



***STUDY ON RAPID INFORMATION EXCHANGE  
ON COUNTERFEITING AND PIRACY***

August 2010



This report / paper was prepared for the IDABC programme by:

- Time.lex
  - Jos Dumortier,
  - Geert Somers,
  - Boris Tshiananga,
- Siemens
  - Eric Meyvis,
  - Kaïs Bachraoui,

## Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

© European Communities, 2010

Reproduction is authorized, except for commercial purposes, provided the source is acknowledged.

## Executive summary

The global explosion in counterfeiting and piracy has created one of the most serious problems facing world business.

Within the EU Member States, multiple operational enforcement agencies are responsible for the fight against counterfeiting and piracy. Therefore, a systematic and organized way to share information appears to be vital for more effective actions in this field. However, currently, information flows and actions are not always synchronised.

This study aims to provide an up-to-date inventory and comparative assessment of existing and planned e-government initiatives at national and European level and a sound assessment of actual needs for administrative cooperation and information sharing on counterfeiting and piracy between administrative and operational enforcement agencies from different Member States.

Section B examines a non-exhaustive list of notable systems in order to determine if they are usable at EU level, as a EU wide system or can be connected to a EU wide system. Additionally this section helps determining what features:

- are useful for the rapid exchange of information on counterfeiting and piracy, and
- should be present in any cross-border EU system serving this purpose.

Section C provides a more general comparative assessment.

Section D offers conclusions and recommendations.

The annexes contain more details and comparative charts on all the systems that have been reported.

One important note: due to the nature of the information held by the law enforcing authorities active in the area of counterfeiting and piracy, these authorities are reluctant to share information with other law enforcement authorities active in the area of counterfeiting and piracy. Therefore the information exchange systems currently available mostly cover only their own policy area, e.g. only customs, only police or only market surveillance, etc. Information exchange between these policy areas therefore mostly happens through ad-hoc requests to one another by classic means like fax and email. IT-based systems are mostly reserved to only one policy area.

### Section B: Most promising projects and trends.

- Austrian Ministry of Finance's FINDOK & ELAK systems are systems that exchange financial information with the aim of coordinating the Ministry of Finance and Customs.
- AIDA is the Italian customs framework. Falstaff is a database bringing together data from customs with technical data from the right holders with the aim of identifying counterfeited products.

- NIPIES is the Bulgarian national system for exchange of information in the area of copyright and related rights and industrial property and aims at coordinating law enforcement actions regarding counterfeiting and piracy.
- PATJA is the database of the Finnish police and addresses the problem of counterfeiting and piracy. Its purpose is to coordinate law enforcement actions regarding counterfeiting and piracy.
- VINCI is an intranet-tool of the Polish customs. It is intended to facilitate the internal coordination of law enforcement actions and has some advanced features.
- ZGR online 1.0 is the system of the German customs authority used for IPR enforcement and aims at coordinating law enforcement by the German customs authorities.
- ZGR online 1.1 is a tool for the evaluation of measures taken in the fight against counterfeiting and piracy. Its aim is to improve the statistical evaluation. However, this system is still being implemented.
- COPIS is an EU-wide information exchange system for all customs operations and is addressing inter alia counterfeiting and piracy by facilitating the information exchange. The system is still under development.
- IMI is an EU-wide electronic tool for the exchange of information. At present, it is not active in the counterfeiting and piracy area. It has been designed to support multiple areas of internal market legislation.
- RAPEX is an EU-wide rapid information exchange system for non-food consumer products. It addresses the circulation of unsafe products by establishing a notification system regarding dangerous products. Dangerous products often concur with counterfeit.
- eMage/eMarks is a cross-border image based trademark search engine. It has unique features but currently lacks funding and is therefore not in use.

### Section C: Comparative assessment.

There are two groups of users of information exchange systems on counterfeiting and piracy:

1. The group of law enforcers consists of customs authorities, police, border police, public prosecutors, competent courts, anti-fraud authorities, consumer safety authorities, tax, fiscal and market surveillance authorities. This group exchanges intelligence resulting from investigations and information originating from company or consumer complaints. The exchange is usually done on a case-by-case basis;
2. The group of administrative IP-authorities and right holders provide technical data for the law enforcers group by means of registers and databases from the national IP offices and right holders organisations.

As mentioned before the cross-policy information exchange between distinctive authorities seldom happens through IT-based systems. Such exchange of information is mostly performed through classic means like fax and e-mail.

Most Member States do not have legal barriers for the exchange of information on counterfeiting and piracy. The amount of institutions involved in the fight against counterfeiting and piracy is very large and Member State institutional frameworks may be very different.

Furthermore most Member States do not have any policymaking documents on rapid information exchange on counterfeiting and piracy.

However several Member States are aware of the issue of piracy and counterfeiting and do have policy documents describing action plans or guidelines addressing intellectual property matters and the fight against counterfeiting and piracy. Only a few of these address explicitly the international exchange of information.

#### Section D: Conclusions and Recommendations.

There are several concrete requirements to facilitate more effective rapid information exchange:

- i) more information exchange across borders and across policy areas in order to coordinate effective countermeasures;
- ii) translation should be available;
- iii) rapid and direct notifications of IP infringements and detained goods;
- iv) pending applications for action should be consultable;
- v) more public private cooperation;
- vi) stronger authentication procedures;
- vii) IPR information searches at European level;
- viii) consumers should be able to contribute to the detection of counterfeits;
- ix) cooperation in the development of preventive measures should be improved;
- x) statistical tools.

The beneficiaries of a rapid information exchange system are the law enforcement institutions. These beneficiaries need information exchange at three levels:

- i) for cross policy cooperation;
- ii) for cross border cooperation and;
- iii) for internal coordination within policy areas.

In summary, there is a vital need for more regular, effective and speedier exchange of information cross policy and cross border in multiple forms and languages between Member States' enforcing authorities. To a lesser extent some Member States' law enforcement authorities could also improve their coordination within their own policy area by implementing more developed tools for the exchange of information, replacing the more common and traditional means of fax and e-mail.

The analysis of the results of the study leads to the conclusion that an EU-wide information exchange system would require the following features:

- i) peer to peer communication and information exchange, allowing exchange of information between law enforcement authorities at all levels;
- ii) standardised communication forms, in order to increase interoperability between different law enforcement authorities;
- iii) multilingual capabilities;
- iv) real time notifications, in order to coordinate actions;
- v) an information exchange platform for public and private cooperation;
- vi) a search function to easily identify the competent authority among the great number of users;
- vii) the exchange of audio-visual content, in order to identify counterfeit;
- viii) database integration allowing users to search different databases through a single interface.

Based on the features mentioned here above the most interesting system seems to be the IMI system.

It is considered that the national systems (e-mage, Falstaff, VINCI and NIPIES) seem not to be the best options for an EU wide deployment.

Both IMI and RAPEX offer notification systems. IMI could complement the existing notification systems for the IPR enforcing authorities and allow cross policy area notifications.

COPIS seems the most complete system but is still under development. Furthermore it will allow only access to the customs authorities. At present it is doubtful that custom authorities would consider allowing other law enforcing authorities having the same amount of access to their system. A realistic approach would be to connect the COPIS system to the IMI system. As a result COPIS could be complemented by the IMI system.

For these reasons it currently seems most advantageous to explore the implementation of IMI to improve the rapid information exchange on counterfeiting and piracy. IMI allows information exchange across borders and policy areas.

The absence of features such as:

- o the ability to upload audiovisual material, and
- o the ability to give access to private entities to upload technical data, and
- o the ability to integrate databases,

can all technically be resolved.

Through a predefined set of questions the IMI user would be allowed to request additional information directly to the competent authority. The current lack of database integration in IMI can be resolved in the same way. In addition it offers an alternative for information exchange for the coordination of law enforcing actions within a distinct policy area, without imposing its structure.

## **Table of Contents**

<b>Executive summary .....</b>	<b>3</b>
<b>Section A: General introduction .....</b>	<b>15</b>
1 Background.....	15
1.1 The IDABC Programme.....	15
1.2 Relevant information .....	16
1.3 Objectives, Scope and Expected Results.....	16
2 Content of this document .....	17
3 Purpose of the Study .....	17
4 Methodology.....	17
5 Preliminary remark: restricted access to information. ....	18
6 Reference documents at European level.....	18
<b>Section B: Most promising projects, trends and systems on the Rapid Information Exchange on Counterfeiting and Piracy. ....</b>	<b>21</b>
1 National Systems.....	21
1.1 Information exchange systems .....	21
1.1.1 Austrian Ministry of Finance’s FINDOK & ELAK systems (Austria) .....	21
1.1.2 FALSTAFF – AIDA (Italy) .....	23
1.1.3 NIPIES (Bulgaria). ....	25
1.1.4 PATJA (FINLAND) .....	27
1.1.5 VINCI (Poland) .....	29
1.1.6 ZGR Online 1.0 (Germany) .....	31
1.1.7 ZGR Online 1.1 (Germany) .....	32
2 European systems .....	34
2.1 COPIS (EU EC/DG TAXUD) .....	34
2.2 IMI (EU EC/DG MARKT). ....	36
2.3 RAPEX (EU EC/DG SANCO, DG ENTR).....	40

2.4	eMage–eMarks (cross-border).....	43
3	Informative systems .....	45
3.1	Portal GAC (Portugal) .....	45
3.2	Project Original (Czech Republic).....	46
<b>Section C: Comparative Assessment .....</b>		<b>48</b>
1	Main systems for information sharing .....	48
1.1	Information Exchange Systems and Databases .....	48
1.2	Informative systems .....	49
1.3	Users and the types of information exchanged .....	50
1.3.1	Law enforcement authorities .....	50
1.3.2	Administrative IP-authorities and right holders. ....	51
1.4	Formal and informal arrangements or cooperation .....	52
2	Policy framework. ....	53
3	Reference documents.....	54
<b>Section D: Conclusions and Recommendations.....</b>		<b>60</b>
1	Introduction.....	60
2	Concrete requirements to facilitate more effective rapid information exchange ...	60
3	Beneficiaries of a rapid information exchange system and levels of exchange.....	63
4	Assessment of needs .....	64
4.1	Existing information .....	64
4.2	Restrictions to access.....	65
4.3	Required Information .....	65
4.4	Conclusion .....	65
5	Recommendations .....	66
5.1	Required features of a EU wide information exchange system.....	66
5.1.1	Peer to peer communication and information exchange.....	66
5.1.2	Standardised communication forms. ....	66
5.1.3	Multilingual capabilities. ....	66
5.1.4	Real time notifications. ....	66
5.1.5	Information exchange platform for public and private cooperation.....	67
5.1.6	Authority/peer search function.....	67

5.1.7 Exchange of audio-visual content ..... 67

5.1.8 Database integration..... 67

6 Suitability for EU-wide implementation of the available systems..... 67

6.1 Recommendations for a European approach ..... 71

**Annex A: List of National Correspondents ..... 73**

**Annex B: System Inventory..... 74**

1 AUSTRIA..... 74

1.1 Findok: ..... 74

1.2 Elak-BMF:..... 74

2 BELGIUM..... 74

2.1 Several databases at different levels (FPS Economy, Customs, Federal police) ..... 74

2.2 ICCF/CICF ..... 74

2.3 AWF ..... 75

2.4 Watch system of the FPS Economy ..... 75

3 BULGARIA..... 76

3.1 NIPIES: ..... 76

4 CYPRUS ..... 76

4.1 THESEAS: ..... 76

5 CZECH REPUBLIC ..... 77

5.1 IPO ..... 77

5.2 AIP SYS ..... 77

5.3 Project Original ..... 77

6 DENMARK..... 77

7 GERMANY ..... 78

7.1 ZGR 1.0 ..... 78

7.2 ZGR online 1.1 ..... 78

7.3 Conlmit..... 78

8 ESTONIA ..... 78

8.1 Custom DB ..... 78

8.2 Databases of the IP office..... 79

9 FINLAND ..... 79

9.1 PATJA system ..... 79

9.2 The Customs Recordal ..... 79

10 FRANCE ..... 79

10.1 COPIS ..... 79

10.2 RIF ..... 80

11 GREECE ..... 80

11.1 AFIS ..... 80

11.2 RIF ..... 82

11.3 CEN-COM ..... 82

12 HUNGARY ..... 83

12.1 eMAGE ..... 83

12.2 COPIS ..... 83

13 IRELAND ..... 83

14 ITALY ..... 83

14.1 FALSTAFF ..... 83

15 LATVIA ..... 84

15.1 SRS ..... 84

15.2 State Register of Innovations; State Register of Industrial Designs; State Register of Semiconductor Topographies; State Register of Trademarks ..... 84

15.3 Integrated Information System of the Internal Affairs. .... 85

15.4 RAPEX ..... 86

16 LITHUANIA ..... 86

16.1 Anti-piracy centre. .... 86

16.2 DB of the National IP Office. .... 86

16.3 The cooperation Agreement ..... 86

17 LUXEMBOURG ..... 87

17.1 PLDA – COPIS ..... 87

17.2 SID ..... 88

17.3 RAPEX ..... 88

17.4 ICSMS system ..... 88

18 MALTA ..... 89

18.1 COPIS ..... 89

18.2	RIF .....	89
19	The Netherlands.....	89
19.1	DIS .....	89
19.2	EU FIDE .....	90
19.3	The Blue View System .....	91
20	POLAND .....	91
20.1	VINCI SYS .....	91
20.2	DP System .....	91
20.3	OC register .....	92
20.4	DKM portal.....	93
21	PORTUGAL.....	94
21.1	IGAC.....	94
21.2	PortalGAC.....	94
22	ROMANIA.....	94
22.1	Common DB.....	94
22.2	Trademarks office DB .....	97
23	SLOVENIA .....	99
23.1	IT support/solutions for IWG by SIPO .....	99
24	SLOVAKIA .....	99
24.1	Webregisters .....	99
25	SPAIN.....	100
25.1	OEPM (Spanish Patents and Trademarks Office) databases .....	100
26	SWEDEN.....	100
26.1	SACG Swedish Anti counterfeiting group.....	100
27	UNITED KINGDOM .....	102
27.1	UK IPID (Intelligence Hub).....	102
27.2	Serious organised crime agency (Programme 17).....	102
27.3	National fraud strategic authority .....	103
27.4	HM Revenue & C.....	103
27.5	Trading standards .....	103
27.6	PCeU .....	103
27.7	IpCass .....	104

27.8 MCPS antipiracy unit ..... 105

27.9 BPI Anti-piracy unit ..... 105

27.10 National IP initiative ‘real deal’..... 105

27.11 Joint memorandum understanding on an approach to reduce unlawful file sharing106

**Annex C: System Analysis .....108**

**Annex D: Comparative matrix of the national reports. ....117**

## Version History

Version/Status	Release Date	Comments
1.0		
4.2	18/02/2010	Document formatted, template updated, comments inserted
4.3	26/02/2010	Section two expanded, proposal to restructure, Section five restructured.
4.4	29/03/2010	Sections reorganised, Annex B
5.0	24/04/2010	Section B Completed
5.1	17/05/2010	Minor addition of content in Section A. Minor adjustments to lay-out and correction of typos in section B and C, Drafting of section D
5.3	09/06/2010	Redrafting section D, Adjustments to 3.4 of section C
Final	30/06/2010	Adjustments to all sections A,B,C,D and Annex A. Drafting of executive summary.
Final	14/07/2010	Update with the latest comments from DG MARKT; update of English language
Final	03/08/2010	Update with the final comments from DG MARKT. Some names corrected in Annex A.

## Distribution

Name	Organisation/Location	Copies	Action/Information


## Section A: General introduction

### 1 Background

Over the past ten years the global explosion in counterfeiting and piracy has created one of the most serious problems facing world business. Despite a growing general awareness of the problems being faced by consumers and business, local and national efforts to coordinate effective responses within Member States and across borders appear to be difficult.

On 16 July 2008, the Commission adopted a Communication proposing a series of measures regarded as being essential to the maintenance of a high quality system of industrial property rights for the EU in the 21st century. The Commission committed itself to explore solutions to establish an effective network for administrative cooperation between Member States to allow for Europe-wide actions.

Following this Communication, in September 2008, the Competitiveness Council adopted a Resolution on a comprehensive European Anti-counterfeiting and Anti-piracy plan. The Council invited the Commission to structure its work to fight against counterfeiting and piracy around a number of major themes. This included a call to set up a network to rapidly exchange key information by stepping up cross border administrative cooperation drawing on national contact points and modern information-sharing tools<sup>1</sup>.

Moreover, the Enforcement Directive (Directive 2004/48) approximates legislative systems to ensure a harmonised, high level of civil judicial protection in the internal market. In particular, Article 19 of the Directive foresees cooperation amongst Member States, including the exchange of information.

Within Member States multiple and diverse operational enforcement agencies are often responsible for the fight against counterfeiting and piracy. However, with the exception of customs authorities, information on IP violations is usually meagre and rarely exchanged. Even in the case of Customs, interactions often stop at the border. Therefore, a systematic and organised way to share information appears to be vital for more effective and meaningful actions in this field.

#### 1.1 The IDABC Programme.

The work described hereafter falls under the scope of Annex I B18 (administrative cooperation) of the IDABC Decision of the European Parliament and the Council of 21 April 2004 on the interoperable delivery of pan European e-government services to administrations, businesses and citizens (IDABC).

More information can be found on <http://ec.europa.eu/idabc/en/document/7802/5637>. The Study is part of the IDABC Work Programme under the entry 'Rapid information exchange on counterfeiting and piracy'.

---

<sup>1</sup> E.g.: COPIS, RAPEX etc....

Within this, the work carried out in parallel on the Internal Market Information System (IMI) should be used and should be closely coordinated with this Study, as this could be a useful infrastructure for interoperable cross-border electronic information exchange.

The framework contract that formed the basis for the study is: “Security consultancy and assessment services for European eGovernment services (ENTR/ 05/058)”

## 1.2 Relevant information

The Study takes into account and builds on existing work and activities by the Commission Services as well as EU Member States.

## 1.3 Objectives, Scope and Expected Results

### **The overall objective of the Study is:**

The identification and assessment of a wide range of existing e-government systems and initiatives at national and European level for the exchange of information on counterfeiting and piracy and on related issues (e.g. dangerous products, customs, and market surveillance).

This Study will also entail the relevance and applicability of security policy developments, including issues of identification, authentication, access controls and authorisation, data integrity, confidentiality, availability.

### **The specific objectives of the Study are to:**

- Identify and describe existing e-government practices and networks, future plans and initiatives, at national level and European level, employed for the sharing of information and/or intelligence on counterfeiting and piracy, including all sector specific systems in related policy areas e.g. customs, dangerous products, market surveillance.
- Provide a structured overview of the key users of these networks as far as they are involved in combating counterfeiting and piracy, including the data these users access/enter/exchange in view of determining gaps and potential areas of overlap.
- Assess the suitability of the existing networks to serve the objective of stepping up administrative cooperation and effective enforcement actions in the area of counterfeiting and piracy across borders.

### **Deliverables the Study provides:**

- An up to date inventory and comparative assessment of existing and planned e-government initiatives at national and European level for information sharing on counterfeiting and piracy and on related issues (customs, dangerous products, market surveillance);
- An up to date and sound assessment of actual needs for administrative cooperation and information sharing on counterfeiting and piracy between administrative/operational enforcement agencies from different Member States.

## Scope

The geographical scope of the Study includes the EU-27 and 4 Commission DG's (SANCO, TAXUD, ENTR and MARKT).

The domains to be investigated concern counterfeiting and piracy and the related issues in the following 3 areas: Customs, dangerous products and market surveillance.

## 2 Content of this document

This document contains the results of the Study on rapid information exchange on counterfeiting and piracy and an assessment and recommendations for the EC. The information collected in this report is based on the responses we have received to questionnaires that we sent to our national correspondents and to contact points at the EC.

Our correspondents reported back to us that some governments were reluctant to cooperate in this study because of the nature of the information exchanged by them. That's why there are sometimes significant discrepancies in the amount of information submitted on the information systems of the Member States. Furthermore four DG's, TAXUD, ENTR, SANCO, MARKT were contacted in the course of this Study, with a view to the IT systems run by them<sup>2</sup>.

Only DG MARKT gave a profound explanation of the IMI system. The amount of information received from the other DG's was rather limited. Therefore information on the other European Systems is generally based on information we received from our national correspondents and information publicly available.

## 3 Purpose of the Study

The findings of the Study should provide the European Commission with a thorough, comprehensive and operational inventory and assessment, including both legal and technical requirements, enabling it to further identify the appropriate solution to facilitate the secure and swift exchange of strategic information on counterfeited and pirated products and services among Member States. This information exchange is of vital importance because counterfeited and pirated products may also be very harmful to the health of our citizens, may undermine our economy and may pose a threat to our overall security.

The outcome of this Study will be used in the context of reporting back to the Commission on progress made on the issues at stake and the analyses of the need for further policy initiatives on combating piracy and counterfeiting.

## 4 Methodology

Many systems seem to be valuable in the light of this study on the rapid information exchange on counterfeiting and piracy. Therefore a number of notable systems have been selected to be examined in section B of this Study, in order to determine their usability at a European level, their usability as a European wide system or their ability to connect to a European wide system for rapid information exchange on counterfeiting and piracy.

---

<sup>2</sup> COPIS (TAXUD), RAPEX (SANCO and ENTR), IMI (MARKT)

Learning what features are useful and should be present in any cross-border EU system for the rapid exchange of information on counterfeiting and piracy is an additional goal of this section.

In section C a more general comparative assessment is made. Finally, in section D conclusions and recommendations are formulated. The annexes contain more detailed information on all the systems reported back to us. The annexes also contain comparative charts on the available systems.

## 5 Preliminary remark: restricted access to information.

It is important to mention that on the matter of exchange of information in the fight against counterfeiting and piracy there are restrictions for accessing the information as well at national level as across borders. This has to do with the limited access that authorities grant each other, in particular because of data protection rules. Consequently, if an authority cannot access certain information directly in the database containing it, because for instance it is a database of another authority with restricted access, one authority has to request information from another administrating authority of that database.

The reason for such restrictions being that often the information that needs to be exchanged in counterfeiting and piracy cases is to be found in criminal files, police files, tax files, files from the market surveillance authorities, customs files and applications for actions held by the IP enforcing authorities. This information is mostly confidential and is considered as 'intelligence'. It is therefore only disclosed on a need-to-know basis.

Moreover, access to information of other national authorities is often not allowed across borders.

Registers and databases of other national IP offices, finally, are generally available but there can also be restrictions.

For the abovementioned reasons there is a wide variety of types of information and filetypes that cannot easily be exchanged. Consequently most national authorities have their own information exchange systems, e.g. a customs information system for customs operations only accessible to customs officials or a police site that allows very limited access to other authorities. Therefore cross border and cross policy information exchange is currently mainly performed through decentralised, occasional, informal and cooperative connections, via traditional means of communication like e-mail and fax.

## 6 Reference documents at European level

The legislative and other official documents adopted at European level are the most important reference documents for this Study.

Council Regulation (EEC) N° 2913/92 of 12 October 1992	Regulations establishing the Community Customs Code
--	---

Commission Regulation (EEC) N° 2454/93 of 2 July 1993	Regulation laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code
Council Regulation (EC) N° 2100/94 of 27 July 1994	Regulation on Community plant variety rights, articles 90 – 91.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995	Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Council Regulation (EC) N° 515/97 of 13 March 1997	Regulation on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters
Council Act 98/C 24/01 of 18 December 1997	Act drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations (the “Naples II Convention”)
Commission Decision of 28 April 1999	Decision establishing the European Anti-Fraud Office (OLAF)
Council Decision 2002/187/JHA of 28 February 2002	Decision setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p.1) as amended by the Council Decision 2003/659/JHA of June 18 2003 (OJ L 245, 29.9.2003, p.44) and by Council Decision 2009/424/JHA of 16 December 2008 (OJ L 138, 04.06.2009, p. 14)
Council regulation (EC) N° 1383/2003 of 22 July 2003	Regulation concerning action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, O.J.L. 196/2003, p.7
Regulation (EC) N° 882/2004 of the European Parliament and of the Council of 29 April 2004	Regulation on official controls performed to ensure the verification of compliance with feed and food law, animal health and animal welfare rules, articles 35 – 36.
Directive 2004/48/EC	Directive of the European Parliament and the Council on the enforcement of intellectual property rights
Commission Decision 2004/418/EC of 29 April 2004	Decision laying down guidelines for the management of the Community Rapid Information System (RAPEX) and for notifications presented in accordance with Article 11 of

	Directive 2001/95/EC
Commission Regulation (EC) N° 1891/2004 of 21 October 2004	Regulation Laying down provisions for the implementation of Council Regulation (EC) No. 1383/2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, as modified by Regulation N°1172/2007 of October 2007
Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005	Directive concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the council and Regulation (EC) No 2006/2004 of the European Parliament and of the council ('Unfair Commercial Practices Directive') (Text with EEA relevance), OJ L 149, 11.6.2005; p. 22-39
Council Regulation (EC) N° 510/2006 of 20 March 2006	Regulation on the protection of geographical indications and designations of origin for agricultural products and foodstuffs
Council framework Decision 2006/960/JHA of 18 December 2006	Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
Council Resolution 2009/C 71/01 of 16 March 2009 on the EU Customs Action Plan to combat IPR infringements for the years 2009 to 2012	Resolution on the EU Customs Action Plan to combat IPR infringements for the years 2009 to 2012.

## Section B: Most promising projects, trends and systems on the Rapid Information Exchange on Counterfeiting and Piracy.

This chapter provides an overview of interesting IT-systems present in EU Member States. The overview is divided into three distinct sub-sections. The first sub-section looks at national systems for information exchange (1.1.1 to 1.1.7). The second sub-section considers European information exchange systems (2.1 to 2.4), while sub-section three looks at wider systems that merely collect information and inform on issues surrounding counterfeiting and piracy (3.1 to 3.2). These are primarily information systems providing portals and websites.

We refer to annex A for a full overview of the systems available, as reported by our correspondents, within the EU Member States. The systems presented hereunder were selected because of their interesting characteristics in relation to the study. More IT-systems are available within the EU; these were however not included in this section because they had more or less similar features as the ones presented below, or because we were not aware of their existence due to the unavailability of information. Therefore, this is a non-exhaustive list.

### 1 National Systems

#### 1.1 Information exchange systems

##### 1.1.1 Austrian Ministry of Finance's FINDOK & ELAK systems (Austria)

**The Austrian Federal Ministry of Finance (BMF)** - The project of the BMF consists of two systems: Findok & ELAK (ELEktronischer AKt des BMF). These are systems that exchange financial information supplied by the Ministry of Finance and can be used in the fight against piracy and counterfeiting. Since most of the systems involved in the fight against piracy and counterfeiting are customs related or law enforcing information exchange systems, it seems interesting to take a closer look at how an information system exchanging more general financial information can be utilised in the fight against counterfeiting and piracy. Moreover the Austrian country report suggests these systems are a good example of efficiently integrated information systems.

#### **A. Findok**

**Legal basis** - Austrian authorities are obliged to provide administrative assistance in accordance with article 22 of the Austrian constitution. In practice, informal arrangements are established in case of regular information exchange between the authorities concerned.

**Addressed problems** - Internal coordination of the Ministry of Finance and Customs.

**Purpose** - Findok is the legal and financial information system for the Austrian Ministry of Finance.

**Type of information exchanged** - Findok provides information on interpretation guidelines of the Ministry of Finance, administrative decisions of the customs service and tax office and case law.

**Institutions involved in governing the system** – Austrian Ministry of Finance

**Institutions involved in providing the information** – The Austrian Ministry of Finance, customs service and tax offices and the independent Tribunal for Tax and Custom Law.

**Users** – There are two categories of users:

1. The general public has online access without any procedure, but internal documents are not accessible.
2. Civil servants of the BMF and the Customs service have access as part of the ICT environment of the Ministry of Finance with user identity and password.

**Functionalities and features** – The Findok system consists of a document retrieval system in an intranet infrastructure. The public has limited access to documents through an internet browser. Feedback via e-mail or social web tools is possible.

**Benefits, drawbacks & remarks** - It is an efficient way of distributing all relevant documentation but the mark-up for semantic search is insufficient. Also, the national privacy rules can be a legal barrier for FINDOK. However the privacy rules are applicable on all information exchange systems.

**Potential interoperability and suitability** - The actual interoperability is too limited. Only civil servants of the BMF itself have full access, other authorities have only access to the publicly available information. For more detailed information, administrative assistance of the BMF needs to be requested. Furthermore, there is only one source of information, the Ministry of Finance. Other stakeholders cannot add relevant documents or information. Therefore Findok should not be addressed as an information exchange system but merely as a tool for internal distribution of information. Without proper adaptation it is not suitable for rapid exchange of information.

**Needs** – Allow other authority officials to access the information in a direct manner. Allow stakeholders to add data.

## **B. ELAK**

**Legal basis** – Austrian authorities are obliged to provide administrative assistance in accordance with article 22 of the Austrian constitution. In practice, informal arrangements are established in case of regular information exchange between the authorities concerned.

**Addressed problems** – Internal coordination of the Ministry of finance and customs.

**Purpose** – ELAK establishes electronic procedures and supports cooperative work within the Ministry of Finance.

**Type of information exchanged** – Tax and customs files.

**Institutions involved in governing the system** – Austrian Ministry of Finance

**Institutions involved in providing the information** – Austrian Ministry of Finance, Customs.

**Users** – Civil servants of the BMF and Customs service have access as part of the ICT environment of the Ministry of Finance with user identity and password.

**Functionalities and features** – ELAK consists of an electronic filing system with electronic procedures. It has groupware facilities. For more details: <http://www.digitales.oesterreich.gv.at/> .

**Benefits, drawbacks & remarks** – The Austrian country report indicates that the ELAK system is a very efficient and integrated system for the handling of all tax and customs files. The integration within the ICT-infrastructure and its electronic filing system allow rapid handling and interaction internally and with other ministries. Semantic mark-up is not properly implemented yet.

