



# Breaking Barriers to eGovernment

Solutions for eGovernment

# Solutions for eGovernment: How to Break the Barriers

## Improving Public Services and Democratic Engagement

The Internet and related electronic information and communication technologies (ICTs) are being used increasingly in Europe to enhance the delivery of public services and citizens' democratic engagements with government. However, many such 'eGovernment' innovations that could benefit all citizens have been hampered by legal, organizational and other obstacles. For example, substantial differences between EU Member States and regions can create barriers to pan-European ePublic Services.

This overview highlights key solutions to help avoid or overcome these blockages, such as creating a network of eGovernment champions and establishing a citizen's 'eRight' to access public services electronically. These recommendations are based on results from the European Commission's 'Barriers to eGovernment' project.

The first section of this Solutions brochure highlights the two main dimensions to the project's results:

- the seven major barrier categories identified by the project; and
- eight key legal areas analysed in detail.

The relative significance of the barriers to the legal issues are illustrated.

Solutions arising from the research are then presented, starting with suggestions for organizational approaches to address an important barrier within each of the seven barrier categories. Summaries are then provided of some key solutions to facilitate smoother eGovernment progress through legal adaptations at European, national, regional and local levels.

Full details of these solutions and the analyses on which they are based are provided in the project deliverables:

- Solutions for eGovernment (Deliverable 3);
- A Legal and Institutional analysis of Barriers to eGovernment (Deliverable 1b); and
- Breaking Barriers Case Study Report (Deliverable 2).

These are available on the project website: <http://www.egovbarriers.org/>

Further information about the project can be found on p.22

## The Seven Main eGovernment Barriers Identified by the Project Team

- **Leadership failures** result in slow and patchy progress to eGovernment.
- **Financial inhibitors** limit the flow of investment to eGovernment innovation.
- **Digital divides and choices** where inequalities lead to differences in motivations and competences that constrain and fragment eGovernment take-up.
- **Poor coordination** across jurisdictional, administrative and geographic boundaries holds back eGovernment networking benefits.
- **Workplace and organizational inflexibility** impair adaptability to new networked forms of information sharing and service provision.
- **Lack of trust** heightens fears about inadequate security and privacy safeguards in electronic networks.
- **Poor technical design** leads to difficult-to-use eGovernment services and/or incompatibilities between ICT systems.

## Key Legal Aspects of eGovernment Barriers

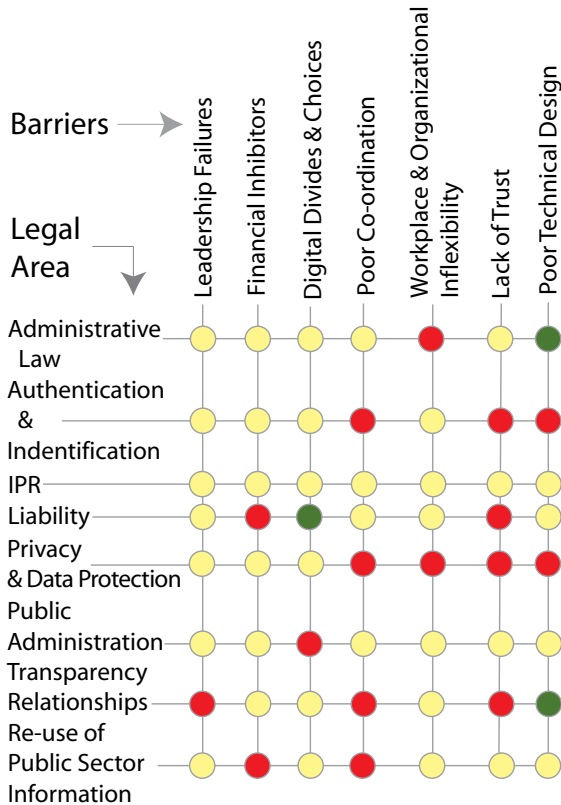
Laws and regulations can facilitate or block eGovernment progress. Such differences between jurisdictions is a particular concern in the EU. The project team analysed eight areas in which legal barriers may arise:

- **Administrative law** in many European countries that recognizes certain formal guarantees which can create legal ambiguities and obstacles for some eGovernment services.
- **Authentication and identification** procedures for online users can become barriers if they are too costly, cumbersome or unreliable.
- **Intellectual Property Rights (IPR)** and copyright laws protect creative works but can also impair flexibility and fairness in some eGovernment applications.
- **Liability** laws affecting new divisions of responsibility between government, businesses and citizens in online relationships can create anxieties and risks that impair eGovernment progress.
- **Privacy and data protection** rights can facilitate or block information sharing in eGovernment activities.
- **Public administration transparency**, such as Freedom of Information laws, can add costs to ePublic Services, as well as opening the possibility of greater access to government information.
- **Relationships between public administrations, citizens and other ICT actors** can be difficult to manage, for example in contractual arrangements between public administrations and ICT suppliers.
- **Re-use of public sector information** can raise complex legal issues when information from networked computer systems and databases are accessible from different jurisdictional and organizational contexts.

## Prioritizing Barriers and their Legal Dimensions

The 'traffic light' table below indicates the relative significance of the main legal dimensions to the seven barrier categories. For example, liability and re-use of public sector information are the most significant legal dimensions for financial barriers to eGovernment. More legal dimensions have crucial implications for the lack of trust barrier: authentication and identification; liability; privacy and data protection; and relationships between public administrations, citizens and other ICT actors.

All barriers have a number of 'significant' or 'very significant' legal dimensions. This suggests coordinated action from across the EU is necessary to help avoid blockages, or to minimize the impacts of those that do occur.



■ Very significant

■ Significant

■ Not significant

## Organizational solutions to barriers to eGovernment

In this section, we propose organisational solutions to some of the barriers to eGovernment. For each of the seven categories of barriers we nominate one key barrier – and identify a solution to that barrier.

Further details of all barrier categories and the specific organizational solutions summarized here can be found in A Legal and Institutional Analysis of Barriers to eGovernment (Deliverable 1b) and Solutions for eGovernment (Deliverable 3) on the project website: <http://www.egovbarriers.org/>

### Leadership failures

A key political and management leadership barrier is the frequent cycles of attention and inattention that lead to patchy, stop-go eGovernment progress. eGovernment needs champions, including political support from the top. These champions should be brought together in a network which extends throughout all tiers of government.

*Solution: Build a Network of eGovernment Champions*

- Create one or more Chief Information Officers (CIOs) in each government department, agency or other body, as has long been common in many private companies and the US federal government. This thread of eGovernment champions throughout public administrations should promote and underpin eGovernment initiatives.
- Establish effective communication between those championing specific eGovernment initiatives, including facilitating networking between formerly isolated IT specialists in different government units.
- Spotlight and motivate champions through prizes and other incentives to drive and deliver successful eGovernment developments.

**The European Commission** should issue guidance to Member States recommending the creation of CIOs in eGovernment developments at all levels. **All public bodies at all levels** should create and support CIO positions where appropriate.

### Financial inhibitors

Key financial blocks on the speed and scope of eGovernment developments include the complexities of calculating tangible long-term benefits to offset the clear - often apparently high - short-term costs of developing eGovernment systems.

*Solution: Calculate the Benefits as Well as All the Costs of eGovernment*

- Work out a comprehensive picture of the benefits and costs of eGovernment, including the risks and costs of not developing and innovating.
- Take account of gains to citizens and businesses of enhanced services as well as internal efficiency savings.
- Calculate the 'asset value' of websites and electronic services, taking account of the real public value of easily available, visible, accessible and navigable government information (e.g. considering income generated from the resource and what it would cost to run the organization's operations without the website).

**The Commission** should initiate research on methods of calculating the asset value of public sector websites in a manner that realistically balances actual costs and benefits. This should complement existing EC research into impact/benefit-oriented eGovernment measurement frameworks. **All public bodies at all levels** should design and implement their own asset value calculations.

### Digital divides and choices

Social and economic divides can lead to eGovernment resources being used in very different ways by different individuals, groups and organizations (or to choices by some not to use ePublic Services at all). Government at all levels must acknowledge there is no simple divide marked by the availability or not of access to the Internet, but rather a segmented citizenry with quite different eGovernment needs. These divides are demarcated by wealth, age, gender, disability, language, culture, geographical location, size of business and other factors.

#### *Solution: Stimulate Wide Take-up by Targeting eGovernment User Groups*

- Segment users of eGovernment services into specific groups and treat them in distinctive ways.
- Ensure eGovernment information and services have high visibility near the top of popular search engine results.
- Make available online as much government activity as possible for the most ardent, skilled Internet users.
- Persuade other users who do not yet see the benefits of going online to deal with government that ePublic Services can provide equivalent benefits to eCommerce or eBanking in the private sector.
- Provide multiple online and offline channels to suit the needs of different user segments, including assistance from appropriate intermediaries (e.g. NGOs dealing with specific groups, such as the elderly or disabled, or general telephone call centres).

**The Commission** should develop policies to support this kind of segmentation within its European Initiative on eInclusion, scheduled for 2008, to ensure that 'No citizen is left behind'. **All public bodies at all levels** should consider developing targeted ePublic Services, advertising campaigns and multi-channel support in all their eGovernment initiatives.

### Poor coordination

The Internet and associated ICTs have opened many efficient new pathways for communicating, coordinating and networking people, information, services and technologies across traditional boundaries. Government websites then become windows to public services from which users can be linked to a large range of information and services shared between different organizational units. However, variations in legal, regulatory and administrative regimes can be obstacles to emerging forms of networked eGovernment service delivery and ways of working that cross traditional government jurisdictions and departmental and other boundaries.

#### *Solution: Facilitate Access Across Fragmented Organizational Activities*

- Develop a strategy for 'government on the web' that matches citizens' online behaviour, particularly search patterns. Agencies should optimise sites for external search engines and commit sufficient resources to develop effective internal search engines.

- Ensure that government web sites, particularly portals, are easily navigable, optimising for key metrics such as path length and carrying out extensive usability testing.
- Ensure legal support is appropriate to assist the information sharing requirements for some coordinated services (e.g. see the sections on intellectual property rights, privacy & data protection, and the re-use of public sector information in the legal solutions below).

**The Commission** should support best practice research on how to optimize eGovernment ‘enterprise search’ strategies and tools. **All public bodies at all levels** should draw on best practice experience and expert advice to design, develop and implement effective coordinated access strategies and tools. **The Commission and Member States and regions** should ensure legal provisions do not unnecessarily constrain better coordinated and shared ePublic Services.

### Workplace and organizational inflexibility

Resistance to innovation by public administration management and staff can slow down, impair or prevent the necessary redesign of organizations and their processes required to deliver effective eGovernment. Government organizations must be agile enough to deal with the challenge of change tied to new electronic media, including potential resistance from managers and staff who have considerable organizational and personal learning invested in offline channels. Widespread use of the Internet and related ICTs has necessitated change at all levels of government, including in previous ‘technology free’ areas. An eLiterate workforce is vital to maximizing the benefits of eGovernment and to making public sector efficiency and effectiveness a reality.

#### *Solution: Encourage and Support an ‘eLiterate’ Workforce*

- Develop systematic programmes to manage organizational change, drawing on best practice advice and experience.
- Encourage staff and managers to incorporate technological innovation into all aspects of their work, including in appropriate contexts, the space to ‘play’ with Internet capabilities to overcome cultural resistance to eGovernment.
- Use the network of CIOs recommended above to promote training and professionalism in IT.

**The Commission** should issue guidance to help Member States for developing strategies to promote an eLiterate workforce (e.g. ensuring all staff and managers are appropriately trained and have access to up-to-date applications in an unrestricted way). **All public bodies at all levels** should be committed to building and supporting an eLiterate workforce.

### Lack of trust

A key concern specific to eGovernment is the ‘trust tension’ between the need to collect data on individuals to provide effective services and fears of data surveillance or other inappropriate uses of personal information once it is held in networked databases. Online take up can also be affected by general trends in perceptions of trust in government. The procedures employed to authenticate and identify online eGovernment users are key to defining the level of trust required to access a service. Where possible, users of eGovernment need to be provided with ‘low-trust’ options, where authentication requirements are minimised.

### *Solution: Tailor Trust Levels to the Specific eGovernment Service Offered*

- Consider high-level 'full strength' authentication and identification procedures only for the most sensitive public sector activities (e.g. obtaining a passport or driving licence).
- Wherever possible, seek to require low levels of authentication and identification, provided that is consistent with the needs of both government and users (e.g. for one-off requests for information or access to non-sensitive public data).
- Assess transactions for authentication requirements in a realistic way. It is usually unlikely, for example, that someone will fraudulently pay fines or taxes on someone else's behalf.
- Use state-of-the-art trust technological developments, allowing low levels of initial authentication but using smart systems to adjust in real-time to high risk situations, to provide the appropriate level of 'trust hurdle' for a given application.

**The Commission** should facilitate the sharing of experiences of initiatives to help minimize trust requirements across Europe. It should also promote research into the development and appropriate application of more advanced 'smart' authentication and identification systems. **All public bodies at all levels** should develop strategies and implement appropriate levels of authentication and identification procedures to access a particular ePublic Service.

### **Poor technical design**

eGovernment systems and services frequently fail or perform poorly because of their inadequate design and poor technical interoperability. Key blockages of this type occur because eGovernment technical design often lags behind business and societal innovation on the Internet.

### *Solution: Draw on User-generated Creativity in eGovernment Applications*

- Ensure eGovernment keeps pace with the technology and style being diffused throughout society by Internet innovations, as this is what citizens and business will increasingly take as the benchmark for a high quality online experience.
- Involve citizens and other 'customers' in eGovernment service and content design and production by offering, where appropriate, similar capabilities to recent 'Web 2.0' developments, such as:
  - » social networking (e.g. Facebook and MySpace): immediate online communication, interaction and sharing of activities and information with individuals, groups and much larger communities;
  - » user-generated content (e.g. Wikipedia, YouTube and user testimonial sites): user creation of information on services and dissemination of multimedia content across the Internet; and
  - » mashups: websites or applications combining content from multiple sources into an integrated experience.
- Government should put the same level of resource into the design of websites as private corporations.

**The European Commission** should support assessments of the extent to which wider trends in Internet use, such as Web 2.0, could and should be incorporated into eGovernment and how its current benchmarking activities can better reward and encourage such innovation. **All public bodies** at all levels should make systematic efforts to keep track of popular and leading-edge Internet usage into their own and wider areas, and seek new ways of incorporating the best and most suitable innovations in their own eGovernment services.

## Legal solutions to barriers to eGovernment

This section provides summaries of some of the legal solutions to barriers to eGovernment.

Further details of all legal areas and the specific legal solutions summarized here can be found in A Legal and Institutional Analysis of Barriers to eGovernment (Deliverable 1b) and Solutions for eGovernment (Deliverable 3) on the project website: <http://www.egovbarriers.org/>

### Administrative law

Administrative Law involves the attribution of significant powers to public bodies, together with the establishment of relevant formal guarantees (e.g. the respect of strict formal and procedural rules). The infringement of these guarantees may lead to an administrative action becoming invalid. This is different from regulation that rules the relationships between individuals, as shown in many Member States by the existence of strict liability systems that are not based in the existence of the notion of negligence. Administrative Law applies in most EU states, but not in such an intensive way in those countries (e.g. the UK) that are influenced by the legal Anglo-Saxon model of public administration, which is ruled mainly by common law. Potential barriers to eGovernment posed by the nature of Administrative Law can be overcome by adapting these rules to take account of the use of electronic media in public administrative activities, thereby helping to increase trust in eGovernment.

#### *Solution 1: Adapt Formalized Regulation of Public Administrations to Support Effective ePublic Services*

Introducing simpler and more flexible regulation relating to ICT-enabled public administration activities is of growing value because many public services and administrative activities can now be carried out more effectively and efficiently through electronic media.

**The European Commission** should stress the importance of this need in official information highlighting the opportunities opened by electronic media. Such adaptations should not imply a decrease in regulatory guarantees, but should be aimed only at accommodating electronic media. Otherwise, traditional administrative burdens would not be eased and both citizens and public bodies would not gain the full potential benefits of ICT capabilities, such as more appropriate ways for citizens to exercise their rights, higher effectiveness and improved cost savings.

**The Commission and Member States** should, for their own administrative services:

- draw up a complete catalogue of all the administrative procedures within the competence of the concerned public administration;
- analyse all existing formalities and documents required by citizens and businesses, with the aim of redesigning any aspect of these where changes are needed to meet the special characteristics of ICT-based ePublic Services;

- eliminate all formalities associated with the traditional approaches being phased out, and substitute them with the administrative documents required by citizens for their online data interchanges with public administrations;
- as a consequence, recognize a citizen's right not to have to present again those documents that are already held by a public administration; and
- introduce a legal requirement at national level for any decision about further development of eGovernment procedures to be preceded by actions that fulfill the above recommendations.

### *Solution 2: Revise General Regulations on ICTs to Meet the Specific Needs of eGovernment*

There is a particular need to undertake reviews at EU and Member State levels to clarify the obligations on public authorities in countries adopting Administrative Law, as public bodies in these countries are governed by different rules to those applicable to private relationships. This can lead to ambiguities about which rules must be applied in the public sphere and what happens if there is a contradiction between the implications for public and private contexts (e.g. in crucial areas like liability, and in relation to the hosting of ePublic Service by larger public authorities on behalf of smaller or less well-resourced public administrations).

**At a European level**, EU Directives related to ICT should, where possible, include a particular reference to the public sector that recommends and/or authorizes Member States to adapt those general rules to the particular requirements of public bodies if necessary.

**Member States** should take into account the singularities of the legal framework regulating the activity of public bodies when implementing Directives related to the use of ICT. This must be done by adapting the general rules to the principles and singularities of public administrations and their activities.

### **Authentication and Identification**

Authentication in an eGovernment context is typically an act of establishing or confirming someone or something as authentic, involving any process through which one proves and verifies certain related information. Identification is an act of establishing or confirming the identity of a person. Poor coordination in the development and application of relevant services and applications and a too low level of trust in eGovernment are the main barriers in this area.

### *Solution 1: Improve Coordination in Authentication and Identification Activities*

Closer cooperation between Member States in the management and authentication of electronic records and archives in public administrations is a key step in enabling greater eGovernment interoperability within the EU. A key role in this is being played by the development of eSignature services and applications.

**EU-wide solutions** should aim to improve such coordination, particularly for cross border uses, recommendations include:

- Keep additional requirements (see Article 3.7 of Directive 1999/93) by the public sector for receiving eSignatures to a minimum.
- Promote interoperability and the cross border use of eSignatures by obliging Member States to notify the European Committee for Standardization (CEN) about national standardization initiatives with regard to eSignatures.

- Prescribe by legislation that eSignatures that are used in the public sector should comply with a certain standard. This can be a national standard, with the CEN controlling the adequate level of standardization of Member States' national standardization initiatives. The CEN could also take the initiative to develop a European standard for eSignatures in the public sector, based on the national initiatives. The EU could also require Member States to cooperate in this respect.
- Require Member States to mutually recognize the eSignature standards developed in other Member States, when these are approved by the CEN. This legislative change could be achieved by amending the eSignatures Directive 1999/93/EC.
- Ensure other EU legislative initiatives, such as the Procurement Directives and the Invoice Directive, increase the cross border use of eSignatures.

