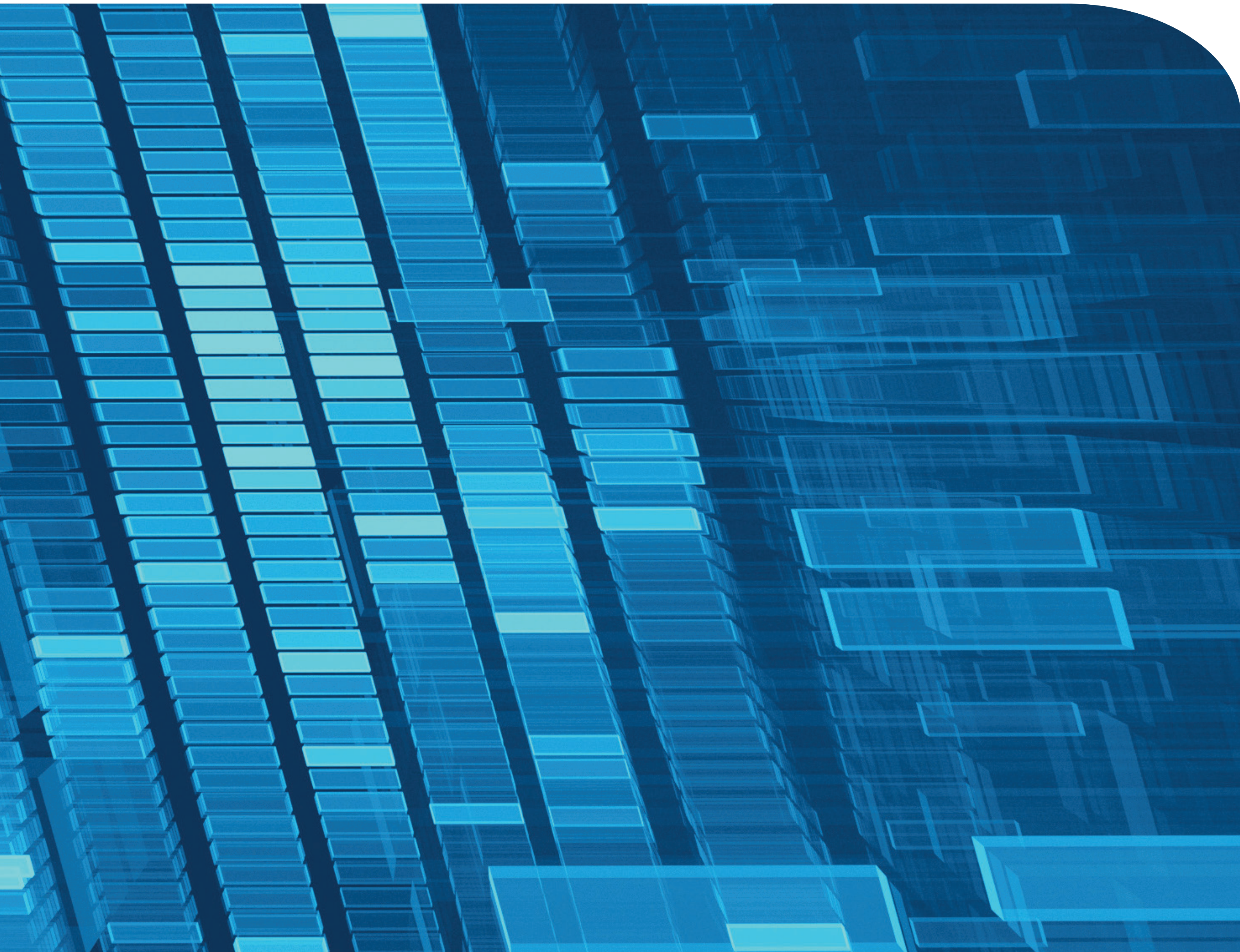
Conference Report

eu-LISA Annual Conference

JHATech 2016

Aligning the capabilities of technology with policy priorities in the areas of migration and internal security

27 October 2016
Tallinn, Estonia



Contents

Photo: Rene Suurkaev
Copyright: eu-LISA

This report is based on audio/video recordings and notes taken during the Conference.
It does not purport to reproduce in extenso all debates and intervention.
The opinions expressed are those of the speaker(s) only and should not be considered as representative of eu-LISA's official position.

Opening statement by the Executive Director of eu-LISA

Mr. Krum Garkov

Executive Director of eu-LISA

Addressing the audience with some opening words, Mr. Garkov greeted all participants and expressed his gratitude towards the Agency's event organisation team and the participants for making the effort to travel.

