

# Security and data protection measures in the context of 'Once-only' and reuse of existing data approaches



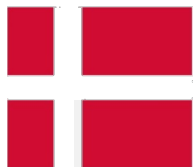
LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG  
Centre des technologies de l'information de l'Etat



# The 'Once-only' principle

*The 'Once-only' principle states that citizens and businesses should have the right to supply certain standard information only once to public administrations on the basis that this information will be shared internally and appropriately by public administrations thus eliminating any additional administrative burden.*

## Examples



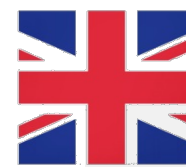
### Denmark

- **Basic Data programme:**  
Making basic information (of citizens and businesses) freely accessible for everyone and for all public authorities (i.e. for commercial as well as non-commercial purposes), by means of 9 connected registers.
- **Mandatory digital self-service:**  
Enforcing by law the digital implementation of a certain number of transactions



### Netherlands

- **The system of 13 base registries:**  
Collection and sharing of citizens and businesses core data across all government authorities, through 13 registers gathering data of persons, businesses, cars, land administrations, maps, income, buildings.



### UK

- **Tell Us Once:**  
Information sharing on births and deaths across government departments, so that citizens are required to provide this information only once to public authorities.
- **The Digital Government Strategy:**  
Overall programme of change impacting multiple departments across the Civil Service to realise efficiencies through the adoption of digital procedures by default.

- Context & background
- Objectives
- Methodology
- Key findings
- Case studies
- Conclusions
- Wrap up from EUPAN HRWG/IPSG
- Appendix

**18.11.2009**

**Malmö Ministerial Declaration on eGovernment**

*"How public administrations can reduce the frequency with which citizens and businesses have to resubmit information to appropriate authorities"*

**24 – 25.10.2013**

**Council Conclusions**

*"EU legislation should be designed to facilitate digital interaction between citizens, businesses and the public authorities. Efforts should be made to apply the principle that information is collected from citizens only once, in due respect of data protection rules"*

**Study on eGovernment and the Reduction of Administrative Burden (EC-2014)**

2009 2010 2011 2012 2013 2014 2015

**15.12.2010**

**eGovernment Action Plan 2011 – 2015**

*"Reduction of administrative burdens: applying the principle of 'Once-only' registration of data for citizens."*

**06.05.2015**

**Digital Single Market Strategy**

*"The Commission will present a new e-Government Action Plan 2016-2020 which will include (i) making the interconnection of business registers a reality by 2017, (ii) launching an initiative in 2016 with the Member States to pilot the 'Once-only' principle"*

*"70% of the countries analysed in this study were implementing projects or programmes related to the 'Once-only' principle"*

1

To provide an overview on the **implementation of the 'Once-only' principle (OOP)** across European countries, with a particular **focus on security and data protection measures**.

2

To **identify best practices** in the area of technology, legislation and organisation regarding security and data protection.

3

To **draw key conclusions** for Member States.



## Desk Research

- In-depth **analysis of studies** produced by the Commission (e.g. Study on eGovernment and the reduction of administrative burden).



## On-line Survey

- To collect **views on the main challenges** related to security policies and data protection as well as on **specific measures and best practices** from EU Member States and other European countries.
- Of a total of 33 countries invited to respond to the survey, we received 27 answers from the following 25 countries (21 EU Member States) : AT, BE, BG, CH, CY, CZ, EE, EL, ES, HR, HU, IE, IS, IT, LV, LU, MT, NL, NO, PT, RO, SI, SK, TR, UK.



## Case studies

- Case studies on Luxembourg, Austria and Estonia.
- In-depth analysis on MyGuichet for Luxembourg and data from Austria and Estonia related to specific case studies identified through the online survey.

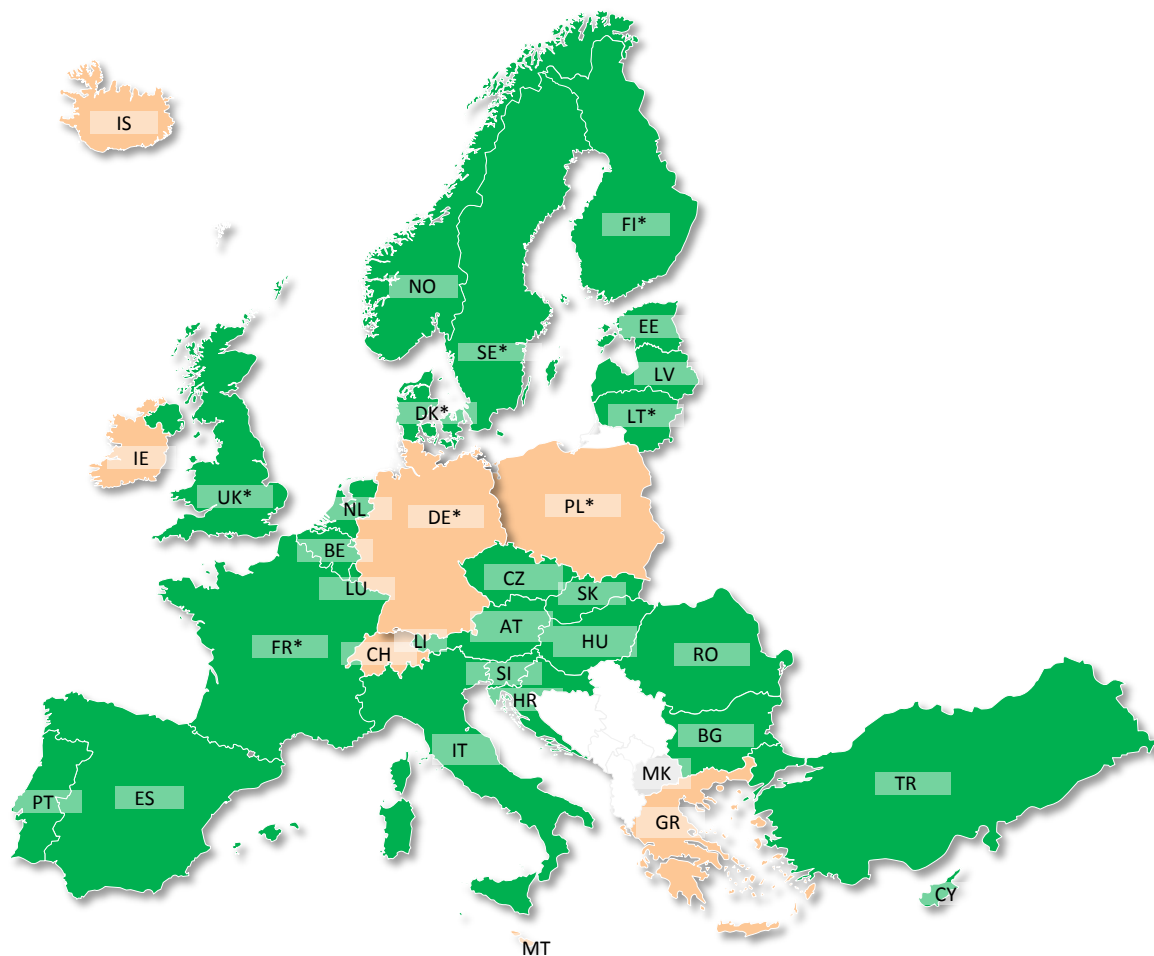


# Key findings

## Has your country started to implement the OOP?

Out of a total of 33 European countries,  
**25** countries have started to implement  
OOP at **national level**.

Among those countries, **7** have started  
to implement this principle at both  
**regional and local levels**.



\* Secondary data source (Study on Administrative burden reduction (EC 2014))

■ Implementing OOP   ■ Not implementing OOP   ■ No data available







# Key findings

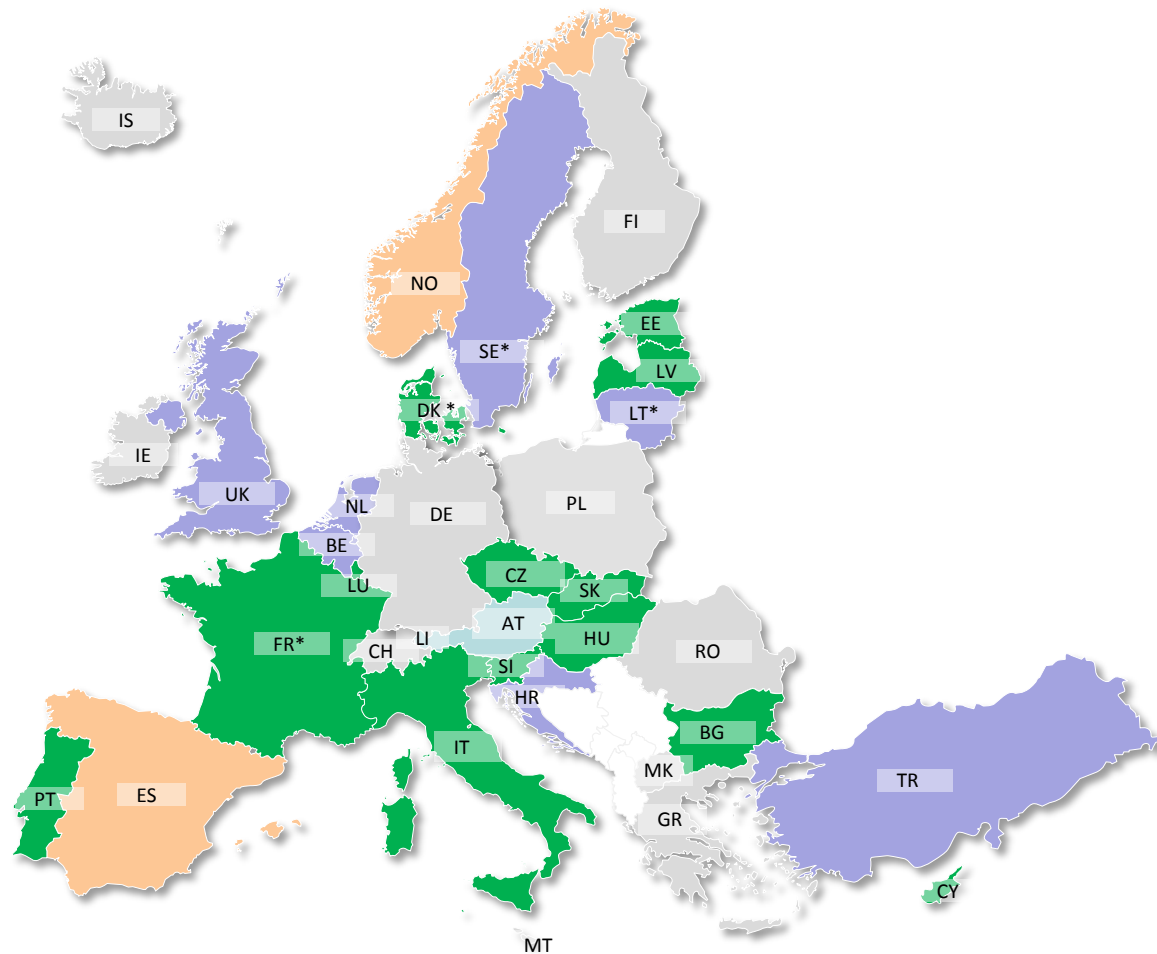
## Is there a strategy/initiatives aimed to implement the 'Once-only' principle in your country?





