

Catalogue of Resources



HIDE

WWW.HIDEPROJECT.EU

THE HIDE PROJECT

Homeland Security, Biometric Identification & Personal Detection Ethics

Catalogue of Resources



HIDE Deliverable D2.1
2008

Prepared by EUTELIS Italia Srl.
Contact: Valerio Cusimano
valerio.cusimano@eutelisitalia.eu

The aim of this Deliverable is to provide an overview of the present debate on ethics of biometrics and personal detection technologies and to collect and compare the main documents, guidelines, policy papers.

The deliverable consists of 2 sections and 7 chapters.

The first of these two sections include Chapter 1 and 2 and in which they take into account project in which its themes and objectives are related to the project HIDE. The second section contains guidelines, directives, documents, and policy papers issued by the EC that provide the guidelines for HIDE.

The first chapter takes into consideration 8 projects belonging to the FP5 programme; the second chapter takes 12 projects of the FP6 programme into account. Each project has been cataloged as follows:

Name, Acronym, Start date, Duration, Status, Short Description, Coordinator, Contact, Contact reference, Tel / Fax, URL, Partners.

For the remaining chapters, the outline of the catalogue has taken reference to the following:

Title of the document, an official reference to which the document was published, the official publication date, author of the document, brief description of the contents, links to the complete document.

In Chapter 3 there are 4 tabs. The first contains information on the Charter of Fundamental Rights of the European Union. The following two refers to the European Union directives, the 95/46/EC and 2002/58/EC. The fourth tab is based on the Regulation (EC) 45/2001 of 18 December 2000.

Chapter 4 contains four communications from the commission to the european parliament and the council all concerning Data Protection.

Chapter 5 contains 2 EC GREEN PAPERS, the first on 'Green paper on detection technologies in the work of law enforcement, customs and other security authorities', the second on a 'European Program for Critical Infrastructure Protection'.

Chapter 6 contains 6 opinions of the european data protection supervisor published in the time interval between 19 December 2005 and 25 April 2006.

Chapter 7 contains 24 opinions of the working party art.29. The time reference goes from the year 2003 to 2007.

All rights reserved.

No part of this publication may be reproduced, distributed or utilized in any form or by any means, electronic, mechanical, or otherwise, without the prior permission in writing from the HIDE Project Consortium.

Download and print of the electronic edition for non commercial teaching or research use is permitted on fair use grounds. Each copy should include the notice of copyright.

Source should be acknowledged.

© 2008 HIDE Project

<http://www.hideproject.eu>

Sommario

1	EC FUNDED PROJECTS From FP5 :	6
1.1	PISA.....	6
1.2	RAPID.....	7
1.3	SABRINA.....	8
1.4	T2R.....	9
1.5	CHALLENGE.....	10
1.6	ELISE.....	12
1.7	PRIVIREAL.....	13
1.8	EUROSOCAP.....	14
2	EC FUNDED PROJECTS From FP6 :	15
2.1	BIOSECURE.....	15
2.2	CI2RCO.....	16
2.3	DIGITAL PASSPORT.....	18
2.4	EJUSTICE.....	19
2.5	FIDIS.....	20
2.6	GUIDE.....	22
2.7	PRIME.....	23
2.8	SECURIST.....	24
2.9	SECURINT.....	25
2.10	SERENITY.....	26
2.11	SWAMI.....	27
2.12	TTSRL.....	28
3	EC DIRECTIVES, REGULATIONS, TREATIES.....	29
3.1	Charter of fundamental rights of the European Union.....	29
3.2	Directive 95/46/EC of 24 October 1995.....	30
3.3	Directive 2002/58/EC of 12 July 2002.....	31
3.4	Regulation (EC) 45/2001 of 18 December 2000.....	33
4	COMMUNICATIONS FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL.....	35
4.1	Promoting Data Protection by Privacy Enhancing Technologies (PETs).....	35
4.2	work programme for better implementation of the data protection directive.....	36
4.3	First Report on the implementation of the Data Protection Directive.....	37
4.4	A strategy for a secure Information Society.....	38
5	EC GREEN PAPERS.....	40
5.1	Green paper on detection technologies.....	40
5.2	Green Paper on a European Programme for Critical Infrastructure Protection.....	42
6	OPINIONS OF THE EUROPEAN DATA PROTECTION SUPERVISOR.....	43
6.1	Opinion of 19 December 2005.....	43
6.2	Opinion of 26 September 2005.....	44
6.3	Opinion of 15 June 2005.....	45
6.4	Second opinion of 26 April 2007.....	46

6.5	Opinion of 26 February 2006.....	47
6.6	Opinion of 25 April 2006.....	48
7	<i>OPINIONS OF THE ART.29 WORKING PARTY</i>	49
7.1	Proposal for a regulation of the european parliament and of the council	49
7.2	Recommendation 1/2007	50
7.3	Opinion 2/2007	51
7.4	Working Document of 15 February 2007	52
7.5	Opinion 1/2007	53
7.6	Opinion 10/2006	54
7.7	Opinion 9/2006	55
7.8	Opinion 7/2006	56
7.9	Opinion 5/2006	57
7.10	Opinion 4/2006	58
7.11	Working document of 24 October 1995	59
7.12	Opinion 3/2005	60
7.13	Results of the Public Consultation on Article 29 Working Document 105	61
7.14	Working document on data protection issues related to RFID technology	62
7.15	Opinion 1/2005	63
7.16	Opinion 9/2004	64
7.17	Opinion 8/2004	65
7.18	Opinion 7/2004	66
7.19	Opinion 6/2004	68
7.20	Seventh report the years 2002 and 2003	69
7.21	Joint Statement in response to the terrorist attacks in Madrid	70
7.22	Opinion 4/2004	71
7.23	Working document on biometrics.....	72
7.24	Level of Protection for the Transfer of Passengers' Data	73

1 EC FUNDED PROJECTS FROM FP5 :

1.1 PISA

Name	Privacy Incorporated Software Agent: Building a privacy guardian for the electronic age
Acronym	PISA
Start date	01/01/2001
Duration	36 months
Status	Completed
Description	<p>Most Member States in the European Union have by now implemented the European Directive 95/46/EC and 97/66/EC. This Directives provides a general legal framework for the protection of personal data.</p> <p>PISA addresses the European policy to foster the security and privacy for the users of new combinations of telecommunications, information technology and media , and the need for interoperability and coherence at a global level. The project is positioned at the crossroad of developments of Software agents, the Internet and E-commerce.</p> <p>The PISA-project will specify, validate and promote open and secure service provision architecture to provide new services by software agents to users, moving across networks and service providers. Most Member States in the European Union have by now implemented the European Directive 95/46/EC and 97/66/EC. This Directives provides a general legal framework for the protection of personal data. PISA addresses the European policy to foster the security and privacy for the users of new combinations of telecommunications, information technology and media, and the need for interoperability and coherence at a global level. The project is positioned at the crossroad of developments of Software agents, the Internet and E-commerce. The PISA-project will specify, validate and promote open and secure service provision architecture to provide new services by software agents to users, moving across networks and service providers.</p>
Coordinator	Netherlands Organisation For Applied Scientific Research – Tno
Contact	Jan Huizinga
Contact reference	
Tel/Fax	Tel: +31-70-3740308 Fax: +31-37-40651
URL	Click Here
Partners	<p>Technische Universiteit Delft Globalsign Registratiekamer (NI Data Protection Authority; Ndpa) Finsa Consulting Societa A Responsabilita Limitata Futuro & Innovazione - Strategie Aziendali Ricerche E Consulenza National Research Council Of Canada - Conseil National De Recherches Canada</p>

1.2 RAPID

Name	Roadmap for Advanced Research in Privacy and Identity Management
Acronym	RAPID
Start date	01/07/2002
Duration	12 months
Status	Completed
Description	Declining revenues and earnings, impending loss of market share and falling share prices are causing growing business uncertainty. Disappointing results force many businesses to rethink the management of their costs. Only a structured approach, combined with goal-oriented cost analysis, benchmarking, best practice comparisons and professional project management will enable a business to identify and realise potential permanent cost reductions. For this purpose it is essential to analyse cost structures and business trends precisely. PricewaterhouseCoopers' Rapid Cost Reduction is a pragmatic cost reduction approach enabling permanent savings to be realised in a relatively short time. The initial analysis phase starts with a brief analysis (comparison of cost structures, benchmarking, identifying quick wins) and is followed by a design and implementation phase, during which medium and long-term measures are developed and implemented.
Coordinator	Pricewaterhousecoopers N.V.
Contact	Otto Vermeulen
Contact reference	
Tel/Fax	Tel: +30-2210-91690 Fax: +30-2210-91695
URL	Click Here
Partners	Katholieke Universiteit Leuven Netherlands Organisation For Applied Scientific Research - Tno Universita Degli Studi Di Milano Stichting Katholieke Universiteit Brabant Centre National De La Recherche Scientifique Stichting Geschillenoplossing Automatisering Geie Ercim

1.3 SABRINA

Name	Secure Authentication by a Biometric Rationale and Integration into Network Applications
Acronym	SABRINA
Start date	01/01/2001
Duration	24 months
Status	Completed
Description	<p>A new on biometrical authentication methodology is proposed which provides much higher security levels as all comparable technologies known today. The methodology is suitable for mass production at very low price. The SABRINA project will develop the first production samples of the sensor unit along with a generic application platform for various test scenarios. The first pilots within this project will address both off-line and on-line authentication.</p> <p>Objectives This project aims at the development and integration of a new methodology framework for secure authentication based on ultra-sonic scans of parts of the human skin. The general methodology consists of the so-called Chip Original Method (COM) and the Touch Echo Method (TEM) and has already been proved under laboratory conditions to deliver the highest level of security known today. It is even able to distinguish between persons of the same genetic code as it is the case for identical twins. The project will establish a full methodology framework based on TEM/COM. This includes all issues associated with its use as an user identification and authentication method within networks, namely security verification, practicability and other quality aspects. The whole approach will be evaluated by integration into ongoing developments of an e-Commerce technology provider and a large network provider.</p>
Coordinator	Universitaet Karlsruhe (TH)
Contact	Edgar Kaucher
Contact reference	
Tel/Fax	Tel: +49-72-16082681 Fax: +49-72-16087669
URL	Click Here
Partners	Forschungszentrum Informatik An Der Universitaet Karlsruhe Hitex-Systementwicklung, Gesellschaft Fuer Angewandte Informatik M.B.H. Wind Telecomunicazioni S.P.A. Non Standard Logics Limited Avantgarde Products Vollert

1.4 T2R

Name	A Trusted Platform for Wireless Data Services
Acronym	T2R
Start date	01/09/2002
Duration	12 months
Status	Completed
Description	
Coordinator	GEMPLUS
Contact	Frederic Laporte
Contact reference	Contact Here
Tel/Fax	Tel: +44-23-66454 Fax: +67-27-81772
URL	
Partners	Orange France Sonera Smarttrust Ab Globalsign Vodafone Group Services Limited Radicchio Limited

1.5 CHALLENGE

Name	The changing landscape of european liberty and security
Acronym	CHALLENGE
Start date	01/06/2004
Duration	60 months
Status	Execution
Description	<p>Contemporary discussions on the merging between internal and external security and the relationship between liberty and security in Europe are seriously constrained by the degree to which the concepts, historical practices and institutions of liberty and security have been examined independently. This analytical division of labour expresses the practical and institutional division of labour encouraged by the structures of the modern international system and its distinction between foreign and domestic policies.</p> <p>The project facilitates more responsive and responsible judgements about new regimes and practices of security in order to minimize the degree to which they undermine civil liberties, human rights and social cohesion in an enlarging Europe. It will do so in the context of the new evolving international environment shaped by the events of September 11, 2001 and the recent wars in Afghanistan and Iraq.</p> <p>The aim is to reframe the security framework emerging in Europe to ensure that it starts with liberty as its point of departure. An Interdisciplinary Observatory will be created to analyse and evaluate the changing relationship between sustainable security, stability and liberty in an enlarging EU, which upholds the values of democracy.</p> <p>The project aims to: " analyse the merging between internal and external security and the dynamic between liberty and security in Europe, regarding the sovereign capacity to declare exceptions to a normal sphere of potential liberties and freedoms; " assess the dynamic between liberty and security over time in sensitive sites and how these relate to the specificity of the European context; " enhance a growing interdisciplinary network of scholars across many regions of Europe, working on the implications of new forms of violence and political identity; " enable a coherent Integrated Project focusing on the State of exception as illiberal practice and illiberal regimes using same tools and methodology.</p>
Coordinator	CENTRE FOR EUROPEAN POLICY STUDIES
Contact	Joanna Apap
Contact reference	
Tel/Fax	Tel: +32-22293925 Fax: +32-22194151
URL	
Partners	<p>Universite De Caen Basse Normandie Fondation Nationale Des Sciences Politiques Universiteit Utrecht National And Kapodistrian University Of Athens Universita Degli Studi Di Genova Stichting Katholieke Universiteit Universitat De Barcelona Koebenhavns Universitet</p>

Centre National De La Recherche Scientifique (Cnrs)
Institut Universitari D'estudis Europeus
King's College London
University Of Keele
Europäische Vereinigung Für Transformationsforschung E.V.
University Of Leeds
Ethnic And National Minority Studies Institute Of The Hungarian Academy Of Sciences
Stefan Batory Foundation
Foundation For International Studies - University Of Malta
European Institute
London School Of Economics And Political Science
Universität Zu Köln
Cultures And Conflicts
University Of Malta
The International Peace Research Institute
Université De Rouen