He began with an illustrative anecdote about two men chopping wood. One of the men, he noted, worked tirelessly and without breaks while the other worked at a leisurely pace, even going so far as to take frequent lunchtime nap. Despite the disparity in work ethics, the results of each man's work at the end of the day were inevitably identical. After some time, the first man confronted the other seeking explanation. "While you are busy chopping wood", noted the second man, "I am taking the time to sharpen my axe." eu-LISA, Mr. Garkov summarised, acts to sharpen the axe to ensure optimal efficiency for those facing today's challenges in the Justice and Home Affairs domain. Nevertheless, he insisted that it was equally necessary to work hard as well as smartly.

Photo: Rene Suurkaev
Copyright: eu-LISA

Reflecting on the day to come, he emphasised the importance of the conference in aiding understanding how technology can support relevant activities. He continued by describing the ever-changing challenges that present. Some arise as a result of the blurring of lines between border management, immigration management and internal security and the increasing interconnections between these topics that were previously viewed in isolation of each other. Others result from the transition from physical to virtual that is on-going within the Justice and Home Affairs domain and the resulting dependence on data and systems that enable sharing and analysis. According to Mr. Garkov, the need to support and facilitate this transformation has been recognised as a political priority only recently. There is a huge opportunity to reshape and rethink the way technology is used, he noted, indicating that eu-LISA is already a major contributor to this process and suggesting that this role will inevitably grow going forward. Over time, the Agency has already proven itself to be a reliable partner to Member States and Institutions; it is ready, he stated, to build upon these foundations and ensure that policy priorities result in tangible positive results in practice.

Such positive outcomes will require joint actions between the Member States, EU Institutions and the industry. The conference, he suggested, was the ideal forum to sow the seeds of such cooperation, especially given that representatives of all relevant stakeholders were present.

Mr. Garkov concluded with a plea to think big throughout the day and indeed as the Agency works with its partners in the days, months and years to come.

SESSION 1
Keynote addresses

Sir Julian King

Commissioner for Security Union, European Commission

Sir King first expressed his joy at being able to attend the conference and also to have been able to avail of the offered opportunity to engage with the Estonian authorities on their priorities for the upcoming Presidency.

He continued by providing some perspectives on the importance and relevance of information systems and information exchange in modern border management and law enforcement activities. Information sharing is central to the securing of borders, to manage migration and to enhance collective security, he suggested. Thus, IT systems are vital for information sharing. Providing examples, he cited the Schengen Information System that helps to identify foreign terrorist fighters at the external borders of the EU and EURODAC that allows for the fingerprinting and registration of migrants, including at the Hotspots that have been set up to manage large migrant influxes in particular areas.

eu-LISA, Sir King noted, should be commended for ensuring that these systems are available 24 hours a day seven days a week, thereby supporting the work of police officers, border guards, immigration officers and others. Any suggestions regarding sub-optimal information exchange, such as those that were put forward subsequent to the horrific terrorist attacks of the past year, arouse his concern. The attacks highlighted that available, accurate and complete data is crucial for law enforcement authorities. Thus, he concluded that the improvement of information sharing across the EU is of key importance.

One strand of the work that Sir King was appointed by President Juncker to engage in, he noted, was to examine development of efficient, interoperable information exchange systems. The Communication on Stronger and Smarter Information Systems for Borders and Security published by the Commission earlier in the year was a contribution to these efforts, he noted. Particular emphasis has been put on the improvement of existing information systems, possible development of new systems to close some of the existing gaps and improvement of the interoperability and interconnectivity of the systems. He spoke about the three different topics in turn.

In relation to the improvement of existing information systems, Sir King continued with a strong statement that existing systems must be fully implemented and used. The systems offer specific capabilities yet all are not making full use of them. Collaboration can only be effective if rules are transposed and implemented but unfortunately this is not always the case, he noted. Thus, the Commission has initiated infringement procedures against five Member States that don't fully comply with the Prüm Decisions of 2008.

Thinking towards the longer term – a key task, Sir King suggested – he spoke about the challenge of implementing the EU PNR (Passenger Name Record) Directive by May 2018 and particularly the requirement that large passenger information units be set up. The efforts required will be significant, he said, implying that this will be an immensely complex undertaking. Some Member States are still at a very early stage in the process. With this in mind, Sir King stated that the

Photo: Rene Suurkaev
Copyright: eu-LISA

Commission stands ready to give assistance to the Member States, be it guidance, legal assistance, expertise or financial support. An implementation plan will be established in November to guide and support the Member States in their efforts to build the necessary infrastructure.