**Potential interoperability and suitability** – The actual interoperability is limited. Only the ministry of finance and customs are involved in providing information, other stakeholders have no access nor can they infuse data into the system. The country report suggests there is interaction with other ministries. However how this occurs is not stated. Also given that only civil servants of the ministry of finance have access to the system it can be assumed that access to the information by different stakeholders is very limited. In spite of the positive evaluation of this system by the Austrian country report there are not many indications of actual interoperability. On the contrary the system seems to offer merely basic functionalities. Nevertheless the report suggests the ELAK system is designed in accordance with Regulation 1383/2003. Moreover the integration of COPIS<sup>3</sup> into ELAK is planned.

**Needs** – Allow input from stakeholders. Allow access to more groups of users.

### 1.1.2 FALSTAFF – AIDA (Italy)

AIDA (**A**utomazione **I**ntegrata **D**ogane **A**ccise – Integrated Automation Customs and Duties) is the Italian customs framework. Falstaff (**F**ully **A**utomated **L**ogical **S**ystem **A**gainst **F**orgery **F**raud) is a database bringing together data from customs with technical data from right holders in an efficient way.

**Legal basis** – AIDA and FALSTAFF are based on a very clear legal framework.

Art. 4, paragraph 54, of the Law 350/03 sets forth the implementation of a database, kept by the customs authority, aimed to collect data able to individual products to be protected against counterfeiting.

---

<sup>3</sup> see supra.

**Addressed problems** – The identification of counterfeited products in regard to customs operations.

**Purpose** – The purpose is to create a database with technical data of original products that need to be protected against counterfeiting.

**Type of information exchanged** – Technical information about a wide variety of food, consumer and industrial products that may be counterfeited. For more details: <http://www.agenziadogane.it/wps/wcm/connect/ee/HomePageEn/Falstaff/About+Falstaff/>

**Institutions involved in governing the system** – Customs

**Institutions involved in providing the information** - The (central) customs agency.

The database is inserted in the system AIDA and is fed by the respective right holders. The database is also integrated into the Customs Circuit of control that analyses in real time all import and export declarations submitted to the customs offices.

**Users** - Users are authorised to use the system after registration in the AIDA-portal and personal verification of the user's identity by the officials of the Customs authority.

Following categories of users are recognised by the system:

- Customs agency
- Customs offices
- Ministry for Economic Development
- Companies/producers
- Private entities and associations
- Consumers

**Functionalities and features** – Every time rights holders need protective intervention by customs they can generate an entry in the database.

Users can interact with the Falstaff database through the AIDA system. This ICT- system of the Italian customs analyses the processes and flows of information. AIDA also guides the user in the fulfilment of the different steps in generating an entry into the database.

The AIDA system not only allows the integration of information databases for a fast analysis of the risks of the goods that go through the customs. It also supports interoperability between customs and other entities involved in the clearance of these goods with the aim to have a “single window approach”.

Furthermore it integrates the ICT services of customs with those of the Italian harbours and airports. It allows managing all customs flows, thus having a unique ICT-based tool that incorporates data such as country of destination and of origin, quality and quantity of products, etc.

**Benefits, drawbacks & remarks** – Since each entry contains all technical information about the product, comparison with the suspected counterfeited products is possible in real time.

It is notable that producers can also play a proactive role by applying for action if they suspect that counterfeited products will be imported.

A drawback regards the acceptance of documents of foreign origin.

The Italian approach to counterfeiting and piracy is essentially driven by the intention to prevent foreign products that infringe Italian brands from entering the country and being distributed. This is basically built on top of the assumption that a certain number of countries in the world (China, Turkey, South American countries, etc.) have many factories specialised in counterfeiting and piracy. To a certain extent this assumption is certainly true, but it does not take into account that often counterfeiting and piracy also originate in Italy itself and are detrimental to Italian and foreign brands.

**Potential interoperability and suitability** – This system seems adequate for the fight against counterfeiting and piracy. It addresses the problem of counterfeiting and piracy by distributing information on possible counterfeit of a wide variety of products. The right holders, important stakeholders, are involved in the detection, reporting and identification of counterfeiting and piracy and can apply for action. Furthermore information is exchanged in real time with the customs officials at the borders, harbours and airports. All this information is made accessible through a single intranet interface. Therefore this system addresses the problem of counterfeiting in an efficient and suitable way. Interoperability with a European system should be possible since the system seems compatible with e-customs tools of other countries and is consistent with EC law.

**Needs** – The report states that the system does not allow international documents to be recognised. Furthermore, the report suggests the Italian authorities may want to add focus on inland counterfeiting.

### 1.1.3 NIPIES (Bulgaria).

NIPIES is the Bulgarian National System for exchange of information in the area of copyright and related rights and industrial property. It has been operational since 2005.

**Legal basis** – There is no known reference in the legal framework to this system but decision n° 42 of January 2006 of the Council of Ministers established the Council for the Protection of the Intellectual Property. This inter-institutional council manages the administration, maintenance and development of NIPIES.

**Addressed problems** – The NIPIES system addresses the trade of counterfeited goods and piracy.

**Purpose** – This system intends to facilitate internal coordination of law enforcement actions regarding counterfeiting and piracy.

***Type of information exchanged*** – The system consists of a database with information from the registers of the IP Office & Ministry of Culture and information on infringements collected during inspections by the Customs Agency.

NIPIES contains detailed information on protected goods, for instance patents, trade marks, industrial designs, copyright objects etc..... Furthermore it contains an application for the registration of goods that need to be protected, the carriers of these goods and the production, import and/or export of these goods.

***Institutions involved in governing the system*** – The inter-institutional Council has been established especially for the development and management of NIPIES.

The technical development and maintenance is generally performed by the IP Office.

Every other institution that uses the system is responsible for maintaining its own equipment and servers, which are used for access to NIPIES.

***Institutions involved in providing the information*** – The sources for NIPIES are the IP Office, the Ministry of Culture and the Customs Agency.

***Users*** – The main groups of users of the National System comprise:

- Law enforcement institutions like the Customs Agency, the Ministry of Home Affairs .
- Other State institutions that have been involved in a later stage like the Ministry of Justice, Ministry of Economics and Energy, Ministry of Agriculture and Forests and the Competition Protection Commission.
- Users of the publicly available part of the system like right holders or other interested parties. The publicly available information is limited.

In regards to the maintenance of the system, there are administrators responsible for the central servers located at the IP Office and administrators for the servers of each institution involved and for the access of the respective officials.

Not all users have the same authorities. Users can have the right to enter new information in NIPIES or solely access information. For instance, the officials of the Ministry of Home Affairs use NIPIES only as a source of information but do not enter any data in its databases.

***Functionalities and features*** –The system consists of two major components:

1. Databases which cover information provided by the registers kept by the IP Office & the Ministry of Culture. This information is much more detailed compared to the information available in the public version of those registers. The system also contains an application for the registration of goods that need to be protected, the carriers of these goods and the production, import or export of these goods.

2. Information provided by the Customs Agency about the inspections performed by its officials and the detected infringements of IP rights. Customs officials are enabled to enter information about the applications for execution of border measures, information about detained goods that refer to the information about the respective infringed IP rights and their objects.

**Benefits, drawbacks & remarks** –The system is an easily customisable tool for sharing information on piracy and counterfeiting.

On the other hand, the NIPIES system, launched in 2005, has not yet been adapted to the new Bulgarian e-government technical standards, adopted in 2008<sup>4</sup>. As a consequence it does not comply with all technical standards and rules for identification, exchange of information between the administrations, interoperability, information security, etc.... Furthermore, financing is an issue because of the shared responsibility.

**Potential interoperability and suitability** – In general NIPIES seems to provide access to quite detailed databases and is developed as one centralised tool for rapid exchange of information for all stakeholders. All institutions responsible for the protection of IP rights are involved. It seems to be a very useful tool for law enforcement since customs information is joined together with detailed information from the IP Office & the Ministry of Culture on possibly counterfeited and pirated goods. This allows law enforcers to easily access detailed information when suspected counterfeit is detected. However, its functionality has not been improved since its initial development in 2005. There is also no direct input from right holders. Nevertheless, this system seems suitable for the rapid information exchange on counterfeiting & piracy and seems to be a textbook example for interoperability in the area of counterfeiting & piracy.

**Needs** – Adaptation to the new e-governance technical standards would facilitate the possible integration into a wider European system. Possible improvements of the system could be the enrichment of content by right holders & some of the other institutions, e.g. applications for action by the right holders, reporting of suspected counterfeit & piracy products by the right holders, uploading of pictures and video, allowing other institutions to enter information collected during the performance of their functions. Beside these improvements, a clearer financial framework would benefit the development & maintenance of the NIPIES system.

#### 1.1.4 PATJA (FINLAND)

PATJA is the database of the Finnish Police Affairs. The database addresses the problem of counterfeiting and piracy but covers also other police matters.

<sup>4</sup> Electronic Governance Act, valid as of 13 June 2008, State Gazette, issue 46 of 12 June 2007, last amendment promulgated in State Gazette, issue 82 from 16 October 2009.

**Legal basis** – There is no known reference in the legal framework to the system but several new acts and amendments of the current acts regarding the cooperation of the Police, Customs and Border Guard Authorities in the field of crime prevention, supervision and international cooperation came into force on 1 January 2010<sup>5</sup>. As a consequence of these changes the legislation gives a general view on the cooperation of the Police, Customs and Border Guard Authorities and provide a clear judicial base for the cooperation of these authorities.

**Addressed problems** – The system addresses counterfeiting and piracy amongst other police issues.

**Purpose** – Facilitate the internal coordination of law enforcement actions regarding inter alia counterfeiting and piracy.

**Type of information exchanged** – The system includes information on e.g. all requests for investigation submitted to the Police or the Finnish National Board of Customs (NBC), investigation memorandums and diaries and information of possible penalties in relation to the issues of counterfeiting and piracy.

**Institutions involved in governing the system** – Finnish Ministry of Home Affairs and the police department.

**Institutions involved in providing the information** – Officials of the Finnish Ministry of Home Affairs and the police department.

**Users** – Police, Customs and the Border Guard Service officials and certain officials of the Ministry of Home Affairs.

Users are designated by the NBC, local Police and the Border Guard Service. They are identified by user identification codes and passwords. The number of users is quite large. On April 2009 the system had 32 450 maintained user IDs.

The users are instructed and trained on how to insert information into the system.

**Functionalities and features** – Users are given detailed instructions and training on how to insert information into the system. Thereupon they can introduce information on, for example, identified counterfeits.

**Benefits, drawbacks & remarks** – Given the great number of users (32 450 user IDs), this is an efficient decentralised way of collecting information.

---

<sup>5</sup> Act on amendment of section 54 of the Police Act, 11. 9.2009/691; Act on amendment of the Customs Act 11.9.2009/690; Act on amendment of the section 19 of the Act on Handling personal information in Border Guard Service, 11.9.2009/689; Act on amendment of the Border Guard Act, 11.9.2009/688; Act on Co-operation of Police, Customs and Border Guard Authorities 11.9. 2009/687.

**Potential interoperability and suitability** – Despite the great number of users that can insert data into the system, the interoperability appears to be very limited. There is no input from the IP Office or the rights holders. These stakeholders could introduce more technical data and report suspected infringements. Also, considering the type of information that is exchanged, it can be assumed that this system is more of a police filing system accessible by multiple users than it is an information exchange system in the fight against piracy and counterfeiting. First of all, the system does not cover only counterfeiting and piracy but also other police issues. Secondly, some elements of the supposedly exchanged information are specific operational tools, e.g., investigation memorandums and diaries. Considering the PATJA system is a tool of the Finnish police forces, the suitability for the integration in a wider European system could be more complicated. The system most likely contains sensitive police data not pertaining to the issue of counterfeiting and piracy and could subsequently create confidentiality conflicts.

**Needs** – Separate the information on counterfeiting and piracy from other sensitive and confidential police information. Allow input from the IP office and right holders.

### 1.1.5 VINCI (Poland)

The Vinci system is an intranet tool of the Polish Customs. It was launched in 2008.

**Legal basis** – The Vinci project is a development of the Polish Programme of Copyright and related rights 2008-2010. More specifically the system is a realisation of a partial objective of the abovementioned policy framework: “Development of IT systems to support activities of the Customs Service of the Republic of Poland, the Border Guard of the Republic of Poland, the Police and the Public Prosecutor’s Office in fighting copyright related rights and other property rights infringements.”

**Addressed problems** – The system addresses the problem of piracy and the trade in counterfeited goods.

**Purpose** – It is intended to facilitate the domestic coordination of law enforcement actions by customs.

**Type of information exchanged** – The system exchanges electronic applications for action by the Customs authorities and information on goods detained and determined as infringing IP rights.

The system connects all 16 Customs Chambers.

**Institutions involved in governing the system** – The Vinci system is managed by the Polish Ministry of Finance and the Polish Customs Chambers.

**Institutions involved in providing the information** - Customs authorities. In the future the Polish IP Office and the Ministry of Culture (with the implementation of the DP System)<sup>6</sup> will also provide information.

**Users** - The Regional coordinators of the Customs Chambers and regular customs officials. Users are designated by the Customs Chambers.

**Functionalities and features** - The system consists of four major functional modules: “Applications”, “Detentions”, “Reports” and “Administration”. The first two are the most important for the Study.

The “Applications” module pulls together electronic versions of applications for action by customs authorities, currently submitted to the Customs Chambers on paper only.

The “Detentions” module covers information on goods detained and determined as infringing IP rights. For every shipment of the goods detained, this module provides detailed information on the country of origin and destination, the exporter and importer according to the customs declarations, category of products and their value, right holders' information, information on the advancement of official actions and a history of inserts into case files.

The tool allows for uploading pictures and videos of protected and counterfeit goods (derived from several sources, e.g. applications for action by customs authorities, databases of national IP offices, the Office of Harmonization for the internal Market and of the World Intellectual Property Organization) and for linking them to relevant applications of the right holders and case files. Along the same lines, audiovisual recordings of the detention actions may be uploaded and managed through the application.

An interface with the database of the Polish IP office (DP system) is planned. This database pulls together all the information from all the registers<sup>7</sup> of the IP Office and the Ministry of Culture<sup>8</sup>.

Furthermore a program interface is under development, enabling right holders to apply for action by the customs authorities as suggested by Art 5(3) of the Regulation N° 1383/2003.

**Benefits, drawbacks & remarks** - Summarizing, the Vinci System is a particularly valuable and easily customizable tool for sharing information on actual detentions, applications for action by customs authorities and concomitant audiovisual materials.

Some distinguishing features were still in development at the moment of the drafting of the national report such as the integration of the DP system or the application for action by the right holders.

---

<sup>6</sup> See infra.

<sup>7</sup> Granted patents, industrial designs, trademarks, topographies of integrated circuits and geographical indications, information from the “bulletin and News of the IP office”

<sup>8</sup> The Optical carrier register of the Ministry of Culture is a database of all optical carriers manufactured in Poland.

**Potential interoperability and suitability** – The Vinci system appears to be a very efficient tool for the rapid exchange of information. Several sources of information are combined in support of Customs operations. Furthermore it has some advanced features, e.g. the possibility to upload audiovisual material. Although the number of groups of users is very limited, i.e. customs authorities, the number of stakeholders involved in providing information is very large, i.e. enforcement authorities, the IP Office, the Ministry of Culture. Furthermore, right holders will in the future be able to apply for action online. This results in an amalgam of multiple databases combining information allowing a more coordinated and effective law enforcement. The ease by which this system integrates with other databases suggests its suitability for interoperability with a wider European system such as the COPIS system.

**Needs** – The system needs to complete the planned improvements to reach its full potential. There is only a limited group of users that have access to the information, other groups involved in law enforcement, such as police officials, might benefit from access to the Vinci system and contribute in the fight against piracy and counterfeiting.

#### 1.1.6 ZGR Online 1.0 (Germany)

ZGR Online is the system of the German customs authority used for IPR enforcement. The necessary IT-infrastructure is hosted by the ZIVIT, which developed the *Zentrales Datenbanksystem zum Schutz Geistiger EigentumsRechte online* (ZGR-online 1.0). The ZGR-online 1.1, see infra, is still under development.

**Legal basis** – There is no known reference to the system in the legal rules.

**Addressed problems** – This system combats counterfeiting and piracy.

**Purpose** – Its purpose is the internal coordination of law enforcement by the German customs authorities.

**Type of information exchanged** – The system exchanges information on applications by right holders.

**Institutions involved in governing the system** – The system is governed by the German customs authorities.

**Institutions involved in providing the information** – The information is provided by the German customs authorities and the right holders.

**Users** – There are three different categories of users:

- Applicants: The right holders have the possibility to file and change applications online. The user administration consists of self-registration with manual activation of access by the Customs authorities.
- CRIME-users: These users are members of the customs authorities and process the applications of the right holders. The user administration of this user group consists of access, upon request to the authority.

- Users of the tool E-AGENT: employees of the federal financial administration. The user administration of this group is processed via LDAP-directory<sup>9</sup> and access is granted by the local LDAP-administrator.

**Functionalities and features** – The system contains three functions to enable the exchange of information:

- Electronic filing of applications (especially for border seizure) and modification of previously filed applications by the right holders at any time.
- Electronic processing of applications (CRIME).
- Information and research tool regarding electronic applications filed by the right holders (E-AGENT).

There is no platform for direct communication between applicants and CRIME-users. However both groups of users can see the relevant measures taken by the other group, i.e. the CRIME-users see changes in the applications or newly filed applications and the applicants can check the status of their pending applications.

**Benefits, drawbacks & remarks** – The advantage of the system is that right holders can file and change applications electronically and can access them at any time.

Also the responsible authority can easily and rapidly access the information on the electronic application of a right holder.

**Potential interoperability and suitability** – The system allows the electronic filing and processing of right holders' applications for action by customs authorities. The system seems to be suitable for the rapid exchange of information. Different authorities have access to the applications of the right holders and the system allows instant access to data. However, only the right holders can change the submitted applications. Furthermore the application is not joined together with available information from other authorities. This concludes that the ZGR online system is a useful tool for the processing of application but that it is lacking in more advanced features and therefore improvements to the system are recommended.

**Needs** – To be a more effective law-enforcement tool the system could put together the information provided by the right holders with databases and registers of the customs authorities and IP Office. Also, more advanced features like the uploading of audiovisual material is advisable. Furthermore, and connected to the abovementioned recommendations, the system should allow more groups of users to access and insert data.

### 1.1.7 ZGR Online 1.1 (Germany)

This system is still in an implementation phase. The system should become a tool in the evaluation of measures taken in the fight against counterfeiting and piracy. Since most of the systems in this section relate to the coordination of law enforcement, it is interesting to study a system with a different purpose.

<sup>9</sup> Lightweight directory access protocol; this is a computer application protocol for querying and modifying directory services.

**Legal basis** – There is no known reference to the system in the legal rules.

**Addressed problems** – This system combats counterfeiting and piracy.

**Purpose** – Its purpose is to improve the statistical evaluation.

**Type of information exchanged** – The electronic registration of seizures with automatic data transfer to the authorities responsible for investigation and evaluation (e.g. risk analysis). It serves to improve the statistical evaluation.

**Institutions involved in governing the system** – The system is governed by the German customs authorities.

**Institutions involved in providing the information** – The information is provided by the German customs authorities.

**Users** – The system is supposed to be used by the German customs authorities for the electronic registration of seizures with automatic data transfer to the authorities responsible for investigation and evaluation, i.e. the Federal Financial Administration. Therefore, there are two types of users identified by the system: users who register seizures and users who analyse statistical data. However, there is a third group of users identified by the system: the users of Info IPR<sup>10</sup> who will have access through an interface.

**Functionalities and features** – This system is supposed to comprise the following features:

- The electronic registration of seizures with automatic statistical recording. Seizure-data is implemented by the users. The system then automatically creates the relevant official forms.
- A database for statistical evaluation. The users have the possibility to perform statistical evaluations on a preset basis as well as free analysis of data.
- An interface with the system Info\_IPR. The data of ZGR-online 1.1. is collected and amended by the statistical data of the customs investigations service.

**Benefits, drawbacks & remarks** – Seizures are electronically registered and data is automatically transferred to the authorities for investigation and evaluation. This will result in an improvement of statistical evaluation.

**Potential interoperability and suitability** – Because the system is still in the implementation phase, many details are not available. However given the fact that the system is supposed to transfer data automatically in a standardised way, using official forms, it can be assumed that the system will be suitable for interoperability. This is confirmed by the projected compatibility with WCO's, Info\_IPR database. The system does not offer many advanced features but approaches the processing and evaluation of data in an interesting way, i.e. by automating statistical recording and allowing performance or statistical evaluations in an effective and rapid way.

<sup>10</sup> Info\_IPR: the information system on intellectual Property rights is a WCO initiative; It is a project for cooperation of customs authorities of the G8-states (still in implementation phase)

**Needs** – The system needs to be fully implemented.

## 2 European systems

### 2.1 COPIS (EU EC/DG TAXUD)

COPIS (**Common European IT System**) is an information exchange system for all customs operations and is addressing inter alia Counterfeiting and Piracy. The system is currently still under development. It is part of a wider project, the Multi Annual Strategic Project (MASP, former PLDA-project), which purpose is to create a paperless environment for customs in order to have a totally automated, interoperable, easily accessible and efficient system for all different procedures. The COPIS System should be operational by 2012.

**Legal basis** – Decision No 70/2008/EC of the European Parliament and of the Council of 15 January 2008 on a paperless environment for customs and trade, OJ 2008, No L 23, p. 21. The EC guidelines need to be implemented by the national authorities. Therefore changes to inter alia the national customs codes will be required.

**Addressed problems** – The COPIS system addresses, among others, the problem of counterfeiting and piracy.

**Purpose** – Its purpose pertaining, but not limited, to this study is to reduce fraud and reinforce the protection of intellectual property rights by creating an information platform containing information regarding counterfeiting and piracy and a communication platform facilitating the information exchange between the customs authorities of the Member States and the EC.

**Type of information exchanged** – The COPIS System will enable information exchange between the EC (DG TAXUD) and Member States with regard to 1) requests to intervene (for a rapid exchange of European requests to intervene) and 2) for restitutions of statistics.

**Institutions involved in governing the system** – The EC is responsible for the project which is implemented according to its guidelines with the contribution of Member States. This system will be supervised in the Member States by a national authority appointed by the Member States, which would be the contact point for all institutions involved in combating counterfeiting.

**Institutions involved in providing the information** – Information is provided by the customs authorities of Member States, most particularly services in charge of authorising requests to intervene and by customs officials during their inspections.

**Users** – The COPIS system should be composed of two parts 1) a part accessible to right holders in order for them to follow the procedure regarding the protection of their intellectual property rights in the case of a suspicion of fraud or of an infringement and 2) a part only accessible by the customs authorities. (e.g. national custom officials, customs administrations, the national appointed responsible authority, DG TAXUD, etc...)

Customs of each Member State will be able to introduce requests for intervention to other Member States but also to post information on the database of other Member States.

The users mentioned hereabove will also be able to interact with each other through the platform. However the functional and technical modalities are not determined yet.

Since the system is still under development, customs authorities have advised that the system should include authorised user identification.

**Functionalities and features** – The system will provide all necessary data to assist customs' officials during their profiling and risk analysis in their routine inspection of cargo and goods.

Moreover it appears that the different users/user groups will be able to upload information onto the system, which can then be made available to the other users of the system.

Right holders will be able to submit information into the respective file by uploading video-files of protected and presumed counterfeited goods. The available data derived from several sources will be updated with the right holder's customs application for action.

The authority introducing the information is the only one able to further modify it (e.g. requests to intervene). Customs authorities of other Member States will however be able to introduce additional information. Moreover the central database will be hosted by the European Commission (DG TAXUD).

The exchange of information will occur between customs' national coordinators (i.e. the appointed responsible authorities) and frontline customs officials on one hand, and between the right holders and the customs administrations on the other hand.

Customs authorities have advised that the COPIS system should be open to members of DG TAXUD, the national customs coordinators and the respective right-holders.

Furthermore, based on the information provided by the Member State customs authorities, the system allows the extraction of numeric information and the exchange of information between European customs authorities.

It is hoped that the COPIS platform will implicate all the institutions and stakeholders involved in the fight against counterfeiting such as members of customs, but also police etc. , through the national responsible authorities.

There is no information available regarding languages that the COPIS system will support and how these languages would be supported.

**Benefits, drawbacks & remarks** – An advantage will be that the exchange or request to intervene at European level will be instantaneous. The system facilitates regular updates by the stakeholders.

Also the up-streaming of trimestrial or annual national statistics will no longer be carried out manually but will be automatically generated by the database.

Furthermore the multitude of stakeholders will be focused towards the national contact points. Hereby increasing the available information.

**Potential interoperability and suitability** – Being still under development, COPIS aims at connecting existing and future national information systems involved in the fight against counterfeit and piracy in the customs area. It appears to be sufficient as far as it enables rapid information exchange. The different stakeholders will be able to submit and have access to necessary information for the enforcement of IPR. One of COPIS' requirements is that every Member State needs to appoint a national contact point coordinating all national institutions involved. These contact points are then connected to the COPIS database of DG TAXUD. This approach makes it possible to include the multitude of involved institutions and its respective information to be applied in the fight against counterfeit and piracy. As with all information exchange systems they are subject to national rules and requirements and require regular updating and maintenance.

**Needs** – Since the system is still under development it is not possible to determine its practical needs. If the objectives that have been stated can be met, COPIS will be a very effective tool in the fight against piracy and counterfeiting.

## 2.2 IMI (EU EC/DG MARKT).

The Internal Market Information system was developed by the European Commission & the Member States. It is an electronic tool that provides a system for the exchange of information. It does not address the problems of counterfeiting and piracy but it may be useful to investigate its suitability for interoperability in the area of rapid information exchange on counterfeiting and piracy. After all, it has been designed as a general system to support multiple areas of internal market legislation and it is envisaged that its use will be expanded to support further legislative areas.

**Legal basis** – Articles 8, 50 and 56 of the Professional Qualifications Directive<sup>11</sup> set out a clear obligation for Member States to cooperate actively and exchange information in the Professional Qualifications policy area. However, the way Member States exchange isn't determined. IMI is offered as a tool and can be used on a voluntary basis.

Articles 28 to 36 and recital 112 of the Services Directive<sup>12</sup> provide a legal basis requiring the Commission and Member States to develop and use IMI. In this policy area the use of IMI is mandatory.

Furthermore, IMI is a contribution to the eGovernment objective to provide efficient and effective government as set out by the IDABC programme.

<sup>11</sup> Directive 2005/36/EC on the recognition of professional qualifications

<sup>12</sup> Directive 2006/123/EC on the services in the internal market

IMI has been designed as a secure and data protection friendly system.

**Addressed problems** – IMI is addressing the problems of different working cultures and different languages within the EU. It is also addressing the lack of administrative procedures for cross-border cooperation and the lack of clearly identified partners in other Member States.

**Purpose** – The purpose is for Member States to engage in more effective day-to-day cooperation in the implementation of internal market legislation.

IMI aims also to overcome practical barriers, reduce administrative burdens and avoid proliferation of information systems.

Furthermore it is intended to lower the unit cost of the communication between Member States and supplement national frameworks in areas that cannot be adequately addressed by a purely national approach.

Finally, IMI helps to exchange and share information and knowledge, both within and across different policy areas.

**Type of information exchanged** – The type of information exchanged is flexible and depends on the policy area wherein IMI is active.

There are two workflows in the IMI system:

1. *One-to-one* exchange: In this case, information is exchanged between two authorities on request. This is done by sets of predefined questions and answers with clear guidelines. Additional sets of structured questions and answers can easily be defined for new policy areas. Free text communication may be included in the information exchange.
2. The other workflow is a *one-to-many* exchange. E.g. alerts. This means whenever needed, a message can instantaneously be broadcasted to all users involved in a certain issue. The alert workflow was developed to support article 32 of the Services Directive. This means that re-use of this workflow for another policy area would require additional development. Like the one-to-one information exchange, the alert complies with strict data protection rules. Once the identified risk no longer exists, the alert is closed and the details are no longer visible, six months after closure the alert is removed from the database.

**Institutions involved in governing the system** – The EC and the Member States are responsible for governing IMI. More specifically a steering committee provides overall guidance of the project. The end-users<sup>13</sup> are represented in the project steering committee by the responsible policy units in DG MARKT. Member State committees representing the different policy areas provide guidance on their specific areas of legislation and a user working

---

<sup>13</sup> See infra

group, (a subset of the Internal Market Advisory Committee) is responsible for horizontal issues. The system itself is supplied by DIGIT

***Institutions involved in providing the information*** – The EC and Member State authorities.

***Users*** – Registration is mandatory. However, at this moment there are still some security constraints. There is no EU-wide system of interoperable electronic identification yet. Still, this issue affects all information exchange systems and not just IMI. Ad-interim the Member States and national coordinators (see infra) are responsible for direct authentication of competent authorities in the system.

For now, administrations and competent authorities in the Member States and 3 EFTA countries (national, regional and local, public and private authorities) are the only registered users. ***It is not foreseen to provide access to private entities such as consumers or rights holders, however, an interface to allow such parties to submit information to IMI via forms might be envisaged but would require development.*** However, ECMT translation, an important feature of IMI<sup>14</sup>, is only available for public and private authorities due to legal constraints ***and would not be available for private entities.*** Furthermore the registration of private entities would be the entire responsibility of the involved authority

***Functionalities and features*** – The IMI system offers a single user interface to all 27 Member States and the 3 EFTA countries' administrations.

It is accessible via a standard web-browser (internet explorer, firefox,...), no deployment of software is needed in the Member States.

In order to overcome the language barriers IMI :

- Offers machine translation (ECMT) for free-text, in ten different European languages;
- Offers limited translation by file;
- Includes a pre-translated interface and sets of pre-translated questions and answers to support the required exchange of information in all official languages.;
- Allows reports to be printed in any language.

Considering the different administrative structures and cultures, IMI:

- Offers flexibility for Member States to organize themselves as they wish. There is no particular structure imposed so they can easily reflect their own structure;
- Includes a search function to identify the appropriate competent authority in the partner Member States. Prior knowledge of the administrative structure in another Member State is not needed in order to use IMI. The database of competent authorities can be searched thanks to a list of keywords submitted by each registered authority. Also, each Member

---

<sup>14</sup> See infra.

State needs to assign at least one national coordinator. If the search does not offer the desired result the inquirer can address these national coordinators.

In order to address the lack of administrative procedures for cross-border cooperation, IMI offers:

- A simple workflow procedure (consisting of 4 steps) to request information from another user;
- A structured exchange of information leading to greater predictability and transparency;
- An optional approval process of sent requests. This is an extension of the four steps when requesting information;
- An escalation procedure in case the provided information is not adequate.

Furthermore, IMI offers the facility to upload and store relevant additional documents or images.

Notifications with reference to the requests for information handled may be sent to any party involved by e-mail.

A high level of data security and data protection is required because the system will be used to exchange information about companies and private individuals.

Also, the European Commission provides a central helpdesk in support of the Member States and national coordinators.

IMI also allows to track requests and alerts that have been submitted for status check-up by the authorities involved. If needed a deadline procedure is possible. This can be a fixed deadline or the submitted request can contain a specified deadline.

**Benefits, drawbacks & remarks** – IMI is a tool that allows easy identification of relevant partners in other MS and reduces administrative burdens. The exchange of information at all levels of administration across Europe becomes possible.

IMI reduces the language barriers through structured and pre-translated screen information.

For these reasons, previously impossible areas of administrative cooperation now become available for administrative cooperation.

Furthermore, IMI creates benefits for the European Union:

- IMI provides information needed to assess the functioning of the existing rules;
- It acts as a platform for ensuring directives, which heavily rely on co-operation or mutual assistance, can be properly implemented;
- The system will provide much of the information needed to assess the functioning of the existing rules in a specific sector.

Benefits for the national Member States administrations:

- Cost savings through more effective structures for information exchange;
- Increased speed and quality of responses;
- Single relationship with IMI network instead of 351 bilateral relationships.

Benefits for the citizens and enterprises:

- IMI allows fast and constructive responses by administrations to assist cross-border activities and thus enable them to take advantage of Internal Market opportunities.

Benefits for other entities:

- IMI results in increased positive public relations, generated by a more accessible, efficient and customer responsive internal market;
- IMI is suitable for any DG managing legislation with an Internal Market legal basis that requires an information exchange system.

**Potential interoperability and suitability** – The IMI system seems to provide an efficient and extremely flexible tool for information exchange between the administrations of the different Member States. It could certainly be applicable in the fight against counterfeiting and piracy. It allows the connection of information networks with different organisational structures and allows the rapid information exchange between users in different languages. Furthermore it has been designed to support information exchange in multiple areas of internal market legislation and the expansion of its use is envisaged. Therefore, it seems that the IMI system is a suitable system for the Rapid Exchange of Information on Counterfeiting and Piracy.

**Needs** – IMI is an information system for the exchange of information between authorities. However involvement of the right holders is crucial in the fight against counterfeiting and piracy. Therefore it should be made possible for right holders to submit information.

### 2.3 RAPEX (EU EC/DG SANCO, DG ENTR)

RAPEX is a rapid information exchange system for non-food consumer products. It is a tool for efficient communication between enforcers and provides information to consumers on dangerous products. Its aim is to ensure that only safe products are placed in the European market. Despite the fact that the system does not address counterfeiting and piracy, it appears to be valuable to take a closer look at how it works as the system exchanges information on dangerous products which also include dangerous counterfeit products.

**Legal basis** – The legal framework of RAPEX can be found in the Directive on general product safety 2001/95/EC and the RAPEX guidelines issued by Decision 2004/418/EC.

**Addressed problems** – The circulation of unsafe products on the market or at the border.

**Purpose** – Its purpose is facilitating the detection of non-viable products by establishing an organised rapid information exchange system and a notification system regarding products, which have been considered as an immediate and major danger for the health and the security of consumers. Moreover, it tries to prevent the supply of these products to consumers and coordinates actions at a European level.

**Type of information exchanged** – The RAPEX system exchanges RAPEX notifications only on non-food consumer products, or products for professional use that can be purchased in a shop by a consumer.<sup>15</sup>

The notified products relating to dangerous consumer products are subject to measures ordered by national authorities or actions voluntarily taken by producers and distributors.<sup>16</sup> The notified products have to pose a serious risk to the health and safety of consumers.<sup>17</sup> The risk-assessment is performed by the national authorities. Only if there is evidence or reasonable suspicion that these products can be found on the markets of at least two countries participating in the system, information is exchanged through RAPEX.

Furthermore the RAPEX system exchanges other information<sup>18</sup> on dangerous products on which preventive or restrictive measures have been taken, e.g. information on products that present only a moderate risk or dangerous products, which nevertheless can't be correctly identified by national authorities.

**Institutions involved in governing the system** – RAPEX relies on a close cooperation between the EC and the national authorities of Member States. Each Member State must appoint or create a responsible authority for the market surveillance, which usually is the RAPEX contact point. The market surveillance authorities are granted the necessary powers to take measures in order to prevent or restrict the marketing or use of dangerous products.

**Institutions involved in providing the information** – The market surveillance authorities and law enforcement authorities within the EU Member States and the EFTA/EEA countries: Iceland, Liechtenstein and Norway.

**Users** – The national contact points and the European Commission are the only groups of users.

Authorization of the users is performed by user name and password. The national contact point is responsible for delivering passwords and user ID's. The access to the server is limited to some members of the national RAPEX contact points and European Commission. However,

---

<sup>15</sup> Most frequently noticed consumer products are: Toys, motor-vehicles, electrical appliances, lighting equipment, cosmetics, children's equipment, clothing and household appliances.

Consumer products that are excluded: Food, feed, medical devices and pharmaceutical  
Information about these products is exchanged through specific alert systems established at European Level. For example the Rapid Alert System for Food and Feed (RASFF) is used to exchange information about food and feed.

<sup>16</sup> E.g. sales bans, withdrawals of dangerous products from the market and recalls of dangerous products from consumers

<sup>17</sup> RAPEX notifications: Notification under article 12: notifications of measures ordered by the national authorities, or actions taken 'voluntarily' by producers or distributors in relation to products presenting a serious risk.

<sup>18</sup> Notifications under article 11: notifications of measures ordered by the national authorities in relation to products presenting a moderate risk.  
Notifications 'for information': notifications of measures ordered by the national authorities, or actions taken voluntarily by producers or distributors in relation to dangerous products, disseminated for information purposes due to insufficient product identification.

some information published by the European Commission is freely available on [http://ec.europa.eu/consumers/dyna/rapex/rapex\\_archives\\_en.cfm](http://ec.europa.eu/consumers/dyna/rapex/rapex_archives_en.cfm).

**Functionalities and features** – A server with restricted access (“the RAPEX server”) has been implemented by the European Commission in order to ensure the applicability and efficiency of this information system.

Member States can interact directly with each other, as well as with the European Commission.

When the competent authorities of a Member State take measures, according to national legislation, to prevent or restrict the marketing or the use of a product considered as dangerous, the RAPEX national contact point informs the European Commission through the RAPEX server.

The RAPEX contact points submit information about products using a standard notification form. This notification form includes details for the identification of the product, in particular its nature and characteristics, a description of the nature and scope of danger and the measures adopted to prevent risks and the distribution channels of the notified product.

Thereupon the Commission needs to validate the notification. It examines the information provided with regard to its completeness and its compliance with the general product safety Directive and the RAPEX guidelines. If the notification is validated, the information is forwarded to the national contact points of all the participating countries. These contact points forward the information to the national competent authorities, which then check if the notified product is present on the market. If necessary, appropriate action will be taken. The result of these market surveillance activities is then reported back to the Commission with possible additional relevant information.

Furthermore, economic operators are obliged to inform the authorities about dangerous products. To simplify this action, producers and distributors can use the online ‘Business Application’, developed by the Commission.

Every Friday, the European Commission publishes a weekly overview of the dangerous products reported by the national authorities online.

The contact points in the Member States may issue the notification in their national language and/or in English. The notifications will be translated into English, French, German, Italian and Spanish by the Commission.

**Benefits, drawbacks & remarks** – The system allows notifications to be rapidly exchanged to the involved authorities. The clear framework and procedures, especially the notification forms, facilitate the rapid information exchange. The commonly used notification-form allows the EC to easily check and validate the notification of the different Member States.

It has been reported by e.g. the Luxembourg market surveillance authority & RAPEX contact point, ILNAS, that the number of notifications on the RAPEX server is too big.

**Potential interoperability and suitability** – The RAPEX system addresses the safety of products and is therefore not directly involved in the fight against counterfeiting. However the structure of the system seems suitable. The RAPEX system has several characteristics that make it interesting for the fight against counterfeiting and piracy. 1) The standard forms and the establishment of national contact points provide a clear and uniform information flow. 2) Moreover other key players such as producers and distributors are involved in the notification-process through the ‘Business Application’ of the EC. 3) The central RAPEX server provides an instantaneous diffusion of notifications to the national market surveillance authorities and therefore serves as an alarm, calling all involved authorities for coordinated measures. 4) In addition possible measures by the notified authorities are reported back to the European Commission for follow up further improving the international coordination.

**Needs** – It seems that the large number of notifications can be an issue for some authorities, therefore restricting the number of notifications could be useful.

There are not many user groups that have access to the RAPEX information system. Currently the RAPEX system is only available for the national RAPEX contactpoints and the Commission. If RAPEX would be applied in the fight against counterfeiting and piracy, it should be kept in mind that other users competent in the area of counterfeiting and piracy, such as customs, police, market surveillance authorities, etc., should at least have the possibility to consult the collected information.

## 2.4 eMage–eMarks (cross-border)

The eMage-eMarks project is an image based trademark search engine. It was developed by a consortium of European companies and authorities<sup>19</sup>.

**Legal basis** – The eMage project was an image retrieval project against fraud within the eContent programme<sup>20</sup> for the period 2004-2006. The eMarks project, which followed the eMage project, was sponsored in the framework of eTen<sup>21</sup> and intended to accomplish a business plan containing the market validation and initial deployment of this system.

**Addressed problems** – It is intended to intensify the fight against the illegal copying of existing trademarks, and industrial designs.

**Purpose** – Its purpose is to determine if an individual trademark or design is already registered with one or more official industrial property offices in the European Union.

**Type of information exchanged** – The eMage database includes national, European and international registered trademarks and industrial designs.

<sup>19</sup> Members of the original eMage consortium: The Austrian Patent Office, the Hungarian IP office, the National institute of Industrial Property of Portugal, Intrasoft international, Lingway, LTU technologies.

Members of the original eMarks consortium: Intrasoft international, the Hungarian IP office, the National institute of Industrial Property of Portugal, and the Austrian Patent Office, Czech Customs Administration, IPR professionals/lawyers g.s. Kostakopoulos and Associates Law Firm, Chamber of Commerce and Industry of Marseille and LTU Technologies.

<sup>20</sup> The European digital content programme: Its objective was to make digital content in Europe more accessible, useable and exploitable.

<sup>21</sup> eTEN is a European Community programme providing funds to help make e-services available throughout the European Union..

***Institutions involved in governing the system*** – Currently it is not in use since the project was in its testing phase and is now looking for appropriate funding.

***Institutions involved in providing the information*** – European industrial property offices

***Users*** – This information is not applicable because the database is not in use.

***Functionalities and features*** – The system consists of a subscriber-accessible web-application for research concerning trademarks and industrial designs.

It includes an image-based search and navigates to associate multilingual natural language search engines in English, French, German and Portuguese.

The eMage-eMarks system can be offered as a complementary search service to the existing IPO search services, which are in most cases publicly available and intended for the protection of trademarks and industrial designs.

The technology used, belongs in the area of content-based retrieval of multimedia collections as it has materialised in feature-based similarity search engines combined with natural language semantic qualifications.

Via an online portal a user of the eMarks service will be able to identify whether a trademark or industrial design is already registered with an EU industrial property office or not, by submitting to the service a digital photo of the trademark or industrial design in question. The photo, as well as multi-lingual search keys are compared with 1.2 million records within a special database, by using image-search and recognition technology powered by LTU. The eMarks user can further qualify the search by natural language and multi-lingual semantic categories of interest.

Government officials and intellectual property professionals can also use the research application to investigate trademark and industrial design copyright infringements.

***Benefits, drawbacks & remarks*** – This tool can be very useful, for example when suspected goods pass through government customs.

The biggest drawback of the product of the eMage-eMarks projects is that it is a market-oriented system in the hands of a consortium of public and private entities. However, the current consortium does not wish to carry on with its activity and did not manage to sell the product yet. Therefore the system is not in use at this moment.

The system has passed the development and testing phases but the consortium has not managed to find a buyer for the system yet. The development of national applications is faced with difficulties due to the consortium's ceasing. The system can be improved by any of the strategic partners (EC, OHIM, WIPO or private companies as Questel Orbit).

**Potential interoperability and suitability** – The system can easily be accessed thanks to its online availability. Furthermore, searches can be done in multiple languages. Also the system has advanced features such as access to audiovisual content. The system seems to be suitable for interoperability. It has been designed to work with other systems quite efficiently.

**Needs** – The system is still looking for proper funding

### 3 Informative systems

Following systems merely collect data from the general public or inform the general public on the fight against counterfeiting and piracy through Portals, websites etc. .

#### 3.1 Portal GAC (Portugal)

Portal GAC is a portal for online claiming and reporting of illegal counterfeiting acts. The launch of the portal is planned for 2010.

**Legal basis** – No legal basis is apparent but Portal GAC is being developed by the Grupo Anti-Contrafacção. This is an interdepartmental workgroup of the Portuguese Government addressing the problem of counterfeiting.

**Addressed problems** – Portal GAC addresses counterfeiting and piracy.

**Purpose** – Besides the online application possibilities the portal also offers informative possibilities.

**Type of information exchanged** – The portal allows the public to report illegal counterfeiting acts. The portal also includes general information on counterfeiting, how to combat it and the identification of the involved authorities. Furthermore it informs the users on security and health dangers and provides information regarding the legal protection of IPR.

**Institutions involved in governing the system** – This system was developed by the Portuguese interdepartmental anti-counterfeiting group<sup>22</sup>.

**Institutions involved in providing the information** – Ministry of Culture. Stakeholders can report counterfeiting acts through the portal.

**Users** – Since the portal is still under development, details on users and user administration are not available yet.

**Functionalities and features** – Details on features are also not available yet.

**Benefits, drawbacks & remarks** – As the GAC is constituted of different entities the launch of the portal is held up. However, if launched the portal appears to be an efficient way to involve

<sup>22</sup> Grupo Anti-Contrafacção (IP office, Ministry of economy, Police, ... )

consumers in the fight against counterfeiting and piracy. The public will be informed on possible counterfeiting through the portal which allows reporting or claiming counterfeiting acts.

**Potential interoperability and suitability** – The portal is still under development and very little data is available on its functionalities and features. Besides, portals are not strictly within the scope of this Study. While the country report however states that online claiming is possible, it's applicability depends on the way this claiming is executed. If it consists of a simple e-mail address whereto information on suspected counterfeiting acts can be sent, then it needs no further attention. On the other hand, if information is collected in a more systematic and structured way and allows follow up, this would increase its added value. However at this moment, given the available information, it is not possible to determine the applicability and subsequently its possible interoperability.

**Needs** – Based on the information available it is not yet clear how the claiming and reporting of illegal counterfeiting will be implemented in the Portal GAC. It is also not clear who will have access to this information. In order to give the Portal added value, it should allow enforcement authorities access to the information and allow submitting additional information at any time. Also, the use of an electronic application form should increase the efficiency and therefore the follow-up of the claims.

### 3.2 Project Original (Czech Republic)

Project Original is an information campaign, operational since the end of 2009.

**Legal basis** – No legal basis is known but Project Original is an element of the Action Plan of the government of the Czech Republic against piracy and counterfeiting of 3 October 2007.

**Addressed problems** – IPR infringements and the fight against counterfeit.

**Purpose** – Project Original aims at 1) campaigns informing the public and also 2) exchange information to facilitate the cooperation between the private sector and the government.

**Type of information exchanged** – It informs the public on the downside of buying counterfeit goods and how to protect IP rights.

**Institutions involved in governing the system** – Czech International Chamber of Commerce & the Czech Ministry of Industry & trade.

**Institutions involved in providing the information** - Czech International Chamber of Commerce & the Czech Ministry of Industry & Trade.

**Users** – Not applicable. The Project consists inter alia of a website accessible to the public.

**Functionalities and features** – It consists of an online portal, which seeks to facilitate the cooperation between the private sector and the government. The website allows the public to provide feedback.

**Benefits, drawbacks & remarks** – The country report states the project will be continuously evaluated and modified as needed.

**Potential interoperability and suitability** – Not applicable because Project Original is not an information exchange system. However, the public can provide feedback, which makes this project interesting for collecting information from the public.

**Needs** – Not applicable.

## Section C: Comparative Assessment

Throughout the EU, information is published, disseminated and exchanged in many ways. National and European authorities and private sector organisations make use of an array of specific information exchange systems, intellectual property databases and registers, websites and portals.

This section makes a comparative assessment of main systems available for information exchange, the arrangements in place that allow exchanges, the main users and the legislative and policy frameworks that exist.

### 1 Main systems for information sharing

As a general remark, we see that all law enforcement authorities regularly exchange information on the fight against counterfeiting and piracy. Several interesting information exchange systems on counterfeiting and piracy are operational<sup>23</sup>. The majority of these information exchange systems, however, are intended to exchange information for the purpose of internal coordination of the different operational units of the same sector or policy area, e.g. to coordinate the operations of the different policing authorities within the member states or throughout the EU, or to coordinate the activities of the different customs officials. Very few ICT-systems aim at exchanging information with other policy areas. Therefore most law enforcing authorities do not use information systems for the information exchange between different policy areas, e.g. between customs and market surveillance, but exchange information by traditional means like official letters, e-mails, fax, phone, etc.... The lack of systematic approach is caused by the multitude of authorities dealing with IPR infringements. Since so many institutions are involved, the relevant information for the enforcement of IPR rights is fragmented over a multitude of institutions. In other words, since there is no general policy area on these matters, information is exchanged case by case on a need-to-know basis. Moreover the information is often considered confidential.

Furthermore smaller countries often claim to have no need for ICT based exchange-systems, since the scale of needed information is relatively small and cooperation between institutions and IP rights holders is considered to be quite effective. However this cooperation stops predominantly at the borders.

This type of exchange is obviously not adapted to an international level of cooperation and to an intensification of the fight against piracy and counterfeiting, which is the goal of the EU. A change in priority will subsequently mean a change in the way these authorities exchange information.

#### 1.1 Information Exchange Systems and Databases

**Information exchange** –depends on the features of the relevant system and to what extent databases and registers can be considered as systems for information exchange.

---

<sup>23</sup> Falstaff, Vinci, ....

There is also the issue of which users have access to a database and which users can change or add content. For instance a database that allows users from different authorities to access, change and/or insert content of the database can be considered an information exchange system. Information exchange means in our opinion that information is shared and flows to and from different users of the system. Therefore a database can be considered an information exchange system if users from different governmental entities have the possibility to interact through that database.

The most widespread and most important tools for authorities in the fight against piracy and counterfeiting are the databases and registers of the different national authorities. It appears that customs authority databases and registers are the most widespread. However, the databases and registers of national IP offices are also very common; these provide information on existing patents, trademarks and designs and can be used to prove ownership.

**Operational databases** - The databases of the law enforcing authorities are of primary importance in the fight against counterfeiting and piracy. Law enforcing authorities usually register applications for action on infringements of IPR. This information is often held in internal databases, to support internal coordination. These databases are not available to the public. Furthermore customs databases are often isolated from other IPR enforcing authorities.

**IP databases** - In most cases these are partially or completely publicly available through portals or websites. The disadvantage with such portals or websites is that, in the main, they do not offer the possibility for interaction and there is no enrichment of content. Another disadvantage is that they are sometimes not updated frequently enough. As a consequence officials of the concerning authorities that need accurate information will recurrently prefer their own intranet instead of the publicly available portals or websites to access these databases.

**Statistical databases** - In some countries like Germany for example statistical data on applications for action or statistical data on recidivists of IPR infringements are also collected and processed. This information can then be used by the involved authorities for policy and strategy development.

## 1.2 Informative systems

Many Member States provide information through websites, intranet or web-registers. These systems provide general information on counterfeiting and piracy, cases and interpretation of legislation. Web-registers contain selected data extracted from certain registers and are made accessible. These systems are generally open for the public, but are in some cases restricted to personnel of a certain authority. A disadvantage of these systems is the lack of interaction. However in some cases there is the possibility to interact through e-mail or social web-tools.<sup>24</sup> Through these systems the authorities try to inform the public on the risks and disadvantages of counterfeiting and piracy. Occasionally the informative purpose is combined with an educational purpose. For example in the Czech Republic civil servants can be instructed and educated through the use of these tools. However these systems cannot be considered information exchange system in the fight against counterfeiting and piracy.

---

<sup>24</sup> e.g. Findok in Austria

## 1.3 Users and the types of information exchanged

### 1.3.1 Law enforcement authorities

The first and most important group for this study are the law enforcement authorities. This group of authorities consists of customs authorities, police, border police, public prosecutors, competent courts, anti-fraud authorities, consumer safety authorities, tax, fiscal and market surveillance authorities. These authorities exchange two types of information:

- i. intelligence, information resulting from the investigation of criminal infringements of IPR;
- ii. information and documents originating from company or consumer complaints or from findings of the involved public services.

These types of information can adopt different forms and the exchange is usually done on a case-by case basis.

**Customs officials** - One particular group of users within law enforcement authorities are the customs authorities and their customs officials. This group is very important because the customs authorities are key authorities in the enforcement of IPR. The customs authorities deal with cases of importing, exporting and transit of suspicious goods to and from third countries. Furthermore, it is more usual for customs authorities than for other IPR enforcing authorities except the police<sup>25</sup>, to have a database for internal coordination in place containing mainly information collected during inspections. Apart from information collected during inspections, these databases can also contain, information on applications for action by customs. The exchange of information on applications for action happens at a national level as well as on an international level and is very important for the internal coordination of customs. European systems addressing this exchange of customs-information are still under development; the COPIS system for example, when fully implemented, will allow customs officials to exchange requests for action with customs officials in other Member States. Nevertheless there is already important crossborder cooperation between the customs authorities of the Member States.

One specific European system (AFIS<sup>26</sup>) offers the possibility to send alerts to its users (only approximately 125 customs officials), when certain incidents or potential threats in regard to counterfeiting occur. This functionality appears to be very useful for customs officials because there is a need to be informed and to be up-to-date at any moment, especially while performing inspections. If counterfeit is detected, it is recommended that an alert can be sent to stakeholders such as other customs officials in a rapid manner.

**Police** - The police has in most Member States the powers of entry, seizure and arrest. They are also involved in the detection and investigation of criminal acts concerning IPR. Therefore this group of law enforcers also has a vital role in the fight against counterfeiting and piracy. The police often works in cooperation with customs authorities. The information needed by the police to conduct their operations is quite similar to the information needed by customs:

---

<sup>25</sup> E.g.:Blue View, Patja,....

<sup>26</sup> See Annex A

Information collected during inspections, applications for action & notifications of suspected counterfeiting but also criminal and judicial data. Furthermore there are several international cooperative agreements on policematters which include the enforcement of IPR. National police authorities communicate with Interpol in order to exchange intelligence on counterfeiting and piracy infringements. Europol also has a specific team aimed at protecting IP.

**Market surveillance, health, safety, and tax authorities** – These authorities conduct inspections on the field in their respective policy areas. The information needed by these authorities is similar to the information needed by customs and police. They mostly need to cooperate with the police authorities in order to seize counterfeited goods. The information provided by other enforcement authorities allows these authorities to detect IPR infringers more easily and to determine if actions already have been taken.

**Public prosecutors, competent courts** – These legal and judicial authorities play more of a coordinating role since they are not detecting counterfeiting & piracy in the field but address the judicial consequences of detected counterfeiting and piracy. The public prosecutor exercises the authority on the investigation and prosecution. This includes the assignment of special instructions and the provision of general directions if a case is investigated. However, they need the same information provided by customs, police or any other enforcing authority in order to collect evidence and to prosecute IPR infringers.

### 1.3.2 Administrative IP-authorities and right holders.

Law enforcement authorities need technical data to identify suspected counterfeits or data to identify the respective right holders in order to allow them to apply for action. This is based on information provided by

- i) the registers and databases of the national IP office or other institutions responsible for the registration and management of IP registers and databases;
- ii) right holders organisations or the right holders themselves.

**Administrative IP authorities** - Administrative institutions such as national IP offices & ministries of culture are responsible for managing IP registers and databases. The information in these registers and databases contains detailed IP information on designs, patents and trade marks and in many cases also technical details needed for the identification of counterfeits. Their role in the fight against counterfeiting and piracy is to manage the registers and databases and to provide the necessary access to information for stakeholders.

However, in some Member States these authorities also play a role in the enforcement of IPR. In those cases they need access to information from customs authorities and other law enforcement institutions such as the police, the prosecutor's office etc.. The types of information exchanged are inter alia: applications for action, criminal files, information on right holders and information on IPR.

**Right holders** - Another group of recurrent users are the right holders. Their role can be separated into two tasks.

- i) Providing IP databases and registers with specific and technical data on suspected counterfeited goods and IPR in order to facilitate the identification of counterfeit;
- ii) Applying for action (if direct application is possible since in some cases this can be an exclusive task of the customs authority) and subsequently reporting suspected counterfeit and goods. Moreover, they provide follow-up of the status of their application for action.

#### 1.4 Formal and informal arrangements or cooperation

Informal arrangements are often made in cases of regular information exchange between authorities concerned<sup>27</sup> in the fight against counterfeiting and piracy. These exchanges however mainly take place through regular interactive means like fax or e-mail.

**Customs and police** - The most common way of formal arrangements exists between customs and police. Both departments are confronted in the field with the enforcement of IPR infringements. Therefore their operations benefit from the use of the information available in each other's registers. Under such agreements the most relevant information is exchanged on a case by case basis. However it may occur that there is a closer cooperation between customs and police, allowing direct access to each other's register or database.

**Public and private organisations** - Another way of cooperation occurs between public and private organisations. Right holders can be asked to directly communicate with law enforcing authorities in order to provide them with technical details on counterfeited goods. Right holders databases can be accessed by the enforcing authorities to monitor the IP market and to analyse collected information. These right holders organisations manage their databases to assist law-enforcement authorities to identify counterfeited goods and facilitate the cooperation of right holders with customs, the prosecutor's office and other law enforcement authorities to identify counterfeited goods. In some Member States non-governmental organisations are strongly encouraged to interact with governmental agencies.<sup>28</sup> In other countries initiatives in the rapid information exchange on counterfeiting and piracy originate from the private sector.<sup>29</sup>

**Intergovernmental groups** - Although most countries do not have a single coordination body for enforcement, it is remarkable that several countries have established or intend to establish cooperation councils, committees, workgroups or bodies (examples: Latvia: "Intellectual property council"; Lithuania: "Anti piracy centre"; Slovenia: " intergovernmental working group for the fight against piracy and counterfeiting"; The Czech Republic: "Intergovernmental Commission"; The Netherlands: "the interministerial contact group 'intellectual property'"; ). These councils and committees mostly aim to achieve maximum results in the field of development and protection of intellectual property rights.

---

<sup>27</sup> E.g. Austria

<sup>28</sup> E.g. the UK

<sup>29</sup> E.g. the Swedish anti counterfeiting group.

This confirms the actual need for close cooperation between different governmental institutions. Proper coordination between different authorities seems to be vital in the development of an effective IPR enforcement policy. Moreover the diffusion of the competence over different authorities makes it more difficult to counteract counterfeiting and piracy. Mostly customs and police have already a rather developed and organised internal coordination through their own systems but there is no system nor database bringing together all different actors in the fight against counterfeiting and piracy. Therefore the committees are vital for the Member States. They act as a common contact point offering the possibility to exchange information, even though this information is exchanged by classic means. The committees and councils join the most important actors in order to develop strategy, coordinate operations and in some Member States even exchange information in actual counterfeiting and piracy cases.

**International cooperation** - At an international level there are numerous cooperation agreements in place. E.g.: The Cannes Declaration against counterfeiting, signed by representatives from Bulgaria, France, Italy, Morocco, Portugal, Romania and Spain; Cooperation of Member State police and Europol, Interpol, OLAF, SECI, Eurojust, RIF, WCO (however none of them deals particularly with IPR infringements); Most informal cooperation at international level is performed by the customs authorities.

## 2 Policy framework.

**Legal barriers** - Most countries do not have any legal barriers to e-government systems and initiatives for the exchange of information nor for intelligence on counterfeiting and piracy. Mostly the EU-initiatives on these matters are fully supported and e-government applications are strongly encouraged by law and policy. Even so authorities need to keep in mind that the processing of personal data through e-government applications needs to be in compliance with privacy regulations.

Only the Czech Republic reported several barriers that prevent the exchange of information and intelligence on counterfeiting and piracy. First, authorities such as the Czech customs or the Czech Trade inspection authority (CTIA) are not allowed to disclose almost any information to other authorities, and even though both share the same or similar enforcement competencies, their cooperation is very weak. Secondly, Czech legislation does not require trade-licensing authorities to inform enforcement authorities of their final decision, so these authorities may encounter the same problems over and over again.

**Main components of the institutional framework** - Institutional frameworks in most Member States have been developed to meet national needs but similarities between these structures are rare. Moreover, the policy of the fight against counterfeiting and piracy is usually dissipated over different departments. Therefore the amount of institutions involved is very large, which creates overlap of competence. These institutions are responsible for the creation of policy and national strategies to combat counterfeiting and piracy. The following overview is a list of possible involved institutions but may differ from country to country:

### A. Government institutions

The governmental institutions, associated with IPR enforcement and exchanges of related information, mainly include the national IP offices, ministries of Home Affairs or economics and the relevant ministries of justice. Governmental institutions also keep registers and databases of IPR, these are normally the national IP offices. In some cases the ministries of culture are involved in a more preventive IPR enforcement role. This includes initiating projects related to anti-piracy action, such as the promotion of exchanges of information about pirated and counterfeited goods.

### **B. Inter-institutional commissions, councils or groups**

While so many institutions are involved in the fight against counterfeiting and piracy some Member States have also created inter-departmental bodies. These bodies are charged with the coordination and/or supervision of actions combating counterfeiting and piracy and are involved in the creation of global policies.

### **C. Law enforcement institutions**

Law enforcement institutions include customs, police, public prosecutors, competent courts and in some countries, border police, tax, fiscal and market surveillance authorities. Their roles are mainly to deal with IPR enforcement and with the investigation on counterfeiting. These authorities are mostly involved in the exchange of related information on counterfeiting. Many of them maintain lists of determined IPR infringements and they investigate IPR violations.

### **D. Private organisations**

Rights holders play an important role in the institutional framework for the exchange of information. They provide technical data to the enforcing authorities and can assist in the detection of IPR infringements.

### **E. IT-Agencies**

Most of the Member States do not have a designated IT-infrastructure for the purpose of exchanging information about counterfeited and pirated goods between law-enforcement and governmental institutions.

## **3 Reference documents.**

**Legislative documents** – Most country profiles include legislative reference documents at national level. Many country profiles refer to Council regulation (EC) no 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, O.J. L 196/2003, p7. National legislative documents exclusively addressing the matter of the rapid information exchange on counterfeiting and piracy are non-existent within the EU according to the country profiles.

**Policymaking documents** - Most Member States do not have any policymaking documents on rapid information exchange on counterfeiting and piracy.<sup>30</sup> However several Member States are aware of the issue of piracy and counterfeiting and do have policy documents describing action plans or guidelines that address intellectual property matters and the fight against counterfeiting and piracy. In most cases these documents include a pillar addressing directly or indirectly the exchange of information. For example:

- **Austria:** The “e-government act 2004” states that the internal and external exchange of information is part of the Austrian e-government policy. The latest strategy was decided in 2005.<sup>31</sup>
- **Cyprus:** “The business strategy of the Department of Customs and Excise for the period 2005-2008<sup>32</sup>” states that the goals of the Customs Department are, inter alia:
  - *to increase cooperation and exchanges of information with other customs administrations and law enforcement bodies; to continue its active participation in the EU IT systems;*
  - *to provide “on line” services with among others improved information and data exchange with third parties; to enhance the national systems capable of interfacing with EU systems;*
  - *to increase cooperation (e.g. through memoranda of understanding) with relevant agencies in the administrative and public domain at both the national and international level.*
- **France:** “Act n° 2007/1544 of 29 October 2007 for the fight against counterfeiting” enables information sharing of intelligence between the Ministries in charge of the fight against counterfeiting. This act introduces a new article into the consumer code that stipulates that *Public services and institutions should inform the DGCCRF<sup>33</sup> and judicial police agents and officers of all information and documents likely to be useful for the fight against counterfeiting, except ones obtained or exchanged under Council regulation n° 1/2003 of 16 December 2002. Investigation secrecy cannot be opposed to the disclosure of such information. DGCCRF, DGDDI and judicial police agents can “spontaneously” exchange all information or documents handled or obtained for the fight against counterfeiting.*

The “cooperation protocol of 8 February 2006” signed by the DGDDI and DGCCRF establishes cooperation procedures between these two authorities for the fight against counterfeiting

<sup>30</sup> e.g. Ireland, Malta, Bulgaria

<sup>31</sup> A good summary is provided by the report Platform “Digitales Österreich”, Bundeskanzleramt Wien 2006; available at <http://www.digitales.oesterreich.gv.at/Docview.axd?CobId=22687>

<sup>32</sup> available in English at: <http://www.mof.gov.cy/mof/customs/Customs.nsf/All/B4252A3CD6>

1F5F31C2257301003470E1/\$file/businessstrategy.pdf?OpenElement, [http://www.mkidn.gov.pl/cps/rde/xbcr/mkid/Program\\_2008\\_en.doc](http://www.mkidn.gov.pl/cps/rde/xbcr/mkid/Program_2008_en.doc)

<sup>33</sup> French General Directorate for competition, consumption and fight against fraud.

(information exchange, common annual control plans, coordination at national and local level and common actions of controls, etc.)

– **Greece:** “The comprehensive action plan on the protection of intellectual property rights in Greece” states the need to:

- *Reach a higher level of coordination among law enforcement authorities (Police-Customs-Municipal Police-Special Control Service);*
- *Establish administrative collaboration and exchange of information, among public authorities, but also between the Public and the Private sector.*

To this end an information working group was created, at an administrative level, that was assigned to inter alia:

- *register the problems raised while taking actions to combat piracy and counterfeiting and present proposals on how to face these problems effectively;*

The action plan proposed the compilation of a study on the creation of an integrated database, which competent authorities all over Greece will have the task to update (Hellenic Police, Municipal Police, Special Control Service, Customs, Ministry of Justice and Port Authorities).

– **Hungary:** “The National Strategy against counterfeiting for the years 2008-2010” contains 3 pillars:

1. *The collection of statistical data concerning infringements related to counterfeiting;*
2. *Awareness rising;*
3. *The development of the legal and institutional background of the assertion of rights.*

The national strategy also contains a number of relevant actions points:

- *The development of a database concerning the injurious activities. The database shall be continuously maintained and shall be accessible for the public too;*
- *To form the cooperation between the Hungarian Patent Office, the national headquarter of the Hungarian Police and the General Directorate of the Hungarian Customs and Finance Guard concerning a database service (eMage-service) and its operation;*
- *For support of assertion of rights, the examination of opportunities regarding the introduction and regulation of technologies of product recognition and of identification (RFID, ADNS); the launch of a pilot project for the application of these technologies.*

- **Italy:** the *“Circolare no. 32”* of 2004 issued by the director of the customs authority sets the basis for the exchange of information on counterfeiting and piracy at national level. It also sets forth the procedures for the customs authorities to fight counterfeiting and piracy, inter alia the implementation of a multimedia database (containing all the specific data allowing the distinction of the products to be protected) is involved.
  
- **Lithuania:**  
The *“Strategy of Means against Unofficial and Unaccounted Economy”* includes an action plan for the fight against counterfeiting and piracy. One of the goals of the strategy is to establish an interdepartmental Commission for the Rapid Exchange of Information on IPR infringements.  
*“Order No JV-401 of July 2008”:*
  - Suggests establishing an anti-piracy centre which would assist the police and other law enforcement institutions;
  - Furthermore the order acknowledges that law enforcement institutions can only collect a small amount of information regarding the dissemination of pirated and counterfeited goods in the market;
  - Also, the order argues that law enforcement institutions should cooperate more actively with associations representing right holders;
  - The goals of the Anti-Piracy centre include: the monitoring of the IPR market, the analysis of collected information, the creation and administration of databases containing information that would assist law enforcement institutions to identify counterfeited goods.
  
- **Latvia:** *“Guidelines on the Enforcement and Protection of Intellectual Property Rights 2008 – 2012”*. This policy-document recognises improvement of the cooperation and information exchange between the public authorities in matters related to IP rights as one of the goals of the policy.
  
- **Poland:** *“the Programme for the Protection of Copyright and Related Rights 2008 – 2010”* recognises *increasing efficiency and continuous coordination of activities of state services in combating piracy* as one of its strategic indirect goals. This goal comprises, among others,
  - A partial objective of *increasing efficiency of activities of state services* (n° 1.1) is to be achieved, among others again, by the “exchange of information and experience between piracy combating services by means of the dedicated knowledge management Portal (DKM)<sup>34</sup>

---

<sup>34</sup> See Annex A.

- Another partial objective within the same major strategic indirect goal is worded as *Development of IT systems to support activities of the Customs Service of the Republic of Poland, the Border Guard of the Republic of Poland, the Police and the Public Prosecutor' Office in fighting copyright related rights and other intellectual property rights infringements* (n° 1.3) is to be accomplished by two methods:
  - *Conducting work on designing and creating an intellectual property database and*
  - *The continuation of work on creating a database of seized goods and the “Vinci” information exchange system for the Customs service of Republic of Poland.*
  
- **Romania:** The *“National Strategy in the field of intellectual property 2003-2007”* was drafted by fourteen Romanian authorities and approved in 2003 by government decision n° 1424. One of its main goals is the *realisation of a transparent cooperation between the authorities and national bodies regarding the protection of intellectual property.*

According to the Strategy, the cooperation will be achieved by creating and implementing a portal, providing access to information and services related to intellectual property.

Another objective of the Strategy is improving the enforcement of intellectual property legislation, which will be realised by creating applications and databases in for the fight against piracy and counterfeiting.

Furthermore, the *“Action plan for the implementation of the Strategy in the field of intellectual property (2005-2007)”* includes the creation of a database through an intranet system regarding the infringement of intellectual property rights. This objective was accomplished by the creation of the Common Database<sup>35</sup>.
  
- **Spain:** The *“Good practices manual”* was coordinated between the Spanish Ministry of Culture and the Ministry of Justice and contains recommendations on the exchange of information among enforcing authorities and promotes the development and integration of databases.
  
- **Slovenia:** The *“National Action plan for cooperation between the Slovenian Intellectual Property Office and the European IP office for the period 2007 – 2010”* states the objective of the establishment of coordination among competent authorities for the fight against piracy and counterfeiting. A partial objective of this coordination is the setting up of a common database or another communication system for the exchange of relevant information.

---

<sup>35</sup> See Annex A

“The “decision of the government of the Republic of Slovenia on establishing an Intra-governmental Working Group for the fight against piracy and counterfeiting” aims to improve the cooperation of state authorities in performing their duties in the fight against piracy and counterfeiting. The tasks of the Intra-governmental Working Group are among others:

- The exchange of operational information and cooperation;
  - The establishment of a common IT support for information exchange as well as for Working Group operations;
  - The improvement of cross-border administrative cooperation.
- **UK:** National IP initiative ‘Real Deal: working Together for Safe, Fair Markets’ includes following objectives inter alia:
- A partnership of local authority trading standards services, market operators, industry groups, copyright and trade mark owners to ensure markets are free of counterfeit and other illegal goods;
  - Local authority trading standard services’ commitment to provide information and support in relation to the sale of illegal goods; to work with industry and trade mark representatives to identify illegal goods; to monitor the market and share intelligence with police, trading standards or other law enforcement agencies as well as industry and rights’ owners;
  - Industry and trademark representatives’ commitment to provide regular and up to date information to trading standards and market operators on how to identify illegal products; to monitor the market and alert all parties to any infringing products found.

These policymaking documents do not necessarily imply the actual implementation. In some cases, action plans are not yet in the implementation phase and objectives are not realised within the projected timeframe. For example the Lithuanian anti-piracy centre is very promising but due to unclear financing options it will be difficult to implement. Another example is the Latvian policy which is generally sufficient but apparently no practical implementation is going on.

If policydocuments are available, as is in the abovementioned Member States, they mostly do build upon the legal regulation.

Moreover the existing and available policies state in most cases their objectives on a national level when it comes to information exchange; only a few of the abovementioned policies address explicitly the international exchange of information, namely: Austria, Greece & Slovenia.

## Section D: Conclusions and Recommendations

### 1 Introduction.

This section assesses the actual needs for information exchange at a European level on the basis of the Study results. The goal is to determine what characteristics should be attributed to an efficient EU wide exchange system for the rapid information exchange on counterfeiting and piracy. The following step is to assess what actors in the fight against counterfeiting and piracy would benefit from an information exchange system, what information they need and finally how they currently exchange it. This should give us an idea of what is missing in the current situation and what improvements are needed. The existing systems that respond to these needs are assessed in the light of an EU wide deployment of these systems allowing us to determine their suitability for this purpose. Based on these findings, recommendations are made.

### 2 Concrete requirements to facilitate more effective rapid information exchange

***EU wide platform to exchange law-enforcement information*** – The fight against counterfeiting and piracy needs a lot more information exchange across national borders and across policy areas to coordinate effective countermeasures.

Some country reports stated the need for a communication system, coordinated at EU level, between the most important stakeholders and law enforcement authorities. The information these authorities hold is often extremely specific and sensitive<sup>36</sup>. Therefore separate law enforcement entities need to be able to connect directly with one another in a secure way, to easily request cooperation. This implies the vital need to easily identify involved law enforcement authorities.

At present, the different types of information exchanged and the different ways that law enforcement authorities are organised often hinders the swift and clear interinstitutional and cross border exchange of information. Therefore there is a need to exchange information in a more efficient, systematic and uniform fashion. The use of consistent information requests would improve interoperability. Currently there is no centrally organised information exchange system allowing different law enforcement authorities to communicate with each other. The most efficient IT based communication systems currently available appear to be information systems with the purpose of coordination within one policy area and therefore, they do not permit access to other law enforcing authorities<sup>37</sup> of other policy areas.

***Translation*** - The European Union has 23 official languages. The information that needs to be exchanged consists of technical data, mainly from investigation reports, assorted documents and judicial information in the form of text. Furthermore, since information is mainly exchanged on a need-to-know basis, the requested information needs to be clearly specified. Therefore an information exchange system at European level would need multilingual capabilities.

---

<sup>36</sup> Only to be disclosed if necessary

<sup>37</sup> E.g.: Falstaff and Vinci are intended to coordinate the operations of customs

The best example of a system with multilingual capabilities is IMI. It offers translation and interfaces in 10 languages.<sup>38</sup> Another available multilingual system is the RAPEX system which offers information, translated by the Commission, in English, Spanish, Italian, German and French. The eMage system is also an example of a system that could be used in the fight against counterfeiting and piracy by supporting multiple languages. The eMage system provides information in 8 different languages. There is no information available yet on the multilingual capabilities of COPIS.<sup>39</sup>

**Real time notifications** – There seems to be a need for rapid and direct notifications of IP infringements and detained goods by law enforcement authorities within and across Member State borders, to other law enforcement authorities. The EC system RAPEX already covers this issue for counterfeited goods, detected by market surveillance authorities, which pose a threat to consumer health and safety. Moreover, customs authorities have the ability to send notifications concerning counterfeit and piracy through the AFIS system<sup>40</sup> to other customs authorities. However a system particularly addressing the EU-wide notification of important IPR infringements for all law enforcing authorities, is not yet present. An instant notification system alerting relevant Member States' law enforcement authorities would contribute to the coordination of the fight against counterfeiting and allow more rapid and collaborative, European-wide, countermeasures.

**Access to applications for action** - For the adequate coordination of actions between law enforcement authorities there is a need to consult pending applications for action. This could be possible through a centralised database which would register all applications for action. The COPIS project seems to be designed to meet this need for customs authorities. The problem is that other law enforcing authorities are not involved in this system. Therefore, there is still a need for accessing information from applications for action, held by other authorities. Some other information exchange systems allow the online application for action.<sup>41</sup> Another possibility would be to force the relevant authorities to send notifications of each application to all involved authorities. Such notifications could be made through a system similar to the RAPEX notification system. However, this option will probably not be satisfactory for customs authorities outside of the COPIS project. As a result, the cooperation of customs would therefore be on a voluntary basis.

**Public private cooperation** - The fight against counterfeiting & piracy would greatly benefit from a closer public-private cooperation. Information from rights holders, enterprises and rights holder organisations can help the law enforcement authorities to identify counterfeiting and piracy. Secondly, it would be very useful for the enforcement authorities to allow online applications for action in order to speed up seizures, counteractions and other procedures.

---

<sup>38</sup> see infra

<sup>39</sup> see infra.

<sup>40</sup> The Anti Fraud System of DG OLAF is a system that allows customs authorities to notify other customs authorities about inter alia. suspected counterfeit goods. See annex A, title 11.1.

<sup>41</sup> The Vinci system

Therefore, there is a need for an information exchange system between law enforcement authorities and private organisations to link national and cross border authorities. This has already been organised at a national level in Italy through the Falstaff system. This system allows rightsholders to submit technical information useful for the identification of counterfeiting in the database. In the Polish VINCI system the ability for rights holders to online apply for action will also be provided.

**Stronger authentication procedures** - In order to secure the access to confidential information provided by the law enforcement authorities there is a need for stronger authentication procedures. For the moment there is no European-wide authentication procedure. However, in the future the e-ID <sup>42</sup> initiative should meet this need.

**Perform EU wide searches** - There seems to be a need to perform information searches at a European level. More specifically in the area of IPR it could be useful for the involved authorities to be able to carry out direct IP searches on a European level.

Achieving a consolidation of all Member States' IP-databases seems to be doubtful due to the proliferation of IP databases. Moreover dataprotection rules will need to be taken into account. Therefore it should be possible to define different levels of access to memberstate databases.

However, a more realistic approach would be to allow for fast formalised requests for information between the relevant authorities. For instance a law enforcement authority in one member state could directly request a search of a database of another authority in another Member State. This other authority would then perform the search and forward the result to the requesting authority. However, one drawback is that the authority in need of information has to be able to identify easily which other authority it should consult. Therefore the requesting authority would need access to tools that would easily and quickly identify the authority holding the needed information.

**Consumer input** - information provided by consumers could support the monitoring tasks of law enforcement authorities. An online portal would allow the public to submit information on possible infringements. However achieving this is doubtful as it would need a massive campaign in order to inform the public. In addition, results could not be guaranteed, since it would depend on the voluntary cooperation of the public and the accuracy and reliability of the information provided. A 'Crimestopper' system exists in the UK and other national examples include portals such as the Czech Project Original or the Portuguese Portal Gac.

---

<sup>42</sup> The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

**Cooperation in the development of preventive measures** - Several country reports stated that there is a need for international cooperation in the development of preventive measures.<sup>43</sup> In order to do so the relevant authorities should be able to exchange policy-documents, information on strategies and information on technological solutions in an efficient way.

As many countries have policies addressing the problem of counterfeiting and piracy, an international database for the exchange of information on strategies and technological solutions was suggested as a tool for this purpose.<sup>44</sup> However it is not clear which authorities should be involved in the composition of the content of such a database. It is also not clear how detailed the information, e.g. on the technological solutions, should be. Furthermore, Member States have different ways of structuring their policies and the competences are often spread over different authorities.

**Statistical data** - Several country reports acknowledge the need for the registration, transfer and extraction of data for statistical evaluation. Statistical tools help defining countermeasures in the fight against counterfeit and piracy and are important for the development of general policy and strategy. Required statistical data would include the recording of IPR infringements and seizures, measures taken against counterfeit and their outcome, etc.. A solution for this need would involve the standardised collection, analysis and reporting of data, which would need to be submitted to a centralised database. The German system ZGR 1.1., which is still in its implementation phase, is an example of the registration and automated transfer of data on seizures. Also the European customs project COPIS, which is still under development, intends to contain the possibility to extract statistical data. However, this need is of lesser importance in the light of this study.

### 3 **Beneficiaries of a rapid information exchange system and levels of exchange.**

**Law enforcement institutions** - Law enforcement institutions such as customs, police, border police, public prosecutors, competent courts, anti-fraud authorities, consumer safety authorities, tax, fiscal and market surveillance authorities can all be involved in the enforcement of IP rights and require fast and accurate information to facilitate their work. Other users such as IP-administrative authorities, rights holders and rights holders representative organisations also play an important role in providing supplementary data needed for law enforcement.

**Levels of information exchange** - In terms of this study, there are three different levels of information exchange needed by law enforcing authorities:

#### i) **Cross policy cooperation:**

Information exchange across law enforcement policy areas is needed for cooperation to combat counterfeiting and piracy. E.g.: throughout Europe the customs policy area provides many systems that allow information exchange. However these information exchange system allow mostly only exchange within the customs policy area and not

---

<sup>43</sup> E.g. Germany, ...

<sup>44</sup> see section C title 1: reference documents.

with other policy areas such as market surveillance or police. In other words these systems only cater to their own authorities within their own policy area and not to authorities in other policy areas. The information exchange between different law enforcement policy areas is mainly needed for the law enforcement of IPR infringements. The information exchanged allows for the identification of counterfeit and pirated products and for speedier and more effective prosecution of IPR infringers.

ii) **Cross border cooperation:**

Cross border exchanges of information between law enforcement authorities is also needed because cooperation in the fight against counterfeiting and piracy too often stops at the borders and therefore, limits the effect of counteractions.<sup>45</sup> Increasing the level of cross border cooperation through rapid information-exchange would increase the impact of repressive measures. However, there are several obstacles in the light of cross border information exchange that need resolution, such as language and organisational differences.

iii) **Internal coordination:**

To a lesser extent there is also a need for information exchange for coordination within different policy areas, e.g. the market surveillance policy area, where officials of the ministry of commerce need to exchange information with their inspectors, agencies etc. Law enforcement authorities coordinate actions on counterfeiting and piracy at a domestic level, and within their respective governmental organisations. This can be considered to be the best developed area, as explained in point I) of this section, in the fight against counterfeiting and piracy, offering formal procedures and ICT based systems. This is particularly true in the case of customs or police<sup>46</sup>. In most Member States these authorities have information exchange systems in place providing adequate tools for internal coordination. However some Member States' authorities still coordinate their national activities by means of e-mail, fax and telephone<sup>47</sup>.

## 4 Assessment of needs

### 4.1 Existing information

Much of the *necessary* information in existence is held by various law enforcing authorities and is derived from investigative files and documents. Furthermore the information is often stored case-by-case, and the files can contain different formats, such as text-documents, audiovisual material, investigation reports and agenda's, etc.... .

---

<sup>45</sup> Examples of international cooperation: Italian-French anti Counterfeiting committee, Mutual assistance Agreement between the Italian Custom Agency and Chinese Customs.

<sup>46</sup> E.g. The Netherlands Blue view.

Moreover, the information collected by these law enforcement authorities can be divided into two types of information:

- 'Nominal' - confidential-information pertaining to the investigation and prosecution of a person or entity, where disclosure can only be made with precision; and
- Non-confidential information pertaining to the identification of the infringing products, such as technical data.

Other more informative or technical data is mainly stored by other national authorities such as national IP offices and can be accessed through databases. However, it is important to note that private sector stakeholders also maintain banks of information that can assist enforcement.

## 4.2 Restrictions to access

As mentioned earlier<sup>48</sup> restrictions to access exist and will always play a role when seeking to establish a EU wide system. Therefore any solution would have to take account of this limitation by restricting the database, at least at a cross-border level, to non-confidential information or by providing different levels of access rights.

## 4.3 Required Information

The primary information needed by law enforcement authorities consists of information held by the other law enforcement authorities, this includes:

- information collected during inspections;
- information on seized goods;
- company or consumer complaints;
- information on applications for action;
- information on criminal actions;
- information on suspicious consignments;
- alerts, complaints and technical information from private sector stakeholders;
- IP-information and technical data from national IP offices and private sector stakeholders to support investigations by identifying suspect consignments and products.

## 4.4 Conclusion

In summary, there is a vital need for more regular, effective and speedier, exchanges of information cross policy and cross border, in multiple forms and languages between Member States' IPR enforcing authorities.

To a lesser extent, some Member States' law enforcement authorities could also improve their coordination within their own policy area by implementing more developed tools for the exchanges of information, replacing the more common and traditional means of fax and e-mail.

---

<sup>48</sup> Section A, title 5.

## 5 Recommendations

### 5.1 Required features of a EU wide information exchange system.

In order to interconnect the Member States' law enforcement authorities the EC should establish a central communication and information exchange platform, that is accessible to all the national and European law enforcement authorities involved in the fight against counterfeiting and piracy. Considering the abovementioned needs and the review, it appears that the following features should be included in a European wide information exchange system in the fight against counterfeiting and piracy.

#### 5.1.1 Peer to peer communication and information exchange.

Given that the current interinstitutional exchange of information in the fight against counterfeiting and piracy by the law enforcing authorities is in many Member States decentralised, and information with other law enforcement authorities is often disclosed case-by-case and on a need to know basis, an EU wide system should allow to make direct links between distinctive authorities in the same way. This would allow law enforcement authorities from different Member States to request for information or cooperation directly from the law enforcing authorities involved in a specific case, without having to go through a national contact-point or a database and it would allow the providing authority to only disclose information to the requesting authority.

#### 5.1.2 Standardised communication forms.

In order to increase interoperability between law enforcing authorities an EU-wide information exchange system should offer predefined forms for rapid and effective information or cooperation requests. These forms would allow the requesting and receiving authorities to specify easily and accurately the needed information or action, thus improving the accuracy and speed of communication and information exchange.

#### 5.1.3 Multilingual capabilities.

Given that the EU has 23 official languages and that the interinstitutional communication between the distinctive Member State authorities is currently performed mainly in a decentralised way, an EU-wide information exchange system should offer multilingual interfaces and applications, automatic translation of text and the translation of documents in as many European language as possible. These multilingual capabilities would improve the accessibility to the system and in doing so, improving international information exchange and communication.

#### 5.1.4 Real time notifications.

In order to coordinate counteractions, detect counterfeiting and piracy more rapidly, prevent unnecessary applications for actions, identify and notify the involved right holders, improve the investigative actions, and complement collected information by the law enforcing authorities the EC should establish a European wide notification system for inter alia:

1. the notification of major IPR infringements and infringers;
2. the notification of detected and seized goods by the law enforcing authorities;
3. applications for actions by the IP enforcing authorities.

However, if technically possible, this should be a smart notification system which would be able to identify the authorities that have to be notified based on a set of predefined parameters. This would prevent an overflow of notifications.

#### **5.1.5 Information exchange platform for public and private cooperation.**

Such a platform would allow the right holders to provide technical information and online apply for action. This would also allow law enforcement authorities to identify right holders and request them to apply for action or request them for additional information on their IP rights or their products.

#### **5.1.6 Authority/peer search function.**

Given that the actual information exchange is performed mainly in a decentralised fashion, that the law enforcement authorities are spread over different policy areas, that Member States are differently organised and that there are a great number of international organisations that could be connected to an EU-wide system, such a system would contain a great number of users. Therefore an EU wide system would need to offer search capabilities for the identification of involved authorities in other Member States or at supranational level. Such an application should allow to do searches based on competences and identify which Member State, what organisational qualification, what activities or what type of information these authorities could provide.

#### **5.1.7 Exchange of audio-visual content.**

The identification of counterfeiting and piracy by law enforcing authorities can be improved by allowing the exchange of audio-visual material.

#### **5.1.8 Database integration.**

Given the multitude of databases relevant in the fight against counterfeiting and piracy an EU wide system could benefit from integration of databases and registers from administrative IP authorities<sup>49</sup> or other law enforcement authorities, if any, in the system. This would allow users to search different databases through a single interface.

### **6 Suitability for EU-wide implementation of the available systems.**

Based on the features mentioned hereabove this section assesses the most interesting systems of section B on their suitability for deployment at a European level or integration into a EU wide information exchange system.

**AIDA/Falstaff** – This is mainly a tool for internal coordination of customs operations. Therefore it would need to expand its user base to allow access for the other law enforcement authorities involved in the fight against counterfeiting and piracy at a European level.

---

<sup>49</sup> See 3.4.2 of Section C

Furthermore the system should accept all sorts of foreign documents which it currently does not. Communication with other entities involved in the clearance of goods is supported and should be expanded to all other law enforcement authorities. There are no indications of multilingual capabilities. Real time notifications of declarations of goods in transit are available and are automatically paired with risk factors in order to detect possible counterfeit; these notifications should be expanded in order to meet the need for notifications by all law enforcing authorities. The AIDA/Falstaff system is sufficient for public private cooperation. Right holders can provide technical data or apply for action. There is no ability in the system to identify other involved authorities since there has not been a need to, at national level. The integration of databases into the AIDA/Falstaff system is supported. There is no indication of any ability to exchange audiovisual material.

With the necessary adaptations mentioned, this system seems quite suitable for an EU-wide deployment. This system also seems suitable for integration in a EU wide information exchange system. However it is designed to connect to the customs COPIS project and in its current state will only grant access to customs authorities. Customs authorities might also be reluctant to integrate this tool for internal coordination into a non-customs system.

**NIPIES** – This system is also intended for the internal coordination of customs operations. For the deployment at European level it would also need to expand its user base to allow all law enforcement authorities involved in the fight against countefeiting and piracy. The key-users, i.e. customs authorities, have extensive access to the information in the shared database and can add or change content. The drawback of this system is that information sharing happens through the shared database, so there is no ability to directly communicate with peers. Subsequently there is no way to request additional information and there is no direct real time notification ability. There are also no indications of multilingual capabilities. Public private cooperation is only indirectly possible because technical data from the right holders can only be introduced indirectly through the IP offices. Application for action can currently only be done indirectly through the customs authorities. There is also no ability in the system to identify other involved authorities since there has not been a need to, at national level. There is no indication of the possiblity for the exchange of audiovisual material. Furthermore the system has not had an update since 2005 and does therefore not comply to the new e-governance technical standards.

This system requires many adaptations in order to be deployed at European level. On the other hand this system seems suitable for integration in an EU wide information exchange system if new e-governance technical standards are implemented. However customs authorities might be reluctant to integrate it into a non-customs system.

**VINCI** – The VINCI system is also a tool for internal coordination of the customs authorities. In case of a EU-wide deployment, an expansion of the user base to allow all law enforcing authorities will be necessary. Because the system mainly aims at supporting customs operations, there is no possibility for users to communicate directly with each other. However the Vinci system will be connected to the Polish Copyright register<sup>50</sup> which allows the Polish law enforcement authorities (Police, offices of public prosecutors, border control and customs) to enquire the users (law enforcement authorities, employees of the Ministry of Culture, right

<sup>50</sup> Optical Carrier register of the Ministry of Culture

holders) of this database about records contained in the register. Nonetheless if deployed at an EU level these communication facilities will need to be expanded. Furthermore no notifications are possible and there are no indications of multilingual capabilities. A program interface, enabling right holders to apply for action by the customs authorities is under development. Technical data from the right holders can currently only be introduced indirectly by the IP offices or together with the application for action. There is no ability in the system to identify other involved authorities since there has been no need at national level. The Vinci system offers the possibility of integration of national IP databases for the support of law enforcement. The great advantages of the Vinci system are the audiovisual capabilities and the swift integration of databases.

With the adaptations mentioned the Vinci system could be a suitable system for deployment at EU level. This system also seems suitable for integration in an EU wide information exchange system. However customs authorities might be reluctant to integrate it into a non-customs system.

**COPIS** – This system is designed to coordinate the Member State customs authorities and addresses inter alia the issue of counterfeiting and piracy. Since only customs authorities and the EC have access to the system, its user base would need to be expanded to all the law enforcement authorities involved in the fight against counterfeiting and piracy. However, the structure of the COPIS project would allow other law enforcement authorities to be involved in an indirect manner through the national responsible authorities. Furthermore the system seems to offer an adequate platform for users to interact with each other. Requests for action or information are transferred instantaneously. Moreover right holders will be able to submit information and technical data in their files. Customs authorities would even be able to alter content of the customs databases of other Member State customs authorities. On the other hand, there is no indication of multilingual capabilities, but since the system is still under development (should be active by 2012) this important feature cannot be excluded at this moment, given the available information. There is also no indication of a notification system or an authority search function. Concerning the latter, this information could however easily be obtained from the national contactpoints.

In general this system seems suitable for the use in the fight against counterfeiting. One possible obstacle is that customs authorities might be reluctant to allow other law enforcing authorities to their system due to the confidential nature of their information. Also the system is not operational yet.

**IMI** – The IMI system is currently not active in the area of counterfeiting and piracy but is designed to support information exchange in multiple areas of the internal market. Therefore the implementation in the policy area of counterfeiting would be possible. The IMI system allows users to connect with each other by means of predefined questions with clear guidelines. This would allow uniform information requests and therefore rapid and effective information exchange. Since the exchange through the IMI system happens from peer to peer, there is no interference from a third party. This is an advantage for the exchange of sensitive information derived from e.g. police or criminal files. Because of this peer to peer structure information exchange becomes possible at all levels of law enforcement and across policy areas. In addition the IMI system offers extensive multilingual capabilities in all EU languages with multilingual interfaces and in ten EU languages for free text machine translation.

The IMI system also allows instant notifications thanks to its *one-to-many* workflow. Also it allows easy identification of relevant partners in other Member States. One drawback is that the IMI system does not yet allow private entities to connect to the system. Furthermore the IMI system does not support audiovisual material. There is also no indication of possible data integration.

With technical adaptations the IMI system could be made suitable for the EU wide information exchange in order to support law enforcement operations. The great advantage of the IMI system is that it has been designed for information exchange across policy areas.

**RAPEX** – This system addresses counterfeiting issues only at a secondary level. Namely when products are identified as counterfeit and could pose an important threat to the health and safety of consumers. This system could be quite useful in the fight against counterfeiting and piracy, if deployed in the policy area of counterfeiting and piracy. RAPEX allows the users of the system to communicate directly with one another and with the Commission through the RAPEX server. However there is no indication of predefined forms in this direct communication. Information about dangerous products is submitted through standard notification forms, in doing so the information is exchanged in a uniform manner. Moreover the Commission needs to validate the submitted information prior to forwarding it to the other users. Furthermore the information is translated in five languages. The system sends a notification to the involved authorities in order to coordinate counteractions. This notification system could easily be implemented in the context of the detection and notification of suspected counterfeiting. The system seems also sufficiently enabling cooperation with private entities by allowing economic operators to submit information through an online application. On the other hand there is no authority search function since the users are only limited to Member State contactpoints and to the Commission. There is currently also no indication of the ability to integrate databases, but this is mainly because in its current context there has been no need to. Moreover there is no indication of the ability to exchange audiovisual content.

This system seems quite suitable for the implementation in the fight against counterfeiting and piracy. However it should be kept in mind that this system offers solely a one-to-many workflow and the information forwarded always needs validation from the EC and needs to pass through national contactpoints. Therefore this system might seem less suitable for the exchange of intelligence. Furthermore it should be taken in account that the number of RAPEX users is currently very low (Member States + EC) and there are no indications how this system would perform with more users. Also the system is providing direct user to user communication but this communication is not formalised. The integration of the RAPEX system into another EU wide information exchange system seems possible because of its clear and simple structure of national contactpoints.

**eMage/eMarks** – This system is a complementary search service for the detection of trademark infringements. It is not suitable as an information exchange system at EU level because it lacks many important features such as an information exchange and communication platform, database integration capabilities and a notification feature. On the other hand it does offer multilingual capabilities and audiovisual content.

For these reasons this system is not suitable as EU wide information exchange system but is suitable for the integration into such a system. One drawback is that the system is not in use for the moment and that it lacks financing.

## 6.1 Recommendations for a European approach

Following the abovementioned reviews, it is considered that the national information exchange systems mentioned (e-mage, Falstaff, Vinci, Nippies) seem not to be the best options for a EU wide deployment. Moreover, the e-mage project is insufficient as an information exchange platform and the national systems of the customs authorities (Falstaff, Vinci and Nippies) do not offer more features than the COPIS system, which is an EU wide system of customs authorities.

Consequently, research and analysis suggest that only the three EU systems seem eligible for use as an EU wide information exchange system: RAPEX, COPIS and IMI.

RAPEX or IMI can both provide a notification system. However, since IMI also offers a superior customisable communication and information exchange platform it seems preferable to choose IMI over RAPEX.

Nevertheless, it would be interesting to examine the possibility of a link between RAPEX and IMI, concerning notifications on counterfeiting and piracy originating from market surveillance authorities. This should also be examined for the notifications of the AFIS system, which offers notifications on counterfeiting to the customs authorities.

In summary, IMI could complement the existing notification systems for the IPR enforcing authorities and allow cross policy area notifications by linking these systems to the IMI notification system.

At present, COPIS seems to be the most complete system, offering swift database-integration, audiovisual content and allowing private entities to submit information. In addition, if a selection between COPIS and the three other national systems was to be made, COPIS would be the preferred system, since it offers the same features, but at an EU level.

However, as a customs system, access is limited to national customs authorities. It should also be noted that COPIS is a customs project not only aimed at counterfeiting but also at the coordination of all customs operations, connecting national customs systems with the EU wide system. Users of the COPIS system will have extended access to each others databases and information including the ability to add, change or remove content.

At present it is doubtful that customs would want other law enforcement authorities to have the same capabilities. Nevertheless, it is recommended that further study takes place to examine the possibility to allow access to other law enforcement authorities to the COPIS system and thus expanding the communication facilities.

A realistic approach would be to connect the COPIS system to the IMI system. To a certain extent, COPIS and IMI could complement each other. COPIS offers no formalised communication platform between users and the users are limited to customs. IMI could fill these gaps by offering the COPIS users this customisable information exchange platform.

This would allow the COPIS users not only to connect with each other if additional communication is needed but also to connect with all the other law enforcing authorities. Furthermore in doing so, the platform allows all the users to benefit from the advanced features of the COPIS system in an indirect way.

As explained, despite the drawback that the IMI system does not yet allow private entities to connect to the system or cannot support audiovisual material, the system allows:

- users to connect with each other by means of predefined questions with clear guidelines;
- uniform information requests and therefore rapid and effective information exchange;
- secure exchanges, which is a vital advantage for the exchange of sensitive information derived from e.g. police or criminal files;
- extensive multilingual capabilities in all EU languages and machine translation in 10 EU languages;
- instant notifications;
- easy identification of relevant partners in other Member States.

For these reasons it seems most advantageous to actively explore the implementation of the IMI system, to improve rapid and effective exchanges between national authorities across borders and policy areas because:

1. IMI currently has the most important features for the international and cross-policy rapid information exchange on counterfeiting and piracy: uniformised peer-to-peer communication and exchange across policy areas, a notification system, an authority search function and advanced multilingual capabilities;
2. the missing features, the uploading of audiovisual material and access to private entities for uploading of technical data and database integration, are technically resolvable; these problems can also be covered by adding the other systems such as COPIS, VINCI or Falstaff to the user base in order to grant indirect access to the information in those systems. Through a predefined set of questions the IMI user would be allowed to ask additional information. The lack of database integration can be resolved in the same way.
3. In addition, IMI offers an alternative to all authorities which do not have an ICT based information exchange system for internal coordination;
4. It does not impose its structure on existing authority structures but on the contrary, it adapts easily to existing organisational structures.

## Annex A: List of National Correspondents

Of course, the provision of individual country information with regard to the information exchange systems and institutional frameworks is only possible through the assistance of local experts who are capable and willing to provide information.

The Study team especially wants to acknowledge the contributions of the following authors for each of the country profiles:

Country	Author(s)
Austria	Prof. Erich Schweighofer (Universität Wien)
Belgium	Boris Tshiananga (time.lex Law offices, Brussels)
Bulgaria	Dr. George Dimitrov (Dimitrov, Petrov & Co Law Offices)
Cyprus	Olga Georgades (Lexact Business & Legal Solutions)
Czech Republic	Tomas Schollaert (Pierstone, Prague)
Denmark	Prof. Henrik Udsen (Københavns Universitet)
Estonia	Kaupo Lepasepp and Kadri Rebane (Sorainen)
Finland	Ella Mikkola and Kaisa Keski-Vähälä (Bird & Bird, Helsinki)
France	Fanny Coudert (time.lex Law Offices)
Germany	Dr. Marcus Schreiberbauer (Lovells LLP, Düsseldorf)
Greece	Eleni Kosta (time.lex Law Offices)
Hungary	Dr. András Gerencser (consultant, Budapest)
Ireland	Prof. Maeve McDonagh and Prof. Fidelma White (University College Cork)
Italy	Davide Parilli (time.lex Law Offices)
Latvia	Agriss Repss and Lasma Rugate (Sorainen)
Lithuania	Renata Berzanskiene and Laurynas Ramuckis (Sorainen)
Luxemburg	Claire Léonelli (Molitor, Fish & Associés Law Offices)
Malta	Dr. Paul Gonzi (Fenech & Fenech Advocates)
The Netherlands	Louise de Gier and Joost Gerritsen (De Gier, Stam & Advocaten)
Poland	Dariusz Adamski (University of Wroclaw)
Portugal	Pedro Simões Dias (legal counsel, Lisbon)
Romania	Peter Buzescu and Corina Papuzu (Buzescu CA. Law Offices)
Slovakia	Zuzana Halasova (NSA, Bratislava)
Slovenia	Spela Kucan (Slovenian IP office)
Spain	Cristina De Lorenzo (Sánchez Pintado & Núñez)
Sweden	Christine Kirchberger (University of Stockholm)
United Kingdom	Stephen Mason (Chambers of Stephen Mason)

## Annex B: System Inventory

This section provides an overview and a brief description of the existing or planned information exchange systems on counterfeiting and piracy per Member State. The COPIS system is mentioned in several countries. This means that we have been informed that these countries are preparing the implementation of COPIS. We refer to the COPIS title in section B for more information on COPIS.

### 1 AUSTRIA

#### 1.1 Findok:

See [FINDOK/ELAK](#) in section B or visit <https://findok.bmf.gv.at>.

#### 1.2 Elak-BMF:

See also [FINDOK/ELAK](#) in section B.

### 2 BELGIUM

#### 2.1 Several databases at different levels (FPS Economy, Customs, Federal police)

The Intranet system for the Belgian customs allows exchange of information regarding right holders. Other authorities can request customs for information by mail.

#### 2.2 ICCF/CICF

ICCF/CICF is a coordination body representing different public services involved in the fight against economic fraud. As from 2007 a working group has been set up within this commission, which will specifically focus on the fight against counterfeit and piracy and discuss the specific problems which the different investigation services have to deal with.

The purposes of this coordination committee are mainly:

- The exchange of information;
- The assessment of best practices;
- The assessment of problem areas;
- The development of policy.

There is no legal basis for the ICCF-coordination meetings. The coordination meetings are ad hoc discussions. Negotiations for the creation of a legal base are foreseen to start in 2011 or later.

Participants are invited by mail and there is an intranet, protected by a password, where the meeting documents can be found. Information is exchanged by e-mail, through the intranet and during the meetings.

### 2.3 AWF

The Analysis Workfile (AWF) is the means by which Europol provides support through intelligence analysis about investigations carried out by the competent authorities of the European Union Member States (MS). The Belgian competent authorities are Belgian customs and the Belgian police.

Information provided by a Member State is seized in an analytical database and can be consulted by other Member States. Intelligence can also be submitted by a Member State that did not join the AWF. If there is a HIT the two Member States are informed. Currently, 11 EU Member States and two organisations (Eurojust and Interpol) joined the AWF.

### 2.4 Watch system of the FPS Economy

FPS Economy (the Belgian ministry of Economy) is developing, in the context of the cooperation in the fight against fiscal and social fraud, an online information network where alerts can be analysed in order to detect and prevent fraud.

The system consists of an application, SharePoint based, that will send immediately an e-mail to all the stakeholders as soon as there is a new entry submitted to the SharePoint application. Everyone can modify or delete the information. The workplace is managed by the FPS Economy. A link to the relevant information sources is provided within SharePoint.

Stakeholders :

- FPS Economy;
- External partners:
  - Bureau d'Intervention et de Restitution (BIRB)
  - FPS Finance
  - Police
  - FPS Justice
  - Food Agency
  - Drug Agency

The stakeholders will be able to report a possible case of fraud in a particular sector through an online form submitted to SharePoint. At the same time, all stakeholders will automatically be informed of this by e-mail. Each stakeholder decides himself which alerts he wants to receive and when to receive them.

### 3 BULGARIA

#### 3.1 NIPIES:

See [NIPIES](#) in section B

### 4 CYPRUS

#### 4.1 THESEAS:

The Theseas system is the first e-government application in Cyprus and supports all customs procedures. The objectives of the system are:

- the modernization of customs clearance procedures in order to comply with E.U. requirements;
- the interconnection of the customs and excise department infrastructure with the corresponding European Union systems;
- increased efficiency and response of the offered services to the traders;
- support and impose stricter controls on imported goods;
- manage the government's revenue from customs and excise taxation;
- the provision of reliable information to support the implementation of government taxation and financial strategies;
- provide reliable and adequate information to other governmental departments, such as the Statistical service.

Theseas is an information portal. It contains a number of administrative reform and trade facilitation components in order to examine current practices and procedures within the customs and excise department.

Access to the system is open to the following users:

- Customs officers located in customs headquarters, and all customs offices in the airports, the ports and post-offices and Nicosia district office. Customs officers are connected through the intranet and have access to Goods Processing Modules functions depending on their rights;
- External trade agents, carriers, importers, which are connected mainly through internet;
- Security officers and system administrators.

Theseas is also used for customs declarations.

The Theseas system is accessible through internet via [www.mof.gov.cy/ce/theseas](http://www.mof.gov.cy/ce/theseas)

## 5 CZECH REPUBLIC

### 5.1 IPO

The system is designed to share information regarding IP Rights (including trademarks, patents, etc.). It also contains information on relevant Authorities and legal Decisions in the Field of IP. This project also includes the education of public servants.

All users have unlimited access to the data but only relevant authorities (mainly the IP office) may edit the data in their field. Anyone can access the system – information is publicly available.

It only includes publicly available data. Therefore, enforcement authorities (such as customs) tend to use the original source or database instead.

### 5.2 AIP SYS

The system provides a database and analysis of IP relevant data. Its purpose is to support the internal coordination of customs and law enforcement in the field of counterfeiting and piracy.

The AIP System is comparatively complex and covers almost every aspect of the Customs' employees work in the field of IP. It appears to successfully reflect the needs and wishes of the current users and it has been further modified accordingly.

### 5.3 Project Original

See [Project Original](#) in section B

Website: [www.respektujoriginal.cz](http://www.respektujoriginal.cz)

## 6 DENMARK

There are currently no Danish projects on the rapid information exchange on counterfeiting and piracy between Danish authorities. The Danish customs authorities participate in a system where information is exchanged between national customs authorities. Furthermore the Danish customs authorities will participate in the common European IT-system ([COPIS](#)) where rights owners can request the customs authorities to react to counterfeiting products under Council Regulation (EC) No 1383/2003 of 22 July 2003. The Danish Medicines Agency Participates in a European Rapid Alert System operated by the European Medicines Agency which among others allows sharing of information about counterfeiting medicines.

The website [www.stoppiraterne.dk](http://www.stoppiraterne.dk) is currently the only national system providing information about counterfeiting.

## 7 GERMANY

### 7.1 ZGR 1.0

See [ZGR 1.0](#) in section B.  
The project is accessible through “[www.zoll.de](http://www.zoll.de)”

### 7.2 ZGR online 1.1

See [ZGR 1.1](#) in section B.

### 7.3 Conlmit

The initiative “Innovation against product piracy” includes Conlmit. In this respect the BMBF (federal Ministry of Education and research) is responsible for the program “research for the production of tomorrow”. Its purpose is to support medium sized companies, to defend themselves from copiers and pirates. E.g.: the BMBF supports research projects aiming to find ways of making machines, services and spare parts almost impossible to copy.

Conlmit enables users to share information and experiences with regard to ten different research projects. The result of these projects are published by the partners of each project.

The project page is [www.conlmit.de](http://www.conlmit.de).

## 8 ESTONIA

### 8.1 Custom DB

This Database tries to facilitate the internal coordination of customs actions regarding the importation and exportation of goods infringing IP rights. This tool is managed by customs. This tool is part of the customs intranet. It consists of three components: “Applications for actions”, “Legal acts” and “Forms and links”. The first and the last are the most important for the present study:

- “Applications for actions” pulls together electronic versions of applications for action by customs authorities, currently submitted to customs on paper or electronically. It has three sub-sections:
  - a) IP rights and applications;
  - b) Applicant (name, address, contact details or details of the representative);
  - c) expiry dates.
- “Forms and links “ contains links to relevant IP databases (e.g. databases of the Patent Office, CTM-ONLINE) which help the officers to check if the relevant IP right (excl. copyright) is protected in Estonia.

The tool also allows for uploading information about original and counterfeit goods (usually submitted by right holders on electronic format).

## 8.2 Databases of the IP office

These Databases pull together information from all registers of the Patent Office and are under the responsibility of the national IP office (granted patents, utility models, industrial designs, trademarks, geographical indications and applications thereof) and information from the official gazettes of the Patent Office (The Estonian Patent Gazette, The Estonian Utility Model Gazette, The Estonian Trademark Gazette, The Estonian Industrial Design Gazette).

The database tools allow users to search information in the databases of the national IP office. Each database allows to perform searches based on the following info:

- Name of the Applicant/Owner;
- Registration number;
- Application Number;
- Title of invention / Denomination of industrial design / Trademark/ Geographical indication.

## 9 FINLAND

### 9.1 PATJA system

See [PATJA](#) in section B.

### 9.2 The Customs Recordal

The NBC is the authority responsible for recording and granting applications for action as defined in article 5 of Council Regulation (EC) No 1383/2003

The function of the system is to centralize the information of granted applications.

The key users of the system are the NBC (national board of customs) and customs officers. NBC officers insert information on granted applications. However, the customs officers may only view such information.

The purpose of the system is to facilitate information sharing within the NBC and the various customs districts.

## 10 FRANCE

### 10.1 COPIS

[EU see COPIS section](#)

## 10.2 RIF

The system is managed by the 33rd Directorate of Customs Law Enforcement (Directorate General of Customs and Excise, Ministry of Economy & Finance).

Each Member State designates a central office and defines services entitled to use it. It aims at the creation of an EU information exchange system for risk assessment and rapid exchanges of information on suspicion of fraud.

RIF are forms exchanged by e-mail between customs services of authorised groups such as RALFH (Harbours of the North Sea), ODYSSEUS (Harbours of the Mediterranean Sea) and ICARUS (airports). These forms contain risk profiles for the fight against counterfeiting.

The information is registered in the system via special forms, pictures and documents and can be uploaded as RIF attachments.

Only designated customs officers who work on risk analysis either in 33rd Directorate of Customs Law Enforcement (Directorate General of Customs and Excise, Ministry of Economy & Finance) or in customs offices have access.

Access to the system is protected by password and username. Each user is assigned an individual username and password by the national administrator.

The information is registered in the system via special forms. These forms contain information on counterfeiting (date of incident, place, involved parties, country of origin of counterfeited products, destination, type of counterfeited products...)

New tools were recently established such as secure e-mail and a forum.

## 11 GREECE

### 11.1 AFIS

The anti-fraud information system (AFIS) was designed to exchange information rapidly, easily and securely between Member States. AFIS is governed by Council Regulation (EC) No 515/97 of 13 March 1997, which defines the rules according to which the administrative authorities of the Member States and certain third countries must mutually provide assistance and collaborate with the Commission with a view to preventing and combating fraud.

AFIS is OLAF's responsibility. It is used, within the framework of mutual assistance, by the Member States' customs and agricultural departments and by the departments responsible for controlling precursors (substances intended for illicit drug production). AFIS is also used by a number of third countries which have signed mutual assistance agreements with the European Commission (Norway, Russia, etc.). Some 200 000 electronic messages are exchanged each quarter via AFIS by the relevant departments in more than 30 countries — i.e. more than 2 500 messages per day.

AFIS is used in many fields. This system makes it possible for customs authorities to report incidents and alert for potential threats in the area of counterfeiting and piracy.

Designated national customs contact points have access to the system and feed the system with information on counterfeiting (date of incident, place, involved parties, type and country of origin of counterfeited products, destination,...). The users also feed the system with information on suspicious cargo.

Furthermore the system allows the direct interaction between the users, who can send each other various kinds of messages via the AFIS system (for example word docs, excel tables etc). There is a designated AFIS computer at each authority which is used for no other purpose and which is not online in order to ensure security.

AFIS has many applications. The aim is always the same: to share and exchange the information received by each Member State and to prevent, identify and punish fraud and other irregularities affecting the Community's financial interests.

## 11.2 RIF

See [RIF](#) in annex A, title 10.2

## 11.3 CEN-COM

The system is managed by the 33rd Directorate of Customs Law Enforcement (Directorate General of Customs and Excise, Ministry of Economy & Finance).

The system aims at the Registration of confiscations from the Hellenic Customs Authorities and the identification of current trends in piracy and counterfeiting via the data sent to the system.

The users, customs authorities, feed the system with information on counterfeiting and piracy (date of incident, place, involved parties, country of origin of counterfeited or pirated products, destination, type of counterfeited and pirated products...). The information is registered in the system via special forms.

Only Customs Officers that belong to the 33rd Directorate of Customs Law Enforcement (Directorate General of Customs and Excise, Ministry of Economy & Finance) have access through a password and username. Each user is assigned an individual username and password by the WCO.

The users feed the system with information on counterfeiting (date of incident, place, involved parties, country of origin of counterfeited products, destination, type of counterfeited products...)

N.A.

## 12 HUNGARY

### 12.1 eMAGE

See [eMage/eMarks](#) in section B.

### 12.2 COPIS

See [COPIS](#) in section B.

## 13 IRELAND

The Irish IP Office offers free and unlimited access to its database systems that are available via [www.patentsoffice.ie](http://www.patentsoffice.ie).

The implementation of European community law in Ireland does not hinder the development of such systems. Moreover, the Electronic Commerce Act 2000 promotes the legal validity of electronic information.

Users may search the patents database under the following heading:

- title;
- abstract;
- application no;
- grant no;
- Priority no. / date;
- Date of application;
- Date of grant;
- Applicant/proprietor;
- Inventor.

The trademark database can be searched under the following heading:

- Text search;
- Applicant/proprietor/holder;
- Goods / service classes.

## 14 ITALY

### 14.1 FALSTAFF

See [AIDA/Falstaff](#) in section B.

## 15 LATVIA

### 15.1 SRS

SRS facilitates the internal coordination of law enforcement actions in respect to IP piracy and counterfeit goods between national customs offices in accordance with the Council Regulation (EC) No 1383/2003.

The data obtained by customs throughout the territory of the Republic of Latvia are sent to the main Customs Office, where authorised persons create and update summaries. No information can be filtered. Each overview provides information on the trademarks concerned, the right holders, relevant contacts, protected goods, etc..

Four main groups of users can be identified :

- Customs officers or any other interested party that wants to obtain information;
- Technical administrators of the webpage;
- Substantial administrators who produce the overview (e.g. competent officers within the Main Customs Office).

There is no authorisation required in order to gain access to the data, all information is publicly available.

An overview has been published on-line, on the webpage of the SRS:

<http://www.vid.gov.lv/default.aspx?tabid=9&id=996&hl=1> in a form of a PDF file.

### 15.2 State Register of Innovations; State Register of Industrial Designs; State Register of Semiconductor Topographies; State Register of Trademarks.

Registers are composed of several data groups for industrial property, such as registration data; application data; priority data; publication data; detailed information about inventions, industrial designs, semiconductor topographies or trademarks'; information about the applicant, inventor, designer or creator of topography, patentee or holder of the registration and the representative; information about the legal status of the patent or registration, etc.

Institutions involved in the combating of counterfeiting and piracy (such as Police, Customs, Border Control and Offices of Public Prosecutors) or any other interested parties have no public access to any of the IT systems or registers mentioned above, except for the State Register of Industrial Designs. However, data from registers may be acquired by filing a request for information in a paper format.

The State Register of Industrial Designs is publicly available on the web-page of the IP office: <http://www.lrpv.lv/index.php?lang=EN&id=149>; therefore there is no authorisation procedure required. However, the information obtained from this database has no legal force. To obtain official extracts from the State Register of Industrial Designs and other

abovementioned registers, the request for information has to be filed in paper format to the Department of State Registers and Documentation of the IP office.

Users may search the information from the State Register of Industrial Designs according to the following indexes:

- Registration No;
- Application No;
- Name of the goods;
- Applicant/ owner/ Designer;
- Classification.

For other registers different categories of users are unable to interact with the system, since they are not permitted access. Data from the register may be acquired by request in a paper format, indicating the necessary information.

It is planned to make the State Register of Trademarks publicly available and online in 2010, but no specific information regarding the technical components, accessibility or legal force of such data has been provided by the IP office. So far there are no plans in respect of improvements to other State Registers

### **15.3 Integrated Information System of the Internal Affairs.**

This information system provides details on infringements of IP rights. It includes administrative and initiated criminal proceedings and information on persons who have committed crimes in relation to IP.

Apart from the fact that the Register works in an interface regime and that SOAP-1.2. webservers and HTTPS protocols are used, no other information on technical components is available.

According to law, these IT systems are accessible only to a limited range of officials and are not available to other public institutions which might need the information in order to combat the counterfeiting and piracy.

Users may search the information from the register according to the following indexes:

- Norm of the law violated;
- Personal data of the offender;
- Case number;
- Types of the offence.

According the Department of Informatics and Communications of the Ministry of Home Affairs, due to the confidentiality issues no references or any information from the registers of the Integrated Information System of the Home Affairs are publicly available through the website.

## 15.4 RAPEX

See [RAPEX](#) in section B.

## 16 LITHUANIA

### 16.1 Anti-piracy centre.

The concept was initiated by the Culture Ministry. However, the Ministry does not act as a founder of the Anti-Piracy Centre. The Anti-Piracy Centre has been founded as an association of collective administration associations and other associations of IPR holders.

The centre monitors IP markets and analyses collected information, through the creation and administration of databases containing information that assist law enforcement institutions to identify counterfeited and pirated goods. It also cooperates with customs, assisting on the confirmation of whether seized goods are counterfeit or pirated copies.

The Centre facilitates the cooperation of IPR holders in the fight against piracy.

Furthermore it assists customs, police, prosecutor's office and other law enforcement agencies in carrying out IPR protection activities.

It collates information collected by IPR holders associations and makes this available to appropriate law enforcement agencies.

The concept of the Anti-Piracy Centre was approved by the ministry of culture on 30 July 2008. However, the implementation was suspended, partly due to the financial situation and an apparent lack of initiative on behalf of IPR holders associations.

### 16.2 DB of the National IP Office.

The databases for patents, trade marks, designs and topography registers, within the National IP Office, are updated each month (including, data related to applications, registrations, refusals, cancellations etc).

The databases are publicly available at <http://www.vpb.lt>.

Advantages: Instant public access to data regarding registered IPR.

Disadvantages: updated monthly.

### 16.3 The cooperation Agreement

A cooperation agreement was set up to strengthen IPR protection on the border and in the market of Lithuania, by means of cooperation between customs and police institutions.

The police department has a register where IPR infringements are recorded. The customs department also maintains a list of indicated IPR infringements.

The customs department and police department have access to each others' registers.

There is a plan to create an information system where all relevant data regarding IPR infringements would be contained in. Such a database would be available to respective governmental institutions, law enforcement agencies and associations of IPR holders. The Ministry of Justice has been given the main responsibility for creating such system.

## 17 LUXEMBOURG

### 17.1 PLDA – COPIS

Reducing fraud and reinforcing the protection of intellectual property rights by creating an information platform containing information regarding counterfeiting and piracy and a communication platform facilitating the information exchange between the competent authorities of the Member States.

The COPIS System is part of a wider project, the PLDA System which purpose is to create a paperless environment for Customs in order to have a totally automated, interoperable, easily accessible and efficient system for all the different procedures.

The PLDA System results from the law of 14 May 2009 regarding the financing of an information technology solution for the creation of a paperless environment for Customs and trade.

The PLDA System will be implemented in three different stages.

#### Stage 1 :

- Since 1st July 2009, the PLDA system allows to electronically carry out, through a web interface or in B2G mode, the customs clearance procedures related to exportations, transits and importation.
- For the security of the electronic declarations through internet, Customs accepts LUXTRUST certificates (smartcards and signing sticks) allowing the electronic signatures of the sent declarations.

#### Stage 2 and 3 :

- Luxembourg has now started to implement interactive and cross-border public information systems according to the Council Regulation 387/2004/EC regarding the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens.
- At this stage, Luxembourg will implement the COPIS system which will be an information platform containing information regarding counterfeiting and piracy but also a communication platform facilitating the information exchange.

The COPIS system should be operational in 2012.

See also [COPIS](#) in section B.

## 17.2 SID

SID allows the national customs authorities to exchange and spread information on counterfeiting activities and intervention requests.

It also helps the research and the prosecution of offences in respect of national laws by strengthening the efficiency of cooperation procedures and the control of customs procedures.

This system rose from Council regulation (CE) N°515/91 of 13 March 1997 concerning the mutual assistance between the administrative authorities of the Member States (Cf I.1.)

## 17.3 RAPEX

[EU see RAPEX section](#)

## 17.4 ICSMS system

The ICSMS System is an information and communication platform which facilitates the communication between market surveillance authorities. The database contains information on products tested by these authorities. The platform also contains information regarding dangerous products, the voluntary recalls of products and warnings regarding counterfeited products.

This system is financed by the participating EU Member States and Switzerland.

All the data is provided by the national market surveillance authority of each Member State through a restricted online platform.

The platform is divided into two parts : (i) a limited access intranet which can only be accessed by some members of the national market surveillance authorities (ii) a public part which is opened on <http://www.icsms.org/icsms/App/index.jsp> to consumers or manufacturers.

A particular access to the intranet part is granted to a restricted number of members of the national market surveillance authorities such as ILNAS, Customs or Luxembourg Police.

These users are appointed by the ICSMS national contact point of each country. The consumers and the authorities can find online several information on a product online such as :

- the person responsible for putting it on the market;
- the applicable standard or directive;
- the certificate of conformity if it was delivered;
- the test results;
- formal defects or defects in the safety areas ;
- classification of the defects;
- incidents;
- measures undertaken by the competent authority;
- possible additional documentation : analysis reports, photographs.

The competent authorities publish all this information through the intranet private part of the website. The private part of the server is divided into two levels: a national and an international level.

Through the platform, a national authority can interact on specific product related questions with the authority of any other Member State when a product remains at national level.

After having determined the status of a product on a European level, communication with the authority of another country is possible on an international level

Consumers and manufacturers can interact with the competent authorities through the “contact” part of the public website.

The system is currently used by 12 countries (Austria, Belgium, Cyprus, Germany, Estonia, Luxembourg, Malta, the Netherlands, England, Slovenia, Sweden and Switzerland).

In Luxembourg, the number of users recognised by the system is around 20.

In a close future, the ICSMS system will become the general information support system mentioned in article 23 of the Council Regulation 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing regulation.

The market surveillance authorities benefit from :

- the rapid exchange of information between authorities;
- avoidance of duplicated activity by the sharing of test results between authorities;
- facility for fast and comprehensive cooperation with customs authorities;
- deterrents to the distribution of unsafe products.

## 18 MALTA

### 18.1 COPIS

See [COPIS](#) in section B.

### 18.2 RIF

See [RIF](#) in annex A, title 10.2.

## 19 The Netherlands

### 19.1 DIS

The purpose of DIS is to exchange information. Where relevant, information will be transferred to other national systems (and vice versa) and shared with colleagues in other EU Member States.

The DIS system is a digital database. The legal basis with regard to the exchange of information between customs services and other government agencies is the Naples II convention. The exchange of information with other parties only occurs if this is in accordance with the law.

There are two categories of users:

- o Users assigned with a role as ‘authoriser’;
- o Regular users (employees).

Users assigned with an ‘authoriser’ role have to approve all DIS registrations. As of April 1, 2010, this role will be deleted from the system. From that date, employees have the final responsibility for their own registrations. These registrations will be reviewed afterwards, inter alia because of privacy law.

The DIS system will be replaced and/or combined with a new system called ‘MAB’. Users with the proper authorisation will be allowed to use both systems at the same time.

OLAF in Brussels is responsible for the provision of the DIS, FIDE and MAB systems. These systems are part of the AFIS platform.

The contact details of OLAF are available at:

[http://ec.europa.eu/anti\\_fraud/contact\\_us/index\\_en.html](http://ec.europa.eu/anti_fraud/contact_us/index_en.html).

## 19.2 EU FIDE

EU FIDE has been developed to exchange information. The system is used in cases of fraud where fines exceed € 15.000,- or a prison sentence of 1 year or more has been imposed.

The EU FIDE system is a digital database. The legal basis with regard to the exchange of information between customs services and other government agencies is the Naples II convention. The exchange of information with other parties only occur if this is in accordance with the law.

There are two categories of users:

- Users assigned with a role as ‘authoriser’;
- Regular users (employees).

Similar to the DIS system, users assigned with an ‘authoriser’ role have to approve all EU FIDE registrations. As of April 1, 2010, this role will be deleted from the system. From that date, employees have the final responsibility for their own registrations. These registrations will be reviewed afterwards, inter alia because of privacy law.

Each user has a personally assigned unique login username and unique login password.

OLAF in Brussels is responsible for the provision of the DIS, FIDE and MAB systems. These systems are part of the AFIS platform.

The contact details of OLAF can be found here:

[http://ec.europa.eu/anti\\_fraud/contact\\_us/index\\_en.html](http://ec.europa.eu/anti_fraud/contact_us/index_en.html).

### 19.3 The Blue View System

Blue View is a system for information hubs and can be considered as a search engine for police data. Its purpose is to gain insight on data with regard to the enforcement and investigation of all national police forces.

Blue View is based on XML-techniques and the core of the system is an Oracle database where optimisations have been carried out to locate the data more quickly. The Blue View system runs within the secure police domain and the database loads in an encrypted manner.

Blue View allows users to access the system, based on their authorisation level. The authorisation model is based on a number of 'vaults', where users – based on their position – receive keys which enables them to open certain vaults. Only 'Infodesk employees' have access to the 'basic data' and only a few people have access to the extended system.

The groups of users with access to the system are people from the Criminal Investigation Department (Dienst Nationale Recherche), the National Informationhub of the KLPD (Nationaal informatieknooppunt van de KLPD), regional and district information hubs of the police forces, administrators and analysts of the Criminal Investigation Department and Kmar.

The responsible regional police force manager maintains a system of authorisations which meets the requirements of due care and the principle of proportionality. The police data may only be processed by police officials who have the proper authority granted by the proper responsible person and only for the purpose within the reach of their authority.

Each user category can use Blue View as a search engine for police data with regard to the enforcement and investigation of all national police forces.

Users can only read the information. They cannot create new datasets or enrich data. It is possible to link external databases. The data from these databases are being retrieved per link, though these data are not included and maintained in the BlueView database.  
(40.000 – 50.000 police officials)

The system has been operational since 2006 and works satisfactorily. The national police systems will be upgraded in 2010/2011. The responsible body for this upgrade is the police ICT-organisation vtsPN.

## 20 POLAND

### 20.1 VINCI SYS

See [VINCI](#) in section B.

### 20.2 DP System

DP is a database pulling together information from all the registers of the IP office (granted patents, industrial designs, trademarks, topographies of integrated circuits and geographical indications, information from the “Bulletin and News of the IP office”) and of the Ministry of Culture (the OC Register).

Users can connect to the system exclusively from authorized locations - registered IP addresses - through a VPN.

They are identified in the system by logins and passwords granted by the administrators of the system (detailed authorization arrangements are drawn by the IP office in liaison with individual beneficiary authorities).

Users may search the information from the register according to the following five indexes:

- the title;
- the right holder;
- the author;
- the number of the registration;
- the number of the register.

Output data feeds are provided either through a browser application, or through a webservice if the beneficiary authority has its own system and wants the source data from the DP System to be presented through its interface.

### 20.3 OC register

The OC register is the responsibility of the Ministry of Culture. It is a database on all optical carriers manufactured (pressed) in Poland.

The system is fed with entries covering identification data of the manufacturer, devices used for the manufacturing of optical carriers, identification codes used by those devices, types of production and their volume, instances of producing the carriers outside the main place of business, and of selling them (§ 1(4)). Input data feeds are delivered by the manufacturers on paper and electronically (§ 2(2)).

The system is administered by the authorized employees of the Ministry of Culture. Only these employees have access to the system.

Moreover, pursuant to the relevant procedures, the Police, through dedicated stations in regional police headquarters and the main headquarters, and offices of public prosecutors, through dedicated stations, have online access to the inquiry forms only.

The Border Control and the Customs Service can access the same inquiry forms through encrypted VPNs.

Other third parties (right holders in the first place) may also obtain information from the register on a need-to-know basis. In their case, however, the application must be lodged on paper. Furthermore, an applicant in this category is obliged to present a brief justification for the application, in order to lend credence to her legal interest in receiving the information.

The system is based on the MS SQL solution with a relatively simple database tool. The database is searchable according to various criteria (e.g. reporting periods, company names, titles of carriers, codes) and has a reporting function.

The Police, offices of public prosecutors, Border Control and the Customs Service can inquire the users electronically about records contained in the register.

Pursuant to the relevant procedure, the Police, through dedicated stations in regional police headquarters and the main headquarters, and offices of public prosecutors, through dedicated stations as well, have online access to the inquiry forms only.

The Border Control and the Customs Service can access the same inquiry forms through encrypted VPNs.

## 20.4 DKM portal

DKM is the portal of the Polish Higher Police School

It provides education on the methodology of investigating and combating copyright infringements.

The system is built on e-GroupWare. It consists of the following modules:

- Knowledge Base,
- Calendar;
- Contacts;
- Files;
- Bookmarks;
- News;
- Wiki;
- A voting application.

A small group of users is authorized to edit the knowledge base, files and bookmarks.

Other users view the content and are able to write messages, cast votes, and edit the calendar and contacts sections.

- The authorisation procedure is relatively simple, according to the idea of making the tool broadly available to the law enforcement and IP protection communities. Applications with a telephone number can be sent to the administrator by e-mail.
- Access is granted after the applicant's identity is confirmed by phone.

A small group of users is authorized to edit the knowledge base, files and bookmarks.

Other users view the content and are able to write messages, cast votes, and edit the calendar and contacts sections

An informal "Internet Group" at the Police School, comprising police officials developing the portal, was dismantled in 2009 and the idea of the portal itself was essentially abandoned by higher ranks. The system, therefore, could not be updated nor maintained properly. Finally, because the anti-piracy community is highly decentralized, potential participants have been insufficiently motivated to contribute to the project.

There are couple of reasons for this failure, all of institutional provenance. Nevertheless, with appropriate manning and stronger emphasis on the IP policy among high-ranking law enforcement echelons, the tool could be very useful for knowledge sharing and expertise building, and form a very valuable element of the information exchange on counterfeiting and piracy.

## 21 PORTUGAL

### 21.1 IGAC

Project IGAC is a project of the public department within the Ministry of Culture. The purpose of the project is to improve information exchange between the law enforcing authorities involved in the fight against piracy and counterfeiting and to develop an action plan at national level.

Furthermore the project includes cooperation with the private sector and aims at developing public awareness campaigns.

### 21.2 PortalGAC

See [PortalGac](#) in section B.

## 22 ROMANIA

### 22.1 Common DB

PM (Public Ministry- Romanian: Ministerul Public) is the authority which administrates the Common Database.

The Customs Authority, the Trademarks Office and the Copyright Office, GIRP and GICBP were also involved in the process of establishing the Common Database.

- Creating a common database providing information regarding the customs seizures, all criminal investigations concerning counterfeiting and piracy, intellectual property rights.
- Facilitating the cooperation between the authorities involved in the actions against counterfeiting and piracy.

The Common Database became available on February 1, 2009 on the intranet of PM. It has secure access and may be accessed by the Customs Authority, Copyright Office, and Trademarks Office.

The Common Database is available starting with February 1, 2009 on the intranet of PM. It has secured access and may be also accessed by the Customs Authority, Copyright Office, and Trademarks Office.

The operational components are: the central database at the level of the PM, the remote databases of the associated institutions (Customs Authority, the Trademarks Office and the Copyright Office, GIRP and GICBP), access web application to the Common Database and secured connections (Virtual private networks - VNPs) between institutions.

It provides information regarding the investigations carried out by the police, and also by prosecutors. It includes information about infringements, infringers, and the incrimination of actions of the infringers.

Information regarding the applications for customs, regarding interventions filed by the trademarks owners, and regarding the customs seizures of counterfeited or suspected counterfeited products is available in the Common Database.

On a daily basis, the Trademarks Office uploads and updates the information regarding the protected intellectual property rights.

The Copyright Office provides access via the Common Database to the National Registers which are under its administration. Also, at the request of the police or prosecutors, expert's opinions and findings issued by the Copyright Office are uploaded into the Common Database.

Thus, the Common Database instantly provides complete information regarding seizures, criminal investigations, intellectual property rights and measures taken by the authorities.

Each institution has a group of specific users which can access the system and have specific tasks and rights.

The individuals are recognized by the system according to the authority where they carry out their activity:

- Prosecutors;
- Police officers from GIRP and GICBP;
- Designated persons of the Trademarks Office;
- Designated persons of the Copyright Office;
- Designated persons of the Customs Authority.

Only employees of the national authorities who are involved in activities regarding counterfeiting and piracy may have access to the Common Database.

Based on the usernames and passwords granted in order to access the system, the users may have full access to the database, and may or may not amend information in the database.

For example, employees of the Trademarks Office, or of the Copyright Office, or Customs Authority cannot amend the information in the Common Database regarding criminal

investigations. Also they have limited access to the information regarding pending criminal investigations, as according to the Criminal Procedure Code, no information can be disclosed to third parties during such investigations.

In addition, each prosecutor may amend the database by inserting information regarding their current cases. They may access information regarding all the other cases without being able to amend the information on such cases.

In order to access the Common Database, a written application has to be filed with the IT server administrators of the Common Database of the PM.

After reviewing the application, the IT server administrators of the Common Database may approve or deny the access to the system.

In case the access is granted, the applicant is provided with a name and password for accessing the Common Database.

No other identification procedure is implemented.

The users interact with the system through a web interface.

The information includes data with regard to criminal investigations (carried out by the police), criminal cases (investigated by the prosecutors).

The Common Database also provides information regarding the customs seizures, applications for customs intervention, information regarding the intellectual property rights, as trademarks or geographical indications, patents, industrial designs provided by the Trademarks Office, and information provided by the Copyright Office, i.e. private multipliers, phonograms, private copies, computer programs, video-grams.

The interaction is possible between police officials and prosecutors as the criminal investigations carried out by the police are transferred to the prosecutors in order to continue the investigations, and eventually to be brought to court.

The actual number of users from the system is 1055:

- Around 246 prosecutors;
- Around 546 police officials from GIRP;
- Around 74 police officials from GICBP;
- 10 designated persons from the Copyright Office;
- 5 designated persons from the Trademark office;
- 174 designated persons from the Customs Authority.

The PHARE project, i.e. FT2007/19343.01.07.02.10 with the objective to improve and develop the current system, started in November 2009. This project represents a continuation of the initial PHARE project 2005 RO 2005/017-553.03.05, which led to the creation of the Common Database.

Among the goals of the new project are:

- To create the means to differentiate the users not only by username and password;
- To be able to upload pictures and videos of the seizures to the system;
- To link the Common Database to the Romanian Trade Registry database;
- To improve the application regarding statistics;
- To improve the system for the data collecting and analysis.

The relevant information in the area of fighting against counterfeiting and piracy is put together in the Common Database by the authorities which are authorized to enforce the intellectual property laws.

The Common Database facilitates the access to information, the cooperation between the authorities, and the coordination of law enforcement actions regarding counterfeiting and piracy.

The Common Database renders the activity of the policemen efficient with regard to the investigation of the criminal cases and of the prosecutors with regard to their settlement.

For example, as all the prosecutors and police officials dealing with cases regarding counterfeiting and piracy have access to the Common Database, it is possible to link cases with the same infringer, being investigated in different parts of the country. Also, it is possible to check if the infringer was investigated or sanctioned in the past.

The Common Database has not only the role of facilitating the communication between the associated authorities, but also provides a general image with regard to counterfeiting and piracy in Romania.

## **22.2 Trademarks office DB**

A publicly available database has been created which provides information included in the intellectual property registers regarding patents, trademarks, industrial designs.

The IP Office database includes three databases, which are available on its website, regarding:

- Patents – the database provides information with regard to all patents registered in Romania. It was launched in 1998, being one of the first online databases regarding patents;
- Trademarks (in course of registration, registered, expired, which have to be renewed). Such database provides information included in the Trademarks Register and which were published in the Official Bulletin of Intellectual Property – Trademarks Section;
- Industrial designs – the database comprises of two web applications, i.e. the register of industrial designs, and the electronic Official Bulletin of Intellectual Property – Industrial Designs section. Such electronic official bulletin is updated

daily. Therefore, any decision issued by the Trademarks Office one day, is published on the online official bulletin the next day.

Users may search information from the registers according to the following indexes:

- For trademarks – name of the trademark, and class according to the Nice Classification, or deposit number, or assigned number of the trademark
- For industrial designs – the deposit number or the assigned number of the industrial design;
- For patents – file name, patent number, name of the patent (both in Romanian and in English), inventor, owner of the patent, or applicant.

Also, users may send messages to the Trademarks Office via an online form which any user may fill in. According to the said online form, the user has to provide his/her name and e-mail address, and describe in a few words the problem he/she encountered. Three types of issues may be reported: technical problems of the webpage, issues regarding the registration procedure of the trademarks, issues regarding the registration procedure of industrial designs.

The users can only interact with the Trademarks Office by filling in the online form mentioned above. Once the online form is submitted to the Trademarks Office, the user receives a message mentioning that the Trademarks Office acknowledged the reported problem.

As mentioned above, there are no distinctive categories of users.

Internally, the Trademarks Office keeps statistics regarding the visits, and access of its online databases.

For example, only in September 2009:

- The Trademarks Office website was accessed 1,805,575 times;
- The trademarks online database was accessed 116,228 times, and 5,974 visits were registered;
- The patent online database was accessed 7,374 times, and 1,401 visits were registered;
- The industrial designs online database was accessed 1,878 times, and 414 visits were registered.

Currently the Trademarks Office applied for structured funds in order to finance a project regarding the improvement of the online databases, and applications provided by the Trademarks Office. The aim of the Trademarks Office is to transform the current databases, and the interface, into a portal providing complete information regarding intellectual property rights.

The Trademarks Office aims to develop the e-learning applications which have already been initiated, to create a contact centre for collecting all questions and therefore improving the communication between the Trademarks Office and the interested persons.

The project mentioned above is supposed to last 2 years, and the estimated time for its implementation is the beginning of 2011.

The databases provide the information included in the Trademarks Office registers regarding the intellectual property rights.

## 23 SLOVENIA

### 23.1 IT support/solutions for IWG<sup>51</sup> by SIPO

SIPO is responsible for all supportive activities for the functioning of the IWG, therefore for both mentioned sub-projects.

#### Sub-project 1:

better exchange of relevant information between the members of the IWG.

#### Sub-project 2:

raising awareness on enforcement of IPR and dissemination of information on different measures, which may be used in case of infringement of IPR, with the aim of directing the right holders to the appropriate competent authority; informing the interested public on the activities of the Slovenian state authorities and relevant activities in the EU as well as internationally; providing practical information on specific cases.

Final goal of both: easier and more efficient use of measures of competent authorities in the fight against piracy and counterfeiting.

## 24 SLOVAKIA

### 24.1 Webregisters

The Webregisters are the responsibility of the Industrial Property Office of the Slovak Republic. Data extracted from Registers, so called Webregisters make information from registers of industrial property rights accessible to public. Webregisters contain the information extracted from databases of patents, utility models, designs, topographies of semiconductor products, trademarks and designations of origin /geographical indications.

Webregisters are available to the public and users can connect to the databases freely. Webregisters are accessible without authorisation or registration via the web site of the Office.

This database contains only selected information from registers provided by the Office, the information is not completed and is not daily updated. Therefore when the customs offices or law enforcement agencies have a need for information about goods concerning the industrial property protection they have to contact individually (ad hoc) competent employees of the Industrial Property Office.

---

<sup>51</sup> Slovenian Intergovernmental Working Group for the fight against counterfeiting and piracy.

## 25 SPAIN

### 25.1 OEPM (Spanish Patents and Trademarks Office) databases

These databases intend to provide public information on files managed by the office (on trade marks, patents and inventions). These databases store information on all files after 1979 and on files for inventions registered between 1964 and 1979 and which are still in effect, also trademarks registered prior to this date and which have been extended and all previous marks now entered on computing records.

In 1999 the OEPM initiated an information service for the law enforcement authorities. This information service includes a contact point through which right holders affected by infringements can provide information in real time to the law enforcing authorities.

## 26 SWEDEN

There are no governmental initiatives on counterfeiting and piracy in Sweden. The initiative Swedish Anti Counterfeiting Group – SACG (<http://www.gacg.org/Member/Details/7>), however, has been, inter alia, working for an improved information exchange for the last years.

### 26.1 SACG Swedish Anti counterfeiting group

GACG is an informal network of national and regional IP protection and enforcement organisations most of which have a strong international dimension to their activities. There are currently 23 Members covering 36 Countries. The objectives are to exchange and share information and best practices and to participate in appropriate joint activities to solve IPR enforcement challenges through:

1. *Coordination, where appropriate, of members' international activities, especially with relation to international government organisations;*

#### **Achievements:**

Co-founder of the Inter-Agency Observatory on Counterfeiting with UNICRI – the United Nations Inter-regional Crime and Justice Research Institute; Joint projects on organised crime involvement in counterfeiting and Piracy with UNICRI; Official observer and active participant in the WIPO Advisory Committee on Enforcement; Co-founder and active participant in Interpol IP Crime Action Group; Co-ordination with WCO, WIPO, EU and others; participation in the UNECE Team of Specialists in IP.

Co-ordination and active participation in several training and education seminars, conferences and bilateral meetings, including events with WIPO, WHO, EU, Interpol, OHIM, EPO, The Baltic Council, Chinese Government, Japan Patent Office, Thailand State Intellectual Property Office; South Africa Department of Trade and Industry, Spanish Government.

Co-ordination of activities and objectives with International Business groups: BASCAP; INTA, AIM, CACP and International Industry Groups: IFPI, MPA, BSA etc.

- 2. Research and dissemination of information, and the encouragement of public awareness of the international dimension of the international trade in fakes;*

**Achievements:**

GACG has been instrumental in establishing and promoting World Anti-Counterfeiting Day as an opportunity to promote public awareness. Several high profile events have been held on this day each year for the past ten years. Generally related to travel and the international movement of fakes, events and day campaigns by several GACG member groups have considerably added to education and awareness in the UK, USA, France, Italy, Germany, Spain, Denmark, Finland and many other countries.

Instituted in 1999 the annual Global Anti-Counterfeiting Awards, jointly administered and sponsored by the GACG, have recognised exceptional work in the international campaign against the trade in fakes by official organisations, right holders, associations and latterly the media. The process of the awards as well as the presentation events generate a high level of publicity and awareness for the cause.

The UNICRI Report on The Involvement of Organised Crime in the Trade of Dangerous Fakes brought together important facts and information and launched the concept of an international observatory on counterfeiting. The CEBR report on the economic impact of fakes in Europe commissioned by the GACG and published in 2000 was an influential piece of research. The report generated a significant number of opportunities to raise awareness internationally and in addition was a prime source of justification (and acknowledged as such) for the EU Green Paper and Action plan on combating counterfeiting and piracy in the EU which led to the Council Directive on Civil Enforcement. The report also led directly to the EU Report “Counting Counterfeits” and later to the OECD study on the world-wide Economic Impact of Counterfeiting and Piracy.

Establishment of a series of Annual seminar meetings to exchange information and best practices between network members.

- 3. Encouragement and fostering of the establishment of national and other anti-counterfeiting groups.*

**Achievements:**

New groups/members in Norway, Portugal, India, the Ukraine, Nigeria, Canada, and the USA. New regional members: CIPR (former FSU) and Marques – The Association of European Trade Mark Owners. Active contact with potential candidate organisations in Mexico, Brazil, Jordan, Pakistan, Australia, Vietnam, Turkey, Hungary, Poland, Romania and South Africa.

## 27 UNITED KINGDOM

### 27.1 UK IPID (Intelligence Hub)

The intelligence hub was set up in the Intellectual Property Office January 2008 and is responsible for coordinating enforcement activities. The team is made up of eight specially trained staff who are qualified in intelligence gathering, financial and internet investigations and analytical accreditations. It is a central repository for information relating to IP crime and houses and runs the national Intellectual Property Intelligence Database (IPID).

Intelligence is provided to the hub by enforcement authorities and relevant industry bodies. The information is recorded, stored and analysed using a dedicated intelligence system (IPID). Enquiries can be sent in by enforcement authorities and any industry body who have signed a memorandum of understanding with the office. Relevant intelligence is then shared with them to assist investigations into IP crime when appropriate.

Work of the Team also includes:

- Strategic policy issues in relation to IP crime;
- Identifying strategic priorities for collaborative action;
- Identifying and disseminating good practice;
- Raising awareness of IP crime.

The production of an annual IP Crime Report that, amongst other things, identifies the scope and scale of IP crime and future trends.

The training of relevant people responsible for the protection of IPR, including enforcement officials.

### 27.2 Serious organised crime agency (Programme 17)

The Strategic Board of Programme 17 is made up of senior representatives from trading standards, police, industry sectors, including optical digital media, the Anti-Counterfeiting Group, the Alliance Against IP Theft and government bodies, such as the Local Authorities Coordinators of Regulatory Services (LACORS), the Intellectual Property Office, HM Revenue & Customs, the Bank of England, the Royal Mint and the Crown Prosecution Service. The group works on identifying long term strategic enforcement opportunities in order to tackle counterfeiting of monies and goods as well as copyright piracy at a national and international level.

The Serious Organised Crime Agency (SOCA) leads on the UK Serious Organised Crime Control Strategy. Its work in this area follows the programmes set out under the UK Control Strategy for Organised Crime. This strategy is made up of a number of linked programmes of activity which are aligned with the threats identified by SOCA in their annual UK Threat Assessment Report. Each of the programmes has a separate area of serious crime to examine and has its

own action plan and governance arrangement with the various bodies involved. Programme 17 looks at threats to the UK from three areas: identity theft, counterfeit currency and IP crime.

### **27.3 National fraud strategic authority**

On 19 March 2009, the first National Fraud Strategy was launched by the Attorney General, Baroness Scotland QC. The strategy aims to tackle all types of fraud by strengthening the counter-fraud community's response and by providing help, protection and support to individuals and businesses. The strategy was developed by the National Fraud Strategic Authority (NFSA), an executive agency of the Attorney General's office that was set up in October 2008.

The strategy brings together over 25 key private and public sector organisations. It intends to tackle fraud through a number of measures. It sets out to improve the building and sharing of knowledge about fraud, with the City of London Police establishing a new National Fraud Reporting Centre and National Fraud Intelligence Bureau.

### **27.4 HM Revenue & C**

The HMRC system is set up to analyse and develop intelligence on e-crime and to produce actionable operational products, in collaboration with other agencies.

It assists in the development and maintenance of a collaborative network of police, government and industry partners on e-crime.

The system allows exchange of information and intelligence concerning e-crime with principal stakeholders, including government departments, industry partners, academia, and the charitable sector.

HMRC have also developed web based systems to provide education and preventative advice about e-crime to industry and the public

Furthermore there are systems available that promote standards for training, procedure and response to e-crime.

### **27.5 Trading standards**

The Trading Standards Service enforces consumer related legislation as determined by central government. The variety of this legislation is vast and is always evolving.

In view of this changing environment, the Trading Standards Institute is dedicated to engaging with central government and other proposals, displayed in our responses to the various consultations which concern consumer protection issues and/or the Trading Standards profession.

[www.tradingstandards.gov.uk/](http://www.tradingstandards.gov.uk/)

### **27.6 PCEU**

The PCeU is run by the Metropolitan Police Service and is aimed at intelligence-led disruption of e-crime. It co-ordinates research on emerging e-crime threats and vulnerabilities (in collaboration with industry partners, government agencies and academia) and provides advice on this to all stakeholders.

The system assists in the Exchange of information and the development and maintenance of a collaborative network of police, government and industry partners on e-crime.

It also helps to provide education and preventative advice about e-crime to industry and the public. Promotion of standards for training, procedure and response to e-crime. Coordination of research on emerging e-crime threats and vulnerabilities (in collaboration with industry partners, government agencies and academia) and provision of advice on this to all stakeholders.

The role of the Intelligence Team is to:

- Act as Single Point of Contact (SPOC) for PCeU;
- Manage communication between National Fraud Intelligence Bureau (NFIB) and PCeU;
- Provide specialist e-crime support to National Fraud Reporting Centre (NFRC) / NFIB;
- Coordinate the response to e-crime allegations across Forces and other law-enforcement agencies;
- Conduct e-crime intelligence development and analysis;
- Manage and disseminate intelligence to law enforcement agencies and partners;
- Partnership Development Team

The role of the Partnership Development Team is to:

- Develop and maintain a collaborative network of police, government and industry partners to enable intelligence and information exchange on e-crime;
- Identify and develop joint working opportunities;
- Identify and develop sponsorship and funding opportunities.

## 27.7 IpCass

IpCass (Intellectual Property Case Search System) is located at:the Intellectual Property Office

<http://www.ipo.gov.uk/ipcass.htm>

The system provides cse summaries that have been prepared and are regularly reviewed by members of Hogarth Chambers. The Chambers, based in Lincoln's Inn, specialize in the Intellectual Property, Information Technology, Media & Entertainment and Chancery/Commercial areas of law.

The web site is hosted by the Intellectual Property office.

IpCass is jointly funded by MCPS (Mechanical Copyright Protection Society) and the Intellectual Property Office.

This service is designed to help the user locate cases involving the prosecution of criminal Intellectual Property (IP) offences.

The site contains a search engine of brief summaries of a wide range of cases relevant to the investigation of the private or public prosecution Intellectual Property (IP) offences. It is aimed at enforcement officers and others involved in the prosecution process.

### **27.8 MCPS antipiracy unit**

Mechanical Copyright Protection Society and the Performing Right Society

The MCPS Anti-Piracy Unit works with UK enforcement agencies to investigate infringements of copyrights.

### **27.9 BPI Anti-piracy unit**

BPI Anti-Piracy Unit (British Recorded Film Industry)

The BPI coordinates a team of regional investigators who work with enforcement agencies to tackle the problem of counterfeit and piracy of intellectual property.

The BPI's investigators do not have powers of arrest, but work with other intellectual property owners to support law enforcement agencies (Department for Work and Pensions, IP office, Trading Standards and Police) to provide expert verification and provision of evidence.

It provides legal support to its members and enforcement agencies in private cases, and training for the law enforcement and government agencies who carry out prosecutions.

Working with the Alliance & Third Parties

The BPI, FACT (films) and ELSPA (games) are members of the Alliance Against Intellectual Property Theft (AAIPT). The BPI formed an enforcement alliance with the DWP, FACT and ELSPA in 2003.

Police and Trading Standards – how BPI Anti-Piracy Unit helps

The BPI APU has seven regional investigators covering the UK, one Bollywood expert, three internet investigators and a technical expert in product identification.

The Unit actively investigates both physical and digital piracy.

There is a dedicated Intelligence Manager and because the Unit has several signed agreements already in place with different Police and Trading Standards authorities and UKIPO, he is able to exchange and help to develop information.

### **27.10 National IP initiative 'real deal'**

National IP initiative 'Real Deal: Working Together for Safe, Fair Markets'

The focus is on tackling the sale of counterfeit goods at UK markets and car boot fairs. It involves different agencies (government and non-government) working together, sharing best practice and intelligence.

Partners in the initiative include the Alliance Against IP Theft, Trading Standards, LACORS, NABMA, RMA, FACT, Industry Trust for IP Awareness and the Local Government Association.

A National Charter for safe, fair markets:

*Our vision*

*Markets are a valuable part of our local communities and make a vital contribution to the consumer shopping experience.*

*Local authority trading standards services, market operators, industry groups, copyright and trade mark owners are working in partnership to ensure markets are free of counterfeit and other illegal goods, so that consumers can shop, and legitimate dealers can trade, in safety and with confidence.*

*The Real Deal logo may be displayed at venues where the market operator abides by the terms of this charter and in agreement with their local trading standards service.*

*Local arrangements will underpin the practical, operational aspects of this charter. Market operators and trading standards are urged to consider the introduction of a code of practice that reflects local circumstances and demonstrates support and understanding. The code of practice will be agreed by the market operators and trading standards at a local level and will be monitored and reviewed as appropriate.*

The Market Operator's Commitment:

- To work in partnership with the local authority trading standards service to prevent the sale of counterfeit and other illegal goods at the market:
- Be aware of who is trading at the market:
- Ensure a commitment to fair trading and make the public aware of this commitment:
- The Local Authority Trading Standards Service's Commitment:
- To work in partnership with market operators to ensure their market is free from counterfeit and other illegal goods:
- Provide information and support in relation to the sale of illegal goods:
- Work with industry and trade mark representatives to identify illegal goods:
- Monitor the market and share intelligence with police, trading standards or other law enforcement agencies as well as industry and rights' owners:
- Industry and Trade Mark Representatives' Commitment:
- Provide regular and up to date information to trading standards and market operators on how to identify illegal products:
- Provide training and support on request:
- Monitor the market and alert all parties to any infringing products found.

### **27.11 Joint memorandum understanding on an approach to reduce unlawful file sharing**

Joint memorandum of understanding on an approach to reduce unlawful file-sharing, signed on 24 July 2008

#### **Objective**

All parties agree that the objective of this MOU is to achieve within 2 to 3 years a significant reduction in the incidence of copyright infringement as a result of peer to peer file-sharing and a change in popular attitude towards infringement

#### **Principles**

This MOU establishes five principles under which action will be taken, and it is accepted that further work will be undertaken on individual issues:

1. Signatories believe that a joint industry solution to this problem represents the best way forward. This will enable progress to be made rapidly on an industry solution as back-up regulatory provisions are implemented and will ensure a light touch and flexible regime. Signatories agree to work together with each other and with Ofcom to agree codes of practice.
2. Signatories, led by the creative industries, will work together to ensure that consumers are educated to respect the value of the creative process, and the importance of supporting creators to invest time and resource in developing new work, and understand that unlicensed sharing of others' work is wrong.
3. Many legal online content services already exist as an alternative to unlawful copying and sharing but signatories agree on the importance of competing to make available to consumers commercially available and attractively packaged content in a wide range of user-friendly formats as an alternative to unlawful file-sharing, for example subscription, on demand, or sharing services.
4. Signatories will work together on a process whereby internet service customers are informed when their accounts are being used unlawfully to share copyright material and pointed towards legal alternatives. In the first instance ISP signatories will each put in place a 3 month trial to send notifications to 1000 subscribers per week identified to them by music right holders, to agreed levels of evidence, as having been engaged in illicit uploading or downloading. Based on evidence from the trial, which will be analysed and assessed by all Signatories, Ofcom will agree with Signatories an escalation in numbers, widening of content coverage, and a process for agreeing a cap.
5. Signatories will be invited by Ofcom to a group to identify effective mechanisms to deal with repeat infringers. The group will report in 4 months and look at solutions including technical measures such as traffic management or filtering, and marking of content to facilitate its identification. In addition, right holders will consider prosecuting particularly serious infringers in appropriate cases.

**Annex C: System Analysis**

	0	1	2	3	4	5
<b>Maturity</b>	Not yet deployed	Less than one year	1 to 2 years	2 to 3 years	3 to 4 years	More than 4 years
<b>Users Numbers</b>	Less than 1000	1001 to 10000	10001 to 25000	25001 to 50000	50001 to 100000	More than 100000
<b>security Level</b>	Not implemented	Existing access role definition	Login and Password verification mechanism	Login and Password verification expiration	Certificate mechanism	Smart card, Usb, Token
<b>interoperability Level</b>	Not implemented	Planned	Just with the same technology RMI	Based on the socket	Existing old technologies interface CORBA	New technologies SOAP/JMS
<b>compliance</b>	N/A	Partial	Government standard	National standard	European standard	International standard ISO
<b>Functionality</b>	Static page	Forum	Mailing	Document Management	Mailing/Alert/Forum/Doc management	Mailing/Alert/Forum/Doc management/RSS
<b>usability</b>	Terminal	Difficult	Need training	Documentation needs	No training needs	User friendly
<b>technological tools</b>	Old technology	Client server NOT web technology	Static page/data	Web CGI	Web php/.net/asp/jsp/	Web 2.0

Table 1: Criteria rating Matrix

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
AUSTRIA	Findok	Unknown	Less than 1000	Existing access role definition	Unknown	Unknown	Forum	Unknown	Unknown	<a href="https://findok.bmf.gv.at/findok/link?bereich=ufs-tx&amp;gz=%22RV/0028-W/05%22">https://findok.bmf.gv.at/findok/link?bereich=ufs-tx&amp;gz=%22RV/0028-W/05%22</a>

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
	ELAK	Unknown	Less than 1000	Not implemented	Planned	Unknown	Mailing/Alert/Forum/Doc management	User friendly	Web	<a href="http://www.digitales.oesterreich.gv.at/site/6571/default.aspx">http://www.digitales.oesterreich.gv.at/site/6571/default.aspx</a>
	COPIIS	Not yet deployed	25001 to 50000	Login and Password verification expiration	Planned	European standard	Mailing/Alert/Forum/Doc management	Unknown	Web 2.0	
BELGIUM		Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
BULGARIA	NIPIES	More than 4 years	1001 to 10000	Existing access role definition	Based on the socket	Unknown	Document Management	Documentation needs	Web	<a href="http://panaton.tyepad.com/photos/technologyicons/nipies.html">http://panaton.tyepad.com/photos/technologyicons/nipies.html</a>
CYPRUS	THESEAS	Unknown	10001 to 25000	Login and Password verification mechanism	Unknown	Unknown	Document Management	User friendly	Web 2.0	<a href="http://www.mof.gov.cy/ce/theseas">http://www.mof.gov.cy/ce/theseas</a>
	MARINFO	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	CEN BALKAN info System	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	AFIS Cooperation with OLAF	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
DENMARK	<a href="http://www.stoppiraterne.dk">www.stoppiraterne.dk</a>	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	<a href="http://www.stoppiraterne.dk">www.stoppiraterne.dk</a>
	COPIIS	Not yet deployed	25001 to 50000	Login and Password verification expiration	Planned	European standard	Mailing/Alert/Forum/Doc management	Unknown	Web 2.0	
GERMANY	ZGR 1.0	1 to 2 years	Less than 1000	Not implemented	Planned	N/A	Mailing	Unknown	Web	<a href="http://www.zoll.de">http://www.zoll.de</a>

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
ESTONIA	ZGR online 1.1	Not yet deployed	Unknown	Not implemented	Planned	Partial	Mailing/Alert/Forum/Doc management	Documentation needs	Web	<a href="http://www.conimit.de">http://www.conimit.de</a>
	Conlimt	2 to 3 years	Less than 1000	Login and Password verification mechanism	Not implemented	Unknown	Mailing	No training needs	Web	
	Custom DB	3 to 4 years	Less than 1000	Login and Password verification mechanism	Not implemented	N/A	Unknown	User friendly	Client server NOT web technology	
	DBs of PO	More than 4 years	Unknown	Not implemented	Not implemented	N/A	Unknown	Unknown	Unknown	
FINLAND	PATJA SYS	Unknown	25001 to 50000	Login and Password verification mechanism	Planned	European standard	Mailing/Alert/Forum/Doc management	Unknown	Unknown	
	The Customs Recordal	Unknown	Less than 1000	Login and Password verification mechanism	Not implemented	Partial	Unknown	Unknown	Unknown	
FRANCE	COPIS	Not yet deployed	25001 to 50000	Login and Password verification expiration	Planned	European standard	Mailing/Alert/Forum/Doc management	Unknown	Web 2.0	
	RIF	Unknown	Unknown	Existing access role definition	Not implemented	Unknown	Mailing/Alert/Forum/Doc management	Unknown	Unknown	
	CEN / INFO--IPR	Unknown	Unknown	Existing access role definition	Unknown	Unknown	Unknown	Unknown	Unknown	
GREECE	Integrated Information System for the	Unknown	Unknown	Certificate mechanism	Unknown	N/A	Mailing	User friendly	Web php/.net/asp/jsp /	

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
	monitoring of the enforcement of the administrative fine regarding IPR cases and collection of statistical data									
	AFIS	Unknown	Unknown	Login and Password verification mechanism	Unknown	European standard	Mailing/Alert/Forum/Doc management	Unknown	Unknown	
	RIF	Unknown	Unknown	Login and Password verification mechanism	Not implemented	Unknown	Mailing/Alert/Forum/Doc management	Need training	Web php/.net/asp/jsp /	
	CEN-COM	Unknown	Less than 1000	Login and Password verification mechanism	Unknown	Unknown	Unknown	Unknown	Unknown	
HUNGARY	eMAGE	More than 4 years	Unknown	Unknown	New technologies SOAP/JMS	European standard	Mailing/Alert/Forum/Doc management	User friendly	Web php/.net/asp/jsp /	<a href="http://emarks.iis@innov.com/Objectives.html">http://emarks.iis@innov.com/Objectives.html</a>
	COPIS	Not yet deployed	25001 to 50000	Login and Password verification expiration	Planned	European standard	Mailing/Alert/Forum/Doc management	Unknown	Web 2.0	
IRELAND					Unknown	Unknown	Unknown	Unknown	Unknown	
ITALY	FALSTAFF	Unknown	1001 to 10000	Certificate mechanism	New technologies SOAP/JMS	Unknown	Mailing/Alert/Forum/Doc management	No training needs	Web php/.net/asp/jsp /	<a href="https://telematic.agenziaadogane.it/TelematicoFunz">https://telematic.agenziaadogane.it/TelematicoFunz</a>

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
										<a href="http://www.vid.gov.lv/default.aspx?tabid=9&amp;id=996&amp;hl=1">ioniDiAccessoWEB/FunzioniDiAccessoServlet?UC=10&amp;SC=1&amp;ST=1</a>
LATVIA	Summary on the applications for protection of IP rights received at C authorities of the Rep. Of Latvia State register of innovations; of industrial designs; of semiconductor topographies; of trademarks	Unknown	Unknown	Not implemented	Unknown	Unknown	Unknown	Unknown	Unknown	<a href="http://www.vid.gov.lv/default.aspx?tabid=9&amp;id=996&amp;hl=1">http://www.vid.gov.lv/default.aspx?tabid=9&amp;id=996&amp;hl=1</a>
	Integrated INFO SYS of internal Affairs	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	RAPEX SYS	More than 4 years	Unknown	Certificate mechanism Login and Password verification mechanism	Unknown New technologies SOAP/JMS	Unknown	Unknown Mailing	Unknown	Unknown Web php/.net/asp/jsp /	<a href="http://ec.europa.eu/consumers/dyna/rapex/rapex_archives_en.cfm">http://ec.europa.eu/consumers/dyna/rapex/rapex_archives_en.cfm</a>
LITHUANIA	• Anti-piracy	Not yet deployed	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
	centre									
	<ul style="list-style-type: none"> <li>• DB of the National IP Office</li> <li>• The cooperation Agreement</li> </ul>	Unknown	Unknown	Not implemented	Unknown	Unknown	Unknown	Unknown	Unknown	<a href="http://www.vpb.lt">www.vpb.lt</a>
LUXEMBOURG		Unknown	Unknown	Not implemented	Not implemented	N/A	Mailing	Unknown	Unknown	
	COPIs SID	Not yet deployed	25001 to 50000	Login and Password verification expiration	Planned	European standard	Mailing/Alert/Forum/Doc managment	Unknown	Web 2.0	
	RAPEX SYS	More than 4 years	Unknown	Login and Password verification mechanism	New technologies SOAP/JMS	Unknown	Mailing	Unknown	Web php/.net/asp/jsp /	<a href="http://ec.europa.eu/consumers/dyna/rapex/rapex_archives_en.cfm">http://ec.europa.eu/consumers/dyna/rapex/rapex_archives_en.cfm</a>
	ICSMS System	More than 4 years	Less than 1000	Unknown	Based on the socket	Unknown	Mailing	User friendly	Unknown	<a href="http://www.icsms.org/icsms/App/index.jsp">http://www.icsms.org/icsms/App/index.jsp</a>
MALTA	COPIs	Not yet deployed	25001 to 50000	Login and Password verification expiration	Planned	European standard	Mailing/Alert/Forum/Doc managment	Unknown	Web 2.0	
	ECP	Unknown	Less than 1000	Login and Password verification mechanism	Not implemented	N/A	Static page	Unknown	Client server NOT web technology	
	RIF	Unknown	Less than 1000	Login and Password verification mechanism	Not implemented	N/A	Static page	Unknown	Client server NOT web technology	
NETHERLANDS	DIS and EU FIDE The BLUE view	More than 4 years	25001 to 50000	Login and Password	Unknown	Unknown	Government standard	Unknown	Web 2.0	

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
	system			verification expiration						
POLAND	VINCI SYS	More than 4 years	1001 to 10000	Login and Password verification expiration	Unknown	Unknown	Document Management	Unknown	Web php/.net/asp/jsp /	
	DP System	Unknown	Unknown	Certificate mechanism	New technologies SOAP/JMS	Unknown	Mailing/Alert/Forum/Doc managment	Unknown	Web php/.net/asp/jsp /	
	OC register	Unknown	Unknown	Login and Password verification mechanism	Unknown	Unknown	Unknown	Unknown	Unknown	
	DKM portal	Unknown	Unknown	Existing access role definition	Unknown	Unknown	Mailing/Alert/Forum/Doc managment/RSS	User friendly	Web php/.net/asp/jsp /	
PORTUGAL	IGAC	Not yet deployed	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	PortalGAC	Unknown	Unknown	Not implemented	Unknown	Unknown	Unknown	Unknown	Unknown	
ROMANIA	Common DB	1 to 2 years	1001 to 10000	Login and Password verification expiration	Planned	Unknown	Static page	User friendly	Web php/.net/asp/jsp /	
	Trademarks office DB	Unknown	More than 100000	Not implemented	Not implemented	N/A	Static page	User friendly	Web php/.net/asp/jsp /	
	Copy right official portal	Unknown	Unknown	Not implemented	Not implemented	N/A	Unknown	User friendly	Web php/.net/asp/jsp /	<a href="http://rn.ordra.ro/default.aspx">http://rn.ordra.ro/default.aspx</a>
SLOVENIA	IT support/solutions for IWG by SIPO	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
SLOVAKIA	Webregistre	Unknown	Unknown	Not	Unknown	Unknown	Static page	Unknown	Web	

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
	rs			implem e d					php/.net/asp/jsp /	
SPAIN	OEPM DB	More than 4 years	Less than 1000	Not implem e d	Unknown	Unknown	Unknown	Unknown	Unknown	<a href="http://www.oepm.es">www.oepm.es</a>
CZECH REPUBLIC	Enforceme nt SYS	Unknown	Unknown	Not implem e d	Not implemented	Unknown	Mailing	User friendly	Web php/.net/asp/jsp /	
	AIP SYS	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	Project Original	Unknown	Unknown	Not implem e d	Unknown	Unknown	Unknown	Unknown	Unknown	<a href="http://www.respektujioriginal.cz">www.respektujioriginal.cz</a>
UNITED KINGDOM	UK IP crime group	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	Serious organised crime agency	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	National fraud strategic authority	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	HM Revenue & C	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	Trading standards	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	PCeU	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	IpCass MCPS antipiracy unit	Unknown	Unknown	Unknown	Not implem e d	Unknown	Unknown	Unknown	Web php/.net/asp/jsp /	
		Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	

Member State	System	Maturity	Number of users	security Level	interoperability Level	compliance	Functionality	usability	technological tools	URL
	BPI Anti-piracy unit	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	National IP initiative 'real deal'	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
	Joint memorandum understanding on an approach to reduce unlawful file sharing	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	
SWEDEN	SACG Swedish Anti counterfeiting group	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	<a href="http://www.gacg.org/Member/Details/7">http://www.gacg.org/Member/Details/7</a>

Table 2: Counterfeiting and Piracy System Analysis

**Annex D: Comparative matrix of the national reports.**

	<b>Institutional Framework+ Authority in charge of described system(→)</b>	<b>Most promising projects</b>	<b>Purpose</b>	<b>Functional and technical components (DB=Database) (INFO=Information) (EX=Exchange) (Admin=Administrator) (SYS=System)</b>	<b>Users (U=User)</b>	<b>General assessment, advantages (Pro.) &amp; disadvantages (Con.)</b>	<b>Recommendations</b>
BE	<ul style="list-style-type: none"> <li>FPS Economy</li> <li>Customs →</li> <li>Federal police</li> </ul>	Customs DB	INFO EX on right holders	INTRANET for customs E-mail network for other authorities Access is allowed with a password. Customs officials have direct access to the DB's, other authorities need to file a request for information	Customs officials (approx. 4000) Officials of the FPS economy (approx. 15)	n.a.	Improvement is always possible A more structural cooperation (economy, customs, police) A more structural cooperation imbedded in mutual agreements and protocol would confirm the present cooperation. A multi-agency service for Belgium where on a fulltime base the three competent services are working physically together in one service. This agency could perform as a national contact point where all new IPR cases are dispatched to one of three services according to the specificity of that case.
	<ul style="list-style-type: none"> <li>FPS economy</li> <li>FPS Justice</li> <li>Food and drug agency</li> <li>Medicine agency</li> <li>Police</li> </ul>	<ul style="list-style-type: none"> <li><b>Interdepartmental project against fraud, including the fight against counterfeiting</b></li> </ul>	<ul style="list-style-type: none"> <li>INFO EX</li> <li>Determination of best practices</li> <li>Determination of problem areas</li> <li>Policy making</li> </ul>	<ul style="list-style-type: none"> <li>ICCF/CICF is a coordination body representing different public services involved in the fight against economic fraud. As from 2007 a working group has been set up within this commission, which will specifically focus on the fight against counterfeit and piracy and discuss the specific problems which the different investigation services have to deal with.</li> <li>There is a workspace with password which contain the meetingdocuments.</li> <li>EX of INFO is done by e-mail or intranet or during the meetings.</li> </ul>	• N.a.	<ul style="list-style-type: none"> <li>No legal basis</li> <li>Ad hoc</li> <li>Input is based on goodwill</li> </ul>	• N.a.

BUL	<ul style="list-style-type: none"> <li>• PO →</li> <li>• C →</li> <li>• Min →</li> </ul>	<ul style="list-style-type: none"> <li>• <b>NIPIES</b></li> </ul>	Internal coordination of law enforcement actions	<ul style="list-style-type: none"> <li>• Register DB</li> <li>• C DB</li> </ul>	<ul style="list-style-type: none"> <li>• Central Admins</li> <li>• Admins @ Institutes</li> <li>• Us with access and authority to enter data</li> <li>• Us with access</li> </ul>	<ul style="list-style-type: none"> <li>• Generally Sufficient</li> <li>• However improvement needed to comply with new e-gov. legislation</li> <li>• Pro.: All institutions responsible are involved</li> <li>• Con.: SYS was adopted before e-gov. legislation</li> </ul>	<ul style="list-style-type: none"> <li>• Adaptation to new e-gov technical standards.</li> <li>• Interinstitutional ↔ Difficult financing</li> <li>• Enrichment of content ↔ enable Min of Home Affairs and Min of Justice to also enter INFO</li> <li>• Improve the IP enforcement ↔ Easy access to applications for action by C tools for sharing and disseminating good enforcement</li> </ul>
CY	<ul style="list-style-type: none"> <li>• CCED (Min Fin) →</li> <li>• Council of Ministers</li> </ul>	<ul style="list-style-type: none"> <li>• <b>THESEAS</b> (C and Excise Computerised SYS) = Fully Harmonised with the procedures of the EU</li> </ul>	Interconnection of C and excise	INFO portal designed for trades	<ul style="list-style-type: none"> <li>• C officials</li> <li>• Ext. trade agents</li> <li>• Security officials and admins</li> </ul>	<ul style="list-style-type: none"> <li>• Sufficient structure for the interconnection of the C and excise department infrastructure with the corresponding European SYSS</li> </ul>	<ul style="list-style-type: none"> <li>• Take advantage of the funds available</li> <li>• Participate in Joint Investigation Teams (for C officials)</li> <li>• Make use of procedures available under the Convention on the use of INFO technology in the C Sector</li> </ul>
DK	<ul style="list-style-type: none"> <li>• Patent &amp; trademark office</li> <li>• Public prosecutor</li> <li>• Tax authorities</li> <li>• Min of culture</li> <li>• Police, Medicine agency, The Danish Safety technology authority, the national consumer agency, the Danish veterinary and food administration and Denmark's export Council</li> </ul>	<ul style="list-style-type: none"> <li>• No projects on the EX of INFO,</li> <li>• Website <a href="http://www.stoppiraterne.dk">www.stoppiraterne.dk</a></li> </ul>	Inform citizens, companies and public authorities about counterfeiting	<ul style="list-style-type: none"> <li>• Standard website</li> </ul>	<ul style="list-style-type: none"> <li>• Citizens</li> <li>• Companies</li> <li>• Public authorities</li> </ul>	<ul style="list-style-type: none"> <li>• EX on a case to case basis.</li> <li>• Pro.: close personal contact between key persons</li> <li>• Con.: cooperation founded on a weak mandate</li> </ul>	<ul style="list-style-type: none"> <li>• A special section for enforcement</li> <li>• A new law facilitating data EX</li> <li>• Defining priority of anti-counterfeiting</li> </ul>
G	<ul style="list-style-type: none"> <li>• C authority →</li> <li>• Zivit</li> <li>• Min of Education and research (BMBF)</li> <li>• Authorities of the Federal states</li> </ul>	<ul style="list-style-type: none"> <li>• <b>ZGR online 1.0</b></li> </ul>	Used for protection of IPR from the import of counterfeit goods.	<ul style="list-style-type: none"> <li>• E-filing of applications and change of filed applications by the RHs at any time</li> <li>• E-processing of applications (Crime)</li> <li>• INFO and research tool regarding e-applications filed by the RHs</li> </ul>	<ul style="list-style-type: none"> <li>• Applicants</li> <li>• CRIME-Us</li> <li>• Us of the tool E-AGENT</li> </ul>	<ul style="list-style-type: none"> <li>• Awareness of issue of counterfeiting and piracy</li> <li>• Pro.: combined approach of repressive (ZGR 1.0 &amp; 1.1) and preventive (Conlimit) measures</li> </ul>	<ul style="list-style-type: none"> <li>• International cooperation should be improved</li> <li>• No meaningful cooperation in the development of preventive measures against counterfeiting and piracy.</li> <li>• International DB for the EX of INFO about strategies &amp; tech. Solutions</li> </ul>
	<ul style="list-style-type: none"> <li>• C authority →</li> </ul>	<ul style="list-style-type: none"> <li>• <b>ZGR online 1.1</b> ( In implementation phase.)</li> </ul>	e-registration of seizures with automatic data transfer to the authorities responsible for investigation and evaluation	<ul style="list-style-type: none"> <li>• E-registration of seizures with automatic statistical recording</li> <li>• DB for statistic evaluation</li> <li>• Interface with the SYS</li> </ul>	<ul style="list-style-type: none"> <li>• Us who register seizures</li> <li>• Us who analyse statistic data</li> <li>• Interface for Us</li> </ul>		

				info_IPR	of Info_IPR		
	• BMBF →	• Conlmit	Support medium sized companies to defend themselves from copiers and pirates.	• Enables persons to share INFO and experiences with regard to the different research projects.	n.a.		
	• Authorities of the Federal States → • BfArM →	• (a) RAS for quality defect including counterfeit • (b) WGEO • (c) IMPACT • (d) Obligation of manufacturers to inform authorities about the suspicion of counterfeit Pharmaceuticals	(a) and (d) : INFO EX on counterfeit pharmaceuticals  (b) and (c) general INFO EX	• e-mail or fax	Only one category		
EST	• Min of culture – Copyright committee →	• C DB	Internal coordination of C actions regarding the importation & exportation of goods infringing IP rights	• C Intranet: • Applications for actions (eApp. 's) • Forms and links (to relevant IP DB's) • Legal Acts	• All C officials	• Solutions fulfil their main purpose to provide quick INFO • Pro.: C DB very valuable tool for sharing INFO on effective applications and makes the enforcement-process more efficient.	n.a.
		• DBs of the PO	Pulling together INFO of all the registers of the PO and INFO from the official gazettes of the PO.	n.a.	• Publicly available	• Pro.: quick, free of charge, easy to use • Con.: no legal status, DBs are updated weekly and do not contain the very latest info.	
FIN	• Min of education • Min of Employment • Min of Economy • Min of Home Affairs → • Police → • National board of C (NBC)	• PATJA SYS	Facilitating internal coordination of law enforcement actions regarding e.g. counterfeiting and piracy	Includes INFO on e.g. all requests of • Investigations submitted to the Police or NBC, • Investigation memorandums and diaries and • INFO of possible penalties in relation to the counterfeiting and piracy issues	• Police, • C and Border Guard service officials • Certain officials of the ministries of the Home Affairs	• NBC & C find the SYS sufficient • Pro.: info is shared efficiently & U friendly, instructions are detailed.	Most valuable DBs are the international DBs → recommended to be the subject of future improvements.
	• NBC →	• The C Recordal	Recording of granted applications for action as defined in article 5 council Regulation (EC no 1383/2003)	• centralise the INFO of granted applications	• NBC • C officials		

F	<ul style="list-style-type: none"> <li>• C</li> <li>• Judicial police</li> <li>• General directorate for competition, consumption and fight against fraud (DGCCRF)</li> </ul>	<ul style="list-style-type: none"> <li>• <b>COPIS (EC)</b></li> </ul>	Enables INFO EX between EC and Member States with regard to requests to intervene and restitutions of statistics	<ul style="list-style-type: none"> <li>• C of Member States authorise and validate national and European requests to intervene and introduce them into COPIS system.</li> </ul>	Work in progress (end of 2011)	<p>Copis seems compatible with the French framework and it appears sufficient as far as it enables rapid INFO EX.</p> <p>Pros.:</p> <ul style="list-style-type: none"> <li>• automatic up-streaming of trimestrial or annual national statistics</li> <li>• Exchange or request to intervene will be instantaneous.</li> </ul>	n.a.
GR	<ul style="list-style-type: none"> <li>• Hellenic copyright organisation –OPI (Min. of Cult.)→</li> <li>• 33rd dir. Of C,</li> <li>• Min Of econ. &amp; fin.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Integrated INFO SYS for the monitoring of the enforcement of the administrative fine regarding IPR cases and the collection of statistical data (OPI)</b></li> </ul>	<ul style="list-style-type: none"> <li>• Overview of the situation in Greece regarding piracy and violations of IPR (via DB)</li> <li>• Control cases of recidivist offenders within the same fiscal year (fine is doubled in such cases)</li> <li>• Informing of the holders of intellectual property rights.</li> </ul>	Syzefxis (existing National Public Administrative Network ) → increased security of the SYS, high availability.	<ul style="list-style-type: none"> <li>• The Hellenic Copyright organisation</li> <li>• The special control service</li> <li>• The C Authorities</li> <li>• The Hellenic Police</li> <li>• The port authorities</li> </ul>	<ul style="list-style-type: none"> <li>• Generally sufficient</li> <li>• Relevant sanctions against counterfeiting and piracy are already in place and the relevant authorities are very successful in their mission.</li> <li>• ICIS will be expanded to allow EX between C.</li> </ul>	<ul style="list-style-type: none"> <li>• Fax &amp; email are basic means of EX → ensure higher availability with the development of INFO SYSs</li> <li>• Stronger authentication procedures</li> <li>• The use of Syzefxis network as the basic infrastructure</li> </ul>
	<ul style="list-style-type: none"> <li>• 33<sup>rd</sup> dir.of C Law Enforcement</li> </ul>	<ul style="list-style-type: none"> <li>• <b>The AFIS system</b></li> </ul>	<ul style="list-style-type: none"> <li>• Interconnection of the Hellenic C authorities</li> <li>• EX of INFO on counterfeiting</li> <li>• EX of INFO on suspicious</li> </ul>	Reports of incidents that have taken place and Alerts for potential threats	<ul style="list-style-type: none"> <li>• Customs Authorities Officials</li> </ul>	<ul style="list-style-type: none"> <li>• Increased security</li> </ul>	
HU	<ul style="list-style-type: none"> <li>• Police</li> <li>• C and finance guard</li> <li>• PO →</li> <li>• HENT</li> </ul>	<ul style="list-style-type: none"> <li>• No special INFO SYSs yet</li> <li>• VPOP -&gt; COPIS</li> <li>• <b>eMage DB</b></li> </ul>	<ul style="list-style-type: none"> <li>• Intensifying the fight against the illegal copying of existing trademarks,</li> <li>• Industrial designs.</li> </ul>	Accessible webapp. Featurebased - similarity search Via an online portal	<ul style="list-style-type: none"> <li>• TBD</li> </ul>	<ul style="list-style-type: none"> <li>• Increase of collaborative ability</li> <li>• Pro.: Robotsam sys. of ORK support traditional industrial property</li> <li>• Con.: no special anti counterfeit and anti-piracy features.</li> <li>• No capability of rapid INFO EX between domestic organisations</li> </ul>	Develop similarly to the EX-service, multilingual and interoperable institutional and technical SYSs on European Level.
I	<ul style="list-style-type: none"> <li>• IP unit</li> <li>• PO →</li> <li>• The revenue commissioners (C)</li> <li>• National bureau of criminal investigations</li> <li>• Department of Enterprise trade and Employment →</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Patent register and DB</b></li> </ul>	Free and unlimited access to the Patents, Trademarks and designs register which contain detailed INFO on specific published patents, trademarks and designs	n.a.	Open to the public	<ul style="list-style-type: none"> <li>• No national policy framework in this area.</li> <li>• No e-gov. SYS. (except register and DB)</li> </ul>	Address issue of rapid EX of INFO on counterfeiting and piracy both on policy and implementation level.
IT	<ul style="list-style-type: none"> <li>• C authority →</li> <li>• Min of economic development</li> </ul>	<ul style="list-style-type: none"> <li>• <b>FALSTAFF (Fully Automated Logical SYS Against Forgery Fraud)</b></li> </ul>	DB of original products to be protected against counterfeiting.	<ul style="list-style-type: none"> <li>• DB is inserted in the SYS AIDA (Automazione integrata Dogane e Accise) .</li> </ul>	<ul style="list-style-type: none"> <li>• C Agency (central level)</li> <li>• Local branches</li> </ul>	<p>Pro.:</p> <ul style="list-style-type: none"> <li>• Interoperability with other e-tools like AIDA</li> </ul>	Use of e-id

	<ul style="list-style-type: none"> <li>National office for patents and trademarks</li> <li>Police forces</li> <li>Other stakeholders</li> </ul>			<ul style="list-style-type: none"> <li>DB is fed by RHs.</li> <li>Entries contain all technical INFO about the product that enable it to be recognised and therefore protected.</li> <li>Integration of the DB and the C circuit of control, that analyses in real time all import and export declarations submitted to the C offices.</li> </ul>	<ul style="list-style-type: none"> <li>of the authority/C offices</li> <li>Min for Economic Development</li> <li>Companies/producers holders of right</li> <li>Private entities and associations</li> <li>Consumers.</li> </ul>	<ul style="list-style-type: none"> <li>Clear policy and legal framework</li> <li>Prevents fake goods of foreign origins to enter the country.</li> <li>Protect the Made in Italy label</li> <li>Full compliance with EU standards</li> <li>User-friendly</li> </ul> <p>Con.:</p> <ul style="list-style-type: none"> <li>Missing= policy to prevent Italian companies from being actors of illicit counterfeiting and piracy actions against foreign brands.</li> <li>Main strengths of Falstaff are:</li> <li>No acceptance of documents of foreign origin (e-signature standards)</li> </ul>	
LAT	<ul style="list-style-type: none"> <li>INFO center of internal affairs</li> <li>SRS</li> <li>PO</li> <li>Consumer rights protection center</li> </ul>	<ul style="list-style-type: none"> <li><b>Summary on the applications for protection of IP rights received at C authorities of the Rep. Of Latvia</b></li> </ul>	Facilitating internal coordination of law enforcement	<ul style="list-style-type: none"> <li>Published on-line in PDF.</li> <li>No INFO can be filtered</li> </ul>	<ul style="list-style-type: none"> <li>C officials</li> <li>Technical administrators</li> <li>Substantial administrators</li> </ul>	<ul style="list-style-type: none"> <li>Framework is sufficient. However no practical implementation of the policy.</li> <li>Generally insufficient normative and institutional infrastructure for establishing rapid INFO EX.</li> <li>Existing SYSs are not efficient and only available to the system-holders.</li> <li>Biggest drawback = inability of involved institutions to connect to each other. INFO EX is paper-based. (not rapid and not systematic)</li> </ul>	<ul style="list-style-type: none"> <li>Ensuring existing IT-SYSS of the institutions to be publicly available.</li> <li>At least a register of TM.</li> </ul>
		<ul style="list-style-type: none"> <li><b>State register of innovations; of industrial designs; of semiconductor topographics; of trademarks</b></li> </ul>	Registers are composed of several data groups about industrial property objects	n.a.	<ul style="list-style-type: none"> <li>Institutions which are involved in combating counterfeiting and piracy</li> </ul>		
		<ul style="list-style-type: none"> <li><b>Integrated INFO SYS of internal Affairs</b></li> </ul>	Provides info regarding <ul style="list-style-type: none"> <li>infringements of IP rights,</li> <li>administrative and criminal proceedings initiated.</li> </ul>	<ul style="list-style-type: none"> <li>SOAP-1.2,</li> <li>Web-server and</li> <li>HTTPS protocols</li> </ul>	n.a.		
		<ul style="list-style-type: none"> <li><b>RAPEX</b></li> </ul>	EX of INFO between Consumer Protection Centre of Latvia and other market surveillance authorities and law enforcement authorities within the EU		<ul style="list-style-type: none"> <li>Consumer Rights Protection Centre</li> </ul>		
LIT	<ul style="list-style-type: none"> <li>Culture Min</li> <li>C</li> </ul>	<ul style="list-style-type: none"> <li><b>Anti-piracy centre</b></li> </ul>	<ul style="list-style-type: none"> <li>Monitoring IP-market</li> <li>analysis of collected INFO,</li> </ul>	n.a.	n.a.	<ul style="list-style-type: none"> <li>Policy framework is lacking clear directions.</li> </ul>	<ul style="list-style-type: none"> <li>Active participation of IPRHs associations</li> </ul>

	<ul style="list-style-type: none"> <li>• Police department</li> <li>• Culture Min</li> <li>• IP office</li> <li>• Home Affairs Min</li> <li>Min of justice</li> </ul>		<ul style="list-style-type: none"> <li>• creation and administration of data bases containing INFO that would assist law enforcement institutions to identify counterfeited and pirated goods</li> <li>• Cooperation with C.</li> <li>• Facilitation of cooperation of IPRH</li> <li>• Assisting C, Police, prosecutors office, other law enforcement.agencies</li> </ul>			<ul style="list-style-type: none"> <li>• Promising initiative = <b>the Strategy of Means against Unofficial and Unaccounted Economy</b> (end of 2009) → Interdepartmental Commission for Rapid EX of INFO on IPR Infringement.</li> </ul>	<ul style="list-style-type: none"> <li>• Single DB SYS which would be accessible by law enforcement agencies and IPRHs associations</li> </ul>
		<ul style="list-style-type: none"> <li>• <b>DB of the IP office</b></li> </ul>	The DBs of patent, trade mark, design and topography registers of the IP office	n.a.	Public		
		<ul style="list-style-type: none"> <li>• <b>The cooperation Agreement</b></li> </ul>	Strengthen IPR protection on the border and in the market of Lithuania by means of cooperation between C and police institutions	<ul style="list-style-type: none"> <li>• The police Department has a register where IPR infringements are recorded.</li> <li>• The C Department maintains a list of indicated IPR infringements.</li> </ul>	n.a.		
LUX	<ul style="list-style-type: none"> <li>• Min of economy and foreign trade and law enforcement</li> <li>• ILNAS (prevention against dangerous products)</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Copis</b></li> <li>• ....</li> </ul>	<ul style="list-style-type: none"> <li>• Info-platform containing INFO regarding counterfeiting and piracy</li> <li>• communication platform facilitating the INFO EX between the competent authorities of the Member States.</li> <li>• COPIS is part of the wider PLDA SYS</li> </ul>	Implementation of PLDA-SYSS: 3 stages	Not yet determined	<ul style="list-style-type: none"> <li>• Until 2012 the practical implementation of the policy framework will mainly concern the general organisation of the activity of the Custom facing fraud.</li> <li>• The SID SYS allows the sharing of the INFO and participate to the mutual cooperation between C but is not specifically active in the fight against counterfeiting and piracy.</li> </ul>	Community INFO and EX SYS specifically on intellectual property infringements
		<ul style="list-style-type: none"> <li>• <b>SID</b></li> </ul>	<p>Allowing national C to EX and spread INFO on counterfeiting activities and intervention requests.</p> <p>Helping the research and the prosecution of offences to national laws by strengthening the efficiency of the cooperation procedures and the control procedure from the C.</p>	n.a.	Direct access to SID is strictly reserved to the national authorities designated by each member state and to the designated services in the European commission These national authorities usually	<ul style="list-style-type: none"> <li>• Pro.: rapex and ICSMS quite efficient for the research of INFO on products</li> <li>• Con.: SID SYS is not currently efficient regarding the interaction on matters concerning infringement of intellectual property rights. C usually prefer to directly communicate by e-mail on such questions.</li> </ul>	

					are C. The member state that provided an INFO is the only one that can ever modify the data.		
		• <b>RAPEX SYS</b>	Facilitating the detection of non viable products by establishing an organised INFO rapid EX SYS and a notification SYS regarding products which have been considered as an immediate and major danger for the health and the security of consumers.	A restricted access server has been implemented by the European commission in order to ensure the applicability and efficiency of this INFO SYS.	The rapex contact points only along with the EC		
		• <b>ICSMS</b> (used by 12 countries )	Info and communication platform which facilitates the communication between market surveillance authorities.	All data is provided by the national market surveillance authority of each member state through a restricted online platform.	A limited access intranet which can be accessed by some members of the national market surveillance authorities. A public part which is on-line and open to consumers or manufacturers		
MAL	<ul style="list-style-type: none"> <li>• The industrial property registrations directorate (Min. Fin+ econ + investment)</li> <li>• IP enforcement unit (C)</li> <li>• The economic Crimes unit (police)</li> <li>• Malta INFO technology Agency(egov.)</li> </ul>	• <b>COPIS</b>	the rapid dissemination of INFO/ data between EU C administrations and Right holders	24/7 to all stakeholders + C frontline officials	C national coordinators and the frontline C officials And between right holders and the C administrators.	Small country: advantage when sharing INFO Easy to contact one's counterpart Pro.: harmonisation of datasharing	Rapid implementation of the Copis project.
		• <b>ECP</b>	Coordinate EU C controls throughout the EU in terms of the IPR Laws	Independent software SYS which is password protected/	different Unames for selected groups from the department		
		<b>RIF</b>	Priority C cases are rapidly disseminated electronically throughout all the EU member states' C administrations	Independent software	different Unames for selected groups from the department		

NL	<ul style="list-style-type: none"> <li>• Min of commerce</li> <li>• Min of justice</li> <li>• Min of agriculture</li> <li>• Dutch customs →</li> <li>• B/CA →</li> </ul>	<b>DIS</b>	To EX INFO ; national + EU MS	Digital DB.	<ul style="list-style-type: none"> <li>• Users assigned with a role as 'authoriser'</li> <li>• Regular users (employees)</li> </ul>	<p>Pro: no chance the information ends up in the wrong hands Con: the system cannot always provide the requested INFO</p>	<p>The complexity of the DIS system can be a problem.</p> <p>A centrally coordinated system of communication between all the important stake-holders, including other ministries.</p>
	<ul style="list-style-type: none"> <li>• Dutch Customs →</li> <li>• FIOD-ECD →</li> </ul>	<b>EU FIDE SYS</b>	EX INFO in cases of flagrant fraud	Digital DB	<ul style="list-style-type: none"> <li>• Users assigned with a role as 'authoriser'</li> <li>• Regular users (employees)</li> </ul>	n.a.	
	<ul style="list-style-type: none"> <li>• Dutch Customs →</li> </ul>	<b>RIF SYS</b>	EX INFO	Digital DB which enables users to quickly access and inform customs authorities	<ul style="list-style-type: none"> <li>• NRAC Employees</li> <li>• Regular users</li> </ul>	<p>Pro rapid exchange of INFO. Con not allowed to exchange personal data</p>	
	<ul style="list-style-type: none"> <li>• Regional police force managers →</li> <li>• The ministry of Home Affairs →</li> <li>• Attorney General's office →</li> <li>• The ministry of Defence →</li> </ul>	<b>The Blue view SYS</b>	Gain insight on data with regard to the enforcement and investigation of all national police forces	Based on XML-techniques the core is an oracle DB where optimisations have been carried out to locate the data more quickly	<ul style="list-style-type: none"> <li>• Criminal investigation department</li> <li>• The national INFOhub</li> <li>• Regional and district INFO hubs the police forces.</li> <li>• Administrators and analysts of the Criminal investigation Department and Kmar</li> </ul>	n.a.	
AU	<ul style="list-style-type: none"> <li>• C,</li> <li>• PO,</li> <li>• Min. Of education, art &amp; culture,</li> <li>• Austrian chamber of commerce</li> </ul>	<b>FINDOK</b>				<p>Quite mature Data EX should be done with semantic mark-up for speeding up the handling and processing of data. ELAK and findok are integrated in the general SYS of the BMF; EX of INFO and interaction is efficiently supported Some weaknesses exist in the expert search of Findok due the lack of semantic mark-up</p>	<p>BMF would like to have a more efficient SYS for data EX and search on the European level.</p>
		<b>ELAK</b>					
P	<ul style="list-style-type: none"> <li>• CIC group</li> <li>• Council of ministers</li> <li>• C</li> <li>• PO,</li> <li>• Min of culture</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Vinci SYS</b></li> </ul>	Facilitating internal coordination of law enforcement actions regarding the IP Piracy and trade in counterfeit goods	The application consist of four major module: Applications Detentions Reports	<ul style="list-style-type: none"> <li>• Technical admins</li> <li>• Substantial admins</li> <li>• Regional coordinators</li> </ul>	<p>Sufficient; but lacking sanctions for disobeying obligations of registering optical carriers in the OC Register. Pro.: a particularly valuable, easily customisable tool for sharing info on</p>	<p>Easy access to applications for action by the C authorities or to IP DBs should be coupled with tools for sharing and disseminating good enforcement practices.</p>

	Polish higher police school			Administration.	Average C service officials	actual detentions, applications for action by C authorities and concomitant audiovisual materials. It is appropriate that technological and functional solutions of the SYS are taken into account in the process of developing the COPIS, a communitywide intellectual property protection SYS	
		<ul style="list-style-type: none"> <li>• DP SYS</li> <li>• OC register</li> <li>• DKM portal</li> </ul>					
PT	<ul style="list-style-type: none"> <li>• Copyrights national authority</li> <li>• Ministry of Culture</li> </ul>	<ul style="list-style-type: none"> <li>• IGAC</li> </ul>	<ul style="list-style-type: none"> <li>• INFO EX and Action Plan at a national level (to be developed)</li> <li>• Cooperation with Private Sector</li> <li>• Development of Public Awareness campaigns</li> </ul>	<ul style="list-style-type: none"> <li>• Competent authorities</li> <li>• Enforcement</li> <li>• Statistics</li> <li>• Public Awareness</li> </ul>	<ul style="list-style-type: none"> <li>• Us from Public Departments with authority to act in piracy fighting</li> <li>• Us from private sector</li> </ul>	<p>Launch of a first portal is expected in 2010</p> <p>Policy framework is insufficient due to lack of human and financial means.</p> <p>Pro: efficient cooperation between authorities although without modern platforms</p> <p>Con: underevaluation from general policy concerning public investment.</p>	<p>INFO EX is presently assured through cooperation between authorities but should be developed by a more comprehensive and global system that would enable INFO EX and adequate planning.</p> <p>An effect allocation of means for the launch of efficient portals.</p> <p>A correct assessment towards recognition of the true value of IP issue, mainly from policy makers that would allow a more accurate definition of goals and correspondant financial and HR means for purposes of expertise development, mainly in what concerns piracy fighting in internet, both at national and international level.</p>
		<ul style="list-style-type: none"> <li>• Portal GAC</li> </ul>	<ul style="list-style-type: none"> <li>• Reporting illegal counterfeit acts.</li> <li>• General INFO on the counterfeiting phenomena, the respective combat and authorities involved</li> <li>• INFO on dangers for Us</li> <li>• INFO regarding legal protection of IPRH and material legislation</li> <li>• Statistics</li> </ul>	n.a.	n.a.		
RO	<ul style="list-style-type: none"> <li>• PM (public ministry) →</li> <li>• trademarks office, →</li> <li>• Copyright office, →</li> <li>• C authority →</li> </ul>	<ul style="list-style-type: none"> <li>• Common DB</li> </ul>	<p>Providing information regarding</p> <ul style="list-style-type: none"> <li>• the customs seizures,</li> <li>• all criminal investigations concerning counterfeiting and piracy,</li> <li>• intellectual property rights.</li> </ul> <p>Facilitating the cooperation between the authorities involved in the actions against counterfeiting and piracy.</p>	<ul style="list-style-type: none"> <li>• Only IT-project in progress regarding the exchange of information between authorities with regard to counterfeiting and piracy.</li> <li>• Central DBs of the PM</li> <li>• Access web application</li> <li>• Secured connections between institutions.</li> <li>• Provides information regarding the investigations carried out by the infringement, the infringer, the incrimination of the actions of the infringers.</li> </ul>	<ul style="list-style-type: none"> <li>• Prosecutors</li> <li>• Policemen from GIRP and GICBP</li> <li>• Designated persons of the Trademark office,</li> <li>• Designated persons of the Copyright office,</li> <li>• Designated persons of the Customs office,</li> <li>• Only employees of the national</li> </ul>	<p>Common DB → efficient tool for REICOP</p> <p>DB of trademarks office and the portal of the copyright office allow interested parties to obtain IP-INFO + tools in educating consumers &amp; providing INFO regarding pirated &amp; counterfeited products.</p> <p>Pro: -INFO of the enforcement authorities is put together in common DB -Common DB will be linked to the trade registry DB = information on companies which may be involved in</p>	<p>More effort with regard to the cooperation</p> <p>Increase specialized personnel for investigating IP-infringements.</p> <p>Convince prosecutors and judges to convince them to enforce and apply existing laws</p>

				<p>intervention filed by the trademark owner, and regarding the customs seizures of counterfeited or suspected counterfeited products is available in the Common database. The Trademarks office uploads and updates daily the information regarding the protected IPRs.</p> <ul style="list-style-type: none"> <li>• Access to the Copyright office national registers; experts opinions and findings issued by the Copyright office are uploaded into the common DB upon request of policemen or prosecutors.</li> </ul>	<p>activities regarding counterfeiting and piracy</p> <ul style="list-style-type: none"> <li>• Authority to access and or amend are based on usernames and passwords.</li> </ul>	<p>Con:</p> <ul style="list-style-type: none"> <li>- improvements to be made, e.g. uploading of photo's &amp; video's, direct intercommunication between users.</li> <li>-common DB has to be improved continuously</li> <li>- common DB only access to the officials of the enforcement authorities, no access for the interested parties e.g., right owners</li> </ul>	
		<ul style="list-style-type: none"> <li>• <b>Trademark office DBs</b></li> </ul>	<p>Publicly available DB which provides INFO included in the registers of the intellectual property regarding patents, trademarks, industrial designs</p>	<p>3 DBs Patents Trademarks Industrial designs</p>	<p>n.a., the database is available on the website of the trademarks office, public.</p>		
		<ul style="list-style-type: none"> <li>• <b>Copyright official Portal</b></li> </ul>	<ul style="list-style-type: none"> <li>• Manages the following electronic national registers:</li> <li>• The Phonograms National Register,</li> <li>• The Computer Programs National Register,</li> <li>• The Video-grams National Register,</li> <li>The Multipliers of Optical Disks, Audio-cassettes and Video-cassettes National Register</li> </ul>	<ul style="list-style-type: none"> <li>• The portal has several applications: company search, applications search....</li> <li>• The portal provides INFO regarding the manufacturers, importers, distributors,...</li> </ul> <p>The information provided by the portal covers not only details regarding the products, and manufacturers, importers, distributors but also regarding the devices, carried out activities, working sites and warehousing.</p>	<ul style="list-style-type: none"> <li>• The INFO which is publicly available may be accessed online on the website of the Copyright Office, and also on the portal created by the copyright office. Copyright office employees have access to detailed INFO</li> </ul>		
SLO VE	<ul style="list-style-type: none"> <li>• Intragovernmental working group for Fight against Piracy and counterfeiting (IWG)→</li> </ul>	<ul style="list-style-type: none"> <li>• <b>IIT support/solutions for IWG by SIPO</b></li> </ul>	<ul style="list-style-type: none"> <li>• Improve INFO EX between members of the IWG</li> <li>• Raising awareness</li> </ul>	<ul style="list-style-type: none"> <li>• Ms exchange server</li> <li>• Website</li> </ul>	<ul style="list-style-type: none"> <li>→ IWG members</li> <li>→ Public</li> </ul>	<p>Policy framework &amp; its practical implementation still in the initial phase of implementation</p>	<p>Build upon existing systems for data exchange and further improvements with national and international networks through national contact points.</p>
SLO VA	<ul style="list-style-type: none"> <li>• Industrial property office of the Slovak Republic,</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Web-registers</b></li> </ul>	<p>Data extracted from registers containing INFO on patents,</p>	<p>n.a.</p>	<p>Public</p>	<p>Con: Contains only selected information from registers provided</p>	<p>Institutional, policy and normative infrastructure for REICOP is</p>

	<ul style="list-style-type: none"> <li>• C, Min of finance,</li> </ul>		utility models, designs,...			<p>by the Office. Info is not updated daily Info is incomplete</p>	<p>insufficient.  No systems are in place (Ad hoc)  An idea to develop an IT-system has been drafted but due to lack of funding it has not been realised yet.</p>
S	<ul style="list-style-type: none"> <li>• OEPM (Spanish Trademarks and IP office) →</li> <li>• Home Affairs Ministry</li> <li>• Customs Borders</li> <li>• Ministry of Culture</li> </ul>	<ul style="list-style-type: none"> <li>• <b>OEPM DB</b></li> </ul>	<ul style="list-style-type: none"> <li>• Online and offline provision of public INFO on the files managed by the Office (on trademarks, patents and inventions).</li> <li>Getting in touch with the representative of the IPRHs, in order to offer the possible actions/lawsuits</li> </ul>	DB Accessible via the internet DB Accessible by public officials	→ any person → interested authorities (internal DB with accurate INFO)	<p>Pro: quick, easy and reliable Con: update every 2 weeks</p>	<p>Policy &amp; framework is already encouraging the exchange of information among public administrations on the fight against piracy &amp; counterfeiting</p>
	<ul style="list-style-type: none"> <li>• EUROPOL →</li> </ul>	<ul style="list-style-type: none"> <li>• <b>EUROPOL AWF COPY analysing file</b></li> </ul>	Support to the competent national authorities of the member state dealing with prevention and fight against any crimes related to activities carried out by organized networks implied on the manufacture or distribution of counterfeiting or pirate items among member states	<ul style="list-style-type: none"> <li>• Europol, analysts:</li> <li>• DB (Oracle)</li> <li>• SIRENE application</li> <li>• Fax servers</li> <li>• Email servers</li> </ul>	Data inserted only by EUROPOL analysts duly authorized Stored data can be accessed only by participating member states	<p>Pro: coordination amongst member states in the field of industrial piracy related to criminal organizations within the EU territory</p>	
CZ	<ul style="list-style-type: none"> <li>• Interdepartmental commission for the fight against illegal actions against IP rights</li> <li>• C</li> <li>• CTIA</li> <li>• Industrial property office →</li> <li>• Min of culture</li> <li>• Police of the czech republic</li> <li>• Min of finance</li> <li>• Min of industry and trade</li> <li>• Min of justice</li> <li>• Czech agriculture and food inspection</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Enforcement SYS</b></li> </ul>	Share information regarding IPR INFO on relevant authorities Education of public servants	<ul style="list-style-type: none"> <li>• Digital system, available online</li> </ul>	Publicly available	<p>The SYS is very comprehensive &amp; clear It only includes publicly available data and enforcement authorities tend to use the original source instead.</p>	<p>Current legislation insufficient + some legal barriers (confidentiality requirements and some duplicity of CTIA an customs competencies)  The systems generally contain all the information needed therefore they have a good potential to support the fight against counterfeiting and piracy.  More cooperation between law enforcement authorities and other authorities.  Customs and CTIA should be involved more in the enforcement project.</p>
	<ul style="list-style-type: none"> <li>• Min of Finance</li> </ul>	<ul style="list-style-type: none"> <li>• <b>AIP SYS</b></li> </ul>	<ul style="list-style-type: none"> <li>• DB an analysis of IP relevant Data.</li> </ul>	n.a.	n.a.	<p>Comparatively complex and covers almost every aspect of the Customs</p>	<p>It is also recommended that CTIA &amp;</p>

			<ul style="list-style-type: none"> <li>Support internal cooperation of C and law enforcement</li> </ul>			employees work in the field of IP. It is isolated from other IP enforcement authorities	Customs competencies in the field of IP rights protection are coordinated and allow other public authorities to share all relevant information and allow them to communicate in real time.
	<ul style="list-style-type: none"> <li>MIT</li> <li>ICC</li> </ul>	<ul style="list-style-type: none"> <li><b>Project original</b></li> </ul>	Information campaign EX INFO, facilitate cooperation between private sector and the government	Website: www.respektujoriginal.cz	<ul style="list-style-type: none"> <li>Target groups: <ul style="list-style-type: none"> <li>entrepreneurs</li> <li>customers</li> <li>Public administration</li> </ul> </li> </ul>	n.a.	
UK	<ul style="list-style-type: none"> <li>UK IP crime group →</li> <li>Serious Organised crime Agency</li> <li>National fraud authority</li> <li>HM Revenue &amp; Customs</li> <li>Tading standards</li> <li>PCeU</li> <li>National IP initiative ‘real deal: working together for safe fair markets’</li> <li>Joint memorandum of understanding on an approach to reduce unlawful file-sharing.</li> <li>IPO intelligence hub →</li> </ul>	<ul style="list-style-type: none"> <li><b>IPO intelligence Hub</b></li> </ul>	<ul style="list-style-type: none"> <li>Create and coordinate an effective approach and raise awareness to IP-crime</li> <li>Bring together Government, enforcement agencies and industry groups.</li> <li>The group aims to ensure a collaborative approach is taken in addressing IP crime.</li> <li>Responsible for coordinating enforcement activities.</li> <li>Intelligence is provided to the hub by enforcement authorities and relevant industry bodies.</li> </ul>	<ul style="list-style-type: none"> <li>National intelligence DB IPID</li> <li>Discussion on strategic policy issues in relation to IP crime</li> <li>Identifying strategic priorities for collaborative action.</li> <li>Identifying and disseminating good practice.</li> <li>Raising awareness of IP crime</li> <li>An annual IP Crime report.</li> <li>Training</li> </ul>	The hub collects, collates provided analysis and disseminates intelligence material between law enforcement, governments and industry sectors. Agencies do not have direct access to the IPID DB. Intelligence is received using the National intelligence report system.	Pro: Central repository for the wider enforcement community. Collection of important statistics and more informed policy and enforcement strategies.	<p>Significant members from all areas of enforcement, government and industry work together for a common goal: the prevention and detection of IP crime.</p> <p>The sharing of IP intelligence strengthens the knowledge of law enforcement enabling a more focussed response from the threat of IP crime.</p> <p>A number of problems arise in respect of dealing effectively with piracy in the UK, including:</p> <ol style="list-style-type: none"> <li>The fragmented approach by law enforcement to counterfeiting and piracy in the uk</li> </ol>
	<ul style="list-style-type: none"> <li>UK IP crime group →</li> </ul>	<ul style="list-style-type: none"> <li><b>UK IP crime group</b></li> </ul>	Informal networking for public private partnership	High level representatives from industry, enforcement and government meet to discuss common interests and problems, identify best practice and awareness raising campaigns.	n.a.	Provides a platform for discussion across government, enforcement and industry, allowing for a more coordinated approach and the identification of common problems and aims	<ol style="list-style-type: none"> <li>Competing objectives and priorities</li> <li>Some weaknesses</li> <li>The diverse nature of the industry landscape</li> </ol>
	City of London Police	<ul style="list-style-type: none"> <li><b>National fraud strategic authority</b></li> </ul>	Centre for collection, collation and dissemination of fraud related crime and intelligence	Centre of excellence for all fraud activities in the UK. Designated reporting desk for IP related fraud and IP intelligence Electronic reporting infrastructure for use by public and enforcement and government agencies.	All UK enforcement agencies and regulatory and government bodies	Provides a central location for the reporting of fraud related criminality and allows IP related intelligence to be analysed using several national information systems to identify common threads and criminal activities.	All of these factors affect effectiveness of the agencies involved in the protection of IPR

SW	<ul style="list-style-type: none"> <li>• C and other national authorities with market control responsibilities</li> </ul>	<ul style="list-style-type: none"> <li>• <b>SACG initiative Swedish Anti counterfeiting group (by stakeholders - no governmental initiatives.</b></li> </ul>	Inter aiia, to improve cooperation between responsible authorities	n.a.	n.a.	<p>There is no institutional cooperation between authorities implemented at this stage. Stakeholders are directly involved through SACG. National authorities have less experience on information exchange and would have to be prepared, both organisational and technical, in order to fully support any type of direct exchange of data.</p>	<p>Improve the existing informal cooperation between national authorities, also on a European level. A simple reporting system would already improve information exchange to a large degree, avoiding that two investigations are ongoing at the same time The European Observatory on counterfeiting and Piracy could serve as the centre for cooperation and strengthen existing frameworks or help to establish new ones.</p>
----	---	--	--	------	------	---	--