1.6 ELISE

Name	Electronic library image service for Europe
Acronym	ELISE
Start date	01/02/1993
Duration	24 months
Status	Completed
Description	<p>Objective: The project modelled a system which provides access to full colour image information banks (slides of museum exhibits and illustrated manuscripts and cartographic material from the Brabant area) held in two libraries in two Member States, through the:</p> <ul style="list-style-type: none"> - design and establishment of a bank of full colour images and associated text for real-time remote access in the participating libraries; - Modelling of interconnection between participating image banks using international networks; - Demonstration of the pilot and communications model. The project investigated: the technical requirements of establishing full colour image banks in libraries; the associated storage and retrieval mechanisms; client needs and design interfaces; and the technical requirements for international interconnection of image-bank systems. <p>Impact and results: The setting up of two image banks (at the Victoria & Albert museum with 3,000 slides of exhibits and at Tilburg University Library with 10,000 images of illustrated manuscripts and cartographic materials), remotely and instantly available to the prototype system, opens up new potential in the libraries sector for on-line, high speed access to images across Europe and develops awareness of image products among users, thus stimulating the market.</p> <p>Among the key results are: a detailed specification of library requirements; definition of relevant, applicable technical standards; specification of retrieval database; the demonstration prototype which will be exploited for commercial use by the partners and incorporated into product development planning.</p>
Coordinator	De Montfort University
Contact	Collier
Contact reference	
Tel/Fax	Tel: +44-533-577039 Fax: +44-533-577170
URL	
Partners	IBM UK Ltd Victoria And Albert Museum Tilburg University Library

1.7 PRIVIREAL

Name	Implementation of the data protection directive in relation to medical research and the role of ethics committees
Acronym	PRIVIREAL
Start date	01/01/2002
Duration	42 months
Status	Completed
Description	<p>Protection of privacy of subjects in medical research depends as much on ethics review as on data protection law, but little is known about how this interacts with implementation of Directive 95/46/EC to protect privacy.</p> <p>PRIVIREAL brings together experts on relevant law and on ethics review of medical research from across the EU and Norway to evaluate the interaction between implementation of the Directive and research ethics review in protecting Directive rights of research subjects, with a view to making recommendations to the Commission about how to optimise protection provided by research ethics review (taking into account the background EU and domestic legal and ethical culture/s).</p>
Coordinator	UNIVERSITY OF SHEFFIELD
Contact	Ian McCormick
Contact reference	
Tel/Fax	
URL	
Partners	MIDLAND BAKERY ENGINEERS LTD

1.8 EUROSOCAP

Name	The development of European standards on confidentiality and privacy in healthcare among vulnerable patient populations
Acronym	EUROSOCAP
Start date	01/02/2003
Duration	41 months
Status	Completed
Description	<p>The requirements of an information society present a significant challenge for privacy and confidentiality of personal information. The purpose of this project is to confront and address these tensions with respect to the acquisition and processing of healthcare information.</p> <p>Healthcare professionals require up-to-date guidance on information sharing, which is ethically and legally sound, informs healthcare practice and has practical relevance for their daily work. The aim of the project is to build a knowledge base, a set of standards and guidelines, which will inform professional practice throughout the healthcare sector of the European Community, which harmonises with EU laws and which informs existing policies and guidelines.</p>
Coordinator	Queen's University of Belfast
Contact	Malcolm Rollins
Contact reference	
Tel/Fax	
URL	
Partners	<p>University Of Warwick University Of Essex Heinrich-Heine-Universitaet Duesseldorf University Of Sheffield The Queen's University Of Belfast Universite De Neuchatel Centre For Science, Society And Citizenship Asociacion Septimania The International Organisation For Migration European Forum For Good Clinical Practice</p>

2 EC FUNDED PROJECTS FROM FP6 :

2.1 BIOSECURE

Name	Biometrics for Secure Authentication
Acronym	BIOSECURE
Action line	IST-2002-2.3.1.5 Towards a global dependability and security framework
Start date	01/06/2004
Duration	40 months
Status	Completed
Description	<p>The main objectives of the BioSecure Network of Excellence are:</p> <ul style="list-style-type: none"> • To strengthen and integrate multidisciplinary research effort in order to investigate biometrics-based identity authentication for the purpose of meeting the trust and security requirements in our progressing digital information society, through effective and dynamic technologies. • To disseminate and spread excellence using a number of dedicated tools that will strengthen the impact of scientific dissemination. Such tools include workshops, conferences, advanced research and evaluation institutes and similar events that will be organised by the network. The international collaboration will also be enhanced by facilitating mobility across Europe through visiting researchers, Post-Doc's and PhD's.
Coordinator	Caisse Des Depots Et Consignationsbcr Unite De Gestion 56 Rue De Lille 75007 Paris France
Contact	Forte, Jean-François
Tel/Fax	Tel: +33-1-58508137 Fax: +33-1-58500678
URL	Click Here
Partners	The University Of Surrey United Kingdom Centre National De La Recherche Scientifique France Stichting Centrum Voor Wiskunde En Informatica Netherlands Institute Of Information Technologies Bulgaria Universidad De Vigo Spain University Of Kent At Cant

2.2 CI2RCO

Name	Identification of research groups on IT security in critical infrastructures
Acronym	CI2RCO
Action line	IST-2004-2.3.6.3 To progress towards the achievement of the objectives of a European Research Area in a given IST field
Start date	01/03/2005
Duration	24 months
Status	Completed
Description	<p>Main objectives:</p> <p>Besides the objective to create and co-ordinate a European Taskforce to</p> <ul style="list-style-type: none"> ▪ encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and ▪ establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security <p>The CI²RCO consortium further on aims to support CIIP awareness and actions in the EU-25 and Associate Candidate Countries (Bulgaria, Romania, Turkey) in order to</p> <ul style="list-style-type: none"> ▪ provide a forum and a platform to bring together the different key players to exchange experineces, share interests and define areas for joint activities, ▪ identify key dependability and security CIIP challenges, ▪ foster truly multidisciplinary and innovative approaches to research that would build on the contributions provided by diverse scientific communities, ▪ encourage and support the national and international co-operation on key global CIIP research issues, ▪ develop recommendations and a roadmap for current and future CIIP research activities, ▪ support policy-makers in charge of financing or managing R&D programmes. <p>Project Approach:</p> <p>In implementing an extended network of experts, expertise, and knowledge for CIIP, CI²RCO starts from the hypothesis that national, regional and international research programmes with a wide variety of objectives do exist which have direct or indirect relation to CIIP. Relevant players of research, research funding actors, policy makers and Critical Information Infrastructure stakeholders are mostly unaware of such CIIP related R&D programme similarities in various fields due to lack of knowledge, fragmentation, and limited networking capability, national need to know, restrictive policies and legal obstacles, as well as varying political structures across Europe. These factors lead to isolation and thus hinder an effectively netted and efficient research infrastructure in Europe.</p> <p>CI²RCO will therefore focus on R&D activities and actions across the EU-25 and Associate Candidate Countries that are essential to be carried out at European level and that require collaborative efforts involving research and research funding actors as well as other stakeholders across the European Research Area. This will be accomplished by the following set of co-ordination activities:</p> <ol style="list-style-type: none"> 1. Establishment of a CIIP-network of relevant players (as identified above) 2. Identification of completed, on-going and planned CIIP R&D programmes and projects on national and EU-level 3. Analysis of the European CIIP research area according to appropriate

	<p>evaluation and assessment criteria</p> <ol style="list-style-type: none"> 4. Calibration of the CIIP activities with CII stakeholders in a continuous feedback loop to identify gaps in the current and planned CIIP actions and activities 5. Elaboration of a European CIIP research agenda (roadmap) to determine R&D priorities 6. The organisation of workshops/conferences to initiate and to foster networks and to evaluate, to complete and to disseminate results 7. Provision of an Internet platform to supply sustainable support for information and co-operation of the CIIP-network.
Coordinator	<p>Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. Fraunhofer Institut Sichere Informationstechnologie (Sit) Hansastrasse 27c 80686 Muenchen Germany</p>
Contact	<p>Bendisch, Uwe</p>
Tel/Fax	<p>Tel: +49-224-1143122 Fax: +49-224-11443122</p>
URL	<p>Click Here</p>
Partners	<p>Deutsches Zentrum Fuer Luft Und Raumfahrt E.V. Germany Ernst Basler + Partner Ag Switzerland Ente Per Le Nuove Tecnologie, L'energia E L'ambiente Italy Groupe Des Ecoles Des Telecommunications France Industrieanlagen-Betriebsgesellschaft Mbh Germany</p>

2.3 DIGITAL PASSPORT

Name	Next generation European digital passport with biometric data
Acronym	DIGITAL PASSPORT
Action line	IST-2002-2.3.1.5 Towards a global dependability and security framework
Start date	01/03/2004
Duration	36 months
Status	Completed
Description	<p>Boarder passage follows in many respects the same patterns as it did a few hundred years ago. The introduction of European digital passport will make a fully automated, secure and convenient walk-through boarder passage possible, thus establishing a completely new pattern in international travel. In order to fully realise their potential for improvement of security, convenience and efficiency, the implementation of European digital passports must be supported by an industrial initiative that shows the way to consistently apply standards, develop a range of techniques and connect to new border control and airport processes.</p> <p>The Digital Passport project will produce a new generation of digital passports based on the combination of a traditional booklet with large capacity IC micro controller containing and processing cardholder's personal and biometric data. An RSA microprocessor will provide the support for PKI based security and capacity for encryption and digital signature. The terminal will support biometry, contact less connection to the passport and connection to applications including models of airport processes. The solution will be fully inside relevant standards such as ISO 7816-15, ISO 14443, ISO WG3 and it will collaborate with Schengen Information System and ICAO specifications. The system will provide a complete, robust, reliable, proven, non-proprietary, standards compliant industrial concept. It will speed up the consistent implementation of next generation European digital passport and prolong the expected life-length of early implementations. The results will be efficiently disseminated to governments, police and boarder control authorities, standardisation bodies, secure printer suppliers and all other interested parties. The proposed project closely follows the objectives of the FP6 IST Programme, which underlines the importance of new trust and confidence solutions with the goal to improve dependability of technologies, infrastructures and applications.</p>
Coordinator	Infineon Technologies Ag Secure Mobile Solutions St. Martin Strasse 53 Postfach 800949 81609 Muenchen Germany
Contact	Houdeau, Detlef
Tel/Fax	Tel: +49-892-3421144 Fax: +49-892-3481130
URL	Click Here
Partners	Universite Henri Poincare Nancy 1 France Smarticware Ab Sweden Emsquares Ag Germany Mirage Holografy Studio Holografija, Sitotisk In Storitve, D.O.O. Slovenia Microdatec-Gesellschaft Fuer Entwicklung Und Produktion Electronischer Systeme Mbh Germany

2.4 EJUSTICE

Name	Towards a global security and visibility framework for Justice in Europe
Acronym	EJUSTICE
Action line	IST-2002-2.3.1.5 Towards a global dependability and security framework
Start date	01/03/2004
Duration	24 months
Status	Completed
Description	<p>With several states starting to implement ID smartcards, the eJustice project meets a clear need by helping to solve one of today's major IT security problems. The central issue is proving that the users of a system are the persons they claim to be. Tackling this problem will help improve simultaneously the security of civil society in Europe, the privacy of the citizen, and provide interoperable access to digital information.</p> <p>The project will develop a seamless environment which:- uses ID smartcards to authenticate individuals,- links this authentication process with the electronic signature of individuals in a number of existing PKIs, already approved by various administrations,- links a person's electronic signature with their rights to access digital data,- links a workflow representation of a legal process with the simultaneous legal rights of the individual. The research will focus on biometric algorithms suitable for use with smart cards, rights management with existing public key infrastructures and PKI interoperability, workflow representation of judicial processes, workflow optimisation and proof of workflow equivalence.</p> <p>This research is targeted at improving the efficiency of the legal process (to reduce delays and risks of procedure errors), thanks to the use by approved users of computer aided tools and industrial methods. For this, eJustice will define, develop, test, and prepare the rollout of a complete and innovative system to improve security and visibility. Some potential users are:- magistrates and other civil servants of national justice and home affairs administrations (criminal, civil, commercial legal services), legal auxiliaries (lawyers, notaries, experts, etc.), European crime prevention organisations,- researchers in the fields of justice, social and political sciences, IT,- citizens of European member states, accession and associated states.</p>
Coordinator	One Northeast Stella House, Goldcrest Way, Newburn Riverside Ne15 8ny Newcastle Upon Tyne United Kingdom
Contact	Hyslop, Maitland Peter
Tel/Fax	Tel: +33-6-62012851 Fax: +33-4-93122413
URL	Click Here
Partners	University Of Leeds United Kingdom Institut Eurecom France Infocamere - Societa Consortile Di Informatica Delle Camere Di Commercio Italiane Per Azioni Italy Unisys Belgium Sa Belgium Grefe Du Tribunal De Commerce De Paris France Bundesverfassungsge