The challenge of improving the quality of data in systems was also referenced. High quality data is vital for the work of many and often those who input incorrect or incomplete data are not those that have to suffer the consequences, he noted. This problem must be addressed whether through technical, organisational or, if necessary, legal measures. Sir King emphasised the importance of eu-LISA in this work. He also explored some other possibilities for improving the functionalities of existing systems. The development and implementation of an Automated Fingerprint Identification System in the central SIS II will allow national authorities to check individuals against the SIS on the basis of their fingerprints, a development he described as revolutionary and that will positively impact a system that he described as already being a cornerstone of work in European law enforcement and border control. Noting that an estimated 30% of the wanted persons in SIS II travel under a false identity, Sir King stated that the AFIS must be delivered on time.

On the topic of information gaps that need to be addressed, the proposed Entry-Exit System was highlighted. eu-LISA will be in charge of the implementation of this system, he noted, which once in operation will improve the effectiveness of border checks by recording when and where a Third Country National enters and exits the EU. The EU Travel and Information Authorisation System (ETIAS), meanwhile, will allow for prior checks on Third Country Nationals who are exempt from needing a visa to enter the Schengen area.

Finally, in relation to systems interoperability, Sir King added that arrangements around current EU IT systems are complex and fragmented. This can lead to blind spots and cause difficulties for authorities in linking different stream of information. He highlighted the attack against a police station in Paris in January 2016 as an example. According to Sir King, the enquiry afterwards revealed that the perpetrator was registered in 8 Schengen countries under 20 different aliases. Given the current situation, this kind of a lack of connectivity couldn't be tolerated, he suggested.

To counter the security threats of today, new, quicker, simpler and more comprehensive ways must be found to make use of existing data. Given the introduction of a new framework for the protection of personal data in the EU, a close look should be taken at how to better use the latest IT security solutions in a manner that fully respects purpose limitations, access and usage rules, he argued, stressing the importance of fundamental rights and data protection. In particular, he noted that security can only be sustainable if citizens are confident that their fundamental rights are being fully respected, especially when their data is being processed in large scale IT systems. Data in systems should be compartmentalised with different rules for access and use for different categories of users. Interoperability should not mean access to increasing amounts of new data, he demanded, but rather a more targeted and intelligent way of using existing data.

Sir King spoke in detail about the four concepts for the improvement of information exchange via interoperability introduced in the Commission Communication of April 2016. Thus far, the focus has been on the single search interface concept, he noted. On this matter, Sir King added that solutions already exist at national levels, including the X-Road system in Estonia that enables searches across several databases. Nevertheless, development of a single search interface at the EU level would enable Member States to better search for information from systems operated by eu-LISA, he suggested. This centralised interface wouldn't replace national interfaces, but would complement and enhance them.

He continued by adding that the High Level Expert Group on Information Systems and Interoperability is looking into further means of improving information exchange via interoperability and interconnectivity, including the interconnectivity of information systems where data registered in one system could be automatically consulted by another system, the establishment of a shared biometric matching service in support of various information systems and a common repository of data that would provide for a core module common to different information systems.
Sir King expressed his anticipation of the results of the expert group while also noting that the challenges should not be underestimated.

As a final thought, Sir King mentioned that information exchange and interoperability are issues of relevance beyond the areas of internal security, border management and migration. The issues that he spoke about apply to public administration and the efficiency of e-government. No matter the domain of applicability, there is still a lot of work to be done, he stated, and this work must be done together. The Commission, the Member States, the European Parliament, EU Agencies, including the Fundamental Rights Agency, and the European Data Protection Supervisor need to work together. Sir King concluded with his view that the world has and will continue to change quickly; in order to create an effective and sustainable security union, we need to become quicker and smarter.

Hanno Pevkur

Estonian Minister of the Interior

Photo: Rene Suurkaev
Copyright: eu-LISA

Minister Pevkur welcomed everyone to the conference and to Estonia. He started off by reflecting on what Commissioner King had said, adding that a lot of the issues mentioned will be focal points for Estonia's EU presidency and work undertaken thereafter. Specifically on the topic of PNR, Mr. Pevkur suggested that the current state of affairs is confusing. The requirement to collect PNR data applies Europe-wide, he said, yet it is up to every Member State to engage in its own implementation work. This approach is extremely expensive, he argued, as every country and each individual air carrier has to create their own systems. Looking in hindsight, he concluded that the decision for such an approach was a mistake.

On the topic of interoperability and particularly that of Single Search Interface mentioned by the Commissioner, Mr. Pevkur noted that Estonia has its own new border guard system called KILP (Shield). It enables access to all the relevant databases available for border protection and even includes live feeds from satellites and sensors. He added that it's a logical conclusion that PNR information will be linked to this system. However, in relation to PNR, he noted a simple problem confronts Member States – it is not clear at this stage what requirements will be for connecting the national systems to others in Europe. He suggested that eu-LISA could provide support by setting clear rules to ensure interoperability and thereby clarify full system requirements.