### *Solution 2: Build Better Trust in eGovernment*

Many factors affecting general trust in government are also relevant to trust in eGovernment. For authentication and identification in eGovernment, privacy-related aspects are crucial, although other dimensions are also significant, such as uncertainty about the functioning of the technology and about the service providers and people engaged in using the Internet to deliver a government service. Legislative strategies for eGovernment should address the strengthening of trust in eGovernment by seeking to make progress in a number of key areas.

**At European, Member State and local levels** this requires focused efforts to:

- manage more effectively the 'trust tension' between the citizen's concern about privacy, security and identity and their obligation to provide personal information to receive eGovernment services;
- establish agreements, guidelines and frameworks to enhance trust;
- enable citizens to gain experience with the use of Internet and, thereby, learn to trust it;
- use Privacy Enhancing Technologies (PETs) to boost trust;
- design, build, run and evolve sustainable ICT systems;
- oblige government agencies to conduct Privacy Impact Assessments (PIAs) for new electronic information systems and information collections that involve the use of personally identifiable information.
- ensure appropriate privacy practices are implemented and the public informed of their nature (e.g. through the posting on a Website of a 'Privacy Notice' describing the practices in operation).

### **Intellectual Property Rights (IPR)**

Both the information disseminated and the supporting ICTs employed in eGovernment are subject to intellectual property rights (IPR), such as copyright, trademark rights or patents. If the public body involved in eGovernment initiatives is not the 'rightsholder' who owns the IPR, licences must be arranged to enable the relevant information and ICTs to be used appropriately. The legal framework governing IPR must therefore establish a balance between the requirements of the rightsholder, the user and the government body wishing to provide an ePublic Service. Addressing potential cost and trust obstacles are crucial to creating this balance.

### *Solution 1: Address the Potentially High Costs of Access to IPR Protected Material*

Concerns about the costs to users of eGovernment services involving IPR-protected material must be addressed in a balanced manner that gives fair compensation to rightsholders, without unnecessarily inhibiting ePublic Service innovation. This could be assisted by greater harmonization of IPR law, particularly regarding uses of third-party works vital to eGovernment services.

**At a European level**, harmonization should be encouraged through provisions such as:

- Make it compulsory (rather than optional as at present) for all Member States to introduce into their copyright law the exceptions to the exclusive rights of the copyright holder specified in Article 5(3e) of Directive 2001/29/EC on the harmonization of copyright. The exception which is of most significance to eGovernment serves inter alia to “ensure the proper performance ... of administrative, parliamentary or judicial proceedings”. This exception ensures that materials can be used for eGovernment purposes, but it does not take away the requirement that rightsholders must receive a fair compensation for the use of their works. Presently, this exception is not available or is severely restricted in some Member States, and subject to varying qualifications in others.
- The same mandatory solution can be considered for rights in databases. which could be based on Directive 96/9/EC on the legal protection of databases, depending on the outcome of a current review of the future of this Directive.

### *Solution 2: Build Trust in Open Source Software as an Alternative to Proprietary Products*

eGovernment dependence on ‘proprietary software’ can become a burden if it makes modifications difficult and costly because the rightsholder retains the ‘source code’ needed to make adaptations. ‘Open source’ software that delivers the source code for use in any modifications can avoid such obstacles. However, this approach also has risks (e.g. legal challenges from proprietary competitors that could eventually disrupt eGovernment services using the open source software).

**The EU and Member States** should encourage their public administrations to consider the following when choosing eGovernment software, bearing in mind these measures can reduce to an acceptable level – but not eliminate – the risk of ‘foreign’ code entering open source software:

- Government bodies using open source software developed by someone else should, where possible, negotiate an indemnification from the provider guaranteeing the software does not infringe rights of third parties. The government body should at least ensure the provider has taken measures to prevent third-party software from entering the open source program code. For instance, Article 6 of the European Union Public Licence contains an indemnification provision. However, vigilance is required because many forms of open source licence exist, and one project may be using different licence types.

- A government body using open source software it has developed in-house should:
  - » clearly instruct all programmers what kinds of code can, and cannot, be entered into open source code;
  - » where necessary, ensure rights in the code written by its employees are transferred or, at least, licensed to the government body (this is an issue only if an employment contract explicitly assigns the rights to the employee – see Article 2(3) of Directive 91/250/EC on the legal protection of computer programs); and
  - » adopt a procedure for quickly dealing with notifications that infringing code is present in the open source program.

## Liability

When eGovernment activities give rise to damages, the victims (citizens, businesses and governments) may want to recoup their loss by holding the wrongdoer liable (e.g. a government agency or ICT service or equipment supplier). If victims are not to lose their trust in eGovernment, this must be possible; at the same time, the law must not make it too easy to hold the wrongdoer liable. Trust and costs are again major eGovernment barriers to address in achieving this balance.

### *Solution 1: Ensure Liability Does Not Undermine Trust in eGovernment*

Trust in eGovernment can be undermined if some stakeholders feel any costs of liability damages are unfairly distributed. European-level intervention is needed to achieve an appropriate balance (e.g. to overcome disparities in existing laws between Member States and because eGovernment activity increasingly encompasses more than one State).

**Member States, supported by Commission recommendations,** encourage key eGovernment stakeholders to establish an appropriate structure for taking the following actions:

- Design eGovernment infrastructures and services in such a way that the risk of damages is reduced as much as is economically feasible.
- Perform an analysis of the remaining risks.
- Where possible, warn concerned stakeholders of the risks.
- Build a complaint-handling mechanism that allows for dealing with incidents in an efficient way and has a low threshold of entry, with complaint handling carried out in-house by the stakeholder allegedly liable for the damage.
- Design a structured process for dealing with certain standard incidents that cannot be prevented in an economically feasible way, with an easy and uniform procedure for reporting on such incidents.
- Open up the option of Alternative Dispute Resolution (ADR), such as mediation, for cases in which the complaint-handling mechanism fails to reach a satisfactory resolution and the incident becomes a dispute.
- Make available an Online Dispute Resolution (ODR) form of ADR in situations where the relevant parties can gain from not having to convene physically.

### *Solution 2: Overcome Fears and Realities Relating to Liability Costs*

The real and perceived potentially significant costs of liability damages can have a chilling effect on new eGovernment activities. The liability problems encountered at all EU and Member State are similar, particularly as local or national services gain a pan-European dimension.

**Member States, supported by Commission recommendations**, should encourage those involved in eGovernment to put structures in place to realize the following aims:

- Design eGovernment infrastructures and services in such a way that the risk of damages is reduced as much as is economically feasible.
- Give accurate information about what the service or infrastructure can, and cannot, be used for. This would avoid costly discussions about the ways that the services or infrastructures can be used and address the limitations of liability disclaimers because of differences in related laws between Member States.
- Before engaging in an eGovernment service, representatives of relevant stakeholders should discuss and agree upon the specific liability rules that govern their mutual relations. This means agreement is needed on more specific rules than are available in statutes or case law, in order to tailor the rules to the specific eGovernment activities at hand. The rules should be laid down in framework contracts that are made public.

### **Privacy and data protection**

Privacy and data protection are fundamental concerns for most eGovernment services. The rules protecting personal data could therefore have a wide impact if they are principally applied to prevent or constrain some activities. However, by protecting individuals' data protection rights they could support the development of eGovernment applications by facilitating the free flow of personal data. This support can be reinforced by overcoming barriers in the disparities in implementing the Data Protection Directive 95/46/EC and by implementing appropriate tools for privacy protection.

### *Solution 1: Overcome Disparities in Implementations of the Data Protection Directive*

Lack of coordination is one of the most potentially significant blockages in this legal area as there still remain substantive disparities between Member States in implementations of the Data Protection Directive (95/46/EC). The following actions would promote more effective harmonization.

- **The European Commission** should pursue actions to enhance the effective application of the Directive by taking cases of Member States' non-compliance to the European Court of Justice (see its Communication of March 2007 on the follow-up of the Work Programme for a better implementation of the Directive).
- **The Article 29 Data Protection Working Party** should update its Working Document on eGovernment and clarify specific relevant new issues related to data protection (e.g. RFID, PINs, etc). This should help to develop specific harmonized 'European common guidelines', to which all National Supervisory Authority (NSA) representatives should refer to assist governments implement their national eGovernment plans.

■ **At Member State level** the appointment of Data Protection Officials should become compulsory within each relevant public administration, as provided by Article 18(2) of Directive 95/46/EC. This will improve awareness of related matters within the public bodies and establish clear ‘interlocutors’ for eGovernment users. Member States should also develop national legal frameworks that give their NSAs effective independence and powers to monitor data protection practices within that State, as provided by Directive 95/46/EC.

■ **All stakeholders, at all levels**, should contribute to enhancing the awareness of citizens and enterprises about their data protection rights and duties, by promoting awareness-raising policies with a strong educational element. NSAs should receive greater financial support in encouraging such wider awareness.

### *Solution 2: Assess the Value of Tools Used for Privacy Protection*

eGovernment techniques affecting privacy protection need to be implemented in ways that respect both citizens’ data protection needs and administrative efficiency requirements. These include Personal Identification Numbers (PINs) and Privacy Enhancing Technologies (PETs), such as the automatic anonymization of data after a certain lapse of time and the application of encryption tools for data encoding to prevent unwarranted access to personal information.

**All stakeholders** should develop a common understanding of the benefits and risks of for citizens, administrators, data controllers and others in using such techniques. For example, because PINs could increase the power of public administrations by easing access to personal information in distinct files, a common understanding of their benefits and risks could avoid blockages caused by differing interpretations of the Data Protection Directive. This delegates to Member States the power to determine conditions for using such identifiers. **At a European level**, a minimal start towards this, given national sensitivities in this area, would be to compile related Working Papers and Opinions of the Article 29 Working Party into a ‘European Guide’ on this issue.

### **Public Administration Transparency**

Freedom of Information (FOI) Acts are the prime legal vehicle for promoting public administration transparency. These include two main types of transparency provisions: ‘passive’ (information requested by a citizen) and ‘active’ (information spontaneously made available by government). A greater deployment of active transparency policies can boost the trust of citizens and business in eGovernment. And better coordination within the EU can lead to more effective implementations of this approach.

### *Solution 1: Promote a Favourable View Towards Active Transparency*

**At a European level**, encouragement should be given to a trend among Member States to introduce more ‘active transparency’ policies, which involve a positive acceptance by public authorities of their responsibility for making information publicly available, including through electronic media. Serious divergences between Member States on this requirement can be addressed effectively by developing a ‘European model’ of an FOI Act. This could assist moves towards more effective coordination of policies by the development of a greater consensus regarding active transparency at pan-European and local Member State levels.

Although the European Commission has no competence to legislate or otherwise act in the field of transparency – as competency lies primarily with Member States – informal harmonization outside a European legal framework is possible. This can be achieved by building on the Commission's current European Transparency Initiative and other major achievements in this field, such as the 'access to documents' legislation in Regulation (EC) No 1049/2001.

An important first step in a broad 'Transparency in the Public Sector Initiative' would be to create more opportunities to share information on active transparency experiments among Member States. This would help States to learn from each others' experience, including those who have already launched active transparency initiatives. The sharing of this information could inspire Member States to establish effective transparency policies, leading to the development of more common conceptions of how to address related issues.

### *Solution 2: Address the Lack of General FOI Legislation at the European Level*

EU Member States have traditionally had prime responsibility for transparency issues. There has therefore been a lack of FOI general legislation at the European level, with exceptions in special areas like information on the environment and public procurement. This means that creating a general Directive on public administration transparency would not be a feasible solution within European law.

**The European Commission** could, instead, open a promising way of achieving better coordination across Europe by undertaking a detailed study at the European level on the state-of-the-art of 'FOI cultures' across Member States. This could assist the Commission to define initial guidelines towards a common approach to FOI legislation. The study could also help to realize a degree of further harmonization between national laws of Member States, including on passive transparency and other relevant issues (e.g. national disparities in costs of obtaining information; access to electronic formats; and lack of 'meta-data' overview guides).

**The Commission, together with Member States**, should also base the measures they undertake on this study. For instance, we recommend the establishment of a Working Party to monitor existing active transparency FOI laws in order to evaluate their effectiveness. Relevant training programmes and other initiatives should also support the competences and cultural and organizational enhancements needed to ensure the successful formulation and implementation of FOI laws and the development of a strong FOI culture.

### **Relationships between public administrations, citizens and other ICT actors**

One of the main conditions for the success of any initiative related to eGovernment is the guarantee of effective communication between all parties concerned. For ICT use to give effective support in enhancing the crucial relationship between government and its citizens, eGovernment policies and actions must have a deeply-rooted citizen focus. This requires legal solutions that remove perceived and actual barriers to gaining appropriate access to the range of online services that they could use to enhance their lives.

### *Solution 1: Establish an eRight For Citizens to Use Electronic Media to Access Public Services*

To help overcome any obstacles remaining at the national level to providing Pan-European services, enhancements are required to existing EU-level freedoms and rights, particularly free movement and the right of establishment.

**At the European level**, a new Directive related to these rights and freedoms should be considered by all stakeholders. This should follow the model of Directive 2006/123/EC on services in the Internal Market, including provisions such as:

- Accessibility of public services by electronic means. Member States should have a clear and direct obligation to ensure any EU citizen can complete electronically, and at a distance, all procedures and formalities concerning access to relevant ePublic Services.
- Simplification of procedures. Member States must examine their procedures and formalities for accessing ePublic Service activities and make appropriate simplifications where appropriate.
- Right to information. Identify key information required about all providers of information established in a Member State, including: contact details of the competent authorities and other relevant bodies; methods and conditions for accessing public registers and databases; and the means of redress available in the event of dispute.
- Harmonization of administrative documents. Enable the Commission to approve harmonized forms that will be considered equivalent to any document required, while requiring a Member State to accept from another State any document serving an equivalent purpose to a certificate or other document needed to prove that a requirement has been satisfied.
- Better coordination among Member States. Encourage improved coordination, particularly in facilitating ICT-enabled exchanges of data to obtain information, including the use of digital certificates. These processes must fully respect data protection requirements.

### *Solution 2: Support Multi-channel Approaches to Delivering and Accessing Public Services*

In order to ensure no citizen is left behind in moves towards eGovernment, despite the existence of digital divides affecting a wide range of groups in the EU, the availability of both electronic and traditional channels for gaining access to public services should be guaranteed. However, there is no EU-wide competence for strong harmonization in this field.

**Member States** therefore have ultimate responsibility to ensure there is the widest inclusivity in eGovernment. Nevertheless, **the Commission** should still be able to develop ways of advising Member States to take account of eGovernment in adapting their legal frameworks governing citizens' relationships with public administrations. This should include legal provisions such as the:

- requirement to offer appropriate multi-channel online and offline public service choices to groups with a range of social and economic difficulties, which should include emphasis on the potentially valuable role of intermediaries and representatives who can assist citizens gain access to ePublic Services;
- need to widen the range of public service channels through strong compliance with the obligations for public administrations to include technical specifications in contract documentation as specified in Directive 2004/17/EC (Article 34 and Annexe XXI) and Directive 2004/18/EC (Article 23 and Annexe VI), such as to include citizens with disabilities; and

- involvement of a wide range of relevant stakeholders in developing ePublic Services, including: social intermediaries; private sector actors; NGOs; and civil servants and other public service agencies.

## Re-use of public sector information

Many eGovernment services depend on the re-use of Public Sector Information (PSI). Directive 2003/98/EC defines this as the use of documents held by public sector bodies for commercial or non-commercial purposes other than for the initial purpose related to the public task for which the documents were produced. However, this 'PSI Directive' does not eliminate all obstacles to the desirable re-use of PSI and the establishment of a pan-European public information market. Two key barriers that remain are the disparities in charges for re-use between Member States and the failure to establish re-use as an obligatory principle.

### *Solution 1: Remove Disparities Between Member States in Charges for PSI Re-use*

According to the PSI Directive, the total income from supplying and allowing document re-use "shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment" (Article 6). However, it also asks Member States to encourage government bodies to make documents available at charges that "do not exceed the marginal costs for their reproduction and dissemination" (Recital 14). This is also the solution adopted recently by the European Commission in its Decision of 7 April 2006 on the re-use of Commission information (Article 7).

**At a European level**, the PSI Directive should be revised to give clear guidance on this issue, as some national laws based on PSI Directive have led to a rapid increase in costs of access for the private sector in crucial fields like meteorological data (e.g. in Finland), which could constitute a misuse of public sector power. Such a revision should support greater PSI re-use across the EU by:

- pursuing the pan-European discussion with all stakeholders through the ePSIplus network to clarify the means and conditions of establishing whatever costs are to be charged, in particular in defining what is meant by a "reasonable return on investment";
- taking account of differences in costs between commercial and non-commercial re-use to avoid discriminations and unfair competition between private and public sectors; and
- implementing at Member State level a transparent policy regarding PSI re-use to respect the PSI Directive's provisions regarding especially: the availability of formats, transparency, and non-discrimination and fair trading.

### *Solution 2: Establish Re-use as an Obligatory Principle*

The PSI Directive leaves to Member States and their public bodies the determination of whether or not to allow the re-use of PSI.

**At a European level**, it is opportune to review how far, if at all, the positions of Member States have evolved towards a point at which the PSI Directive could be amended to make re-use a fundamental obligatory principle for all Member States. This could include relevant restrictions or exceptions to protect national interests, such as the economic viability of a particular public service.

**At Member State level**, this can be achieved by:

- ePSIplus network recommendations on the need for pro-active action to be taken by Member State lead public bodies to assist the public sector as a whole to implement and comply with the PSI framework in a cost effective manner (this network supports the better implementation of the PSI Directive until its review in 2008).
- The creation of an independent national authority for PSI in each Member State (e.g. OPSI in the UK), whose actions could be coordinated at the pan-European level by the PSI Expert Group by reinforcing its role and competences in this field. This should help to: overcome the lack of trust of re-users; increase awareness and the exchange of good practices among public bodies on the new commercial opportunities made possible by PSI re-use; and provide clear guidance to national PSI holders (e.g. in areas such as IPR, data protection and technical barriers).

## The Breaking Barriers to eGovernment Project

This three-year Modinis study, which started in January 2005, has identified and analysed barriers to successful eGovernment within the EU. Its results, summarized in this brochure, offer organizational and legal solutions to overcome these obstacles.

The project team reached these conclusions after undertaking in-depth case studies, an online survey and reviews of other work in this field. It also engaged closely with many leading experts, practitioners and other eGovernment stakeholders.

### The Study Team

- Oxford Internet Institute (OII), University of Oxford, which is the base of the Project Management Team (<http://www.oii.ox.ac.uk>)
- Centre de Recherches Informatique et Droit (CRID), University of Namur, Belgium (<http://www.fundp.ac.be/facultes/droit/recherche/centres/crid/>)
- Gov 3 Ltd, an eGovernment Consultancy (<http://www.gov3.net>)
- Tilburg Institute for Law, Technology, and Society (TILT), University of Tilburg, Netherlands (<http://www.uvt.nl/tilt>)
- Department of Administrative Law, University of Murcia, Spain (<http://www.um.es/dereadm>)

### Find out more

Visit the project website ([www.egovbarriers.org](http://www.egovbarriers.org)) for comprehensive information about the project's work and outputs. Click on the "Project Outputs" tab on the home page for detailed reports on the barrier categories, legal areas and solutions proposed. You can also send us your feedback online.

All deliverables are also available on epractice.eu: <http://www.epractice.eu/library>

*The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission. Reproduction is authorized, provided the source (eGovernment Unit, DG Information Society, European Commission) is clearly acknowledged, save where otherwise stated.*