Out of a total of 25 European countries:

- 13 have both a strategy & initiatives in place;
- 2 have only a strategy in place;
- 7 have only initiatives in place; and
- 3 did not provide any data.

A few examples of initiatives:

-  MyGuichet
-  X-Road
-  'Basic Data' programme
-  'Tell us once' programme



-  Both a strategy & initiative(s) exist
-  Only a strategy exists
-  Only initiative(s) exist(s)
-  No data available

\* Secondary data source (Study on Administrative burden reduction (EC 2014))





Sources: Online questionnaire (KURT SALMON 2015), n=33  
Study on Administrative burden reduction (EC 2014)

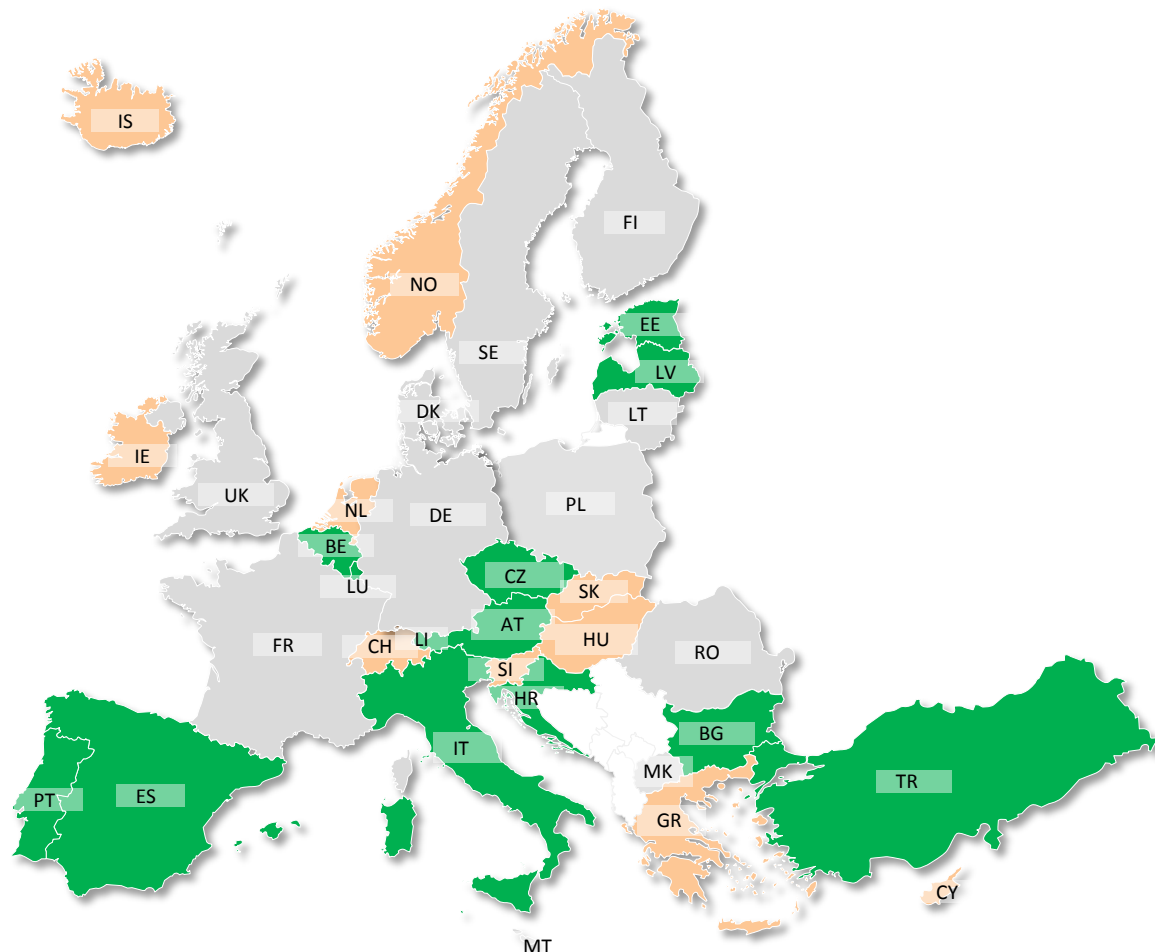





## Is there a legislation supporting the implementation of the OOP in your country?

Out of a total of 25 European countries,  
13 have legislation in place supporting the  
implementation of the 'Once-only' principle.



















A few examples of legislation:

-  The Act of 5 May 2014 on the establishment of the principle of the unique data collection
-  The Decree-Law 73/2014
-  Law of State Information Systems of 2002
-  e-Government act of 1 March 2004



 A piece of legislation exists  No specific legislation  No data available

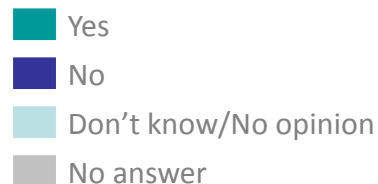
## What types of data are supplied only once by citizens and/or businesses?

Country	Personal data related to citizens	Identification data related to businesses	Geographic data	Fiscal/Financial data	Health data	Other
 Austria	✓	✓	✓	✓	✓	✓
 Latvia	✓	✓	✓	✓	✓	✓
 Estonia	✓	✓	✓	✓	✓	
 Netherlands	✓	✓	✓	✓		✓
 Luxembourg	✓	✓		✓		
 Romania	✓	✓		✓	✓	
 Spain	✓		✓	✓		✓
 Croatia	✓	✓	✓			
 Cyprus	✓	✓	✓			
 Belgium	✓	✓			✓	
 Sweden	✓		✓			✓
 Bulgaria	✓	✓				
 Slovakia	✓	✓				
 Slovenia	✓	✓				
 Turkey	✓				✓	
 Czech Republic		✓	✓			
 Portugal	✓					
 Italy						✓
<b>Total</b>	<b>16</b>	<b>13</b>	<b>9</b>	<b>7</b>	<b>6</b>	<b>6</b>

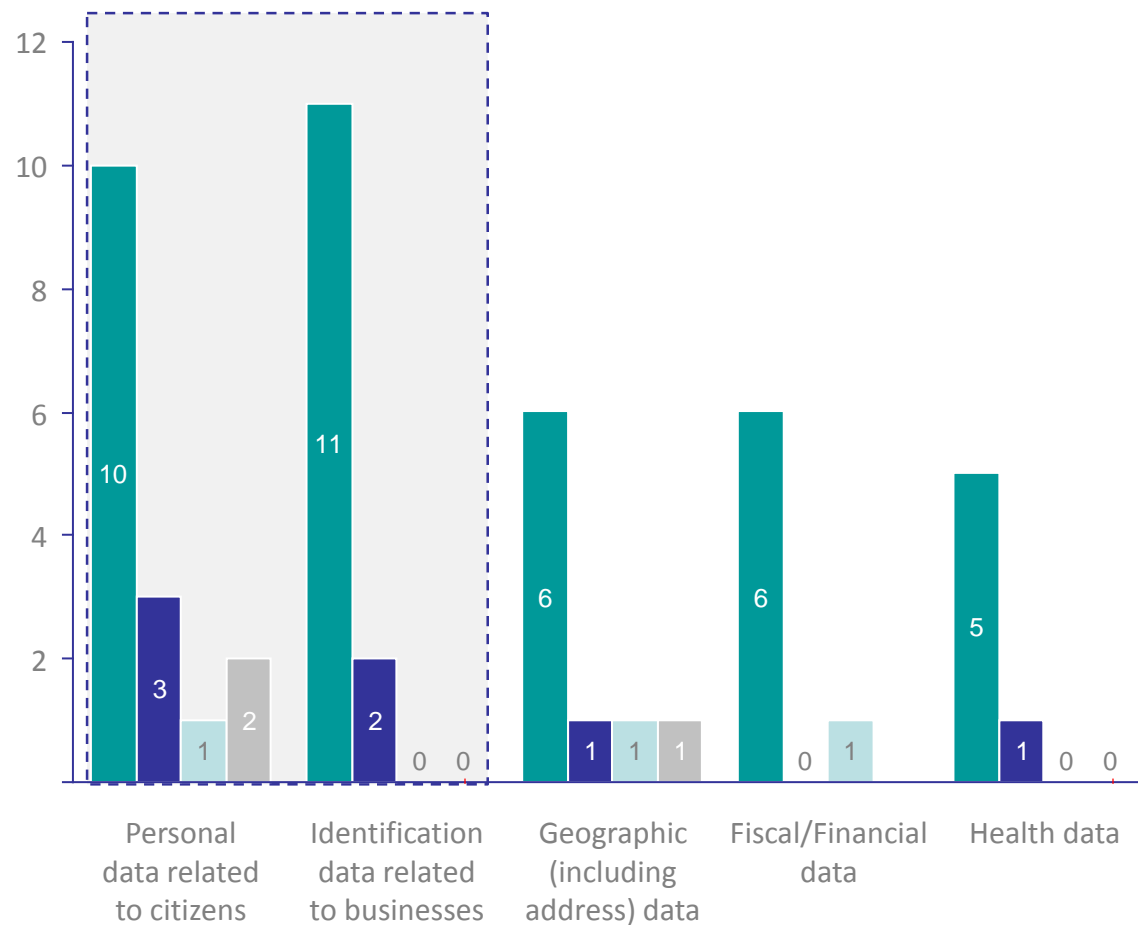
As part of 'other', data related to vehicles were cited by two different countries as data supplied only once by citizens and/or businesses.

## Is there, in your country, a law establishing authentic sources?

For each type of aforementioned data, the establishment of related authentic sources is widely supported by a specific law.