2.5 FIDIS

Name	Future of Identity in the Information Society
Acronym	FIDIS
Action line	IST-2002-2.3.1.5 Towards a global dependability and security framework
Start date	01/04/2004
Duration	60 months
Status	Execution
Description	<p>The European Information Society (EIS) requires technologies, which address trust and security yet also preserve the privacy of individuals. As the EIS develops, the increasingly digital representation of personal characteristics changes our ways of identifying individuals, and supplementary digital identities, so-called virtual identities, embodying concepts such as pseudonymity and anonymity, are being created for security, profit, and convenience or even for fun. These new identities are feeding back into the world of social and business affairs, offering a mix of plural identities and challenging traditional notions of identity. At the same time, European states manage identities in very different ways. For example, in Germany holding an ID card is mandatory for every adult, while in the UK state-issued ID cards do not exist. FIDIS objectives are shaping the requirements for the future management of identity in the EIS and contributing to the technologies and infrastructures needed.</p> <p>FIDIS work is structured into 7 research activities:- "Identity of Identity"- Profiling- Interoperability of IDs and ID management systems- Forensic Implications- De-Identification- HighTechID- Mobility and IdentityAs a multidisciplinary and multinational NoE FIDIS, appropriately, comprises different country research experiences with heterogeneous focuses, and integrates European expertise around a common set of activities. Additionally, all relevant stakeholders are addressed to ensure that the requirements are considered from different levels. FIDIS overcomes the extreme fragmentation of research into the future of identity by consolidating and fostering joint research in this area. Research results will be made accessible to European citizens, researchers and in particular to SMEs.</p> <p>FIDIS will accomplish ERA objectives by durably integrating the research implementation efforts, as well as the medium term target setting, and in the long run the strategic objective planning.</p>
Coordinator	Ohann Wolfgang Goethe-Universitaet Frankfurt Am Main Professur Fr Bwl, Insbes. Wirtschaftsinformatik, Mehrseitig Senckenberganlage 31 60325 Frankfurt Am Main Germany
Contact	Rannenberg, Kai
Tel/Fax	Tel: +49-697-9825301 Fax: +49-697-9825306
URL	Click Here
Partners	Johann Wolfgang Goethe - Universität Frankfurt am Main Joint Research Centre (JRC) Vrije Universiteit Brussel Unabhängiges Landeszentrum für Datenschutz

Institut Europeen D'Administration Des Affaires (INSEAD)
University of Reading
Tilburg University
Universiteit Leuven Research and Development
Karlstads University
Technische Universität Berlin
Technische Universität Dresden
Albert-Ludwig-University Freiburg
Masarykova universita v Brne
VaF Bratislava
London School of Economics and Political Science
Budapest University of Technology and Economics (ISTRI)
International Business Machines Corporation (IBM)
Institut de recherche criminelle de la Gendarmerie Nationale (IRCGN)
Netherlands Forensic Institute
Virtual Identity and Privacy Research Center
Europäisches Microsoft Innovations Center GmbH
Institute of Communication and Computer Systems (ICCS)
AXSionics AG
SIRRIX AG Security Technologies

2.6 GUIDE

Name	Government User IDentity for Europe - creating an European standard for interoperable and secure identity management architecture for eGovernment
Acronym	GUIDE
Action line	IST-2002-2.3.1.9 Networked business and governments
Start date	19/12/2003
Description	<p>In 2001 a Ministerial declaration on eGovernment "recognised that appropriate security and trust is a precondition to the successful introduction of on-line eGovernment services. Ministers agreed to strengthen co-operation across Europe to ensure the security of networks and guarantee safe access to eGovernment services". Small progress has been made and businesses and citizens are signing up to identity services out of necessity and governments are left with poor take-up of services. Meanwhile identity theft is growing into a massive security and economic issue.</p> <p>GUIDE recognises the specific needs of Europe based upon the social, ethical and legislative differences regarding privacy and data protection. Europe is currently at risk of having to accept unsuitable US driven solutions. Therefore the Institutional Setting of Identity in Europe and Excellence in eGovernment Systems and Technology are major elements of GUIDE.</p> <p>Services must be citizen-centric, user-driven and technology-enabled, which is why the other Major Building Blocks address A2A, A2B and A2C transactions and their accompanying processes and platforms. Research will be tested, demonstrated and validated by working closely with a number of Member State administrations.</p> <p>Scientifically, GUIDE will create a European conceptual framework for electronic identity management for eGovernment. Technologically, it will begin the development of an architecture for secure transactions between administrations, citizens and businesses and fostering back-office process integration. The social objective will start to create the institutional setting in Europe to endorse take-up of eGovernment services including social, ethical and legislative research.</p> <p>GUIDE has a long-term vision to make Europe the global leader of eGovernment services by creating an open architecture for eGovernment authentication.</p>
Coordinator	British Telecommunications Plc Bt Global Solutions 81 Newgate Street Ec1a 7aj London United Kingdom
Contact	Borthwick, Lia
Tel/Fax	Tel: +44-208-5878227 Fax: +44-1977-594709
URL	
Partners	Crealogix Ag Switzerland Modirum Oy Finland Cyota Israel Ltd. Israel Netsmart S.A. Greece Siemens Schweiz Ag Switzerland Elca Informatique Sa Switzerland Budapest University Of Economic Sciences And Public Administration Hungary The Chancellor, Mas

2.7 PRIME

Name	Privacy and Identity Management for Europe
Acronym	PRIME
Action line	IST-2002-2.3.1.5 Towards a global dependability and security framework
Start date	01/03/2004
Duration	48 months
Status	Completed
Description	<p>Information technologies are becoming pervasive and powerful to the point that privacy of citizens is now at risk. In the Information Society, individuals want to keep their autonomy and retain control over personal information, irrespective of their activities. The widening gap on this issue between laws and practices on the networks undermines trust and threatens critical domains like mobility, health care and the exercise of democracy.</p> <p>PRIME addresses this issue via an integrative approach of the legal, social, economic and technical areas of concern to build synergies about the research, development and evaluation of solutions on privacy-enhancing identity management (IDM) that focus on end-users. The work plan supports this integration over the project lifetime through multiple iterations of increasing ambition.</p> <p>PRIME elaborates a framework to integrate all technical and non-technical aspects of privacy-enhancing IDM. During and after the project, the framework will act as a lingua franca between all actors and reinforce their roles and responsibilities for full effectiveness. PRIME advances the state of the art far beyond the objectives of existing initiatives to address foundational technologies (human-computer interface, ontologies, authorization, cryptology), assurance and trust, and architectures. It validates its results with prototypes and experiments with end-users, taking into account legacy applications and interoperability with existing and emerging IDM standards.</p> <p>PRIME creates awareness and timely disseminates its results, in particular through computer-based education. PRIME involves leading experts from application and service providers, data protection authorities, academic and industrial research, and invites all major stakeholders to join its Reference Group. PRIME participation prepares the transfer of its results to industry and standardisation to strongly support European privacy regulations and reinforce European leadership.</p>
Coordinator	International Business Machines Belgium Sa Avenue Du Bourget, 42 1130 Bruxelles Belgium
URL	Click Here
Partners	Ibm Research Gmbh Switzerland Katholieke Universiteit Leuven Belgium Fondazione Centro San Raffaele Del Monte Tabor Italy Deutsche Lufthansa Aktiengesellschaft Germany Centre National De La Recherche Scientifique France Swisscom Ag Switzerland Hewle

2.8 SECURIST

Name	Security IST Projects cluster support
Acronym	SECURIST
Action line	IST-2002-2.3.6 Programme Level Accompanying Measures
Start date	01/11/2004
Duration	27 months
Status	Completed
Description	<p>The purpose of the SecurIST project is to deliver a Strategic Research Agenda for ICT Security and Dependability R&D for Europe. It will do this through meeting the following objectives: 1. Establish and Co-ordinate a European ICT Security & Dependability Taskforce 2. Drive the creation of an "ICT Security & Dependability Research strategy beyond 2010" 3Leverage the knowledge base of existing/future ICT Security and Dependability researchers and projects The Strategic Research Agenda to be developed by the Security taskforce will elaborate the ICT Security & Dependability Research strategy beyond 2010. It will provide Europe with a clear European level view of the strategic opportunities, strengths, weakness, and threats in the area of Security and Dependability. It will identify priorities for Europe, and mechanisms to effectively focus efforts on those priorities, identifying instruments for delivering on those priorities and a coherent time frame for delivery. Through the use of thematic areas, the project will leverage the knowledge base of projects and people already engaged in Security & Dependability R&D. The thematic areas will enable projects to address how their research activity will contribute to higher-level issues, and to the elaboration of the Strategic Research Agenda. All this will be achieved this through the efforts of a European ICT Security & Dependability Taskforce. This taskforce will be constituted and co-ordinated through the SecurIST project, which will act as the Secretariat and Steering committee of the Taskforce. A core taskforce of 20-25 key player/influencer is complemented by a wider taskforce of 200- 400 providing the basis for the structured emergence of a 'European Technology Platform' in ICT Security and Dependability in FP7.</p>
Coordinator	Waterford Institute Of Technology Telecommunications Software And Systems Group (Tssg) Cork Road Ireland
Contact	Mcintyre, Diarmuid
Contact reference	
Tel/Fax	Tel: +353-5-1302970 Fax: +353-5-1302901
URL	Click Here
Partners	Telscom Consulting Gmbh Switzerland Vodafone Group Services Limited United Kingdom Siemens Aktiengesellschaft Germany Fundacao Da Faculdade De Ciencias Da Universidade De Lisboa Portugal Groupe Des Ecoles Des Telecommunications France

2.9 SECURINT

Name	European Union Internal Security Governance
Acronym	SECURINT
Action line	
Start date	01/08/2005
Duration	36 months
Status	Completed
Description	<p>Since the Treaty of Amsterdam (1999) the European Union has an explicit mandate, under the treaty objective of establishing and maintaining an "area of freedom, security and justice", to provide citizens with a "high level of safety/security", a mandate reinforced by the Tampere and Seville European Councils. As a result the EU has acquired a growing role in the provision of internal security to European citizens, one of the most fundamental public goods and an essential pre-condition for societal and political stability as well as steady economic development.</p> <p>The proposed Marie Curie Chair is intended to carry out leading edge research and to provide high quality research training on the conditions, challenges, the potential and the limits of EU internal security governance, focusing on the following four main objectives:(1) the conceptualisation of "internal security" at the EU level;(2) the analysis of the cost/benefit balance of EU action in the selected fields of the fight against international terrorism, organised crime and illegal immigration;(3) the comparative analysis of the relative efficiency of different "soft" and "hard" methods of EU governance in the internal security field;(4) the analysis and evaluation of democratic and judicial control procedures applied to EU governance in the internal security domain.</p> <p>By bringing together a political scientist with a leading expertise on EU internal security governance with the outstanding legal expertise of a host specialising in this area this transnational mobility is intended to lead to a European centre of excellence of research and postgraduate teaching on EU internal security governance issues.</p>
Coordinator	Université Robert Schuman
Contact	Constance Grewe
Contact reference	
Tel/Fax	Tel: +33-3-88143031 Fax: +33-3-88143032
URL	Click here
Partners	

2.10 SERENITY

Name	System engineering for security and dependability
Acronym	SERENITY
Action line	IST-2004-2.4.3 Towards a global dependability and security framework
Start date	01/01/2006
Duration	36 months
Status	Completed
Description	<p>The primary goal of SERENITY IP proposal is to enhance security and dependability for Aml ecosystems by capturing security expertise and making it available for automated processing. SERENITY will provide a framework supporting the automated integration, configuration, monitoring and adaptation of security and dependability mechanisms for such ecosystems. Technically, SERENITY will be based on(i) the enhanced notions of SandD Patterns and Integration Schemes, and(ii) the support for run-time pro-active and reactive monitoring of requirements. SERENITY focus on five key areas to provide security and dependability mechanisms:(i) Organization and Business,(ii) Workflow and Services, and(iii) Network and Devices levels,(iv) provision of integrated solutions for these mechanisms and(v) support for run-time monitoring. The results coming from these areas will be integrated to produce the SERENITY framework. The results will be driven by the scenarios and the industrial requirements that will influence the research results to make them ready to be exploitable. Exploitation of results will be achieved through different routes but with the common theme of partners incorporating these results in current or planned products.</p> <p>SERENITY brings together software companies, application solution developers and research institutions and will be driven by the need for security and dependable solutions in e-business, e-government and communication domains. SERENITY is integrated in the following ways:- technically, through complementary focus areas addressed by strong research teams, industrially, through multi-sectors application partners who share a common vision for the potential of security issues,- managerially, through a strong management structure based on entrepreneurial practices,- internationally, with partners from 9 different countries,- personally, through strong existing working relationships between partners.</p>
Coordinator	Engineering - Ingegneria Informatica - S.P.A. Research And Development Laboratory Department Via San Martino Della Battaglia 56 00185 Roma Italy
Contact	Presenza, Domenico
Tel/Fax	Tel: +39-064-9201421 Fax: +39-064-920134
URL	Click Here
Partners	Telefonica Investigacion Y Desarrollo Sa Unipersonal Spain Universita Degli Studi Di Trento Italy Atos Origin Sociedad Anonima Espanola Spain Athens Technology Center S.A. Greece Universidad De Malaga Spain Fraunhofer Gesellschaft Zur Foerderung Der

2.11 SWAMI

Name	Safeguards in a World of AMbient Intelligence
Acronym	SWAMI
Action line	POLICIES-3.5 Information Society issues (such as management and protection of digital assets, and inclusive access to the information society) Specific Support Action
Start date	01/02/2005
Duration	18 months
Status	Completed
Description	<p>This project aims to identify and analyse the social, economic, legal, technological and ethical issues related to identity, privacy and security in Ambient Intelligence (Aml), as called for in the Work Programme. The partners will review existing Aml projects, studies, scenarios and roadmaps to ensure that the SWAMI project captures, as far as possible, the major trends and issues. The partners will compose 'dark' scenarios, the aim of which will be to expose key socio-economic, legal, technological and ethical risks and vulnerabilities related to issues such as identity, privacy and security that may emerge from the deployment of Aml technologies and services, many if not most of which will be invisible to the public. The partners will define and study various research and policy options, which could serve as safeguards and privacy-enhancing mechanisms. The aim will be to identify mechanisms, which will ensure user control, user acceptance and enforceability of policy in an accessible manner, as well as to ensure that all Europeans have real equal rights and opportunities of accessibility to the Ambient Intelligence space. The partners will seek to validate their findings through two workshops with other Aml and IST experts before presenting the options to the Commission in a final report. Project results will be disseminated widely and continuously throughout the project and will be presented at a final, high-level conference.</p>
Coordinator	Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung E.V. Hansastrasse 27c 80686 Munchen Germany
Contact	Friedewald, Michael
Contact reference	
Tel/Fax	
URL	
Partners	Vrije Universiteit Brussel Belgium Valtion Teknillinen Tutkimuskeskus (Vtt) Finland Trilateral Research & Consulting Llp United Kingdom Commission Of The European Communities - Directorate General Joint Research Centre Belgium

2.12 TTSRL

Name	Transnational Terrorism, Security and the Rule of Law
Acronym	TTSRL
Action line	CITIZENS-2004-6.2.1 Transnational terrorism, security and rule of law Specific Targeted Research Project
Start date	01/06/2006
Duration	30 months
Status	Completed
Description	<p>Project Objectives: The overall objective is twofold. First, we will analyse the nature and significance of the evolving threat of trans-national terrorism to the European Union and its individual Member States. Based on this, we will examine the appropriateness and effectiveness of response options aimed at dealing with these threats and their impacts. Project Description: Considering the ongoing integration of Europe, a Union-level strategy towards trans-national terrorism is imperative. In support of the formulation of such a strategy, this project will study the conceptual nature of the problems and the possible measures flowing from its findings. This project will conduct of a structured survey of the response options to trans-national terrorism and their respective assumptions. Both policy-areas specifically dealing with terrorism as well as affected policy-fields are taken into account. The project is unique in that it integrates diverse aspects of the issue into one comprehensive and multidisciplinary project. The main added value of the project will lie in the benchmarking of approaches and policy-options in use in the various Member States. Combined with the project's conceptual underpinnings, it will yield insights into the suitability and effectiveness of various approaches and measures from national and European perspectives, the relevant ethical issues, and cost-benefit considerations. Expected results:- an overview of the varying conceptual views on terrorism and its diverging role in the European security discourse, and to advice on how to deal with these divergences;- a better insight into the societal and economic costs of (counter-) terrorism;- an analysis and benchmark of the numerous policies set up across Europe;- the detection of gaps in the policy where counter-terrorism measures are inadequate;- a tool to track changes in policy and societal discourse on terrorism.</p>
Coordinator	Cot-Instituut Voor Veiligheids- En Crisismanagement B.V.
Contact	Dennis De Hoog (Ma)
Tel/Fax	Tel: +31-70-3122026 Fax: +31-70-3122012
URL	Click Here
Partners	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek - Tno Fundacion Para Las Relaciones Internacionales Y El Dialogo Exterior Ustav Mezinarodnich Vztahu, Praha Dansk Center For Internationale Studier Og Menneskerettigheder

3 EC DIRECTIVES, REGULATIONS, TREATIES

3.1 CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Title	Charter of fundamental rights of the European Union
Reference	Official Journal C 364, 18/12/2000, P 0001-0022
Date	18.12.2000
Author	European Parliament, Council, European Commission
Description	<p>The peoples of Europe, in creating an ever closer union among them, are resolved to share a peaceful future based on common values.</p> <p>Conscious of its spiritual and moral heritage, the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity; it is based on the principles of democracy and the rule of law. It places the individual at the heart of its activities, by establishing the citizenship of the Union and by creating an area of freedom, security and justice.</p> <p>The Union contributes to the preservation and to the development of these common values while respecting the diversity of the cultures and traditions of the peoples of Europe as well as the national identities of the Member States and the organisation of their public authorities at national, regional and local levels; it seeks to promote balanced and sustainable development and ensures free movement of persons, goods, services and capital, and the freedom of establishment.</p> <p>To this end, it is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter. This Charter reaffirms, with due regard for the powers and tasks of the Community and the Union and the principle of subsidiarity, the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Social Charters adopted by the Community and by the Council of Europe and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights.</p> <p>Enjoyment of these rights entails responsibilities and duties with regard to other persons, to the human community and to future generations.</p> <p>The Union therefore recognises the rights, freedoms and principles set out hereafter.</p>
URL	Click Here

3.2 DIRECTIVE 95/46/EC OF 24 OCTOBER 1995

Title	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Reference	Official Journal L 281, 23/11/1995 P 0031-0050
Date	24.10.1995
Author	European Parliament, Council
Description	<p>Object of the Directive:</p> <ol style="list-style-type: none"> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1. <p>Scope:</p> <ol style="list-style-type: none"> 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Directive shall not apply to the processing of personal data: <ul style="list-style-type: none"> o in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law, o by a natural person in the course of a purely personal or household activity.
URL	Click Here

3.3 DIRECTIVE 2002/58/EC OF 12 JULY 2002

Title	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
Reference	Official Journal L 201, 31/07/2002, P 0037-0047
Date	12.07.2002
Author	European Parliament, Council
Description	<p>Scope and aim:</p> <ol style="list-style-type: none"> 1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community. 2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons. 3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law. <p>Definitions:</p> <p>Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(8) shall apply.</p> <p>The following definitions shall also apply:</p> <ol style="list-style-type: none"> a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service; b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof; c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service; d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information; e) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time; f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC; g) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

URL

[Click Here](#)

3.4 REGULATION (EC) 45/2001 OF 18 DECEMBER 2000

Title	Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
Reference	Official Journal L 8,12/01/2001 P 0001-0022
Date	12.01.2001
Author	European Parliament, Council
Description	<p>Scope and aim:</p> <ol style="list-style-type: none"> 1. In accordance with this Regulation, the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities, hereinafter referred to as "Community institutions or bodies", shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC. 2. The independent supervisory authority established by this Regulation, hereinafter referred to as the European Data Protection Supervisor, shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Community institution or body. <p>Definitions:</p> <p>For the purposes of this Regulation:</p> <ol style="list-style-type: none"> a) "personal data" shall mean any information relating to an identified or identifiable natural person hereinafter referred to as "data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity; b) "processing of personal data" hereinafter referred to as "processing" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; c) "personal data filing system" hereinafter referred to as "filing system" shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis; d) "controller" shall mean the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act; e) "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; f) "third party" shall mean a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

- g) "recipient" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
- h) (h) "the data subject's consent" shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

URL

[Click Here](#)

4 COMMUNICATIONS FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

4.1 PROMOTING DATA PROTECTION BY PRIVACY ENHANCING TECHNOLOGIES (PETs)

Title	Promoting Data Protection by Privacy Enhancing Technologies (PETs)
Reference	COM(2007) 228 final
Date	2.5.2007
Author	European Commission
Description	<p>The intensive and sustained development of information and communication technologies (ICT) is constantly offering new services which improve people's life. To a large extent, the raw material for interactions in cyberspace is the personal data of individuals moving around in it when they purchase goods and services, establish or maintain contact with others or communicate their ideas on the world wide web. Alongside the benefits brought about by these developments, new risks also arise for the individual, such as identity theft, discriminatory profiling, continuous surveillance or fraud. The Charter of Fundamental Rights of the European Union recognises in Article 8 the right to the protection of personal data. This fundamental right is set forth in a European legal framework on the protection of personal data consisting in particular of the Data Protection Directive 95/46/EC and the ePrivacy Directive 2002/58/EC as well as the Data Protection Regulation (EC) 45/2001 relating to processing by Community institution and bodies. This legislation lays down several substantive provisions imposing obligations on data controllers and recognizing rights of data subjects. It also prescribes sanctions and appropriate remedies in cases of breach and establishes enforcement mechanisms to make them effective. However, this system may prove insufficient when personal data is disseminated worldwide through ICT networks and the processing of data crosses several jurisdictions, often outside the EU. In such situations the current rules may be considered to apply and to provide a clear legal response. Furthermore, a competent authority to enforce the rules may also be identified. However, considerable practical obstacles may exist as a result of difficulties with the technology used involving data processing by different actors in different locations and there may be hurdles intrinsic to the enforcement of national administrative and court rulings in another jurisdiction, especially in non-EU countries. Whilst strictly speaking data controllers bear the legal responsibility for complying with data protection rules, others also bear some responsibility for data protection from a societal and ethical point of view. These involve those who design technical specifications and those who actually build or implement applications or operating systems. Article 17 of the Data Protection Directive lays down the data controller's obligation to implement appropriate technical and organisational measures and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive. A further step to pursue the aim of the legal framework, whose objective is to minimise the processing of personal data and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult. The purpose of this Communication, which follows from the First Report on the implementation of the Data Protection Directive, is to consider the benefits of PETs, lay down the Commission's objectives in this field to promote these technologies, and set out clear actions to achieve this goal by supporting the development of PETs and their use by data controllers and consumers.</p>
URL	Click Here

4.2 WORK PROGRAMME FOR BETTER IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE

Title	The follow-up of the work programme for better implementation of the data protection directive
Reference	COM(2007) 87 final
Date	7.3.2007
Author	European Commission
Description	<p>Directive 95/46/EC set a milestone in the history of the protection of personal data as a fundamental right, down the path paved by Council of Europe Convention 108. Pursuant to Article 33 of the Directive, the Commission's First report on its implementation concluded that, although no legislative changes were needed, work had to be done and that there was considerable scope for improvement in implementing the Directive.</p> <p>The report contained a Work Programme for better implementation of the data protection Directive . This Communication examines the work conducted under this programme, assesses the present situation, and outlines the prospects for the future as a condition for success in a number of policy areas in the light of Article 8 of the European Charter of Fundamental Rights, recognising an autonomous right to the protection of personal data.</p> <p>The Commission considers that the Directive lays down a general legal framework that is substantially appropriate and technologically neutral. The harmonised set of rules ensuring a high standard of protection for personal data throughout the EU has brought considerable benefits for citizens, business and authorities. It protects individuals against general surveillance or undue discrimination on the basis of the information others hold on them. The trust of consumers that personal details they provide in their transactions will not be misused is a condition for the development of e-commerce. Business operate and administrations co-operate throughout the Community without fearing that their international activities be disrupted because personal data they need to exchange are not protected at the origin or the destination.</p> <p>The Commission will continue to monitor the implementation of the Directive, work with all stakeholders to further reduce national divergences, and study the need for sector-specific legislation to apply data protection principles to new technologies and to satisfy public security needs.</p>
URL	Click Here

4.3 FIRST REPORT ON THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE

Title	First Report on the implementation of the Data Protection Directive
Reference	COM (2003) 265(01),
Date	15.5.2003
Author	European Commission
Description	<p>The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32, on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments.’ (Article 33 of EC Directive 95/46) The present report is the Commission’s response to the above requirement. The Commission has delayed its report by 18 months because the Member States have been slow to transpose the Directive into national law¹.</p> <p>The Commission has approached the preparation of this report from a broad perspective. It has gone beyond the simple examination of the Member States’ acts of implementation and has conducted in addition an open public debate, encouraging a wide participation on the part of stakeholders. This approach is not only in line with the Commission’s approach to governance at the European level as set out in its White Paper of July 2001²; it is also justified by first, the specific nature of Directive 95/46 and second, the rapid pace of technological development in the information society and other international developments which have brought about significant changes since the Directive was finalised in 1995.</p>
URL	Click Here

4.4 A STRATEGY FOR A SECURE INFORMATION SOCIETY

Title	A strategy for a secure Information Society
Reference	COM(2006) 251
Date	31.5. 2006
Author	European Commission
Description	<p>The Communication “i2010 – A European Information Society for growth and employment”, highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society.</p> <p>The purpose of the present Communication is to revitalise the European Commission strategy set out in 2001 in the Communication “Network and Information Security: proposal for a European Policy approach”. It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS).</p> <p>Drawing on the experience acquired by Member States and at European Community level, the ambition is to further develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment .</p> <p>In tackling security challenges for the Information Society, the European Community has developed a three-pronged approach embracing: specific network and information security measures, the regulatory framework for electronic communications (which includes privacy and data protection issues), and the fight against cybercrime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for a coordinated strategy. This Communication sets out the strategy and provides the framework to carry forward and refine a coherent approach to NIS.</p> <p>The 2001 Communication defines NIS as “ the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems ”. Over recent years, the European Community has implemented a number of actions to improve NIS.</p> <p>The regulatory framework for electronic communications, the review of which is underway, includes security-related provisions. In particular, the Directive on Privacy and Electronic Communications contains an obligation for providers of publicly available electronic communications services to safeguard the security of their services. Provisions against spam and spyware are laid down.</p> <p>Trust and security also play an important part in the European Community programmes devoted to research and development. The 6th Research Framework Programme addresses these issues through a wide range of projects. Security-related research is to be reinforced in the 7th Framework Programme with the establishment of a European Security Research Programme (ESRP). Furthermore, the Safer Internet Plus programme supports networking projects and the exchange of best practices to combat harmful content circulating on information networks.</p> <p>As a part of its response to security threats, the European Community decided in 2004 to create the European Network and Information Security Agency (ENISA). ENISA contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union (EU).</p> <p>The EU also plays an active role in the international fora addressing these topics, such as the OECD, the Council of Europe or the UN. At the World Summit on the Information Society in Tunis, the EU strongly supported the discussions on the availability, reliability</p>

and security of networks and information. The Tunis Agenda, which together with the Tunis Commitment sets out further steps for the policy debate on the global Information Society as endorsed by the world's leaders, highlights the need to continue the fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression. It identifies the need for a common understanding of the issues of Internet security and for further cooperation to facilitate the collection and dissemination of security-related information and the exchange of good practice among all stakeholders on measures to combat security threats.

URL

[Click Here](#)

5 EC GREEN PAPERS

5.1 GREEN PAPER ON DETECTION TECHNOLOGIES

Title	Green paper on detection technologies in the work of law enforcement, customs and other security authorities
Reference	COM(2006) 474
Date	01.09.2006
Author	European Commission
Description	<p>Security is a cornerstone of Commission policy. Combating crime and terrorism is a crucial dimension of security policy. The Commission set out its counter-terrorism policy in its "Communication on Prevention, preparedness and response to terrorist attacks" of October 2004. This Communication highlights Public-Private Security Dialogue as a tool for private and public sectors to engage in a meaningful dialogue on Europe's security needs. The Hague Programme: strengthening freedom, security and justice in the European Union adopted by the European Council in November 2004, which constitutes at present the political programme of the Union on Justice and Home Affairs, also highlights the importance of public-private interaction in the fight against organised crime and terrorism. This Green Paper aims to provide the ingredients for initiating such dialogue within the field of detection technologies.</p> <p>Detection technologies are increasingly used in the daily work of security authorities to fight terrorism and other forms of crime. Detection technologies are widely used to protect passengers when boarding aeroplanes and sports fans when watching their favourite sports events, and to detect dangerous substances in the air, water or food. Security authorities also use these technologies to protect our borders and check goods entering the territory of the European Union. Moreover, detection technologies are essential for guarding private property and critical infrastructure. This Green Paper aims to find out what role the Union could play in order to foster detection technologies in the service of the security of its citizens. On the other hand, detection technologies are inherently intrusive into privacy or can pose a challenge to freedoms and rights. Therefore, each time when considering improvement and use of detection technologies, this aspect and the fundamental question of what the limitations of their intrusiveness should be, will have to be carefully analysed. The Commission intends to contribute to both issues with this initiative.</p> <p>The Commission organised a conference – Public-Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against Terrorism – in Brussels on 28-29 November 2005. The participation of over a hundred representatives both from major European business and industry associations and from the public sector attested to the interest of stakeholders in pursuing a policy in this area. The public sector was represented by members of law enforcement, customs and other security authorities.</p> <p>The role of Europe, in areas such as security research or standardisation, is clearly established. Although considerable work has been achieved in certain areas in close cooperation with the Member States, industry and other interested parties, there is still room for an enhanced European policy on detection technologies as such. With respect to aviation security, both Regulations (EC) No 2320/2002 and No 622/2003 contain detailed requirements as regards the performance of the screening equipment to be used and the methodology. In this field, standards and test protocols have been established in close cooperation with the European Civil Aviation Conference, which regroups experts from the appropriate authorities of the Member States and other European States. In addition, the Commission is regularly in close contact with the industry and other stake holders concerned (Stakeholders Advisory Group on Aviation Security – SAGAS Group).</p> <p>In view of strengthening the common approach towards detection technologies the</p>

Commission took this initiative to further enhance interaction between public and private sectors in an effort to focus investment on standardisation, research, certification and interoperability of detection systems and to transform research results into useful and applicable tools. A virtuous circle has to be established in which the private sector is guided in its research effort and expenditure by a public sector that knows what it wants and what the private sector can offer. This should help to develop an advanced market in detection products and security solutions, which in turn should lead to greater availability of products and services at lower cost.

Common action and better coordination and information exchange between everyone involved in Europe are essential if this aim is to be reached. Needs have to be defined better and both technologically and economically viable solutions brought to the surface. This Green Paper certainly does not aim to overlap with other activities either at national or European level. The Commission does not wish to reinvent the wheel but to find out more about existing good approaches and practices, and to support them and spread them across the Union.

The Commission is keen for this Green Paper to generate as many thought-provoking answers and concrete suggestions on steps ahead as possible. Extensive participation by Member States, the private sector and other relevant stakeholders is therefore indispensable. The Commission is, however, aware of confidentiality requirements in both the public and the private sectors, both for security and for commercial reasons. Therefore, respondents are asked to indicate any answers that are too sensitive to be shared and to suggest an alternative approach to take account of such concerns.

Policies relating to detection and associated technologies have to comply in full with the existing legal framework, including the EU Charter of Fundamental Rights, the European Convention on Human Rights and data protection principles and rules as laid down in Directive 95/46/EC. In this context, the Commission stresses that the design, manufacture and use of detection technologies and associated technologies, together with legislation or other measures aiming to regulate or promote them, must fully comply with Fundamental Rights as provided for in the EU Charter of Fundamental Rights and the European Convention on Human Rights. Particular attention must be paid to compliance with the protection of personal data and the right to private life. Indeed, as the use of detection technologies will usually mean an intrusion of the fundamental rights to private life and protection of personal data, any intrusion of fundamental rights has to be in compliance with the European Convention on Fundamental Rights; in particular, it must be in accordance with the law and necessary in a democratic society to protect an important public interest and must be in proportion to the public interest pursued.

URL

[Click Here](#)

5.2 GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION

Title	Green Paper on a European Programme for Critical Infrastructure Protection
Reference	COM(2005) 576
Date	17.11.2005
Author	European Commission
Description	<p>The main objective of the green paper is to receive feedback concerning possible EPCIP policy options by involving a broad number of stakeholders. The effective protection of critical infrastructure requires communication, coordination, and cooperation nationally and at EU level among all interested parties - the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public.</p> <p>The Green Paper provides options on how the Commission may respond to the Council's request to establish EPCIP and CIWIN and constitutes the second phase of a consultation process concerning the establishment of a European Programme for Critical Infrastructure Protection. The Commission expect that by presenting this green paper, it will receive concrete feedback concerning the policy options outlined in this document. Depending on the outcome of the consultation process, an EPCIP policy package could be put forward during 2006.</p>
URL	Click Here

6 OPINIONS OF THE EUROPEAN DATA PROTECTION SUPERVISOR

6.1 OPINION OF 19 DECEMBER 2005

Title	Opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters
Reference	Official Journal C 47,26/02/2006 P 0027-0047
Date	25.02.2006
Author	EUROPEAN DATA PROTECTION SUPERVISOR
Description	<p>The Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters has been sent by the Commission to the EDPS by letter of 4 October 2005. The EDPS understands this letter as a request to advise Community institutions and bodies, as foreseen in Article 28 (2) of Regulation nr. 45/2001/EC. According to the EDPS, the present opinion should be mentioned in the preamble of the Framework Decision.</p> <p>The EDPS underlines the importance of the present proposal, from the perspective of the fundamental rights and freedoms of natural persons to have their personal data protected. The adoption of this proposal would mean a considerable step forwards for the protection of personal data, in an important area which in particular requires a consistent and effective mechanism for the protection of personal data on the level of the European Union.</p> <p>In this context, the EDPS emphasises that police and judicial cooperation between the member states, as an element of the progressive establishment of an area of freedom, security and justice, is of growing significance. The Hague Programme has introduced the principle of availability in order to improve the cross-border exchange of law-enforcement information. According to the Hague Programme, the mere fact that information crosses borders should no longer be relevant. The introduction of the principle of availability reflects a more general trend to facilitate the exchange of law enforcement information (see for instance the so called Prüm Convention as has been signed by seven Member States and the Swedish proposal for a Framework Decision on simplifying the exchange of information and intelligence between law enforcement agencies). The very recent approval by the European Parliament of a Directive of the European Parliament and of the Council on the retention of communication data can be viewed in the same perspective. These developments require the adoption of a legal instrument to guarantee an effective protection of personal data within all the Member States of the European Union, based on common standards.</p> <p>The EDPS points to the fact that the present general framework for data protection in this area is insufficient. In the first place, directive 95/46/EC does not apply to the processing of personal data in the course of activities which fall outside the scope of Community law, such as those provided for by Title VI of the Treaty on the European Union (Article 3 (2) of the directive). Although in most Member States the scope of the implementing legislation is wider than the directive itself requires and does not exclude data processing for the purpose of law enforcement, significant differences in national law exist. In the second place, the Council of Europe Convention No 108 by which all the Member States are bound does not provide for the necessary preciseness in the protection as has been recognised already at the time of the adoption of Directive 95/46/EC. In the third place, neither of these two legal instruments takes into account the specific characteristics of the exchange of data by police and judicial authorities.</p>
URL	Click Here

6.2 OPINION OF 26 SEPTEMBER 2005

Title	Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC
Reference	Official Journal C 47 ,26/02/2006 P. 0027 - 0047
Date	26.09.2005
Author	EUROPEAN DATA PROTECTION SUPERVISOR
Description	<p>The EDPS welcomes the fact that he is consulted on the basis of Article 28(2) of Regulation (EC) No 45/2001. However, in view of the mandatory character of Article 28(2) of Regulation (EC) No 45/2001, the present opinion should be mentioned in the preamble of the directive.</p> <p>The EDPS recognises the importance for law enforcement agencies of the Member States of having all the necessary legal instruments at their disposal, in particular in the combat of terrorism and other serious crime. An adequate availability of certain traffic and location data of public electronic services can be a crucial instrument for those law enforcement agencies and can contribute to the physical security of persons. In addition it should be noted that this does not automatically imply the necessity of the new instruments as foreseen in the present proposal.</p> <p>It is equally evident that the proposal has a considerable impact on the protection of personal data. If one considers the proposal solely from the perspective of data protection, traffic and location data should not be retained at all for the purpose of law enforcement. It is for reasons of data protection that Directive 2002/58/EC establishes as a principle of law that traffic data must be erased as soon as storage is no longer needed for purposes related to the communication itself (including billing purposes). Exemptions to this principle of law are subject to strict conditions.</p> <p>In this opinion, the EDPS shall highlight the impact of the proposal on the protection of personal data. The EDPS shall furthermore take into account that, notwithstanding the importance of the proposal for law enforcement, it may not result in people being deprived of their fundamental right to have their privacy protected.</p> <p>This opinion of the EDPS must be seen in the light of these considerations. The EDPS envisages a balanced approach, in which the necessity and the proportionality of the interference with data protection play a central role.</p> <p>As to the proposal itself, this must be seen as a reaction to the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism ("the draft Framework Decision"), that was rejected by the European Parliament (in the consultation procedure).</p> <p>The EDPS has not been consulted on the draft Framework Decision, nor has he given an opinion on his own initiative. The EDPS does not intend to give as yet an opinion on the draft Framework Decision, but will in the present opinion refer to this draft decision, where he deems this to be useful.</p>
URL	Click Here

6.3 OPINION OF 15 JUNE 2005

Title	Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data
Reference	Official Journal C 218 ,06/09/2005 P. 0006 - 0010
Date	15.06.2005
Author	EUROPEAN DATA PROTECTION SUPERVISOR
Description	<p>The EDPS welcomes that he is consulted on the basis of Article 28(2) of Regulation (EC) No 45/2001. This confirms the viewpoint of the EDPS as laid down in his policy paper of 18 March 2005 ("The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents") that the advisory task extends to the conclusion of agreements between the EC and third countries and/or international organisations with regard to the processing of personal data.</p> <p>In view of the mandatory character of Article 28(2) of Regulation (EC) No 45/2001, the present opinion should be mentioned in the preamble of the Council decision.</p> <p>According to its recitals, the agreement at stake, between the European Community and Canada, has regard to a Commission decision, pursuant to Article 25(6) of Directive 95/46/EC, whereby the relevant Canadian competent authority is considered as providing an adequate level of protection for API/PNR data ("The Commission decision"). In the view of the EDPS, the Commission decision should have been sent for consultation as well, being part of the joint legal package.</p> <p>This proposal is the second in a row, after the agreement of 17 May 2004 between the European Community and the United States of America, of which the legality was contested by the Parliament under Article 230 of the EC-Treaty. In his intervention before the Court of Justice, the EDPS supported the conclusions of the Parliament to annul the agreement.</p> <p>This proposal for an agreement is of a similar nature to the agreement with the United States of America. It is linked to a decision of the Commission, pursuant to Article 25(6) of Directive 95/46/EC, the objective is to improve public security and the air carrier is obliged to transfer data to a third country.</p> <p>In substance however, there are major differences, as has been noted in two opinions of the Article 29-Data Protection Working Party. The EDPS emphasises four essential differences that will play a role throughout this opinion. In the first place, the proposal foresees a "push"-system (and not a "pull"-system) which has as a consequence that the airlines in the European Community can control the transfer of the data to the Canadian authorities. In the second place, the commitments taken by the Canadian authorities are binding (Article 2(1) of the agreement), which contributes to a more balanced proposal, compared to the agreement with the United States of America. In the third place, the list of PNR-data to be transferred is more limited and does not comprise "open categories" of passenger data that could reveal sensitive information. Finally, the agreement profits from a much more developed legislative system of data protection, that offers protection to the data subject including supervision by an independent Data Commissioner. However, the Canadian legislation does not give a full protection to citizens of the European Union. The commitments taken by the Canadian authorities aim to find a solution for those citizens.</p>
URL	Click Here

6.4 SECOND OPINION OF 26 APRIL 2007

Title	Second opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters
Reference	Official Journal C 91 ,26/04/2007 P. 0009 – 0014
Date	26.04.2007
Author	European Data Protection Supervisor
Description	<p>On 19 December 2005, the EDPS issued an opinion on the Proposal of the Commission for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. In this opinion, he underlined the importance of the proposal as an effective instrument for the protection of personal data in the area covered by Title VI of the EU-Treaty. Such an instrument should not only respect the principles of data protection as laid down in the Council of Europe Convention No 108 and more specifically in directive 95/46/EC, but also provide for an additional set of rules taking into account the specific nature of the area of law enforcement. For the EDPS it is essential that the framework decision covers all processing of police and judicial data, even if they are not transmitted or made available by competent authorities of other Member States. Consistency of the protection of personal data is essential, regardless of where, by whom or for which purpose they are processed. The EDPS has made several proposals to improve the level of protection.</p> <p>On 27 September 2006, the European Parliament adopted a legislative resolution on the Commission proposal. In general terms, the resolution has the same objectives as the opinion of the EDPS: support for the proposal in general and amendments aiming to enhance the level of protection afforded by the Framework Decision.</p> <p>The Commission proposal is currently being discussed within Council. The Council is reportedly making progress and is modifying essential elements of the text of the proposal. A serious effort is being made by the Council Presidency to make even more significant progress. It aims at reaching a common approach on the main elements by December 2006.</p> <p>The EDPS welcomes that the Council is giving much attention to this important proposal. However, he is concerned about the direction of the developments. The texts currently being discussed within Council do not incorporate the amendments proposed by the European Parliament, nor the opinions of the EDPS and of the Conference of European Data Protection Authorities. On the contrary, in quite a few cases provisions in the Commission proposal, offering safeguards to the citizens, are deleted or substantially weakened. As a result, there is a substantial risk that the level of protection will be lower than the level of protection afforded under Directive 95/46/EC or even under the more generally formulated Council of Europe Convention No 108 which is binding on the Member States.</p> <p>The EDPS notes that also the Libe-committee of the European Parliament has recently voiced its concerns regarding the choices of Council on this proposal for a framework decision.</p> <p>It is for these reasons that the EDPS now issues a second opinion. This second opinion focuses on some essential concerns and does not repeat all the points made in the opinion of the EDPS in December 2005, which all remain valid.</p>
URL	Click Here

6.5 OPINION OF 26 FEBRUARY 2006

Title	Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability
Reference	Official Journal C 116,17/05/2006 P 0008-0017
Date	28.02.2006
Author	European Data Protection Supervisor
Description	<p>The principle of availability has been introduced as an important new principle of law in the Hague Programme. It entails that information needed for the fight against crime should cross the internal borders of the EU without obstacles. The objective of the present proposal is to implement this principle in a binding legal instrument.</p> <p>The exchange of police information between different countries is a popular subject for legislators, within and outside the framework of the EU. Recently, the following initiatives drew the attention of the EDPS. In the first place, on 4 June 2004 Sweden proposed a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. On this proposal, the Council has reached an agreement on a general approach in its meeting of 1 December 2005. In the second place, on 27 May 2005, seven Member States signed a Convention in Prüm (Germany) on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. It introduces inter alia measures to improve information exchange for DNA and fingerprints. The Convention is open for any Member State of the European Union to join. The Contracting Parties aim to incorporate the provisions of the Convention into the legal framework of the European Union. In the third place, the availability of law enforcement information across the internal borders of the European Union will also be further facilitated by other legal instruments, such as the proposals regarding a Second Generation Schengen Information System (SIS II), the proposal for access for consultation to the Visa Information System (VIS) and the proposal for a Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States. In this respect, it is also useful to mention the Communication on improved effectiveness, enhanced operability and synergies among European databases in the area of Justice and Home Affairs, issued by the Commission on 25 November 2005. Because all of these initiatives have been issued, it follows that the present proposal for a Framework Decision on availability should not be examined by itself, but other approaches to the exchange of law enforcement information should also be taken into account. This is even more important since it is the current tendency within the Council to give preference to other approaches to information exchange and to the concept of availability than the general approach proposed by the Commission in the present proposal. The present text of the proposal might even not be the object of discussion in the Council. Furthermore, this proposal is closely linked to the Proposal for a Framework Decision on the protection of personal data. The present opinion must be understood in connection with the more profound opinion on the latter Framework Decision. In his opinion on the Proposal for a Framework Decision on the protection of personal data, the EDPS underlined the importance of adequate data protection as a necessary consequence of a legal instrument on availability. According to the EDPS, such a legal instrument should not be adopted without essential guarantees on data protection. The EDPS takes the same position in respect of the adoption of other legal instruments that facilitate the flow of law enforcement information across the internal borders of the EU. The EDPS therefore welcomes that the Council as well as the European Parliament have dedicated priority to the aforementioned proposal for a Framework Decision on the protection of personal data.</p>
URL	Click Here

6.6 OPINION OF 25 APRIL 2006

Title	Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences
Reference	Official Journal C 97,25/04/2006 P 0006-0010
Date	25.04.2006
Author	European Data Protection Supervisor
Description	<p>The Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (hereinafter: "the proposal") was sent by the Commission to the European Data Protection Supervisor (EDPS) by letter of 24 November 2005. The EDPS understands this letter as a request to advise Community institutions and bodies, as foreseen in Article 28(2) of Regulation (EC) No 45/2001. According to the EDPS, the present opinion should be mentioned in the preamble of the Decision.</p> <p>The EDPS deems it important to deliver an opinion on this sensitive subject because this proposal follows directly from the establishment of the VIS, which will be subject to his supervision, and on which he has issued an opinion on 23 March 2005. In that opinion, the hypothesis of access by law enforcement authorities was already envisaged (see below); the creation of new access rights to the VIS has a determinant impact on the system, in terms of data protection. Therefore, giving an opinion on the present proposal is a necessary follow-up of the first opinion.</p>
URL	Click Here

7 OPINIONS OF THE ART.29 WORKING PARTY

7.1 PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Title	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications
Reference	COM(2006) 269 final
Date	31.05.2006
Author	European Commission
Description	<p>The present proposal is intended to create the legal basis for Member States to take mandatory biometric identifiers - the facial image and ten flat fingerprints - from visa applicants and to give a legal framework for the organisation of Member States consular offices in view of the implementation of the Visa Information System (VIS). The Hague programme invited the Commission to present "a proposal on the establishment of common application centres focusing inter alia on possible synergies linked with the development of the VIS." This measure has been taken up by the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union. In order to avoid all Member States having to install the necessary equipment for collecting biometric identifiers in every consular office, the idea of creating "Common application Centres" (CAC) was born. The CACs have a double advantage: the reinforcement of local consular cooperation, streamlining and cost-saving for Member States as resources can be pooled and shared. In this context Member States also discussed other options for organizing the application procedure in order to reduce the costs of the use of biometrics, for instance outsourcing in locations where consular posts are faced with particularly high numbers of applications. Different options such as representation and outsourcing are outlined; Member States can choose from these options in relation to the proper execution of their legal obligations in the framework of visa issuance. This proposal will take account of these options and it could be a first step to the further enhancement of the harmonisation of the application of the CCI and in view of future Common Visa Offices, without prejudice to the future European External Action Service.</p> <p>The proposal stresses that the fundamental rights of visa applicants have to be respected by Member States particularly in respect of data protection. It is also consistent with the policy in view of the establishment of an External Action Service.</p>
URL	Click Here

7.2 RECOMMENDATION 1/2007

Title	Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data
Reference	Working Party document WP 133
Date	10.01.2007
Author	Directorate-General for Justice, Freedom and Security
Description	
URL	Click Here

7.3 OPINION 2/2007

Title	Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities
Reference	Working Party document WP 132
Date	15.02.2007
Author	Directorate-General for Justice, Freedom and Security
Description	<p>This opinion and its annexes (frequently asked questions and model notices) are aimed at travel agents, airlines, and any other organisations providing travel services to passengers flying to and from the United States of America. This opinion and the annexes update and replace the previous opinion of 30 September 2004 (WP97). The current legal framework for transferring PNR information to the US authorities is covered by the interim agreement of 16 October 2006. Negotiations for a new agreement are expected to start in 2007. There remain obligations on travel agents, airlines and other organisations to provide information to passengers about the processing of their personal information, and this opinion aims to give advice and guidance on who needs to provide what information, how and when. Information should be provided to passengers when they agree to buy a flight ticket, and when they receive confirmation of this ticket. The opinion gives advice on providing information by phone, in person and on the internet. The Art. 29 Working Party has established the model information notices (the annexes to this opinion) to make providing this information easier for organisations, and to make sure the information provided is consistent across the European Union. The shorter information notice gives passengers summary information about transfers of their data to the US authorities, and how to find out more information. The longer notice is in the form of frequently asked questions and has more details about the processing. It explains passenger data more widely, before focusing on PNR data. It also includes links to the interim agreement and other relevant documents.</p>
URL	Click Here

7.4 WORKING DOCUMENT OF 15 FEBRUARY 2007

Title	Working Document on the processing of personal data relating to health in electronic health records
Reference	Working Party document WP 131
Date	15.02.2007
Author	Directorate-General for Justice, Freedom and Security
Description	<p>In this Working Document on the processing of personal data relating to health in electronic health records (EHR), the Article 29 Working Party provides guidance on the interpretation of the applicable data protection legal framework for EHR systems and explains some of the general principles. The Working Document also gives indications on the data protection requirements for setting up EHR systems, as well as the applicable safeguards. The Article 29 Working Party first examines the general legal data protection framework for EHR systems. The Article 29 Working Party recalls the general prohibition of the processing of personal data concerning health of Article 8 (1) of the Data Protection Directive 95/46/EC, and then discusses the possible application of the derogations in Article 8 (2), (3) and (4) of the Directive in the context of EHR systems by stressing the need for interpreting such derogations in a narrow fashion. The Article 29 Working Party also reflects on a suitable legal framework for EHR systems and provides recommendations on eleven topics where special safeguards within HER systems seem particularly necessary in order to guarantee the data protection rights of patients and individuals. These topics are:</p> <ol style="list-style-type: none"> 1. Respecting self determination 2. Identification and authentication of patients and health care professionals 3. Authorization for accessing EHR in order to read and write in EHR 4. Use of EHR for other purposes 5. Organisational structure of an EHR system 6. Categories of data stored in EHR and modes of their presentation 7. International transfer of medical records 8. Data security 9. Transparency 10. Liability issues 11. Control mechanisms for processing data in EHR <p>The Article 29 Working Party invites the medical profession, all health care professionals, all involved persons and institutions as well as the general public to comment on this Working Document.</p>
URL	Click Here

7.5 OPINION 1/2007

Title	Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities
Reference	Working Party document WP 129
Date	09.01.2007
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The European Commission has adopted its Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities (COM (2006) 474) on 1 September 2006 (the "Green Paper"). The aim of the Green Paper is to stimulate the discussion in the area of detection technologies at the European level and gather "thought-provoking answers and concrete suggestions" towards "strengthening the common approach towards detection technologies" to be construed in the "broadest sense". The Article 29 Working Party, along with other parties, was invited to participate in the consultation process. The replies to the questions raised in the Green Paper as well as other comments made will determine concrete steps and actions that could be subsequently taken. Furthermore, depending on priorities identified in the course of the public consultation, specific steps could be taken as soon as possible. If stakeholders show their interest, a task force delivering actions on specific subjects could be created. Such a task force could consist of representatives from various Members States authorities and experts from the private sector. The Article 29 Working Party welcomes the fact that the Commission in its Green Paper has taken into account that policies relating to detection and associated technologies have to comply in full with the existing legal framework, including data protection principles and wishes to contribute to the discussion on the Green Paper as follows.</p>
URL	Click Here

7.6 OPINION 10/2006

Title	Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)
Reference	Working Party Art.29
Date	23.10.2006
Author	Directorate-General for Justice, Freedom and Security
Description	<p>At its last session on November 21/22, 2006 the Article 29 Working Party has again been dealing with the SWIFT case and has unanimously adopted Opinion 10/2006 (WP 128) on its findings in this case. In this Opinion the Article 29 Working Party emphasizes that even in the fight against terrorism and crime fundamental rights must remain guaranteed. The Article 29 Working Party insists therefore on the respect of global data protection principles. SWIFT is a worldwide financial messaging service which facilitates international money transfers. SWIFT stores all messages for a period of 124 days at two operation centres, one within the EU and one in the USA – a form of data processing referred to in this document as "mirroring". The messages contain personal data such as the names of the payer and payee. After the terrorist attacks of September 2001, the United States Department of the Treasury ("UST") issued subpoenas requiring SWIFT to provide access to message information held in the USA. SWIFT complied with the subpoenas, although certain limitations to UST access were negotiated. The matter became public as a result of press coverage in late June and early July 2006. As a Belgian based cooperative, SWIFT is subject to Belgian data protection law implementing the EU Data Protection Directive 95/46/EC ("the Directive"). Financial institutions in the EU using SWIFT's service are subject to national data protection laws implementing the Directive in the Member States within which they are established.</p>
URL	Click Here

7.7 OPINION 9/2006

Title	Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data
Reference	Working Party document WP 127
Date	27.09.2006
Author	Directorate-General for Justice, Freedom and Security
Description	<p>On April 29, 2004 the Council adopted Directive 2004/82/EC on the obligation of air carriers to communicate advance passenger data on request to authorities in charge of controlling the external borders of the European Union. The Directive is complementary to the provisions of the Schengen Convention since the latter ones are also intended to curb migratory flows and combat illegal immigration. The Directive had to be transposed by the Member States of the European Union into national law by September 5, 2006. The Article 29 Working Party notes that a number of Member States have not met this deadline and that national laws transposing the Directive are still under discussion. It is still not clear whether all Member States will have implemented the Directive by the end of 2006. Other Member States may have to decide on the practical measures they have to take for the implementation of the directive. It has to be pointed out that for the sake of air passengers and air carriers alike the Directive should be implemented as soon as possible in a uniform, harmonised manner, in order to avoid diverging regulations within the European Union. All persons concerned flying into the European Union should be treated in the same way and should enjoy the same rights. Situations where passengers are treated in different ways must be avoided. The Working Party is furthermore of the view that the provisions of the Directive should be interpreted and implemented in a privacy-consistent way, in full compliance with data protection principles as laid down in Directive 95/46/EC, by respecting data protection as a fundamental right to be enjoyed by all individuals throughout the European Union. Bearing this objective in mind, the Working Party has found it appropriate to adopt some interpretive and implementing guidelines that may be of help to Member States in transposing the Directive as well as in developing the operational mechanisms. The Article 29 Working Party is well aware of the growing importance attached worldwide to the use of API (Advance Passenger Information) data for checking passengers. It also recalls its view expressed earlier¹ that it is necessary for the middlelong term to develop a more consistent approach towards the exchange of passenger data to ensure air traffic security, the fight against illegal immigration, and respect for human rights on a global level.</p>
URL	Click Here

7.8 OPINION 7/2006

Title	Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of PNRs to the United States and the urgent need for a new agreement
Reference	Working Party document WP 124
Date	27.09.2006
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The ruling by the European Court of Justice of 30 May 2006¹ annuls both the Commission Decision on the adequacy finding and the Council Decision on the conclusion of the PNR Agreement. It obliges the Community Institutions to terminate the Agreement with the United States on the transfer of passenger data at the latest by 30 September 2006. For that reason any transfer of passenger data to the US would be without a legal basis in European law after the termination of the Agreement. National legislation may require action to be taken such as the complete suspension of data flows to the US authorities. In the light of this situation, the Article 29 Working Party adopted an Opinion on 14 June 2006 (WP 122) urging the timely adoption of a new agreement between the US and EU before the deadline in order to avoid any legal gaps and to ensure the rights and freedoms of passengers continue to be protected at least at the present level. To date no new agreement has been concluded. Therefore, the Working Party is extremely concerned at the risk of the absence of such an agreement and the potential consequences when the existing arrangements lapse on 1 October 2006. Whilst the Working Party still hopes that a new agreement can be concluded even at this late stage, national data protection authorities must now prepare for a situation where no agreement is concluded and the existing arrangements are no longer in place. Given these concerns, the Working Party has considered what further steps may be appropriate should no replacement agreement be concluded. This is in order to help national supervisory authorities when considering whether enforcement action is appropriate under their own national law and the sanctions available to them.</p>
URL	Click Here

7.9 OPINION 5/2006

Title	Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States
Reference	Working Party document WP 122
Date	14.06.2006
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The Article 29 Working Party adopts the following Opinion and urges the competent European Institutions to take due note of the following:</p> <ul style="list-style-type: none"> • In order to avoid a legal gap as from 1 October 2006 for the transfer of passenger data and to ensure that the rights and freedoms of passengers continue to be protected, the Article 29 Working Party considers a timely adoption of a new agreement with the US on EU level crucial. In order to achieve a harmonised and consistent EU approach, bilateral agreements between the US and the EU Member States should be avoided. • Such an agreement must at least preserve and integrate the current level of data protection as laid down in the US Undertakings so as to make them binding and, in addition, should take into account the critical considerations voiced by the Article 29 Working Party in its previous Opinions on PNR including the reduction of data elements. • Such an agreement should be based on a push system since all technical requirements are in place. • A strict purpose limitation is necessary for the transfer of PNR data comprising the onward transfer of these data. • The Working Party expects that the mechanism of an annual joint review will be maintained in line with the current agreement. • A new agreement should not have a longer duration than the terminated one, i.e. November 2007. <p>The Working Party assumes that the national data protection authorities and the EDPS are heard and consulted. It offers any possible assistance to come to a new agreement that meets the above-mentioned requirements.</p>
URL	Click Here

7.10 OPINION 4/2006

Title	Opinion 4/2006 on the Notice of proposed rule making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71)
Reference	Working Party document WP 121
Date	14.06.2006
Author	Directorate-General for Justice, Freedom and Security
Description	<p>This opinion by the Article 29 Working Party is a reflection on the new US legislative proposal concerning the collection of passenger information by air carriers and shipping lines for the control of communicable diseases (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71). The US draft proposal if enacted would impose some general obligations on European air carriers and and shipping lines and would in particular require them to put into practice the following:</p> <ol style="list-style-type: none"> 1) to collect and store in the EU for 60 days a number of data regarding all passengers flying to the US that are currently not included neither in the companies' passenger name record system (PNR) nor in their departure control system (DCS) such as emergency contact numbers, email addresses, travelling companions and information on the return flight in order to being able to trace them later on; 2) to send these passenger details electronically within a 12 hour period of a request directly to the Director of the US Center for Disease Control and Prevention (CDC). <p>The Article 29 Working Party finds that the fight against communicable diseases is a valuable goal shared by all nations and has, therefore, to be supported in the best possible way. It is in the interest of mankind to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world.</p> <p>The Article 29 Working Party is on the other hand of the opinion that the fundamental right to personal data protection has to be respected when measures are taken to fight communicable diseases and that any measures have to be proportionate. The right to personal data protection and the fight against communicable diseases are no contradictions but may work well alongside if a balanced approach is chosen. This opinion on the new US legislative proposal examines carefully the foreseen regulations and analyses them not only in the light of the EU-Directive on Data Protection 95/46/EC, but also in the light of the WHO International Health Regulations (2005) which is non-binding in its nature but intends to support nations in their fight against communicable diseases.</p> <p>The Article 29 Working Party comes to the conclusion that the US proposal if enacted in its current version would conflict with pertinent privacy provisions of the EU-Data Protection Directive 95/46/EC and the WHO International Health Regulations (2005).</p>
URL	Click Here

7.11 WORKING DOCUMENT OF 24 OCTOBER 1995

Title	Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995
Reference	Working Party document WP 114
Date	25.11.2005
Author	Directorate-General for Justice, Freedom and Security
Description	<p>This working document provides guidance as to how Article 26(1) of Directive 95/46 should be understood and applied by data controllers intending to initiate data transfers to countries which do not ensure an adequate level of protection, in the sense of Article 25 of the said Directive. The Working Party issued this document to address its concern that differing interpretations are made of the provisions of Article 26(1) in practice, which prevent these provisions from being uniformly applied in the different Member States. Similar concerns were voiced by the European Commission's report of 2003 on the implementation of Directive 95/46. The report recalled that neither an overly strict approach to the provisions of Article 25 and 26, nor an overly lax approach to those provisions (and then specifically those of Article 26 (1)) would be in line with their intended purposes, i.e. striking a fair balance between the protection of the individuals whose data are to be transferred to non adequate countries with, inter alia, the imperatives of international trade and the reality of global telecommunications networks". In clarifying Article 26(1) derogations, among others by elaborating on Chapter 5 of working document WP12 on international data transfers which the group previously adopted in July 1998, this paper has sought to maintain the proper balance between the above mentioned interests. In Section 1 of this document, the Working Party sketches a general picture of how these provisions relate to others and together compose the global system of the Directive on international data transfers. It then provides elements of interpretation and recommendations which apply to the provisions of Article 26(1) as a whole. A central element of this interpretation is the necessity that the provisions of Article 26(1) must be strictly interpreted. Another element is that the derogations for the most part concern cases where risks to the data subject are relatively small or where other interests may be considered to override the data subject's right to privacy. Section 1 further elaborates on this interpretation and expresses different recommendations which are designed to encourage controllers to ensure "adequate protection" in as many situations as possible. In its Section 2, the document provides further guidance as to how each of the derogations of Article 26(1) must be interpreted. It specifically expands on the notions of "consent" and "performance of a contract", which are the derogations that controllers most often wish to rely upon in practice. The Working Party believes that this document will be useful to clarify how data controllers may, and sometimes should make use of the derogations in Article 26 (1). The Working Party considers this document as an essential element of its policy on data transfers to third countries. This document should accordingly be read in conjunction with other work done by the Working Party in this domain, namely on "binding corporate rules", standard contractual clauses, and adequacy in third countries, including Safe Harbor.</p>
URL	Click Here

7.12 OPINION 3/2005

Title	Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States
Reference	Working Party document WP 112
Date	30.09.2005
Author	Directorate-General for Justice, Freedom and Security
Description	<p>In its "Working document on biometrics"² the Working Party stressed that "the rapid progress of biometric technologies and their expanded application in recent years necessitates careful scrutiny from a data protection perspective. A wide and uncontrolled utilisation of biometrics raises concerns with regard to the protection of fundamental rights and freedoms of individuals. This kind of data is of a special nature, as it relates to the behavioural and physiological characteristics of an individual and may allow his or her unique identification."</p> <p>Since these fundamental comments on biometrics the legislative developments have proceeded rapidly. The European Council of Thessaloniki, on 19 and 20 June 2003, confirmed that a coherent approach is needed in the European Union on biometric identifiers or biometric data for documents for third country nationals, European Union citizens' passports and information systems (VIS and SIS II). In autumn 2003 the European Commission submitted a draft Council Regulation amending Regulations 1683/95 and 1030/2002 laying down a uniform format for visas and for residence permits for third country nationals respectively.</p>
URL	Click Here

7.13 RESULTS OF THE PUBLIC CONSULTATION ON ARTICLE 29 WORKING DOCUMENT 105

Title	Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology
Reference	Working Party document WP 111
Date	28.09.2005
Author	Directorate-General for Justice, Freedom and Security
Description	Following the adoption of the Working Document on data protection issues related to RFID technology on January 19, 2005, the Working Party 29 decided to put it up for public consultation. After the closing of the public consultation, the Working Party 29 prepared the following summary of the content of the responses received on the Working Party 29 paper on RFID. The Working Party 29 considered that it would be useful to share this summary of main contents with stakeholders in general.
URL	http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

7.14 WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY

Title	Working document on data protection issues related to RFID technology
Reference	Working Party document WP 105
Date	19.01.2005
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The use of Radio Frequency Identification (commonly known as “RFID technology”) for different purposes and applications may benefit business, individuals and public services (governments included). As further illustrated in this paper, RFID can help retailers manage their inventory, enhance consumers' shopping experience, improve drug safety as well as allow better control access by persons to restricted areas. While the advantages related to the use of RFID technology seem obvious, the widespread deployment of the technology does not come without its potential drawbacks. On the data protection front, Working Party 29 (“Working Party 29”) is concerned about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights. In particular, concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals. The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens. The awareness of this new risk has compelled Working Party 29 to look into the privacy and other fundamental rights implications of RFID technology. To this end, among others, Working Party 29 has consulted with interested parties, including manufacturers and deployers of the technology as well as with privacy advocates. The outcome of the subsequent analysis carried out by Working Party 29 is the current working document which has the following two main purposes: firstly, it aims to provide guidance to RFID deployers on the application of the basic principles set out in EC Directives, particularly the data protection Directive² and the Directive on privacy and electronic communications³ and secondly, with this working document Working Party 29 wishes to provide guidance to manufacturers of the technology (RFID tags, readers and applications) as well as RFID standardization bodies on their responsibility towards designing privacy compliant technology in order to enable deployers of the technology to carry out their obligations under the data protection Directive. Taking into account the relatively low level of experience of the use of RFID technology, Working Party 29 regards this paper as a first assessment of the situation. The Working Party will continue examining the situation, and as more experience is gained, it will provide further guidance. This will be particularly necessary if RFID technology becomes, as expected, one of the main “bricks” of the future ambient intelligence environment. In sum, this is an initial paper, and the Working Party 29 will continue working on this issue.</p>
URL	Click Here

7.15 OPINION 1/2005

Title	Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines
Reference	Working Party document WP 103
Date	19.01.2005
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The present Opinion is issued in the light of the Commitments. The Working Party notes that the negotiations have led to substantial and important changes in the Canadian PNR program as reflected by the Commitments. The Working Party also notes that the relevant Canadian law on the transmission of API and PNR data has remained unchanged (see section 1 of the Commitments) and refers in this respect to its analysis thereof in its Opinion 3/2004.</p> <p>The present Opinion is issued with reference to the level of protection ensured by Canada once airlines have transmitted API and PNR data relating to their passengers and crewmembers to the CBSA, on the basis of Canadian law and the Commitments. In its assessment of the adequacy of protection afforded by Canadian law, the Working Party has been guided by the general criteria set forth in previous documents⁴ as well as in its Opinions on the subject of API/PNR data required by the United States⁵.</p>
URL	Click Here