Mr. Pevkur continued by speaking about border protection in Estonia. Estonia has 6.5 million yearly visitors from outside of the European Union, he noted. Although only a fraction of the total visitors to the European Union, he emphasised that Estonia takes its communal task of finding travellers that aren't welcome in Europe seriously. Highly capable IT systems are needed. As an example, he went on to reference Estonia's X-Road platform, noting that it is now also being implemented in Finland.

The Minister expressed his hope the High Level Expert Group on Information Systems and Interoperability will inspire both good ideas and concrete solutions for the future. Amongst the issues needing further study, he alluded to the underutilisation of EURODAC, especially in hotspots in Greece and Italy and the sometimes incorrect data being entered into systems.

eu-LISA, he noted, must and likely will keep growing as it implements and maintains current systems while also playing a key role in the development of future systems, including ETIAS, the Entry-Exit System and perhaps some in other domains such as justice and customs. Another role in providing expertise to political discussions was also foreseen. He again emphasised that the Agency could fulfil such a role in work on PNR, bringing together Member States that are in very different development stages – from those that haven't taken any steps whatsoever to those advanced like the UK who have had a system since 2008. Although the challenges ahead are significant, Mr. Pevkur argued, success is unavoidable if we join forces and capabilities. For this to happen, the political will must be present and this is sometimes lacking at this stage, he opined. Nevertheless, he still suggested that in 5 years we will have a safer Europe, particularly given that all databases should be interoperable and used to their full extent.

He finished his presentation by mentioning the importance of fundamental rights and data protection. As an example, he noted that during his time as the Minister responsible for social affairs and health care in Estonia between 2009 and 2012, digital prescription and e-health systems were created. The developments raised numerous questions regarding data protection. At the time, he had argued on the basis of the many physical copies of a person's health file that a general practitioner will typically make that are unknown to the patient. In contrast, every move, inquiry and change in the e-systems can be followed, making tracking of the data and its use easier and simpler for everyone involved. The general principle was that everybody must win – the patient, the doctor as well as the pharmacies. The same principle must apply to systems in the fields of justice and migration, he argued.

Maive Rute

Deputy Director General of the Joint Research Centre, European Commission

Mrs. Rute greeted all participants and started off by speaking about the work of the Joint Research Centre (JRC) of the European Commission in the broader field of security. In relation to this matter, she expressed her interest in the fact that Commissioner King and Minister Pevkur had indicated that security issues are higher in the political agenda than ever before.

She spoke briefly about the JRC itself. Specifically, they are a research institution within the framework of the European Commission. Elaborating, she described the JRC's 6 locations in 5 member states, its up to date research infrastructure complete with facilities and its vast staff at work on various aspects of the Commission's policies. Its expertise includes preparation and execution of simulations and modelling, running various tests assessing occurrences such as earthquakes and their potential impacts on large scale infrastructures and on economic, biophysical and nuclear-related work. In all such efforts, the JRC's role is to support policy making, to collect, provide and analyse evidence as well as to monitor implementation.

Photo: Rene Suurkaev
Copyright: eu-LISA

On the JRC's work in the security field, she noted that within the European Commission, responsibilities for policy lie with DG HOME and DG JUST. The JRC complements their activities as the Commission's knowledge and science service. Mrs. Rute noted the JRC's efforts to enhance EU preparedness to withstand large-scale cyber-attacks, particularly through its support to the EU critical information platform action plan and its exercising of a key role looking for technical solutions to increase the level of realism in all exercises delivered. They are also working to build a classification system in the field of critical infrastructure protection alongside a qualitative measurement system assessing the severity of cyber incidents. Current work emphasises development of capabilities for analysing complex networks, interdependencies, and the economic impact of critical infrastructure disruptions, largely through use of various big data sets. A new related field of research also mentioned was assessment of vulnerabilities from hybrid threats.

Mrs. Rute added that the JRC also engages in research in the domain of maritime surveillance and has expertise in space technologies and data fusion; in the latter case, their work is directly relevant for the strengthening of the EU's capabilities in this area. Further work is ongoing in communication technologies, where the European Media Monitor, a data scraping system, is in place. The JRC harvests a huge amount of multilingual information from internet based sources in order to create the open-source system that provides near real-time monitoring of vast sets of information. The system is currently used for health management, crisis management and security management.

One role of the JRC mentioned was to bring together experts and facilitate their discussion of relevant topics. In this regard, Mrs. