedom, security and justice[36]" of the 20th of July 2010 affords two **examples of the usefulness of the so-called Swedish Initiative** in terms of crime investigation: In 2009, there was an attempted murder in the capital city of a Member State. The police took a biological sample from a glass from which the suspect had drunk. Having extracted the DNA from the sample, the forensic experts generated the DNA profile. The comparison of this profile with the profiles stored in the national DNA databases proved fruitless. Therefore, the police investigating the case, via the Prüm contact, issued a request to compare it with the reference DNA profiles of other Member States, which had been authorised to exchange data on the grounds of the Prüm Treaty. This cross-border comparison did provide a result. By virtue of the Swedish Initiative, the police force investigating the case requested further information on the suspect. The national contact received responses from other Member States within 36 hours, enabling the police to identify the suspect. In 2003, an unidentified individual raped a woman. The police gathered samples from the victim; however, the DNA profile that was generated from the sample did not coincide with any of the reference profiles in the national DNA database. A DNA comparison was requested, sent by the Prüm contact to other Member States that had been authorised to exchange DNA reference profiles by virtue of the Treaty of Prüm, and a positive result was obtained. The police force investigating the case therefore requested further information on the suspect in accordance with the Swedish Initiative. The national contact received responses from other Member States within 8 hours, enabling the police to identify the suspect.

[36] COM (2010) 385 final, Brussels, 20/07/2010.

- The Explanatory Memorandum for Decision 2008/615/JHA was explicit in admitting "making full use" of the regulatory material incorporated into the Treaty of Prüm in order to meet the requirements of the Hague Programme with regards to the principle of availability, employing the following terms:
    - In the Hague Programme for strengthening freedom, security and justice in the European Union of November 2004, the European Council set forth its conviction that for such a purpose an innovative approach to the cross-border exchange of law enforcement information was needed. The European Council accordingly stated that the exchange of such information should comply with the conditions applying to the principle of availability.
    - For effective international cooperation it is of fundamental importance that precise information can be exchanged swiftly and efficiently. The aim is to introduce procedures for promoting fast, efficient and inexpensive means of data exchange.
    - These requirements are satisfied by the Prüm Treaty. To ensure that all Member States comply with the substantive requisites of the Hague Program within the deadlines therein established, it is apposite that the essential content of the Treaty of Prüm be applied to all Member States. This Decision therefore contains provisions which are based on the main provisions of the Prüm Treaty and are designed to improve the exchange of information, whereby Member States grant one another access rights to their automated DNA analysis files, automated dactyloscopic identification systems and vehicle registration data.
    - Closer police and judicial cooperation in criminal matters must go hand in hand with respect for fundamental rights, in particular the right to respect for privacy and to protection of personal data, to be guaranteed by special data protection arrangements, which should be tailored to the specific nature of different forms of data exchange.

7. The Prüm Treaty

7.1. Origin, nature and scope of application.

- The Treaty of Amsterdam of 1997 created the formal possibility for a number of states of establishing enhanced cooperation between themselves within the framework of the Treaties. The Treaty was formally incorporated in the Feira European Council of the 20th of June 2000.

- The Treaty of Nice of 2001, in force whilst the Treaty of Prüm was being drawn up, facilitated the establishment of enhanced cooperation: the right to veto with regards to the establishment of enhanced cooperation that was possessed by Member States disappeared (with the exception of foreign policy), the number of Member States required to initiate the process was changed from the majority to a set number of eight Member States and the scope of application was extended to take in common foreign and security policy (CFSP). The provisions relating to the initiation of the procedure and subsequent participation of a Member State were different within each of the three "pillars". The Treaty of Nice added an additional condition to the existing conditions: this type of cooperation must strengthen the process of EU integration and should not in any way affect the internal market, or the economic and social cohesion of the Union. Moreover, it must not represent an obstacle to or discriminate against exchanges between Member States, nor distort competition between them. The "last resort" nature of this type of cooperation is established, where the Council holds that the objectives could not be fulfilled within a reasonable period of time via the application of the relevant provisions of the Treaties. Moreover, this type of cooperation was to be open to all Member States, once established. It was also specified that the acts adopted within the context of enhanced cooperation would not form a part of the acquis of the Union, but rather, would be applied in the participating Member States, without impeding application in the remaining Member States. Finally, it was envisaged that the Council and the Commission would safeguard to ensure the coherence of the actions undertaken within the framework of enhanced cooperation with the remaining policies and actions of the Union.
- Specifically, the procedure for enhanced cooperation was enabled both within the Second Pillar, relating to a common foreign and security policy, and the Third Pillar, relating to police and judicial cooperation in criminal matters. The possibility of establishing enhanced cooperation within the sphere of the "second pillar" (Title V of the EU Treaty) represents one of the main advances of the Treaty of Nice in this area. Nevertheless, the procedures envisaged are different and more rigorous than those applicable within the Third Pillar and it is not always easy, particularly with a view to the content of the Treaty of Prüm, to

distinguish those procedures that fall with one pillar or the other.

- The Treaty of Lisbon facilitates recourse to this possibility that the constitutional Treaty had conserved. The Treaty of Lisbon established as nine the minimum number of states to set up enhanced cooperation and enable the application of "passerelle clauses" within enhanced cooperation, except in decisions with military implications or in the sphere of Defence. These passerelle clauses enable passing from unanimity to a qualified majority and from a legislative procedure to an ordinary legislative procedure. At a general level, excluding common foreign and security policy, Member States intent on establishing enhanced cooperation will issue a request to the Commission, which, in turn, will present a proposal to the Council. Following authorisation of the Parliament, the Council may approve the establishment of enhanced cooperation. In contrast to the general procedure, enhanced cooperation within the sphere of CFSP is not subject to proposals on the part of the Commission or approval on the part of the European Parliament. The decision to establish such cooperation is normally taken within the Council. The Council authorises or rejects the enhanced cooperation requested by Member States. Approval is granted unanimously. Moreover, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy are obliged to issue a report. The European Parliament is merely informed of the request. The Treaty of Lisbon created three types of specific cooperation in the field of Defence and facilitated recourse to enhanced cooperation in the sphere of judicial cooperation in criminal matters. The procedure for activation is more flexible where a Member State employs a "brake clause" to oppose the adoption of a legislative act in this area. In such instances, enhanced cooperation is established as a matter of course, based on the legislative project in question, where at least nine Member States participate. This clause, referred to as the "accelerator clause" thereby compensates for the "brake clause". A further two accelerator clauses are established for the creation of the European Public Prosecutor and police cooperation. In each case, to establish enhanced cooperation, at least nine Member States must participate. Therefore, such cooperation does not require a proposal from the Commission or the voting of the Council.

- On the 5th of December 2006, a Technical and Administrative Agreement was signed, in accordance with the stipulations of article 44 of the Treaty.
    - The Agreement is divided into six sections. The first is concerned with the objective and definitions; the second, with DNA profiles, where attention should be drawn to the fact that for comparison, the parties will employ existing regulations, such as the ISSOL (INTERPOL Standard Set of Loci for Europe), and the exchange of data relating to DNA between parties will be carried out via the TESTA II communication network
    - Section three, concerning dactyloscopic data, stipulates that the Parties must establish a reciprocal technical access system within their "national automated fingerprint identification systems" (AFIS) and that the electronic exchange of dactyloscopic data and related data between Parties must be carried out via the TESTA II,[37]
    - The fourth section refers to data originating from the vehicle registration records. For the exchange of information originating from vehicle registration records, the Parties will employ the TESTA II communications network and a EUCARIS[38] software application specifically designed with the objectives of the system envisaged in article 12 of the Treaty in mind.
    - **Section five is about police cooperation and includes very specific rules on joint interventions and interventions involving crossing the border in cases of imminent danger. Annex D.2 outlines which authorities must be informed immediately in this last type of collaboration, in accordance with article 25 section 3 of the Treaty.**
    - **Regarding the first type of collaboration, it can be organised through a mission statement, by one or more Parties, in accordance with article 24 of the Treaty. Before initiating the collaboration, everything relating to the nature of the intervention must be agreed in writing or orally, and specifically:**

        a) the competent authorities of the Parties in the mission statement;

        b) the specific aim of the intervention;

[37] the Trans European Services for Telematics between Administrations.
[38] The European Vehicle and Driving Licence Information System

c) the State of the territory in which the intervention will take place;

d) the geographical area of the State of the territory in which the intervention will take place;

e) the time period to which the intervention's mission statement refers;

f) the specific assistance that the State of origin must provide to the State of the territory in question, including officers or other officials, material and funding;

g) the officers who will participate in the intervention;

h) the officer who will be in charge of the intervention;

i) the powers that may be exercised by the officers and other officials of the State of origin in the State of the territory during the intervention;

j) the weapons, munitions and specific equipment that the officials involved may use during the intervention;

k) logistical issues related to transport, accommodation and safety;

l) the sharing of costs of the joint intervention, where it diverges from the provisions of article 46 of the Treaty;

m) any other necessary elements.

- As can be seen in this Agreement, no measures are taken with respect to illegal immigration.

7.2. Content

7.2.1. Automated access to national files

7.2.1.1. DNA profiles

- On this issue it is important to insist, following the EDPS Report we referred to[39], on the **fundamental difference between DNA samples and DNA profiles**.
  - DNA samples (often collected and stored by police authorities) should be considered particularly sensitive, as it is likely that they contain the whole DNA of a person. They can provide information on the genetic

[39] Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final). Official Journal C 116 of the 17/05/2006, pp 0008-0017.

characteristics and state of health of a person, something that may be required for completely different purposes such as providing medical advice to people or to young couples.

- On the other hand, DNA profiles contain only partial information extracted from the DNA sample; they can be used to verify a person's identity, but they do not generally reveal genetic characteristics of a person. Scientific progress has increased the amount of information that can be obtained through DNA profiles: what at one time was considered an "innocent" profile may at a later stage reveal much more information than what is expected or required, and in particular information relating to a person's genetic characteristics. The information that can be obtained through DNA profiling must therefore be considered dynamic.

- The EDPS stresses that **any legal instrument used to establish exchanges of DNA** should:
  - Clearly limit and define the type of DNA that can be exchanged (also with respect to the fundamental difference between DNA samples and DNA profiles).
  - Establish common technical rules that aim to prevent variations in the handling of DNA databases by forensic science officers in member states from generating difficulties and incorrect results when exchanging information.
  - Facilitate adequate and legally binding guarantees to prevent scientific advances from obtaining personal information from DNA profiles that is not only sensitive but also unnecessary for the objective for which they were taken.
- The inefficiency of the exchange of this information was highlighted at the informal meeting in Dresden on the 15th of January 2007, where the German initiative for transposing the Prüm Treaty to the Community legal framework was proposed. At the end of this meeting, the German Minister for the Interior Wolfgang Schäuble revealed that a comparison between the German and Austrian DNA databases, over just a month and a half from December of 2006 and using the hit/no hit method, found 1500 coinciding profiles that were labelled as not identified in the German database, and 1400 in relation to profiles of the same type in the Austrian database.

7.2.1.2. Fingerprinting data

- The existence of the Interpol AFIS database and the European EURODAC for asylum seekers, should be noted.

7.2.1.3. Vehicle registration data

7.2.1.4. Other information

Although it does not mention it explicitly, the Treaty subscribes to the controversial principles enshrined in the Council Resolution of the 29th of April 2004 on the security of European Council meetings and other similar events (2004/C 116/06). The aforementioned Resolution defines the basis upon which the transmission of personal data is allowed as the existence of "reasonable grounds for believing that [individuals or groups] intend to enter the member State with the objective of disturbing public order and the security of the event, or to commit offences related to the aforementioned event". In art. 14 of the Treaty, there is a reference to the "existence of final convictions or other circumstances [that] justify the presumption that these individuals are going to commit a crime motivated by the event or that they constitute a threat to security and public order". Despite what the text purports to say, there have been criticisms that this transmission of personal data - based on suspicions that are "legitimated" but not necessarily legitimate - is aimed at people who are defined not so much by their behaviour but by a political ideology: in short, political activists.

7.2.2. Measures for the prevention of terrorist attacks

7.2.2.1. Transmission of information

- The idea of gathering information for this purpose is certainly not new. A **similar system for exchanging information** to fight against terrorism existed in the context of the old TREVI Group**,** which was launched in 1976 and whose scope was extended considerably in the 80s to include not just terrorism but also organised crime, drug trafficking and illegal immigration. This was the basis for the creation of the BDL-network (liaison office) as a system of encrypted transmission of classified information. The need for a fast and reliable information system related to terrorist attacks became a major priority, for obvious reasons, after September 2001. The nature and functioning of this network is different from that of the national contact points envisaged in the Treaty of Prüm, as the latter goes further by referring to exchanges of a "preventive" nature, such as those "under suspicion". In that respect it is not clear, for example, how the national contact points can obtain "knowledge" that a particular person or suspect is going to commit a crime. However, under the Treaty this "knowledge" or unilateral conviction that someone "may be or may become a terrorist" is enough for the

authorities to transfer personal data and a large amount of information as envisaged in art. 16, and with an approach that is notably broader than that authorised by art. 46.1 of Schengen; there is more emphasis on the "preventive and visionary" aspect entrusted to the national contact points in the fight against terrorism[40], as invoked by Framework Decision 2001/475 of the 13th of June 2002, which aimed to overcome the difficulty of agreeing to a common and broad definition of terrorism that encompasses the threat of committing terrorist acts.

- There are certain doubts surrounding the **designation of national contact points** referred to in Art. 16.3 of the Treaty, which were the subject of repeated recommendations by the Council and the Commission. In particular, there are concerns about the lack of democratic control in designating who qualifies as a genuine "oracle" in charge of predicting whether a particular individual will or will not become a terrorist, and of transmitting personal data and information to another State on the basis of such a prediction. The designation of contact and coordination points in relation to articles 17 and 18 is also envisaged. But it is left to each State to decide what authority or authorities are designated, without excluding the possibility of designating staff from the intelligence services. It would even be possible to designate contact points "by subject" or else a single contact point for all information that the Treaty refers to. However, the principle of availability, as conceived in the Hague Programme and what has developed from it, points to an exchange of information that is restricted to national police authorities and to Europol. For example, Belgium chose an individualised designation by subject: the National Institute of Criminalistics and Criminology, within the Ministry of Justice, for transmitting DNA profiles; and the Federal Police, within the Ministry of the Interior, for fingerprints and other data.

7.2.2.2. Deployment of security escorts in flights

- The same authors referred to in the previous section criticised the excessive degree of discretion implied by the reference to "other public employees with corresponding training" to define these security escorts.
- After 9/11 the USA requested this type of accompaniment in certain flights coming from Europe. This triggered a wide debate within the International Civil Aviation Organisation, driven by concerns for personal freedom, with a noteworthy opposition from Scandinavian countries. The Treaty welcomes this

[40] BALZACQ et al. “Security and the two level game. The Treaty of Prüm, the EU and the management of threats”

proposal, and in so doing it raises issues relating to the principle of solidarity and good faith, insofar as it could establish a separate regime for flights originating from the USA.

- Concerns have also been raised about the exception to prior notification in writing "in case of imminent danger". There is no definition of what constitutes such a danger, which could be invoked with the affirmation that there exists (or existed) a "permanent state of danger or emergency" that would allow for the systematic assignment of security escorts to flights, making the exception the norm.

7.2.3. Measures for combating illegal migration

7.2.3.1. Sending document advisors

7.2.3.2. Support in cases of repatriation

- Immigration was not initially seen as a Community policy. The only mention of immigration in the Treaty of the European Union of the 25th of March 1957 refers exclusively to emigrant workers from member States and the object of the provision is to assure these workers adequate social benefits so as to allow an effective freedom of movement and right of establishment in all member States. The situation in later years meant that immigration, especially from non Community countries, became a priority issue for European governments, and was consequently mentioned in a Community Treaty, the Single European Act, signed on the 28th of February 1986.
- The Treaty on the European Union is the first Community Treaty to specifically regulate immigration, which it considers an "area of common interest" for attaining the objectives of the Union, in particular the free movement of persons, and states it as such in the article. K.1, paragraph 3.
- The Amsterdam Treaty modifies that of the European Union, and understands immigration measures as an integral part of the aim of developing the Union as an area of freedom, security and justice. It allows the European Community to adopt measures in the following areas:

  1) the lifting of internal border controls on persons, both for Union nationals and for nationals of third countries
  2) crossing the external borders of the EU
  3) asylum and refuge
  4) the immigration policy
  5) the fight against crime and consequently police and judicial cooperation in criminal matters

6) judicial cooperation in civil matters

7) cooperation to this end between the member State administration services and those of the Commission.

- The Nice Treaty essentially maintains the above regulation without making any important additions to the field in question.
- After the modifications brought by the Lisbon Treaty of the 13th of December 2007, the immigration policy becomes clearly framed within the area of freedom, security and justice. Hence, "the Union offers its citizens an area of freedom, security and justice without internal borders, within which the free movement of persons is guaranteed with adequate measures for external border controls, asylum, immigration and preventing and combating crime" (article 3.2 of the current Treaty on European Union). The policies on border controls, asylum and immigration are regulated in the second Chapter of Title IV, with the requirement that a common immigration policy must be developed that is "designed to guarantee at all times an effective management of migratory flows, an equitable treatment of third-country nationals residing legally in Member States, and the prevention of, and enhanced measures to combat, illegal immigration and trafficking in human beings" (art. 63 bis 1).
- There are numerous Community provisions on this issue. For the purpose of information, and without forgetting the important contents of the Schengen Agreement, some of these provisions, which cover many aspects of common policy, are outlined below:
    - Council Recommendation of the 22nd of December 1995 on harmonising the means of combating illegal immigration and illegal employment and improving the relevant means of control (DO C 5 of 10.1.1996).
    - Council Recommendation of the 2th of September 1996 on combating the illegal employment of third-country nationals (DO C 304 of 14.10.1996).
    - Directive 2001/40/EC of the Council, of the 28th of May 2001, on the mutual recognition of decisions on the expulsion of third country nationals (DO L 149 of 2.6.2001).
    - The Council's Framework Decision of the 28th of November 2002, on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence (DO L 328 of 5.12.2002).
    - Regulation (EC) no. 377/2004 of the Council, of the 19th of February 2004 on the creation of a network of immigration liaison officers (DO L

64 of 2.3.2004).

- Council Decision of the 29th of April 2004 on the organisation of joint flights for removals from the territory of two or more Member States, of third-country nationals who are subjects of individual removal orders (DO L 261 of 6.8.2004).
- Regulation (EC) no. 562/2006 of the European parliament and of the Council, of the 15th of March 2006, establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (DO L 105 of 13.4.2006).
- Council Decision of the 26th of April 2010, supplementing the Schengen Borders Code as regards the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Co-operation at the External Borders of the member States of the European Union (DO L 111 of 4.5.2010).

7.2.4. Other forms of cooperation

7.2.4.1. Joint patrols and other forms of joint intervention
7.2.4.2. Border crossing
7.2.4.3. Assistance in connection with major events, disasters and serious accidents
7.2.4.4. Cooperation upon request

7.2.5. Provisions on the protection of personal data

7.2.5.1. Definitions
7.2.5.2. Level of data protection
7.2.5.3. Principle of a link to the purpose and other limits to data use and processing
7.2.5.4. Guarantees of accuracy, current relevance and storage time of data
7.2.5.5. Technical and organisational measures to ensure data protection and data security
7.2.5.6. Documentation and registration

- In accordance with article 8 of the Charter of Fundamental Rights of the European Union, everyone has the right to the protection of personal data concerning him or her, and such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Moreover, everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- As is well known, the Treaty on the European Union included police cooperation between member States in the so-called Third Pillar of the European Union,

and yet there were no rules harmonised at European level concerning data protection derived from this cooperation. There is however a basic common level of data protection legislation throughout member States as they all belong to the Council of Europe, and this common legislation is based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) that applies to all data processing in the public or private sector, including that carried out by the State Security Forces as referred to in the Treaty of Prüm.

- In 1987 the Council of Ministers of the Council of Europe approved Recommendation (87) 15 regulating the use of personal data in the area of policing. This Recommendation, as stated by ACED FÉLEZ "has become the de facto standard for data protection in the processing of personal data in police investigations, by being incorporated as a minimum requirement in various conventions and decisions of the EU such as Schengen, Europol, the Customs Information System and Eurojust". The Recommendation is articulated around eight principles: control and reporting, data collection, data storage, use of data by the police, disclosure of data, publicity and the rights of individuals, duration of storage and updating of data, and data security. These are the basic principles upon which the processing of personal data in the area of policing is regulated.
- It is a policy of the European Union that the exchange of personal data in the area of freedom, justice and security be based on clear rules, especially in the area of police and judicial cooperation, where the principle of availability applies, and a balance must always be struck between security and the right to privacy. This clarity increases trust between the competent authorities and guarantees the protection of information; a guarantee that cannot be provided by existing legal instruments at the level of the European Union. Thus, Directive 95/46/EC of the European Parliament and of the Council, of the 24th of October 1995 does not apply to data processing related to public safety, defence, State security or the activities of the State in criminal matters.
- To address the problem of protecting data that is processed in the framework of police and judicial cooperation in criminal matters in the European Union, Framework Decision 2008/977/JAI was passed, under the principle of subsidiarity, aiming to protect the fundamental rights and freedoms of natural persons when their personal data are used for preventing, investigating, detecting or prosecuting criminal offences and imposing criminal sanctions.

- However, it should be noted that a number of acts adopted by virtue of title VI of the Treaty on the European Union contain specific provisions on the protection of exchanged personal data, and in some cases constitute a complete and coherent set of rules that regulate these matters in more detail than the Framework Decision, and so it should be understood that such instances lie outside scope of application of the latter. When the existing provisions of Title VI of the Treaty on the European Union impose conditions for specific actions upon member States that are stricter than those regulated by the Framework Decision, then such cases also lie outside scope of application of the Framework Decision.
- Thus, article 28 of the Framework Decision establishes that "Where in acts, adopted under Title VI of the Treaty on the European Union prior to the date of entry into force of this Framework Decision and regulating the exchange of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaty establishing the European Community, specific conditions have been introduced as to the use of suchdata by the receiving Member State, these conditions shall take precedence over the provisions of this Framework Decision onthe use of data received from or made available by another Member State".
- Data may only be collected by applying the principles of lawfulness, proportionality and purpose, as established in article 3. The following issues, among others, are also dealt with in the Framework Decision: rectification, erasure and blocking (ex oficio or at the request of an interested party); verification of quality of data that are transmitted or made available; logging and documentation; processing of data received; exercising the right of information and access to data by interested parties; as well as the right to rectification, confidentiality and security in processing data.

8. The partial incorporation of the Treaty of Prüm into the legal framework of the European Union

8.1. Decision 2008/615/JHA

8.2. Decision 2008/616/JHA

Decisión Prüm

Respuestas positivas obtenidas por Alemania en la comparación transfronteriza de perfiles DNA, según el tipo de delito (2009)[40]					
Respuestas positivas por tipo de delito	Austria	España	Luxemburgo	Países Bajos	Eslovenia
Delitos contra intereses públicos	32	4	0	5	2
Delitos contra la libertad de las personas	9	3	5	2	0
Delitos sexuales	40	22	0	31	4
Delitos contra las personas	49	24	0	15	2
Otros delitos	3 005	712	18	1 105	71

Source: Communication from the Commission to the European Parliamentand the Council offering an "Overview of information management in the area of freedom, security and justice", 20th of July 2010

9. The principle of availability in the Stockholm Programme

- In the Stockholm Programme, the complete list of **priorities** that the European Union should bear in mind in its activities over the coming years is as follows:
  - Promoting citizenship and fundamental rights. For example, the exercise of these rights and freedoms should be preserved beyond national borders, in particular the private sphere of the citizen, and especially in relation to the protection of personal data.
  - A Europe of law and justice.
  - A Europe that protects
  - Access to Europe in a globalised world
  - A Europe of responsibility, solidarity and collaboration in the areas of migration and asylum
  - The role of Europe in a globalised world
  - The external dimension

- The following are mentioned as regards **instruments**:
  - Mutual trust.
  - Complete and effective implementation, execution and evaluation of existing instruments.
  - Legislation.

- Increased coherence.
- Evaluation.
- Training
- Notification
- Dialogue with civil society
- Funding
- Action Plan

- The fourth section, related to **security** ("A EUROPE THAT PROTECTS") includes the following sub-sections:

4.1. Internal security strategy

4.2. Modernising work instruments

4.2.1. Forging a common culture

4.2.2. Managing the flow of information

4.2.3. Mobilising the necessary technological tools. In this section, the European Council invites the Council, the Commission and, if applicable, the member States to:

- draw up and implement policies to ensure a high level of network and information security throughout the Union and improve measures aimed at protection, security preparedness and resilience of critical infrastructure, including Information and Communication Technology (ICT) and services infrastructure,
- promote legislation that ensures a very high level of network security and allows faster reactions in the event of cyber attacks.
- The European Council also invites the Council and the Commission to ensure that the priorities of the internal security strategy are tailored to the real needs of users and focus on improving interoperability. Research and development in the field of security should be supported by public-private partnerships.

4.3. Effective policies

4.3.1. More effective European law enforcement cooperation

4.3.2. More effective crime prevention

4.3.3. Statistics

4.4. Protection against serious and organised crime

4.4.1. Combating serious and organised crime, especially the following types of crime:

4.4.2. Trafficking in human beings

4.4.3. Sexual exploitation of children and child pornography

4.4.4. Cyber crime

4.4.5. Economic crime and corruption

4.4.6. Drugs

4.5. Terrorism

4.6. Comprehensive and effective Union Disaster Management: reinforcing the Union's capacities to prevent, prepare for and respond to all kinds of disasters

- Regarding the **principle of availability**, and in the **critical** line expected in Level I, the **Stockholm Programme Action Plan** expressly recalls that:
  - "The principle of availability is liable to allow the exchange of personal data that have not been collected legitimately and lawfully, and so it must be underpinned by common rules".
  - "Expresses doubts with regard to the facilitation of operational activities that do not include a European definition and common standards concerning covert investigations, surveillance of citizens, etc" (perhaps a veiled reference to the Treaty of Prüm).
  - "Believes that, before EU action is envisaged in this field, clear criteria should be laid down for assessing the proportionality and necessity of limitations to fundamental rights"
  - "Expresses its concern about the increasingly widespread practice of profiling, based on the use of data-mining techniques and the generalised collection of innocent citizens' data for preventive and policing purposes"
  - "Recalls the importance of the fact that law-enforcement actions must be based on respect for human rights, from the principle of the presumption of innocence to the right to privacy and data protection".
  - Stresses the need for clearer and tighter limits on exchanges of information between Member States and the use of common EU registers; takes the view that, otherwise, building up large registers at EU level is liable to threaten personal integrity and registers may become ineffective whilst the risk of leaks and corruption will increase".
- Regarding **specific proposals** on the study's objective, the **Action Plan**:
  - Advocates improvements to ECRIS.
  - Requests a revision of Framework Decision 2008/977/JHA of the Council of

the 27th of November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; (EC) Regulation 45/2001 of the European Parliament and of the Council of the18th of 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 (3); and article 13 of Directive 95/46/EC of the European Parliament and of the Council of the24th of October1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- Deplores the lack of progress in implementing the upgraded SIS II and the new VIS, and urges that further delays be avoided;
- Stresses the need to develop efficient, sustainable and secure administrative arrangements for major European IT systems such as SIS II, VIS and Eurodac, thereby ensuring that all the rules applicable to such systems, with regard to purpose and rights of access as well as security and data-protection provisions, are implemented in full; emphasises in this regard that it is essential for the EU to have a comprehensive, uniform set of rules on the protection of personal data;
- Recalls that in certain areas the creation of agencies, for instance the FRA, Eurojust, Europol, Frontex and the EASO, has been very useful for the establishment of an AFSJ; considers that, given that Schengen is the core of the AFSJ, it is fundamental and vital to create an European agency for the management of substantial information systems in this area, namely SIS II, VIS and Eurodac, because this is the most reliable solution.

▪ In the initiatives under way for implementing a general data protection regime in the European Union, it is recalled that the centrepiece of **existing EU legislation on personal data protection** is Directive 95/46/EC3, adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. It was complemented by various instruments establishing specific standards for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters (the previous third pillar), including Framework Decision 2008/977/JHA. The European Council invited the Commission to evaluate the functioning of EU instruments on data protection and to present, where necessary, further legislative and non-legislative initiatives. In its resolution on the Stockholm Programme, the European

Parliament welcomed a comprehensive data protection scheme in the EU and among others called for the revision of the Framework Decision. The Commission stressed in its Action Plan implementing the Stockholm Programme the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies. Framework Decision 2008/977/JHA has a limited scope of application, as it only applies to the cross-border processing of data and not to processing by police and judicial authorities at a purely national level.

- Although it was not mentioned in the Stockholm Programme, in January of 2010 the Spanish presidency presented an initiative for a Police Information Exchange Platform, later renamed **IXP: Information Exchange Platform for Law Enforcement Authorities.** The aim was to provide a central access point for police (and judicial) authorities to any police/judicial information exchange instrument at EU level. The idea was developed by Spain and Europol, and was backed by Belgium, Germany, Lithuania, Hungary, Slovakia and the Commission itself. Although still in an early phase of development, its main thrust is as follows:
    - To have a single web page as a starting point for accessing products or services related to international legal cooperation, for a more efficient development and maintenance, easier data protection management and the advantage of shared experience, in a friendly environment that facilitates the identification of contacts in other member States.
    - To make this resource available across the European community to all law enforcement authorities, including local, regional and national police forces; border and coast control and customs officials; FRONTEX (European Agency for the Management of Operational Co-operation at the External Borders of the Member States of the EU); OLAF, Interpol, EMCDDA (European Monitoring Centre for Drugs and Drug Addiction), CEPOL, EuroJust and Europol, judges, prosecutors, prison services, etc.
    - To respond to the operational needs of cross-border police cooperation, providing access to or redirecting the user towards the available tools, channels and information, to cover areas such as knowledge management, user intercommunication, access to specific tools for joint operations, operative consultations redirected to databases managed

within the framework of justice, freedom and security, including at a national level.

- The Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the 25th of January 2012 on "Safeguarding privacy in a connected world. A European data protection framework for the 21st century" justifies the new legal framework that will include the Proposal for a Directive of the European Parliament and 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 and the Proposal for a Regulation of the European Parliament and 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) which will replace Framework Decision 2008/977/JHA and Directive 95/46/EC. The processing of data by police and judicial authorities in the criminal field is currently covered principally by Framework Decision 2008/977/JHA, which predates the entry into force of the Lisbon Treaty. In view of its nature as a Framework Decision, the Commission has no powers to enforce its rules, which has contributedto its very uneven implementation. In addition, the scope of this Framework Decision is limited to cross-border processing activities. This means that the processing of personal data that has not been made the subject of exchanges is currently not covered by EU rules governing such processing and protecting the fundamental right to data protection. In some cases this also creates a practical difficulty for police and other authorities who are not always able to easily distinguish between purely domestic and cross-border processing or to foresee whether certain data may become the object of a cross-border exchange at a later stage. The EU's new reformed data protection framework therefore aims to ensure a consistent, high level of data protection in this area to enhance mutual trust between police and judicial authorities of different Member States, thus facilitating the free flow of data and cooperation between police and judicial authorities".
- With the aim of ensuring a high level of protection of personal data within the context of police and judicial cooperation in criminal matters and in order to facilitate the exchange of personal data between the police and judicial

authorities within the Member States, the Commission proposes, as part of a reform package for the protections of data, a Directive that:

- applies general data protection principles to police cooperation and judicial cooperation in criminal matters, while respecting the specific nature of these fields;
- provides for minimum harmonised criteria and conditions on possible limitations to the general rules; This concerns, in particular, the rights of individuals to be informed when police and judicial authorities handle or access their data; Such limitations are necessary for the effective prevention, investigation, detection or prosecution of criminal offences;
- establishes specific rules to cover the specific nature of law enforcement activities, including a distinction between different categories of data subjects whose rights may vary (such as witnesses and suspects).

- One must recognise the impact of ECHR decisions upon these new measures to homogenise the data protection regime, such as the **Ruling of the Grand Chamber in S. and Marper versus the United Kingdom of the 4th of December 2008**, in which the British State was condemned for violating article 8 of the European Convention on Human Rights in relation to due respect for private life. The case arose from two demands of citizens considered not guilty by the courts, through acquittal and filing of the case respectively, but whose fingerprints, cell samples and genetic profiles were kept by the British authorities, and their requests to the Police and administrative courts to have these data cancelled were rejected. The ECHR found that a general and undifferentiated power to retain the fingerprints, biological samples and DNA profiles of individuals suspected of having committed crimes, but not convicted, does not strike a fair balance between public and private interests, and that through such regulations and practices the respondent State overstepped any acceptable margin of discretion on this issue. In the court's view, retaining such data in those circumstances is a disproportionate infringement of the plaintiffs' right to respect for their private lives, and it cannot be deemed necessary in a Democratic society.
- As a final reading, the Communication from the Commission to the European Parliament and the Council offering an "Overview of information management in the area of freedom, security and justice[41]", of the 20th of July 2010, is both disappointing and "illuminating". One of its paragraphs, a veritable "alphabet

[41] COM (2010) 385 final, Brussels, 20/07/2010.

soup", gives a fairly accurate description of the situation in 2010: "Most of the instruments analysed above have a unitary purpose: EURODAC seeks to enhance the functioning of the Dublin system; API to improve border control; the Swedish initiative to enhance criminal investigations and intelligence operations; the Naples II Convention to help prevent, detect, prosecute and punish customs fraud; CIS to assist in preventing, investigating and prosecuting serious violations of national laws by increasing the effectiveness of cooperation between national customs administrations; ECRIS, FIUs and AROs to streamline cross-border data sharing in particular areas; and the Prüm Decision, Data Retention Directive, TFTP and PNR to combat terrorism and serious crime. SIS, SIS II and VIS appear to be the main exceptions to this pattern: the original purpose of VIS was to facilitate the cross-border exchange of visa data, but this was later extended to preventing and combating terrorism and serious crime. SIS and SIS II aim to ensure a high level of security in the area of freedom, security and justice and facilitate the movement of persons using information communicated via this system. With the exception of these centralised information systems, purpose limitation appears to be a core factor in the design of EU-level information management measures (...) Other measures process highly specialised personal information relevant for their unique objectives: PNR systems process passengers' flight reservation details; FIDE, data relevant for the investigation of customs fraud; the Data Retention Directive, IP addresses and mobile equipment identifiers; ECRIS, criminal records; AROs, private assets and company details; cybercrime platforms, internet offences; Europol, links to criminal networks; and the TFTP, financial messaging data."

10. Criminal records

10.1. Introduction

- PALOMO DEL ARCO[42] lists the main instruments for recognising foreign criminal convictions that exist to date. They are inadequate, both in terms of their irregular implementation by member States and their complete failure to achieve full recognition, and this justifies a search for new mechanisms:

[42] PALOMO DEL ARCO, A. *Antecedentes penales (registro de condenas) en el ámbito europeo*, [Criminal records at European level] in *El proceso penal en la Unión Europea:*

- The Convention on the International Validity of Criminal Judgments of the Council of Europe (CEVISP); signed in The Hague on the 28th of May, 197043. The fundamental concept that underlies it, according to its explanatory report, is the assimilation by a foreign judgment (of any State Party) of those that emanate from any national courts, with the express purpose, in accepting the transfer of enforcement of criminal sentences, of encouraging the social rehabilitation of the convicted individuals. Although its content actually covers three separate issues: i) the enforcement of the judgment (articles 2-52); ii) the effect of the ne bis in idem principle (articles 53-54); and iii) the consideration of foreign judgments in the so-called indirect effects (articles 56-57)". It came into force with the third ratification on July 26th, 1974. Currently only 22 countries have ratified it: Albania, Austria, Belgium, Bulgaria, Cyprus, Denmark, Spain, Estonia, Georgia, Iceland, Latvia, Lithuania, Moldova, Montenegro, Norway, the Netherlands, Romania, San Marino, Serbia, Sweden, Turkey and Ukraine.
- Convention on the Enforcement of Foreign Criminal Sentences passed in Brussels on November 13th, 1991, with provisional application between the Netherlands (including the Netherlands Antilles and Aruba) and Germany and Latvia respectively 44.
- The 1998 EU Convention on driving disqualifications, adopted under the Maastricht Treaty, which allows driving disqualification sanctions to be extended to other European states where the offence was not committed, and which has not entered into force.
- Chapter 3 of Title III of the Convention implementing the Schengen Agreement of 14th of June 1985 on the gradual abolition of checks at common borders (Schengen, June 19th, 1990) contains rules on applying the ne bis in idem principle (articles 54-58). The interpretation of this principle has been the subject of several ECJ rulings, often directly related to the consideration of drug trafficking convictions in another EU Member State.

---

garantías esenciales [Criminal proceedings in the European Union: essential guarantees] pages. 371.-399. Published by Lex Nova. Valladolid, 2008.

[43] Instrument of ratification of September 2nd, 1994 (Official State Gazette 30.03.96).

[44] Cyprus, Spain and Portugal have also ratified, but have not signed the provisional application clause

10.2. Framework Decision 2008/675/JHA

In France, art. 17 of Law no. 2010-242 of March 10th, 2010, for reducing the risk of recidivism and the reform of various criminal law procedures, transposes the Framework Decision 2008/675. Articles 132-16-6 of the French Penal Code already envisaged considerations of recidivism in convictions handed down by the criminal jurisdiction of a Member State. The new article 132-23-1 introduces the rule of equivalence when considering convictions imposed by the criminal jurisdiction of any other Member State in relation to those imposed in France, with either type of conviction producing equivalent legal effects. Interpreters of the law clarify that these effects include the granting of a stay of execution, with or without conditions, or the criteria for pre-trial detention, adopted hereafter; but it also includes the revocation of a suspension, with or without conditions, or of conditional release granted previously. Regarding the effects of foreign sentences on rehabilitation, that is, with regards to the cancelation of criminal records, the coming into force of the reform, in general proposed for the 1/7/2010, was delayed until the 1/4/2012, given that these effects required, in turn, a more demanding reform of the automated registry of criminal records, then a study for the transposition of Framework Decision 2009/315/JAI.

- In the United Kingdom, the "Criminal Procedure (Amendment) Law" of 2011 was designed to transpose the Framework Decision 2008/675.

- On the 6th of December 2011, the Luxembourg State Council issued an Opinion on the Draft Law on International Recidivism which will comprise the transposition into French law of the Framework Decision 2008/675/JHA. Among other issues, there is the difficulty for the judge in establishing the necessary equivalences when the sanctions are different in nature to those envisaged by his/her national Law, in order to ensure that foreign and domestic convictions are treated and considered equally. The project, unlike its French equivalent, also requires a prior knowledge of the conviction via the traditional means of judicial assistance, and thus ignores Decisions 2009/315 and 2009/316.

10.3. Framework Decision 2009/315/JHA

10.4. Decision 2009/316/JHA

- In the meeting of the Working Group on Cooperation in Criminal Matters (ECRIS Experts) on the 28th of March 2012, it was considered that Member States might require **support** in implementing ECRIS. Although the

corresponding Community software was implemented in time (which Member States may choose whether to use or not), differing degrees of technical implementation and legal transposition in the various Member States was observed in the spring of 2012, with five of them predicting that they would be unable to meet the deadline of 27.4.2012.

- It appears that a handbook on ECRIS for central authorities and end users, including judges, prosecutors and police, is about to be published, and that a central platform to provide information, with different levels of access, is to be created.
- It is important to note the work of the General Secretariat of the Council in updating the lists annexed to the Decision with information that the States are required to provide on a regular basis.

