EUROSMART
The Voice of the Digital Security Industry

Europe lacks a reference point for AI

In the race for artificial intelligence (AI) technologies, the EU is lagging behind the USA and China, especially when it comes to investment in AI companies. However, the EU has excellent research and the European Commission is determined to develop an "ecosystem of excellence" for AI in the coming years. This approach was further developed in the Commission's White Paper on AI published last year.

Excellence shall go hand in hand with trust, meaning that AI technologies must adhere to Europe's ethics and principles. This includes protection of Fundamental Rights, data protection, transparency, safety and security. These principles should be incorporated by design in all AI systems placed on the EU market. This is particularly important for the concept of fundamental-rights-by-design, which must be applied to the design, test and evaluation of AI systems.

Eurosmart believes that such an ecosystem of excellence and trust requires the creation of an AI Competence Centre, a horizontal structure covering different market sectors. This Centre would work on strategic priorities, simulation, standardisation and certification, all of these being crucial components of trust in AI technologies. The AI Competence Centre would gather AI top experts and networks working on these issues in the European Economic Area (EEA).

Ultimately, this structure would become the reference point for AI in Europe. It would foster trust in AI made in Europe by ensuring that these technologies are designed and developed according to European values, evaluated against European criteria, focusing on European interests & use cases, and using data relevant to Europe's situation.

Why do we need an AI Competence Centre?

✓ Support European autonomy in AI technologies for all sectors.

✓ Structure the European AI value chain, from hardware, embedded software, mobile software, server software, to databases, and applications.

> *"AI is too important a technology for Europe to depend on non-European companies and algorithms. We must therefore organise ourselves to foster the emergence of European alternatives."*
>
> Commissioner Thierry Breton, 26 October 2020
> Speech to the AIDA Committee, European Parliament

Missions of the AI Competence Centre

Eurosmart believes that the AI Competence Centre should be tasked with the following missions:

- Define strategic priorities for R&I in Europe
- Assist EU institutions on the legal implications of AI
- Organise access to sensitive data for industry and research
- Organise funding for R&I projects on AI
- Develop coherent standards in line with EU values
- Support European AI research and industry to narrow the gap with international competitors
- Foster simulation and evaluation
- Support compliance of AI applications with legal provisions
- Provide legal and technical expertise to European AI research and industry

Define strategic priorities for research and innovation in Europe

The AI Competence Centre could act as a lighthouse for Europe's research and innovation in Europe. This would ensure that research efforts are not unnecessarily duplicated or spread in unconnected projects.

The Centre would define the strategic priorities for research, taking into account both:

- **short-term aspects**: e.g. research on AI in the health sector in pandemic times, review and assessment of applications of AI in the field of public security in order to build trust, etc.
- **long-term ones**: e.g. autonomous driving/drones/trains/robots, including swarm intelligence, smart farming, intelligent travel/mobility assistant, medicine assistant for health professionals, autonomic intrusion detection/protection system for enterprises and public authorities, quality/logistic/development assistant in smart factories etc.

The AI Competence Centre should be involved in the creation and management of the future European Common Dataspaces as those are essential components for researching and developing AI applications. Thus, it is only logical to have a strong link between the list of Common European Dataspaces -underpinned by GAIA-X- that the European Commission plans to create, and the strategic priorities for research and innovation on AI. There should be a tight link between public bodies holding data of citizens (e.g. electronic patient data), enterprises providing AI solutions (e.g. AI-based data analytics) and public authorities in need of innovative solutions (e.g. online services, such as chatbot).

Moreover, the priorities for AI could include the need to adhere to European principles, i.e. developing human-centred AI applications, respecting Fundamental Rights, and guaranteeing security. Thus, cybersecurity-by-design, privacy-by-design, fairness-by-design, transparency, ethic and sustainability could be key principles part of these strategic priorities defined by the Centre.

Organise funding for research and innovation projects on AI

EU funding programmes, such as Horizon Europe and Digital Europe, have a key role to play in strengthening Europe's AI ecosystem. These programmes foster resource pooling and innovative exchanges across countries. They are also an efficient tool to stream AI development into a particular direction, for instance into specific use cases or standards.

The AI Competence Centre would be in an ideal position to allocate EU funding as it would also define the above-mentioned strategic priorities. It would have the expertise to organise the drafting of the calls for proposals, and the subsequent launch of such calls.

EU funding should be complemented by national contributions to maximise the impact of the projects.

Assist EU institutions on the legal implications of AI

Artificial intelligence will disrupt many domains and will have major impacts on laws and the legal principles on which they were laid down. Over the years to come, laws and administrative rules makers will face the consequences of the transformation of the world resulting from the advent of AI. In that respect, a sharp expertise on AI will be more and more needed when preparing legal framework and instruments, as well as administrative decisions.

The AI Competence Centre could help the European institutions (Commission, Parliament and Council) to face this challenge to come. The AI Competence Centre could assist and provide insight, state-of-the-art knowledge and expertise to these institutions so that they clearly understand the implication of AI before they prepare or approve any legal acts or administrative decisions.

Develop coherent standards in line with EU values

Standards are instrumental to ensure that the development and usage of AI applications are in line with European values and principles. Moreover, it is of the utmost importance that harmonised standards are available for AI applications in order to foster the development of their cross-border use and trade.

The AI Competence Centre would be the main reference point for developing European AI standards. It would ensure that all standards (1) are consistent with each other, (2) cover all necessary requirements, such as cybersecurity, ethics and privacy, and (3) are in line with the values and principles of Europe.

Moreover, the AI Competence Centre should be assigned the objective to foster European leadership on AI by ensuring that standards applicable to the European industry are prepared under European supervision with European stakeholders and taking into account European values and principles. In that respect, the AI Competence Centre should be transferred all the AI-related standardisation responsibilities and activities currently exercised by CEN-CENELEC and ETSI. However, the work of the AI Competence Centre should reuse the work of the current European Standardisation Organisations.

Foster simulation and evaluation

In some application areas, standards or technical documents cannot be created due to lack of data, e.g. for identifying rare disease or simulating rare environmental events, like an earthquake or plane crash on a nuclear power plant. In that regards, the AI Competence Centre could nevertheless help gaining better understanding of these phenomena by performing simulation thanks to AI capacities and by gathering the rare source of available data.

The AI Competence Centre could verify key functionalities, performance and overall behaviour of the AI products and systems. It would be an ideal environment to make tests, which might otherwise not be performed by companies, due to lack of expertise, data, resources, or for practical reasons. For instance, companies might not be able to make such tests in running productions in their smart factories.

Support compliance of AI applications with legal provisions

Certification of high-risk AI applications is likely to be required by the AI-related legislation to come. These high-risk types of AI applications are expected to meet the highest level of trust. The same instrument may also provide for optional, voluntary certification for other AI applications. In order to support this legal instrument, certification schemes need to be defined and operated, to demonstrate the compliance of AI applications with the principles it enacts.

The AI Competence Centre should play a key role to support the implementation of the upcoming legislation. This new structure should be tasked with (1) developing evaluation methodologies for AI applications and (2) setting up and organising the corresponding certification schemes of AI applications, based on these methodologies.

The development of evaluation methodology shall rely on an evaluation of the risk, the management of these risks, and the classification of criticality of the application, in similar way to the admission of medical products. For instance, it is important to distinguish two types of AI applications - as illustrated by the following table - whose criticality substantially differs:

Type of AI	Brief description	Examples (today)
Algorithm Decision Making (ADM)	Decision is made by an algorithm	High frequency trading Luggage sorting system (airport) Self-driving cars Autopilot aircraft Road safety application
Assistant system	Decision is made by a person taking into account a recommendation made by an algorithm	Medical service Travel routing service Anomaly detection of data traffic in enterprise IT network Public security application Chatbot at public authorities

In the case of ADM systems, the AI application should be considered much more critical as no human is involved in the decision. Therefore, ADM systems need stronger requirements and a mandatory assessment of compliance.

Also, these evaluation methodologies should take into account the (1) cybersecurity, (2) privacy, (3) safety and also (4) ethical aspects of AI applications. These evaluation methodologies should be the foundation of certification schemes that could follow the approach developed in the Cybersecurity

Act, where different levels of trust in AI applications corresponding to different levels of risks are defined: basic, substantial, high.

The development of evaluation methodologies and certification schemes should be coordinated with standardisation activities run in this very same AI Competence Centre.

Organise access to sensitive data for research and industry

The creation of European Data spaces is instrumental to foster the development of AI applications, as they require access to large amounts of data so that their algorithms can be trained. As such, it is a major step ahead to support AI research and industry in Europe.

However, European Data Spaces are not sufficient to organise the exploitation of a large amount of sensitive data (e.g. medical data, biometric data…) by a company willing to develop or train an AI application (innovation) – or even for research purposes.

The two main hurdles faced by European research and industry on AI are the following:

- **Security and compliance issues resulting from the sensitive character of the data;**

  Security and compliance issues resulting from the sensitive character of the data may be cumbersome, long and complicated to apply for a European research centre or company willing to use the data. In that respect, the AI Competence Centre could help by (1) giving them the possibility to exploit this sensitive data, and (2) putting in place all necessary security measures and compliance tasks for their exploitation. **The AI Competence Centre would not give access to the sensitive data to third parties per se, but would rather provide a service where it would (1) organise and supervise exploitation of sensitive data by third parties in a manner respectful of the security requirements laid down by the GDPR and (2) ensure and demonstrate compliance with it. This approach would provide simplicity and flexibility to third parties willing to exploit these sensitive data**. For instance, the AI Competence Centre could host the AI application to be trained in its infrastructure so that the reference data set remains hidden to third parties. The existing relative level of standardisation and interoperability of the current dominant AI technical frameworks support this approach.

- **Access to large amounts of sensitive data**

  Large amounts of sensitive data are usually held by national or European entities (public or private) and it is usually very difficult to benefit from this data for innovation or research purposes. This is the case for instance of medical data or biometric data (face and fingerprint) held by eu-LISA. Yet, it is instrumental to have a large amount of data, originated from a trusted source, available in order to foster innovation and research. Both quantity (large amount) and quality (data have not been modified nor tampered, data are originated from a genuine source, but collected in an operational, therefore relevant to real-life applications) matter. **Without the possibility to use large amount of sensitive data, no European research could be carried out, and no strong AI European industry could emerge. The AI Competence Centre should act as a trusted proxy between the European industry and research on one hand, and European entities holding sensitive data (eu-LISA,…) on the other hand, and should organise the exploitation of the sensitive data they hold by the European industry and research. One of the first key actions the AI competence Centre should launch is to organise the exploitation of the biometric data hold by eu-LISA. It is instrumental to help AI European industry and research on biometric data to stay in the race compared to US, Russia or China.**

  Today, the exploitation of sensitive data is hampered by the lack of a clear and harmonised legal basis ruling the usage of sensitive data for research or innovation purposes. Yet, it may fall within the provisions of article 9.2(g) of GDPR ("*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim*

> *pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"*), but there are currently no European laws on which it could rely, even though some national laws exist. This creates fragmentation resulting from diverse national legislation, and above all impede research and innovation within Europe. **In order to remove this barrier, the AI Competence Centre may be the solution. First of all, a European legislative instrument should vest the AI Competence Centre to decide whether a data processing falls into the provisions of article 9.2(g). Secondly, the AI competence Centre should have the needed power and authority to enforce and verify the required conditions are met.**

In that respect, the AI Competence Centre could be very helpful when it comes to the exploitation of sensitive data. The AI Competence Centre could contribute to the implementation of the future Data Governance Act and Data Act. For instance, the AI Competence Centre could be an intermediary for the re-use of certain categories of data held by public sector bodies, as it will soon be regulated by the Data Governance Act. These two upcoming legislations should refer to and rely on the AI Competence Centre.

The table below illustrates some of the potential benefits and applications that could be drawn from exploitation of data:

Type of data	Potential benefits and applications
Health data	Identify lethality origins Improve public health Improve cure of some diseases (cancer…) ….
Financial data	Better understand dynamics of each economic sectors (car industry, semiconductor, pharmacy…) Better understand dynamics of stock exchanges, of currencies... …..
Facial images	Train facial recognition algorithms in accordance with European phenotype pursuant to European values Establish standards and performance reporting protocols regarding fairness of AI algorithms Develop anti spoofing techniques able to sort out a genuine face from an impersonation attempt (spoofing of someone else's face). ….

Support European AI research and industry to narrow the gap with international competitors

There is a fierce international competition around AI, and the two leaders are currently US and China. Europe must not only stay in the race but also catch up. Furthermore, it is paramount that Europe controls all the AI technologies to secure its technical and industrial autonomy, and beyond that, its sovereignty and prosperity.

The main reason explaining why US and China managed to lead the race on AI is that their research and industry could easily access large amounts of data. For instance, the main internet platforms such as Facebook or Google have already access to large amounts of data (including portrait) that is fed into the development of their own AI applications. They do not only access data from their nationals, but also from European citizens. Their monopolistic situation allows them to collect large amounts of data from European citizens, while European research and industry cannot because they do not benefit from such a monopoly. This creates a major distortion, highly detrimental to European research and industry. **The AI competence Centre should be tasked to focus on helping European research and industry to fill the gap, and counter and curb this distortion.**

> *"We need to secure this data for Europe and make it widely accessible. We need common data spaces - for example, in the energy or healthcare sectors. This will support innovation ecosystems in which universities, companies and researchers can access and collaborate on data."*
>
> President Ursula von der Leyen, 16 September 2020
> State of the Union Speech

The main problem European research and industry is facing is the lack of access to large amounts of data (sensitive or not). Therefore, European policies shall focus on tackling this issue very quickly, to help Europe to stay in the race. However, if these European policies also benefit to foreign research and industry (including platforms) – that do already lead the race, it will worsen the situation of European research and industry for the following reasons:

- Foreign research and industry (including platforms) already leading the race will stay ahead of the race as they will benefit from the support of European policies. It will not help (1) the emergence of a strong European research and industry on AI, and (2) Europe to gain its technical and industrial autonomy, and beyond that its sovereignty and prosperity;
- This could even create a foreclosure effect for European research and industry. It may end up with the situation where foreign research and industry (including platforms) - already leading the race - could pre-empt access and exploitation of European data, because they are much more powerful and can afford it, and thus would create a foreclosure effect for European research and industry.

In that respect, Europe shall take bold initiatives, and should reserve all benefits of the AI Competence Centre only to European companies and research centres, such as (1) access to sensitive data, and (2) any supporting actions.

Moreover, the upcoming Data Governance Act should explicitly stipulate that the re-use and processing of public sector body data should be limited to European companies and take place in the EU territory <u>in all cases</u>. Likewise, access to the European common data spaces should be limited to EU actors.

Provide legal and technical expertise to European AI research and industry

The AI Competence Centre should provide strong support to European AI research and industry to foster their emergence. In particular, it should provide support and assistance to European AI research and industry in domains where they may not have all the necessary knowledge and expertise:

- Legal support pertaining to GDPR – as AI relies on exploitation of data - and AI future legislation;
- Support to set up and achieve compliance with the GDPR and AI future legislation;
- Technical expertise.

Structure of the AI Competence Centre

There is no need to re-invent the wheel for the structure of the AI Competence Centre. Its organisation should be largely based on the model of the future European Cybersecurity Competence Centre. The AI Competence Centre should have a Board of Directors involving the European Commission -including DG CNECT, DG GROW, JRC - the EU Cybersecurity Competence Centre (EUCCC), ENISA, and national authorities.

The AI Competence Centre should rely on the expertise of an AI competence community composed of high-level experts from academia, industry and civil society entities. Relevant members of the industry may be providers of sub-components of AI systems, developers, operators of AI, evaluation laboratories etc. Interdisciplinary cooperation is the key for success.

It is of utmost importance to have a mirror of the AI Competence Centre at national level. These national coordination centres would be the main reference point for AI in each Member State. They could implement projects initiated at EU level or bring out ideas from the field to the EU level. The EU Competence Centre would be in charge of coordinating the network of national coordination centres.

Links to the ecosystem

It is crucial for the AI Competence Centre to be perfectly connected to its environment. AI is in many ways a transversal topic, which requires the cooperation of different EU entities. For cybersecurity aspects, ENISA and the new agency EU Cybersecurity Competence Centre (EUCCC) are key actors that should be involved at governing and/or community level. For exploitation of biometric data by European AI research and industry, eu-LISA, Frontex and EUROPOL should be involved. For data protection, the European Data Protection Supervisor (EDPS) should contribute to the discussions at strategic and/or technical level. For the protection of public institutions, EU-CERT is an important stakeholder. Fruitful technical collaboration could also be established with the JRC.

The AI Competence Centre could also collaborate with stakeholders from the financial industry to foster the development of applications in the financial sector in line with EU values, standards and legislations. Thus, ECB, EBA, ESMA should be associated to the Centre.

In addition, the AI Competence Centre should closely work with the Joint Undertaking ECSEL, as semiconductors are crucial components underpinning AI technologies.

The EU is a continent open to the world and it is important to address the issue of international relevance of this AI Competence Centre. The outcome of its activities (standards, certification schemes) should be promoted on the international stage so that the EU can become a norm-setter -as it did with GDPR.

Eurosmart offering cooperation

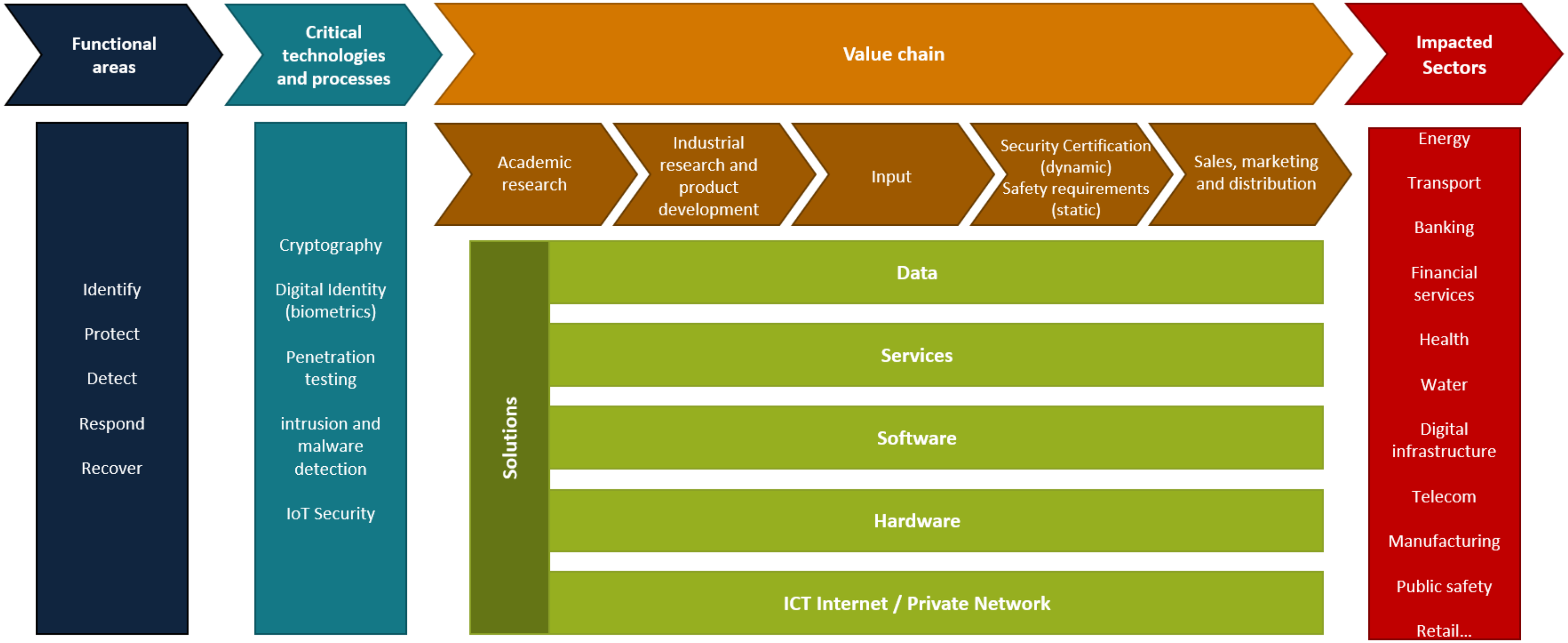
Eurosmart is a European association at its core, standing for AI made in Europe in line with European values. Eurosmart cooperates with international players to promote its European vision.

Eurosmart members are placed at the beginning of multiple value chains on electronic devices, systems, services and digital security. Therefore, Eurosmart and its members are fully familiar with different market segments, such as transports, financial services, health services, mobile network systems, border controls and many others.

Eurosmart members have in-depth knowledge on encryption, secure certification, data protection and more generally digital security. They also have a complete understanding of Algorithm Decision Making (ADM) systems (e.g. as used for automatic border control (ABC) applications), or assistant systems (e.g. as used in medical service, travel routing service or public security applications) as well on dedicated technologies, such as match on card.

Therefore, Eurosmart would be pleased to contribute in drawing the picture of the current and the future AI value chain. Our association created a similar mapping for the cybersecurity value chain within the IPCI project (see Appendix).

Appendix: The cybersecurity value chain



Functional areas

Identify

Protect

Detect

Respond

Recover

Critical technologies and processes

Cryptography

Digital Identity (biometrics)

Penetration testing

intrusion and malware detection

IoT Security

Value chain

Academic research

Industrial research and product development

Input

Security Certification (dynamic)
Safety requirements (static)

Sales, marketing and distribution

Solutions

Data

Services

Software

Hardware

ICT Internet / Private Network

Impacted Sectors

Energy

Transport

Banking

Financial services

Health

Water

Digital infrastructure

Telecom

Manufacturing

Public safety

Retail...

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com