Number of answers

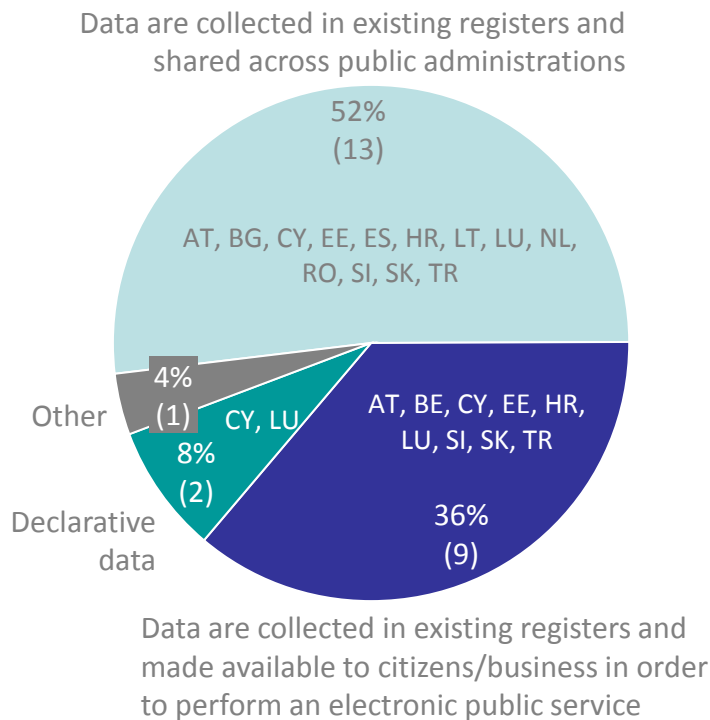


### Note:

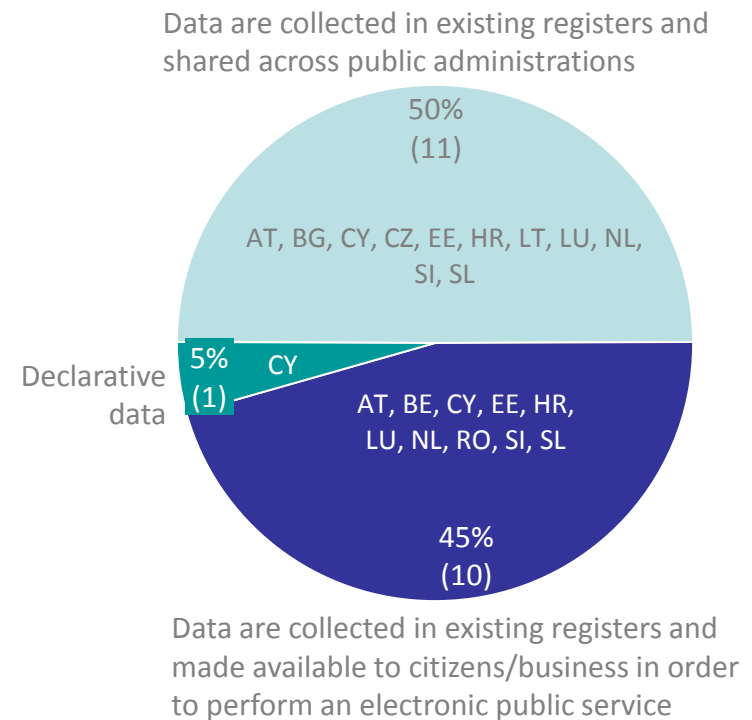
An authentic source is a high quality database, accompanied by explicit guarantees ensuring for its quality assurance and that contains essential and/or frequently-used data pertaining to persons, institutions, issues, activities or occurrences.

## How are data related to citizen/businesses provided?

### Personal data related to citizens



### Identification data related to businesses



Personal data related to citizens and identification data related to businesses are primarily collected in existing registers and shared across public administrations but also, to a minor extent, made available to citizens /businesses in order to perform an electronic public service.

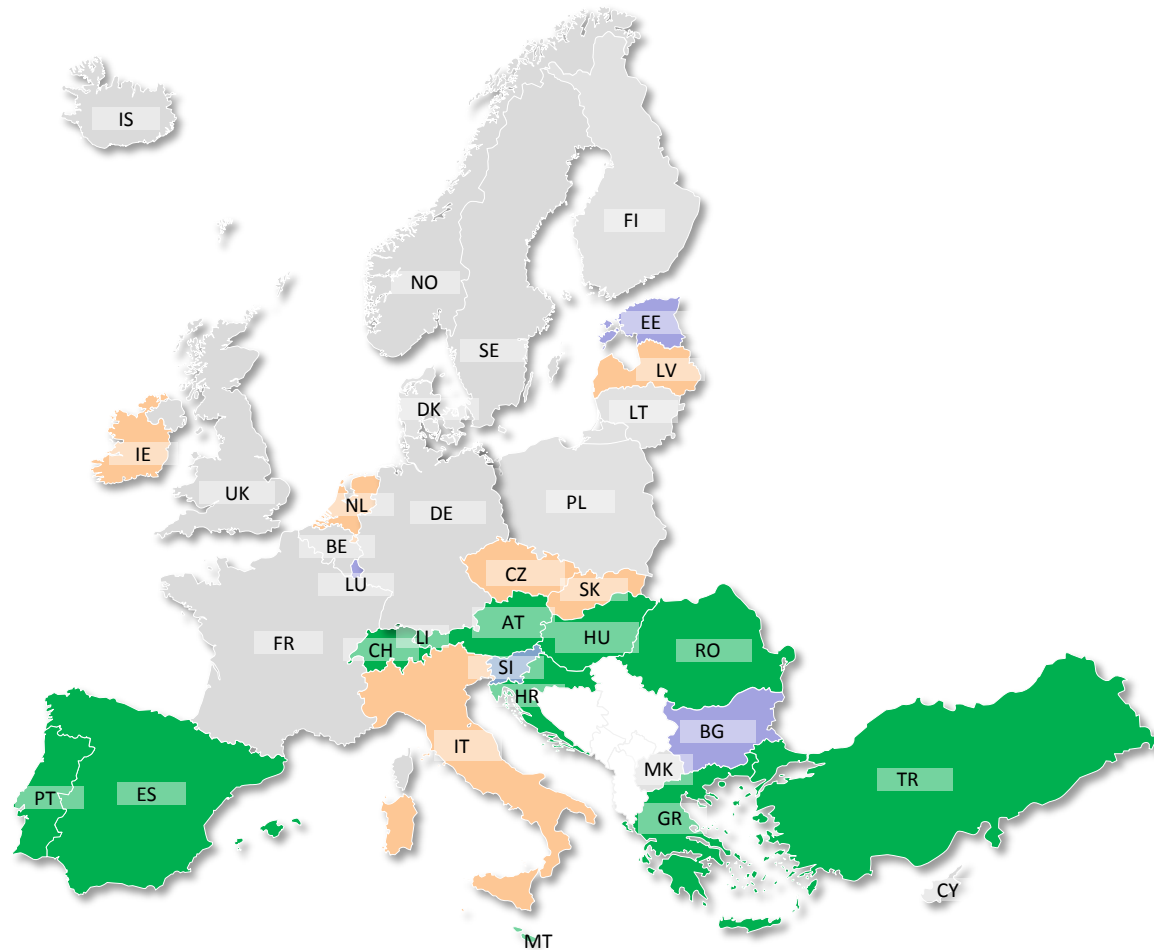
### Note:

‘Declarative data’ refers to the data provided by the citizens/businesses themselves, for example in a personal space, in order to be reused afterwards for other electronic public services.

## How does your country concretely implement the consent of 'data subject'?

Out of a total of 25 European countries, **10** countries apply the principle that **explicit consent has to be given by the 'data subjects'** before their related data can be processed, whereas this processing is **set by default by law in 6 other countries**.

Depending on the concerned data, 3 additional EU countries require the explicit consent of 'data subjects' if the processing of those data is not imposed by law.



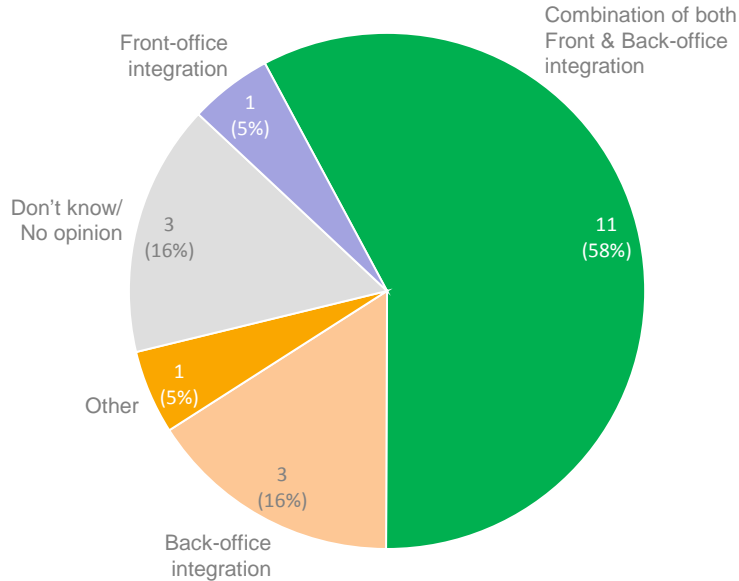
Source: Online questionnaire (KURT SALMON 2015), n=25

What are the main barriers that your country aims to overcome in order to ensure the implementation of the OOP? What are the measures taken to overcome these barriers?