7.16 OPINION 9/2004

Title	Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.
Reference	Working Party document WP 99
Date	09.11.2004
Author	Directorate-General for Justice, Freedom and Security
Description	In recent years, the Working Party has repeatedly commented on the issue of retention of communication traffic data ² , and the European Conference of Data Protection Commissioners has issued several joint statements on the same subject ³ . The proposal for a draft Framework Decision on the retention of such traffic data presented by four member states in the Council of the European Union once again calls for an opinion of the Working Party. In view of the early stage of discussion in the relevant working party of the Council, this opinion has a preliminary character. The Working Party intends to reconsider the subject, on the basis of a revised draft, at a later stage.
URL	Click Here

7.17 OPINION 8/2004

Title	Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America
Reference	Working Party document WP 97
Date	30.09.2004
Author	Directorate-General for Justice, Freedom and Security
Description	<p>In its Decision of 14 May 2004², the Commission considered the United States' Bureau of Customs and Border Protection (CBP) to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States.</p> <p>This Decision concerns the adequacy of protection provided by CBP with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC. It does not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States. One of them is the obligation by data controllers to inform data subjects about the main elements of the data processing. Therefore, data controllers carrying out processing of PNR data subject to national laws of EU Member States adopted pursuant to Directive 95/46/EC are obliged to provide passengers with complete and accurate information on the transfer of PNR data to CBP, in accordance with those national laws adopted pursuant to Articles 10 and 11 of the Directive.</p> <p>The Working Party has adopted the information notices included as Annex 1 and 2 to the present Opinion. They should serve as guidance as regards the information that should be provided to passengers on transatlantic flights, and should be used as broadly as possible by air carriers, travel agents and Computer Reservation Systems taking part in the booking process.</p>
URL	Click Here

7.18 OPINION 7/2004

Title	Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)
Reference	Working Party document WP 96
Date	11.08.2004
Author	Directorate-General for Justice, Freedom and Security
Description	<p>approach is needed in the EU on biometric identifiers or biometric data, which would result in harmonised solutions for documents for third country nationals, EU citizens' passports and information systems VIS and SIS II" and invited the Commission "to prepare the appropriate proposals, starting with visas". At the end of September 2003, the European Commission submitted a draft Council Regulation amending Regulations 1683/95 and 1030/2002 laying down a uniform format for visas and for residence permits for third country nationals respectively. On 18 February 2004, it also submitted a draft Regulation on standards for security features and biometrics in EU citizens' passports. The proposed amendment to the uniform formats for visas and residence permits essentially involves asking the Member States, on the one hand, to bring forward to 2005 the target date for the obligatory inclusion of a photograph in visa stickers and residence permits (originally scheduled for 2007 in the Regulations adopted in 2002) and, on the other, to include henceforth, as obligatory elements, two items of biometric data stored on a highly secure medium (contactless chip), i.e. a full-face digital photograph of the holder as the principal element for biometric identification together with two digital images of the holder's fingerprints taken with the fingers flat. According to the explanatory memorandum, the number of fingerprints could be increased on the basis of experience and the quality of the results obtained. The biometric data incorporated into visas and residence permits should be made interoperable and entered into the European information system on visas (VIS). Similarly, the digital fingerprints of the persons referred to in the Schengen Convention would be entered into the Schengen information system (SIS II). Both SIS II and VIS are currently being set up². The preparation of the European information system on visas (VIS) resulted in the adoption by the Council on 19 February 2004 of Conclusions providing general guidance that the Commission is invited to take into account when drawing up a proposal for the legal framework for the establishment and operation of this system. These Conclusions state that at a later stage, in coherence with the choice of biometrics in the field of visas and taking into account the outcome of the on-going technical developments, biometric data on visa applicants should be added to the VIS. Shortly afterwards, in its Declaration on Combating Terrorism of 25 March 2004, the European Council provided for optimisation of information systems as part of the strengthening of the existing cooperation between Member States. In particular, the Declaration states that "the Commission and the Council are urged to take forward work on the Visa Information System (VIS) in line with the conclusions adopted in February 2004", thus stressing the need for swift action. Answering this concern for speed, the Council recently adopted a decision establishing the Visa Information System (VIS) on 8 June 2004³, thus providing the legal base necessary to permit the engagement of the corresponding financial means. In addition, in the same Declaration of 25 March 2003, the European Council calls on the Commission to submit proposals for enhanced interoperability between European databases and to explore the creation of synergies between existing and future information systems (SIS II, VIS and EURODAC) in order to exploit their added value within their respective legal and technical frameworks in the prevention of and fight against terrorism. All initiatives in this field are likely to have a major impact on the fundamental rights of the persons concerned (that is to say, every foreign national who applies for a visa – in other words, tens of millions of people). When future decisions are taken on setting up and implementing these new European information systems, due account must be taken of the principles of data protection enshrined in Article 8 of the European Charter of Fundamental Rights and referred to in</p>

Directive 95/46/EC and national legislation. This document should, therefore, be understood merely as a preliminary opinion. It primarily concerns the proposals for regulations on uniform formats for visas and residence permits, for which the Working Party has been made formally responsible by the European Commission. The Working Party also comments on the points of principle raised by the Council's conclusions of 20 February 2004 on the establishment of an information system on visas (VIS), in the knowledge that the invitations to tender for this system are already under way. This global approach is in line with both the Commission's wishes and actual wording of Article 30 of Directive 95/46, which gives the Working Party general competence on proposed Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data. The Working Party stresses, in this respect, that it needs to be consulted before any proposals are drawn up in this area, since only if there is genuine transparency in the processes under way will it be able to perform the functions assigned to it by the Directive. Finally, the questions relating to the possible creation of a centralised database containing the biometric data collected from passport holders is outside the scope of the present document and will be dealt with separately. These questions will be examined by the Working Party in the near future.

URL

[Click Here](#)

7.19 OPINION 6/2004

Title	Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.
Reference	Working Party document WP 95
Date	22.06.2004
Author	Directorate-General for Justice, Freedom and Security
Description	<p>In its Decision of 14 May 2004², the Commission noted the adequate level of protection provided for personal data in the United States with regard to the processing of air passenger data to be made available by airlines to the American authorities in line with American regulations.</p> <p>The Commission has only partially taken into account the demands made by the Article 29 Working Party regarding, in particular, the scope of the data to be transferred, their retention period and the way in which they are used (Opinion 4/2003 of 13 June 2003, WP 78, Opinion 6/2002 of 24 October 2002, WP 66). The Article 29 Working Party notes that the European Parliament might call on the European Court of Justice to examine whether the rights of air passengers are violated by this Decision and the Agreement³, and whether the European Parliament's approval of the Agreement should have been sought in view of the restrictions the Agreement places on passengers' rights. Until these issues have been resolved, the Working Party considers the following practical measures to be essential to keep encroachments on passengers' rights as minimal as possible.</p>
URL	Click Here

7.20 SEVENTH REPORT THE YEARS 2002 AND 2003

Title	Seventh report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2002 and 2003
Reference	European Commission
Date	21.06.2004
Author	Directorate-General for Justice, Freedom and Security
Description	<p>This is the seventh report covering the years 2002 and 2003 of the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter 'the Working Party' or 'the Article 29 Working Party'. The Working Party is the independent European Union advisory body on data protection and privacy set up by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (data protection directive) and composed of the national supervisory authorities. The Working Party draws up an annual report which is intended to give an overview of the situation of the protection of individuals concerning the processing of personal data in the European Union and in third countries. The report is addressed to the Commission, the European Parliament and the Council, as well as to the public at large. In order to catch up with last year's backlog, the Working Party decided that the present report should exceptionally cover two years' developments, namely 2002 and 2003. The seventh report continues the tradition of the previous reports as far as its structure is concerned. It gives an overview of main developments in the European Union, both in the Member States and at Community level and presents the issues addressed by the Working Party. The report further provides information about the main developments in third countries. In 2002, the Working Party met five times and adopted 13 documents that were transmitted to the Commission and to the Article 31 Committee and, where appropriate, to the presidents of the Council, the European Parliament and others. In 2003, the Working Party met six times and adopted 14 documents that were transmitted to the Commission and to the Article 31 Committee and, where appropriate, to the presidents of the Council, the European Parliament and others.</p>
URL	Click Here

7.21 JOINT STATEMENT IN RESPONSE TO THE TERRORIST ATTACKS IN MADRID

Title	Joint Statement in response to the terrorist attacks in Madrid
Reference	Working Party document WP 93
Date	17.03.2004
Author	Directorate-General for Justice, Freedom and Security
Description	After the cruel terrorist attacks that struck Madrid, Spain's capital city on Thursday, 11 March, we, the members of the Group of European Personal Data Protection Authorities, meeting in Brussels on 17 March 2004, wish to convey to the victims of terrorism our deepest sorrow and our solidarity. We also wish, especially, to express our support for the Spanish people, who are so very much in our mind since the last Spring Conference held in Seville in April 2003, and our certainty that the unity and serenity they have shown will help them through this very sad and trying hour.
URL	Click Here

7.22 OPINION 4/2004

Title	Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance
Reference	Working Party document WP 89
Date	11.02.2004
Author	Directorate-General for Justice, Freedom and Security
Description	<p>Public and private bodies have been having increased recourse to image acquisition systems in Europe for the past few years. This circumstance has raised a lively debate both at Community level and in the individual Member States in order to identify prerequisites and limitations applying to the installation of equipment giving rise to video surveillance as well as the necessary safeguards for data subjects. The experience gathered in the latest years also following transposition at national level of Directive 95/46/EC showed the huge proliferation of closed circuit systems, cameras and other more sophisticated tools that are used in the most diverse sectors. Furthermore, the development of the available technology, digitalisation and miniaturisation considerably increase the opportunities provided by image and sound recording devices also in connection with their deployment on intranets and the Internet. In addition to the processing operations in the employment context, which have already been addressed by the Working Party in a detailed document (Opinion 8/2001 on the processing of personal data in the employment context²), the growing proliferation of video surveillance techniques can be easily appreciated by all citizens. There is also a growing trend towards interconnection of video surveillance systems.</p>
URL	Click Here

7.23 WORKING DOCUMENT ON BIOMETRICS

Title	Working document on biometrics
Reference	Working Party document WP 80
Date	01.08.2003
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The rapid progress of biometric technologies and their expanded application in recent years necessitates careful scrutiny from a data protection perspective². A wide and uncontrolled utilisation of biometrics raises concerns with regard to the protection of fundamental rights and freedoms of individuals. This kind of data is of a special nature, as it relates to the behavioural and physiological characteristics of an individual and may allow his or her unique identification³. Biometric data processing is now often used in automated authentication/verification and identification procedures, in particular for the control of entry to both physical and virtual areas (i.e. access to particular electronic systems or services). Previously, the use of biometrics was mainly confined to the areas of DNA and fingerprint testing. The collection of fingerprints was used in particular for law enforcement purposes (e.g. criminal investigation). If society encourages the development of fingerprint or other biometric databases for further routine applications, it may increase the potential re-use by third parties as an element of comparison and research in the framework of their own purposes, without such an objective having initially been sought; these third parties may include law enforcement authorities. A specific concern related to biometric data is that the public may become desensitised, through the widening of the use of such data, to the effect their processing may have on daily life. For example, the use of biometrics in school libraries can make children less aware of the data protection risks that may impact upon them in later life. The purpose of the present document is to contribute to the effective and homogenous application of the national provisions on data protection adopted in compliance with Directive 95/46/EC upon biometric systems. This paper will focus primarily on biometric applications for authentication and verification purposes. The Working Party intends to provide uniform European guidelines, particularly for the biometric systems industry and users of such technologies.</p>
URL	Click Here

7.24 LEVEL OF PROTECTION FOR THE TRANSFER OF PASSENGERS' DATA

Title	Level of Protection ensured in the United States for the Transfer of Passengers' Data
Reference	Working Party document WP 78
Date	13.06.2003
Author	Directorate-General for Justice, Freedom and Security
Description	<p>The Data Protection Authorities convened in the European Working Party in Brussels have set out the safeguards applying to the transfer of data concerning passengers of airline flights to the USA, requested by the US Authorities. The opinion sets out the concerns of the Working Party from a data protection perspective in assessing the level of protection ensured in the US with a view to a possible Commission Decision. The overall objective is to establish as quickly as possible a clear legal framework for any transfer of airline data to the US in a way which is compatible with data protection principles. While recognising that ultimately political judgements will be needed, the Working Party urges the Commission to take its views fully into account in its negotiations with the US authorities. The fight against terrorism is both a necessary and valuable element of democratic societies. Whilst combating terrorism, respect for fundamental rights and freedoms of the individuals including the right to privacy and data protection must be ensured. Such rights are protected in particular by Article 8 of the European Convention on Human Rights and Directive 95/46/EC, and are enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union. In the aftermath of the events of 11 September 2001, the United States adopted a number of laws and regulations requiring airlines flying into their territory to transfer to the US administration personal data relating to passengers and crew members flying to or from this country. The Working Party is of the opinion that, pursuant to the provisions made in Directive 95/46/EC, such personal data may only be transferred in the presence of adequate safeguards afforded by the US Authorities.</p>
URL	Click Here