LEVEL III: REFERENCE MATERIAL

11. The principle of availability

11.1. Definition

- "The Hague Programme: 10 priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice"

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0184:FIN:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0184:EN:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0184:FR:HTML

11.2. Transposition of the principle

- FD 2006/960/JHA of the 18th of December 2006

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:FR:PDF

- Report of the European Data Protection Supervisor on the Council's proposal for a framework Decision on the exchange of information by virtue of the principle of availability (COM(2005) 490 final).

http://eur-law.eu/ES/Dictamen-Supervisor-Europeo-Proteccion-Datos-propuesta-Decision-marco,296571,d

http://eur-law.eu/EN/Opinion-European-Data-Protection-Supervisor-Proposal-Council-Framework,296571,d

http://eur-law.eu/FR/Opinion-of-the-European-Data-Protection-Supervisor-the,296571,d

12. The Prüm Treaty

12.1. Origin, nature and scope of application.

- The Treaty of Prüm (there is no authentic version in English)

ES.- http://www.boe.es/boe/dias/2006/12/25/pdfs/A45524-45534.pdf

FR.- http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000017865342

Technical Agreement on implementing the Treaty of Prüm

FR.- http://textes.droit.org/JORF/2009/07/31/0175/0009/

12.2. Content

12.2.1. Automated access to national files

12.2.1.1. DNA profiles

12.2.1.2. Fingerprinting data

12.2.1.3. Vehicle registration data

12.2.1.4. Other information

- **Council Resolution of 30 November 2009 on the exchange of DNA analysis results**

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:296:0001:01:ES:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:296:0001:01:EN:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:296:0001:01:FR:HTML

12.2.2. Measures for the prevention of terrorist attacks

12.2.2.1. Transmission of information

12.2.2.2. Deployment of security escorts on flights

- Framework Decision no. 2002/475/JHA of the Council of the European Union, of the 13th of June 2002, on combating terrorism.

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:ES:NOT

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:EN:NOT

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:FR:NOT

12.2.3. Measures for combating illegal migration

12.2.3.1. Sending document advisors

12.2.3.2. Support in cases of repatriation

- Council Decision of the 29th of April 2004 on the organisation of joint flights for removals from the territory of two or more Member States, of third-country nationals who are subjects of individual removal orders 2004/573/EC.

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0573:ES:NOT

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0573:EN:NOT

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0573:FR:NOT

- Council Directive 2003/110/EC of 25 November 2003 on assistance in cases of transit for the purposes of removal by air

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0110:ES:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0110:EN:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0110:FR:HTML

12.2.4. Other forms of cooperation

12.2.4.1. Joint patrols and other forms of joint intervention

12.2.4.2. Border crossing

12.2.4.3. Assistance in connection with major events, disasters and serious accidents

- COUNCIL RESOLUTION of 29 April 2004 on security at European Council meetings and other comparable events (2004/C 116/06).

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:116:0018:0019:ES**:PDF**

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:116:0018:0019:EN**:PDF**

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:116:0018:0019:FR**:PDF**

12.2.4.4. Cooperation upon request

12.2.5. Provisions on the protection of personal data

12.2.5.1. Definitions

12.2.5.2. Level of data protection

12.2.5.3. Principle of a link to the purpose and other limits to data use and processing

12.2.5.4. Guarantees of accuracy, current relevance and storage time of data

12.2.5.5. Technical and organisational measures to ensure data protection and data security

12.2.5.6. Documentation and registration

- **European Parliament and Council Directive 95/46/EC 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**

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML

- Council Framework Decision 2008/977/JHA of 27 November 2008on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:es:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:fr:PDF

13. The partial incorporation of the Treaty of Prüm into the legal framework of the European Union

13.1. Decision 2008/615/JHA

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:ES:NOT

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:EN:NOT

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:FR:NOT

13.2. Decision 2008/616/JHA

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:FR:PDF

14. The principle of availability in the Stockholm Programme

- The Stockholm Programme

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:es:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:fr:PDF

- Action plan implementing the Stockholm Programme

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:FR:PDF

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the 25th of January 2012 on "Safeguarding privacy in a connected world. A European data protection framework for the 21st century"

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:FR:PDF

15. Criminal records

15.1. Introduction

15.2. Framework Decision 2008/675/JHA

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:220:0032:0034:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:220:0032:0034:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:220:0032:0034:FR:PDF

15.3. Framework Decision 2009/315/JHA

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0023:0032:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0023:0032:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0023:0032:FR:PDF

15.4. Decision 2009/316/JHA

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:ES:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:EN:PDF

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:FR:PDF

Annex: Other documentary resources available in English or French

- **BALZACQ, Thierry**: *The Treaty of Prüm and the Principle of Loyalty (art. 10 TEC)*. Centre for European Policy Studies IP/C/LIBE/FWC/2005-08.

- **BALZACQ, T., BIGO D., CARRERA S., GUILD E**.: *Security and the two level game. The Treaty of Prüm, the EU and the Management of Threats*. Centre for European Policy Studies no. 234. January 2006.
  http://www.ceps.be/book/security-and-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats

- **BELLANOVA, Rocco**: *The "Prüm Process: "The Way Forward for EU Police Cooperation and Data Exchange?*
  http://vub.academia.edu/RoccoBellanova/Papers/603598/The_Prum_Process_The_Way_Forward_for_EU_Police_Cooperation_and_Data_Exchange

- **BIGO, D. et al**.: *The principle of information availability.* (there is a French version) http://www.libertysecurity.org/article1376.html

- **BUNYAN, Tony**: *The principle of availability*. Statewatch, December 2006.
  http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf

- **GUILD E., GEYER, F.:** *Getting local. Schengen, Prüm and the dancing procession of Echternach: Three paces forward and two back for EU Police and judicial cooperation in criminal matters.*
  http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=122940

- **JONES, Chris:** *Implementing the "principle of availability": The European Criminal Records Information System The European Police Records Index System The Information Exchange Platform for Law Enforcement Authorities*
  http://cadmus.eui.eu/bitstream/handle/1814/6401/LAW-2006-32.pdf?sequence=1

- **VERVAELE, John A.E. :** *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?*
  http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/1/1
  Translation into Spanish updated in 2007:
  http://igitur-archive.library.uu.nl/law/2012-0104-200403/Vervaele%20Terrorismo2008.pdf

- **ZILLER, Jacques**: *Le Traité de Prüm. Une vraie-fausse coopèration renforcée dans l'espace de sécurité, de liberté et de justice*.
  http://cadmus.eui.eu/bitstream/handle/1814/6401/LAW-2006-32.pdf?sequence=1