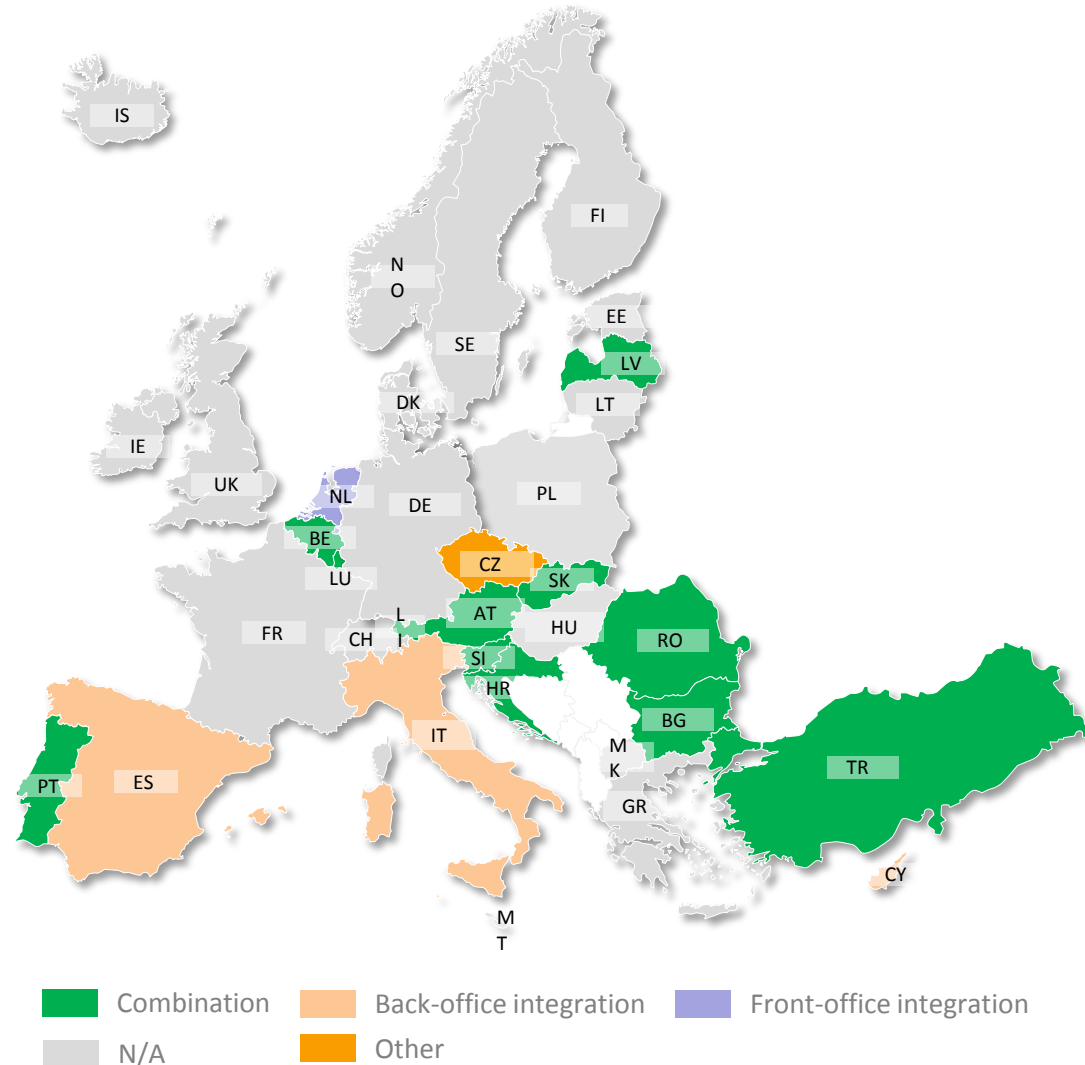
	Organisational barriers (21)	Semantic barriers (16)	Legal barriers (13)	Technical barriers (9)
Main barriers encountered	<ul style="list-style-type: none"> <li>› Lack of resources</li> <li>› Lack of willingness to share data with other administrations</li> <li>› Lack of harmonisation of different processes</li> </ul>	<ul style="list-style-type: none"> <li>› Inconsistencies in data elements definition</li> <li>› Different data models</li> </ul>	<ul style="list-style-type: none"> <li>› Specific provisions related to the processing of personal data</li> </ul>	<ul style="list-style-type: none"> <li>› Legacy systems</li> </ul>
Measures proposed	<ul style="list-style-type: none"> <li>› Identification of information ownership</li> <li>› Common strategy coordinated by one entity</li> </ul>	<ul style="list-style-type: none"> <li>› Establishment and promotion of common vocabularies</li> </ul>	<ul style="list-style-type: none"> <li>› No measures mentioned</li> </ul>	<ul style="list-style-type: none"> <li>› No measures mentioned</li> </ul>

Other barriers mentioned: implementation cost related to the implementation of the OOP and lack of budget.

## What approach is currently used by your country to implement the OOP?



A combination of both Front and Back-office integration is used by a vast majority of countries to implement the OOP. In fact, this approach facilitates the different applications and related processes used to implement the OOP.



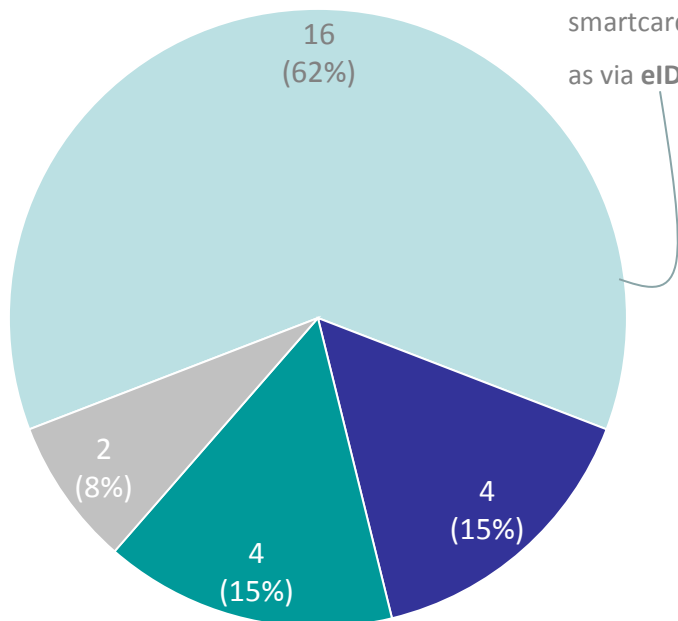


# Key findings

## What security measures are applied in order to ensure authentication and authorisation?

### Authentication

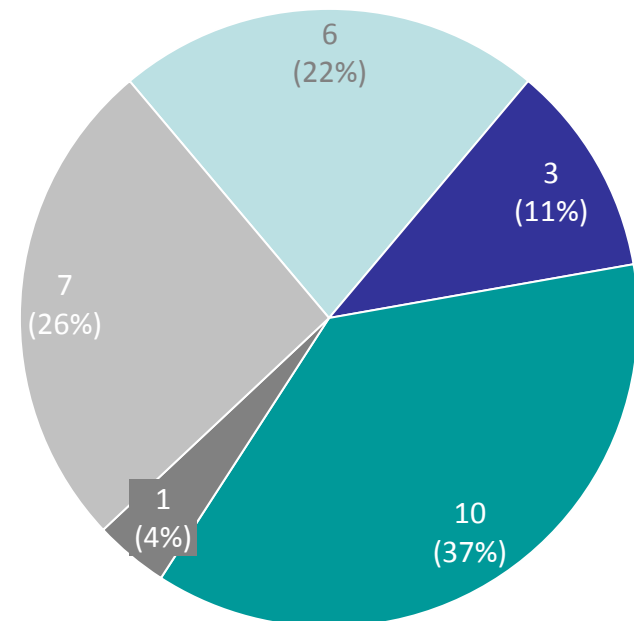
Strong authentication via  
different means (via tokens,  
smartcards, SMS, etc.) as well  
as via eID card.



Strong authentication Username/password Other measures No answer

Three countries (PT, IE, IT) use a two-factor authentication depending on the system used and the type of data held.

### Authorisation



RBAC ABAC Other measures Access Control Lists No answer

Other measures depend on the application and system used, and the type of data held.  
One country (LU) is using both RBAC and ACL.

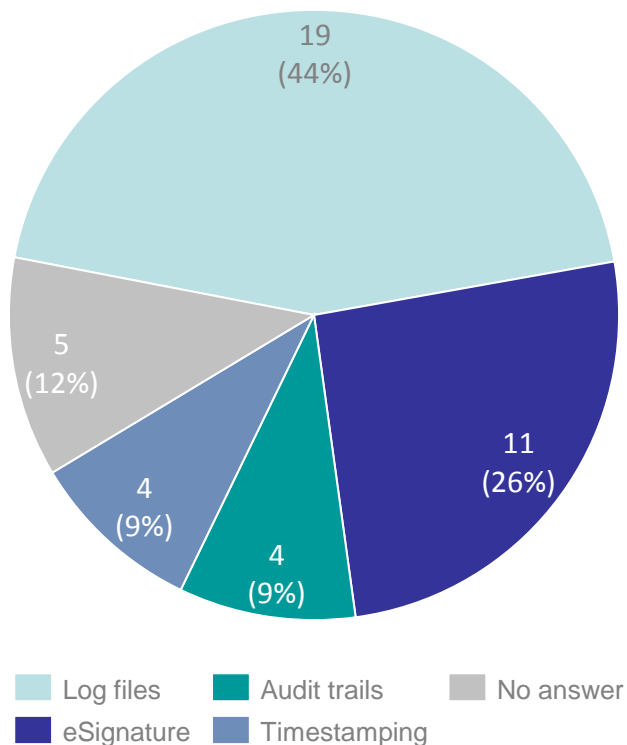




# Key findings

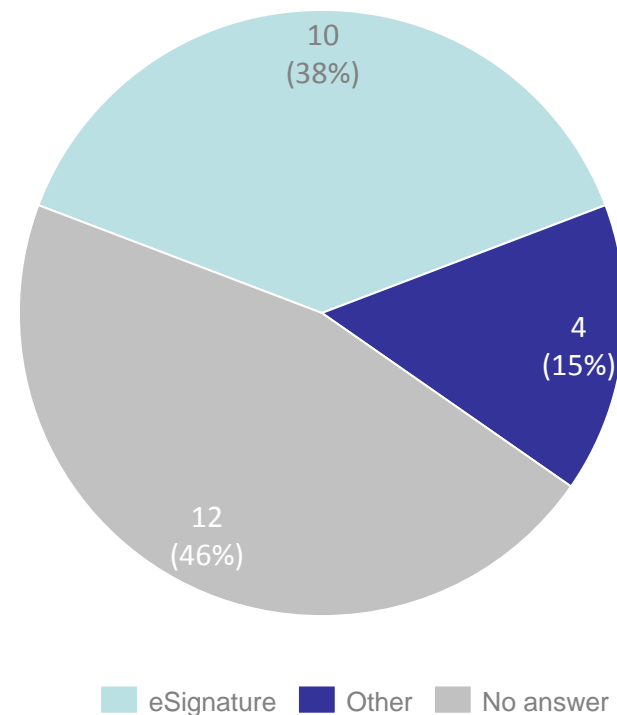
## What security measures are applied in order to ensure traceability, non-repudiation and integrity?

### Traceability & Non-repudiation



10 countries use a combination of these different measures in order to ensure traceability and non-repudiation.

### Integrity



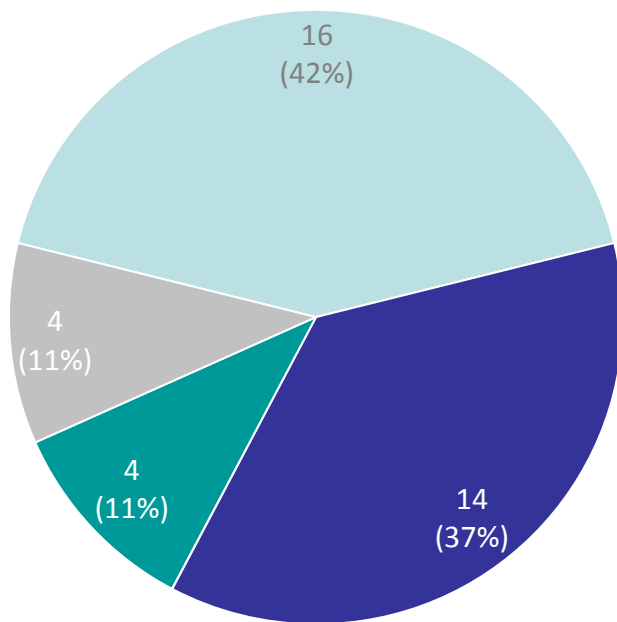
10 countries use eSignature in order to ensure data integrity (71% of the countries having replied to this question).



# Key findings

What security measures are applied when accessing data (confidentiality measures) and transmitting data from the location where they are stored to a public administration?

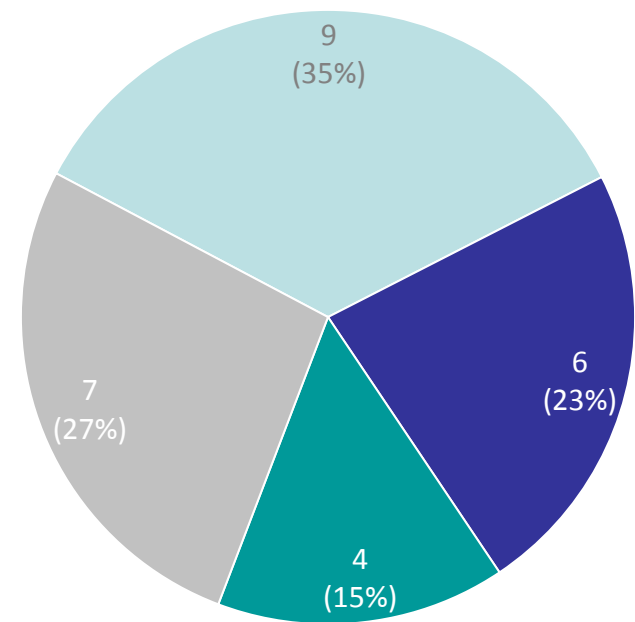
## Confidentiality



Encrypted data Restricted access to data Confidentiality agreements No answer

10 countries currently use a combination of these different measures in order to ensure confidentiality of data.

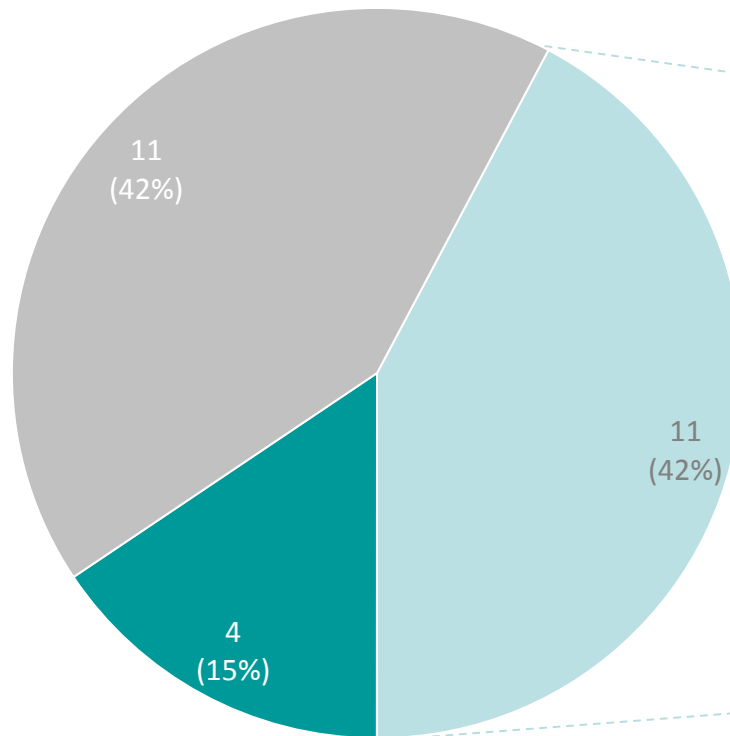
## Data transmission



Secure dedicated network Secured communication protocol (e.g. HTTPS) Other No answer

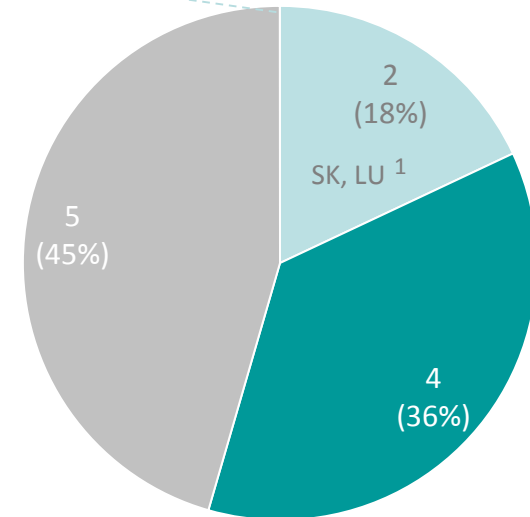
A secure dedicated network is widely used when transmitting data from the location where they are stored to a public administration. (47% of the countries having replied to this question).

Does your country implement an encryption system in order to protect user's personal data?



Yes No Don't know/ No opinion

Does this implementation provide the possibility to access users' data using a Key Escrow system?



Yes No Don't know/ No opinion

The use of Key Escrow System is not imposed by any legal basis (for the 11 countries having implemented a Key Escrow System in order to protect user's personal data).

<sup>1</sup> An encryption system is only used on MyGuichet.



# Case study N°1: Luxembourg

## ➤ Context on the 'Once-only' principle in Luxembourg

**02.08.2002:**

Act relating to the protection of individuals in relation to the processing of personal data

**19.12.2002:**

Law on the Register of companies

**19.06.2013:**

Law on the Register of physical persons

Art. 4. (2) prescribed that **authentic data already contained in the register of physical persons have to be reused** by public administrations and that these **administrations cannot ask the citizen to produce once more pieces to prove the exactitude of the data already existing in the register.**

...

2013

2014

2015

**2008**

Roll out of Guichet.lu (citizens)

**2011**

Roll out of Guichet.lu (businesses)

**04.02.2013:**

Roll out MyGuichet (v3)

**06.12.2013:**

Adoption of the new Government programme

**03-04.06.2014:**

Adoption of "Digital Lëtzebuerg"

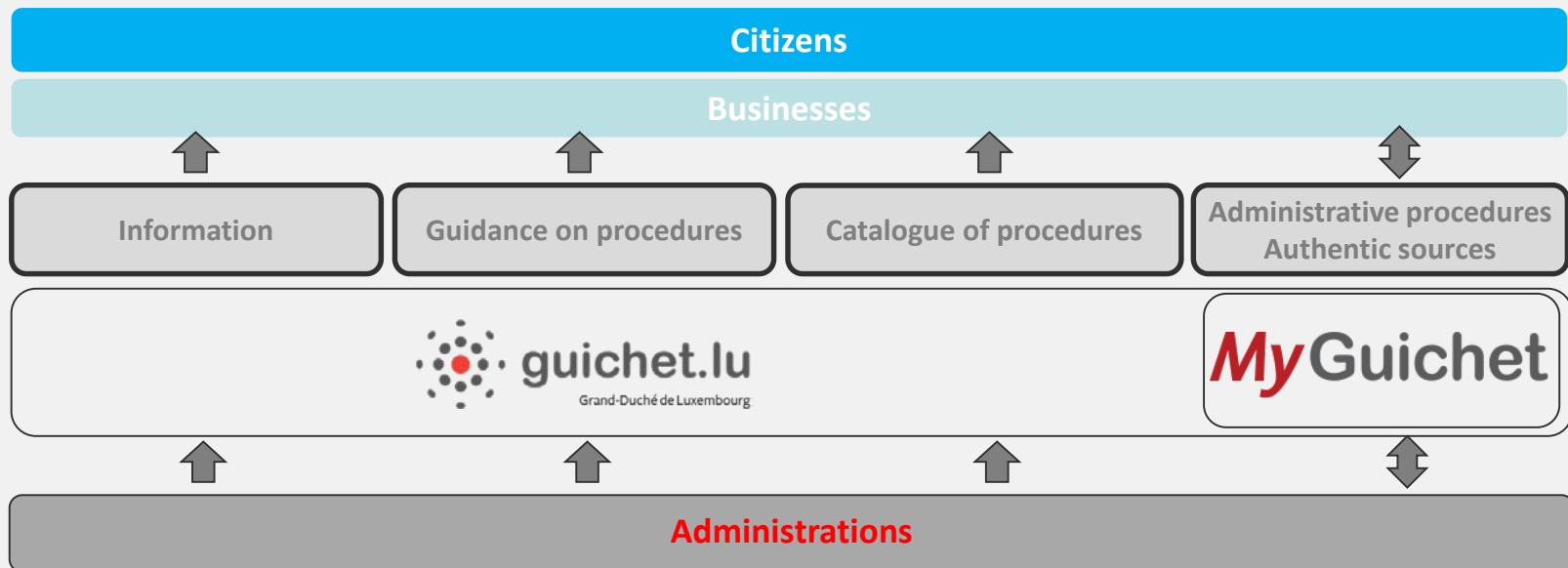
**24.07.2015:**

Adoption of five principles aimed at accelerating state modernisation and the digitisation of administrative procedures (including the OOP)

1. Digital by default; 2. **Once-Only principle**; 3. Transparency; 4. Improved electronic payment methods; 5. « **MyGuichet** » as the main channel of interactions with public administrations

## ➤ The 'Once-only' principle into action: **MyGuichet**

- **Single Point of Contact (SPOC)** for nearly all administrative procedures in Luxembourg.
- Main building block and backbone for the **implementation of the 'Once-only principle'** for administrative procedure.
- The solutions offered by MyGuichet will be systematically extended to **more and more online services** in the coming years.



## What type of data are supplied only once by citizens and/or businesses?

### Data supplied only once by citizens and/or businesses

#### Personal data related to citizens

Data are collected in one central register for personal data related to physical persons and shared across public administrations (e.g. national registry)

Data are collected in existing registers and made available to citizens to perform an electronic public service (e.g. national registry)

Declarative data (e.g. descriptive data, bank account, fiscal data)

#### Identification data related to businesses

Data are collected in the company register and the eVAT register and shared across public administrations

Data are collected in the company register and the eVAT register and made available to citizens/business to perform an electronic public service (e.g. VAT balance sheet, tax credit, business permit applications)

Declarative data (e.g. NACE code)

#### Fiscal/Financial data

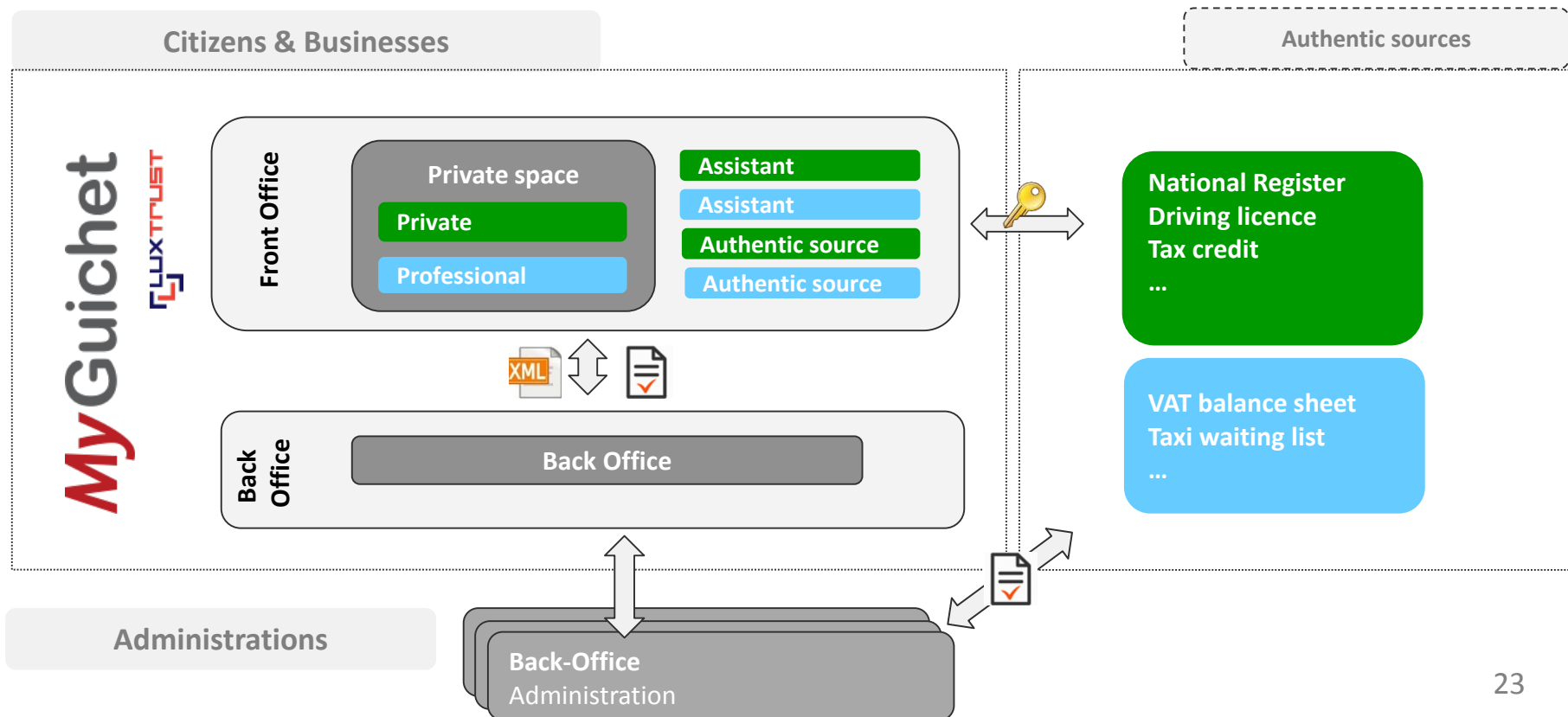
Data are collected in existing registers and shared across public administrations

Declarative data



## What approach is currently used by your country to implement the OOP?

- **Combination of both front- and back-office approaches:** (i) Integration in front-office applications of citizens and businesses data provided by authentic sources or by declarative data in order to pre-fill forms. (ii) Integration of citizens and businesses data in back-office applications after consent of the data subject.
- APIs for more and more databases or registers containing authentic sources will be implemented.





## What security measures are applied on MyGuichet?

### Authentication

#### Strong authentication

- › Electronic ID card (using LuxTrust certificates)
- › LuxTrust solutions (Smartcard, Signing stick, Token)

### Confidentiality

- › Restricted access to data
- › Sensitive personal data encrypted (e.g. the SSL protocol).

### Integrity

- › eSignature

**MyGuichet**

### Authorisation (access control)

- › ACLs (Access Control Lists)
- › RBAC (Role-based access control)

### Traceability & Non-repudiation

- › eSignature
- › Log files
- › Time stamping added before the document transmission



## ➤ Context on the 'Once-only' principle in Austria

**03.2001:**

Roll-out of HELP.gv.at; an interface  
between authorities and citizens

*The portal was awarded in Berlin the BIENE 2006 in Gold  
for the best barrier-free German language information portal.*

**01.03.2004:**

Adoption of Austria's E-Government Act:  
Federal Act on Provisions Facilitating Electronic  
Communications with Public Bodies

**12.2013:**

Adoption of the Working programme  
of the Austrian Federal Government  
for 2013 - 2018

...

2010

2013

2015

**01.01.2010:**

Roll-out of USP.gv.at;  
the one-stop-shop  
Business Service Portal

**05.2014:**

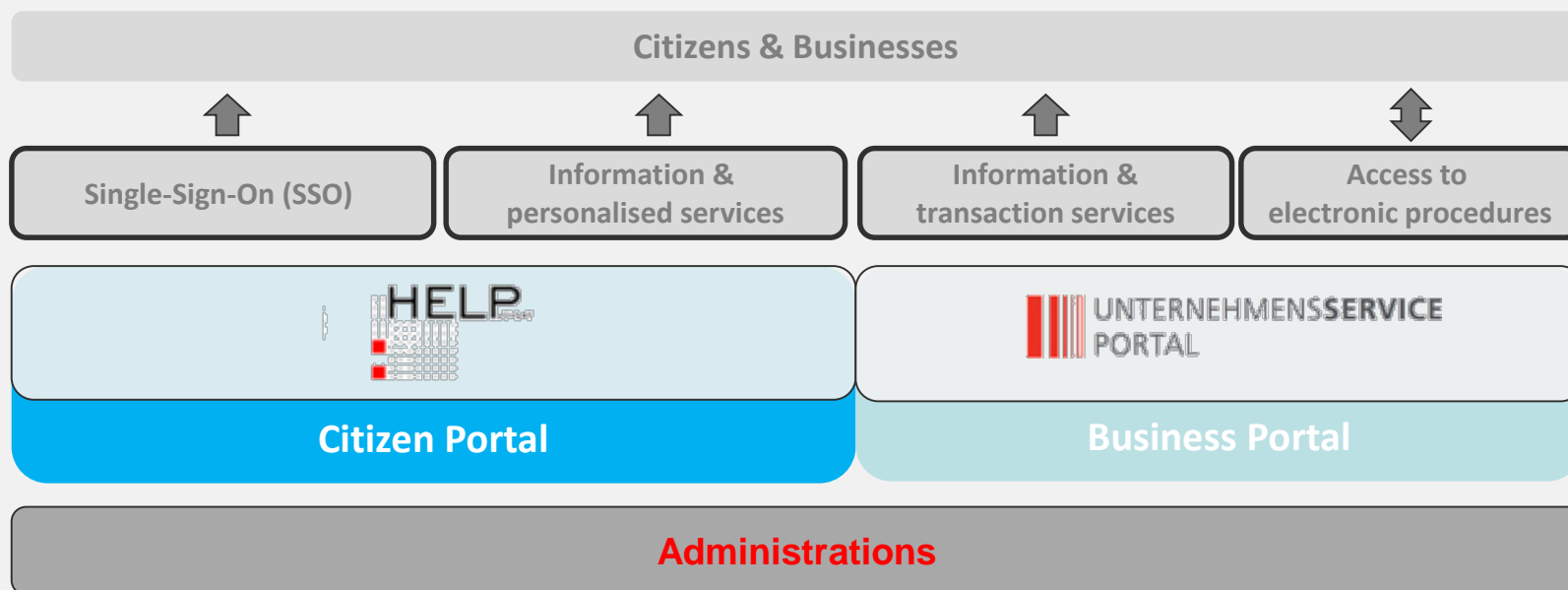
Adoption of eGovernment  
strategy; see  
"Administration on the Net  
– The ABC guide of  
eGovernment in Austria"

*Main pillars of the Austrian implementation of the 'once only' principle:*

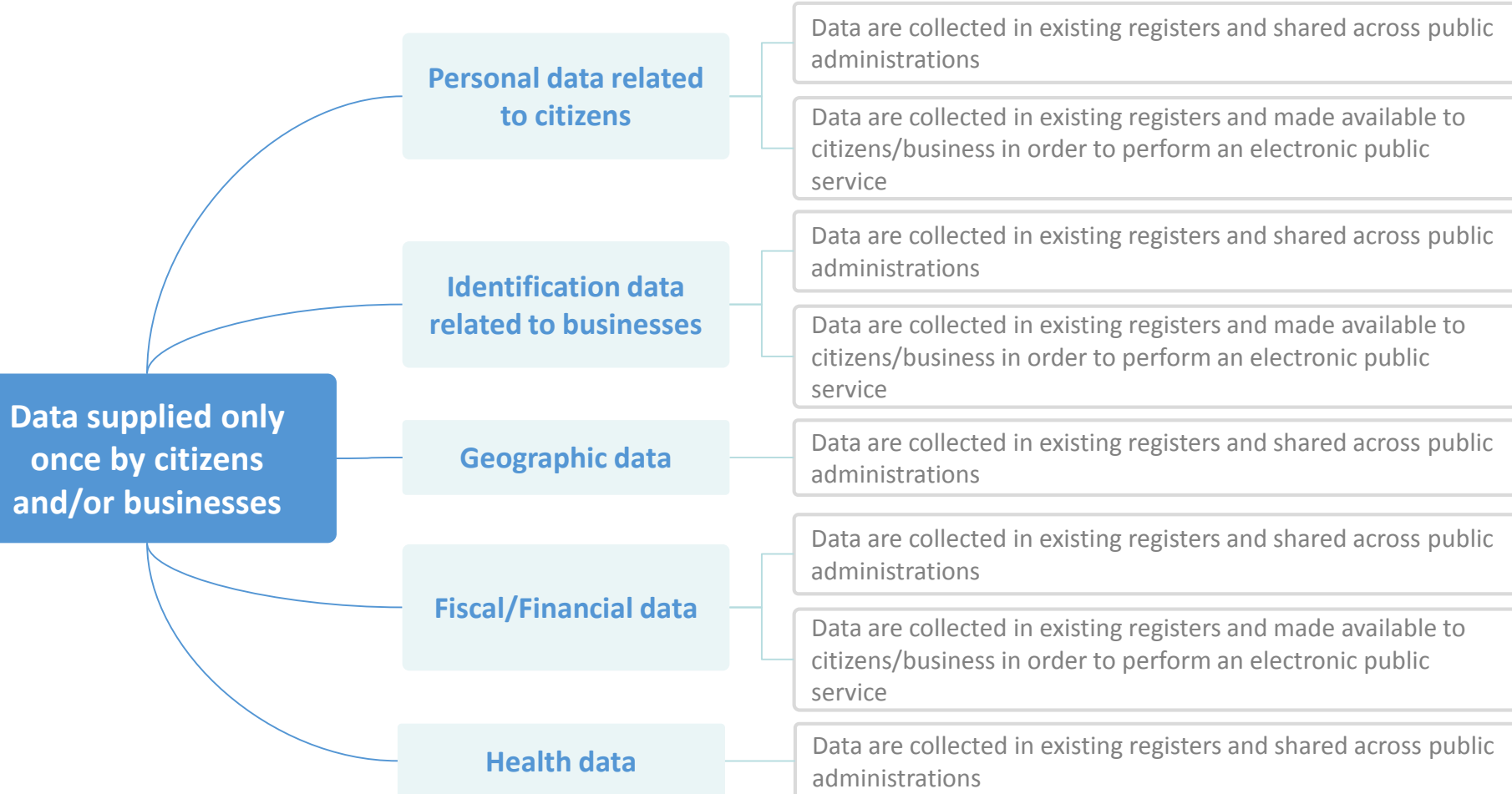
1. Full respect of data protection laws and regulations.
2. Interconnection of base registers, e.g. through harmonised and standardised interfaces based on open standards.

## ➤ The 'Once-only' principle into action: **HELP.gv.at** and **USP.gv.at**

- The Business Service Portal ([www.usp.gv.at](http://www.usp.gv.at)) serves as a **single entry point for businesses** to the administration whereas the [HELP.gv.at](http://HELP.gv.at) website offers online services according to the **one-stop principle** to anyone who wants to find out more about administrative procedures in Austria.
- By offering information, transaction and personalised services, these portals intend to support citizens as well as to help businesses to fulfil their legal obligations and to **reduce the administrative burdens** for both of them.

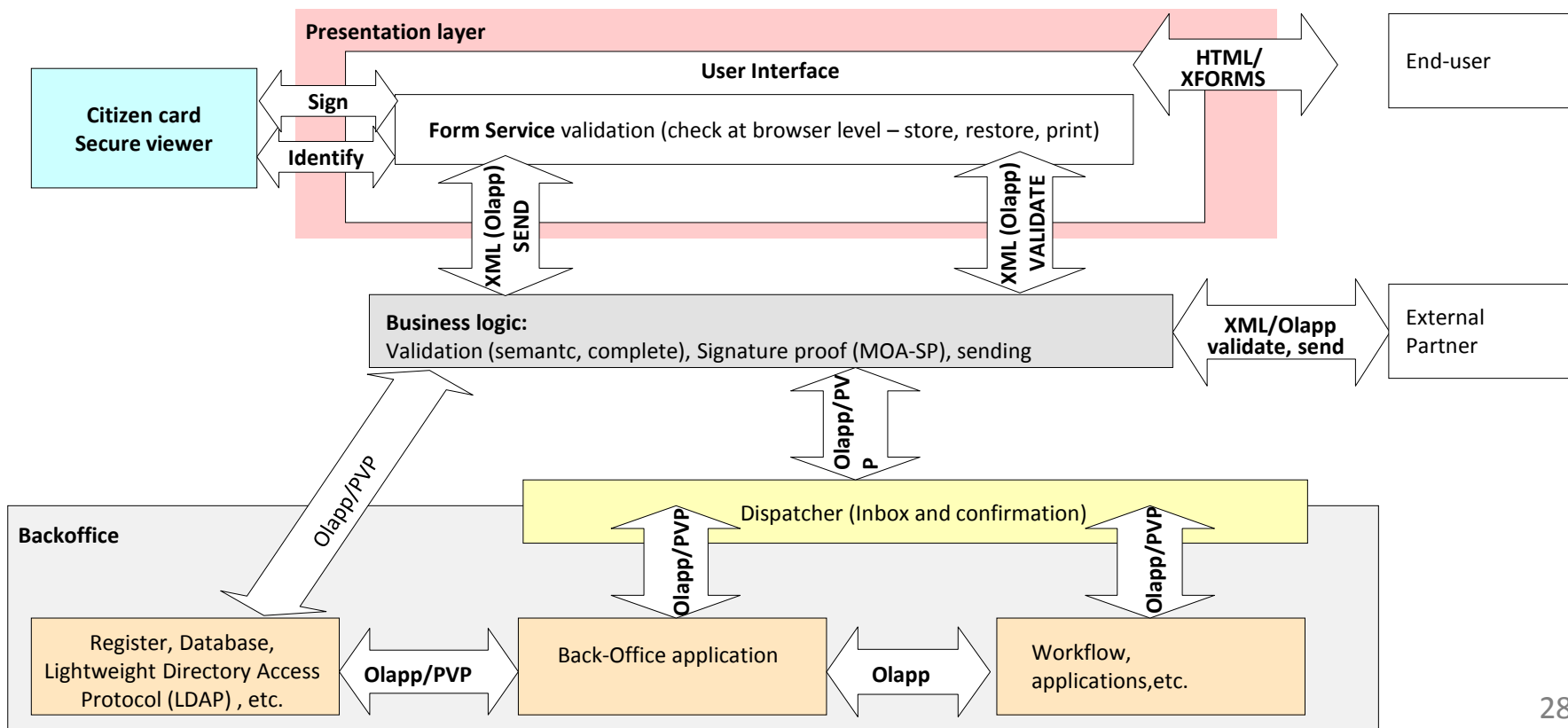


## What type of data are supplied only once by citizens and/or businesses?



## What approach is currently used by your country to implement the OOP?

- **Combination of both front- and back-office approaches:** Back-Office is the most common solution, but there are also applications rather following the front-office approach. Back-Office Approach is being done by administration-internal requests to base Registers based on common interfaces and specifications.
- On a very high level, Austria encourages a distributed solution based on **interconnection of various registers**.



## What security measures are applied on the citizen portal?

### Authentication

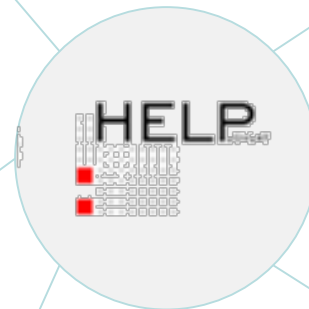
- › Multi-factor authentication mechanisms for citizens and businesses
- › At least username/password for public servants willing to access data

### Confidentiality

- › Data encrypted (e.g. TLS transport channel).  
*Caveat: depends on the system*

### Integrity

- › eSignature



### Authorisation (access control)

- › No need for a specific assignment of access rights for citizens (strong authentication)
- › Authorisation of public servants based on a rights model set out by the specific application

### Traceability & Non-repudiation

- › eSignature  
*Caveat: depends on the individual (citizens vs. Public servants)*

## ➤ Context on the 'Once-only' principle in Estonia

**31.05.2000:**

Adoption of the  
Population Register Act

**15.11.2000:**

Adoption of the Public Information Act

**12.02.2003:**

Adoption of the Personal  
Data Protection Act

**17.02.2011:**

Adoption of the Spatial  
Data Act

**04.2014:**

Adoption of the Digital Agenda 2020 for  
Estonia - Estonia's current digital strategy

*The first version of the Public Information Act took effect in January 2001. A newly revised, updated Public Information Act entered into force on 1 January 2008.*

*Since then, it became compulsory to connect all public and private sector base registries to X-Road, Estonia's data exchange platform: § 43 (2) indeed mentions that the "establishment of separate databases for the collection of the same data is prohibited".*

...

2010

2013

2015

**2001:**

Roll-out of  
the Data  
exchange  
layer X-Road

**22.12.2011:**

Adoption of the Estonian  
State Information System  
interoperability  
framework v3.0

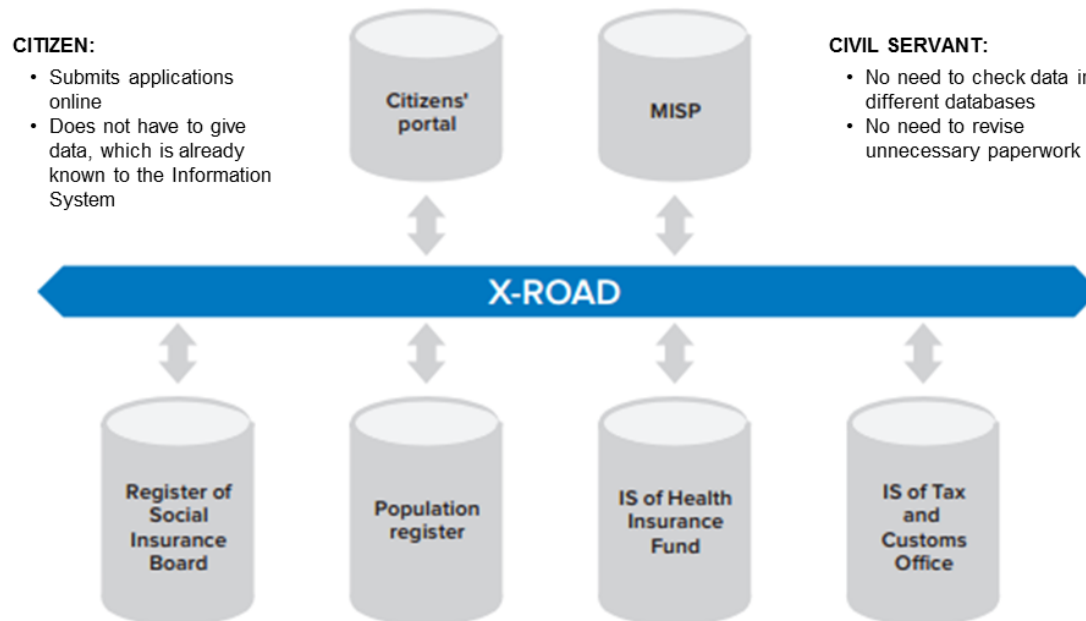
**09.2013:**

Adoption of the Estonian  
Entrepreneurship Growth  
Strategy 2014-2020

*In order to reduce the administrative burden, we will try to exclude the situation where the data that has once been submitted to the state has to be submitted again.*

## ➤ The 'Once-only' principle into action: X-Road data exchange layer

- X-Road is a platform-independent secure data exchange layer, allowing institutions/people to securely exchange data and ensuring access to the data maintained and processed in state databases.
- Public and private sector enterprises and institutions can connect their information system with the X-Road. This enables them to use X-Road services in their own electronic environment or offer their e-services via the X-Road.



## What type of data are supplied only once by citizens and/or businesses?

### Data supplied only once by citizens and/or businesses

#### Personal data related to citizens

Data are collected in existing registers and shared across public administrations (many registers contain personal data)

Data are collected in existing registers and made available to citizens/business in order to perform an electronic public service

#### Identification data related to businesses

Data are collected in existing registers and shared across public administrations (e.g. Estonian Business Register, based on the Estonian Commercial Code)

Data are collected in existing registers and made available to citizens/business in order to perform an electronic public service

#### Geographic data

Data are collected in existing registers and shared across public administrations (e.g. Land Cadastre, Spatial data registers)

Data are collected in existing registers and made available to citizens/business in order to perform an electronic public service

#### Financial/ Fiscal data

Data are collected in existing registers and shared across public administrations (e.g. Register of Taxable Persons)

Data are collected in existing registers and made available to citizens/business in order to perform an electronic public service

#### Health data

Data are collected in existing registers and shared across public administrations (e.g. Estonian Health Information System)

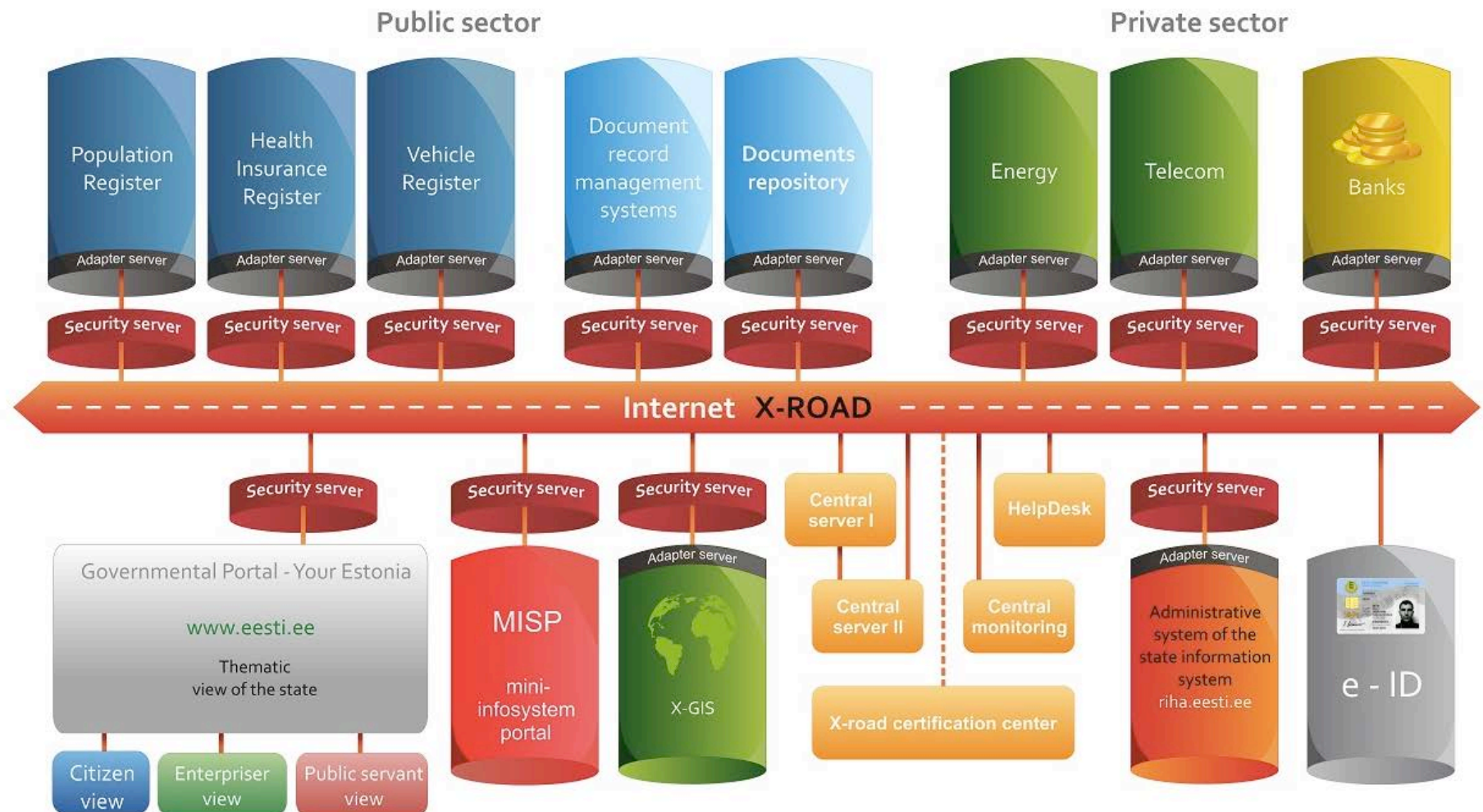
Data are collected in existing registers and made available to citizens/business in order to perform an electronic public service



# Case study N°3: Estonia



What approach is currently used by your country to implement the OOP?



## What security measures are applied to the X-Road data exchange layer?

### Authentication

#### Strong authentication

- › Public Key Infrastructure (certificates)
- › Electronic ID card for citizens

### Confidentiality

- › Restricted access to data

### Integrity

- › Depends on an information system, on the user rights.



### Authorisation (access control)

- › Access to types of data in a register by services in the State Information System is agreed previously between the information system owners and based on consent of the data owner.

### Traceability & Non-repudiation

- › Log files
- › A person (and the supervisor) has control over the data and can thus trace illegal transactions with his/her data and notify a supervisor to take legal action against the offender.

## Conclusion 1

- 70% of the countries analysed in a study conducted by the European Commission (“eGovernment and the Reduction of Administrative Burden”) were implementing projects or programmes related to the OOP in 2013.
- This percentage has slightly increased in the course of 2015 with new countries having started to implement the OOP (e.g. Sweden).
- Overall, 25 countries out of a total of 33 European countries (76%) have now started to implement the OOP at national level.

## Conclusion 2

- Most of the countries implement the OOP primarily for personal data related to citizens as well as for identification data related to businesses.
- For these types of data, the establishment of related authentic sources is widely supported by a specific law.



## Conclusion 3

- Personal data related to citizens and identification data related to businesses are primarily collected in existing registers and shared across public administrations but also, to a lesser extent, made available to citizens /businesses in order to perform an electronic public service.

## Conclusion 4

- Organisational barriers are the first type of barriers that countries aim to overcome in order to ensure the implementation of the OOP.
- This confirms the results of the study conducted by the European Commission on eGovernment and the Reduction of Administrative Burden.



## Conclusion 5

- A combination of both Front and Back-Office integration is currently used by a majority of countries to implement the OOP.
- This approach facilitates the different applications and related processes used to implement the OOP.

## Conclusion 6

- Strong authentication mechanisms (e.g. single-use password, eID card, etc.) are used by a wide majority of countries to identify who is accessing the data and to ensure that they are who they say they are.
- However, a few countries still only authenticate users by means of a username and password.



## Conclusion 7

- eSignature is broadly used to ensure that information can be relied upon and is accurate and complete (integrity).
- eSignature is also used in order to prevent intervening persons or systems to deny or challenge their access to authentic data sources (non-repudiation).

## Conclusion 8

- Confidentiality of data is primarily ensured by encryption in order to ensure that none of the data can be deciphered.
- Encryption systems provide the possibility to access users' data by authorised third parties using a Key Escrow system in only two countries (LU & SK).

# Wrap up from EUPAN HRWG/IPSG (1/2)

Meeting held on 16<sup>th</sup> October 2015

## ➤ Good practices aimed at implementing the OOP at national level:

- France allows SMEs to participate to eProcurement procedures by providing their identification number (only data requested).
- In Latvia, citizens are able to perform their annual income declaration in a few clicks (declaration forms pre-filled with the information provided by citizens in the past).
- In the Netherlands, all communications between citizens and public administrations related to tax declarations aim to digital, as recently declared by the State Secretary of Tax Policies in the Netherlands.

## ➤ Role of legislation in the implementation of the OOP:

- In Latvia, legislation is key to define technical requirements and to ensure interoperability between systems so that the data supplied by citizens and businesses can be efficiently reused.
- In Bulgaria, on the contrary, legislation represents a barrier to the implementation of the OOP since it stipulates that data from citizens and businesses can only be reused by a public administration if the latter made this request, leaving no space for proactivity.

# Wrap up from EUPAN HRWG/IPSG (2/2)

Meeting held on 16<sup>th</sup> October 2015

## ➤ Challenges related to the implementation of the OOP at national level:

- In the Netherlands, trust and security issues are continuous concerns.
- Belgium highlighted one organisational measure that is recommended to other countries:

Only a selected number of civil servants should have access to citizens' or businesses' data to avoid potential abuse. In case a civil servant is changing position in the administration, then his or her access rights should be reviewed based on strict procedures.

- In Bulgaria, the lack of harmonised processes is the main challenge identified.

## ➤ Recommendations for a better implementation of the OOP:

- Latvia recommended fostering cooperation between the different level of administrations, i.e. national, regional and local, enhancing their knowledge and communicating on the benefits of implementing the OOP.
- Bulgaria suggested to put in place a development training programme for policy, legal and IT units to promote an integrated approach to implementing OOP.
- France supports an integrated approach in order to break silos within national administrations.
- The Netherlands highlighted the importance for the different Member States to share their best practices between each other.

- **Authentication:** Aims to identify who is accessing the data and ensure that they are who they say they are.
- **Authorisation:** Aims to give adequate access rights to end-users who are accessing authentic data sources and verify whether they have the rights to do what they are trying to do.
  - **Role-Based Access Control (RBAC)** is an approach to restrict system access to authorised users. Permission to perform certain operations is in fact assigned to specific roles.
  - **Attribute-Based Access Control (ABAC)** is an approach to determine access control based on the attributes of involved entities. It aims to overcome the limitations of the classical access control models such as RBAC.
  - **Access Control Lists (ACL)** is a table defining, for a computer operating system, which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges.
- **Integrity:** Aims to ensure that information can be relied upon and is accurate and complete.
- **Traceability:** To chronologically inter-relate any transaction on authentic data sources to a person or system that performed the action in a way that is verifiable.

- **Non-repudiation:** Aims to prevent the intervening person or system from accessing authentic data sources in an event or action to deny or challenge their access to authentic data sources.
  - **Audit trail** (also called audit log): It is a chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.
  - **Timestamping:** Refers to the use of an electronic timestamp to provide a temporal order for a set of events.
- **Confidentiality:** Aims to prevent unauthorised access to information stored in authentic data sources.
  - **Encrypted data:** Transferred data is encrypted to ensure that none of the data can be deciphered.
  - **Restricted access to data:** Access to data is limited only to a restricted set of users.
  - **Confidentiality agreements:** Confidentiality and non-disclosure agreements to be signed when accessing specific data.





LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG  
Centre des technologies de l'information de l'Etat

With the support of:

**Kurt Salmon**   
Success for what's next

**Centre Des Technologies de l'information  
de l'Etat**

1, rue Mercier  
L - 2144 - Luxembourg  
Luxembourg

[www.ctie.public.lu](http://www.ctie.public.lu)

**Kurt Salmon**

41, Zone d'activité Am Bann  
L-3372 Leudelange  
Luxembourg

[www.kurtsalmon.com](http://www.kurtsalmon.com)



**Marc Blau**

[Marc.blau@ctie.etat.lu](mailto:Marc.blau@ctie.etat.lu)

**Gérard Soisson**

[Gerard.soisson@ctie.etat.lu](mailto:Gerard.soisson@ctie.etat.lu)



**Alessandro Zamboni**  
Senior Manager

T+352 621 321 053  
[Alessandro.zamboni@kurtsalmon.com](mailto:Alessandro.zamboni@kurtsalmon.com)



**Ludovic Mayot**  
Senior Consultant

T +352 691 321 007  
[Ludovic.mayot@kurtsalmon.com](mailto:Ludovic.mayot@kurtsalmon.com)



**Céline Monteiro**  
Consultant

T +352 691 321 210  
[Celine.monteiro@kurtsalmon.com](mailto:Celine.monteiro@kurtsalmon.com)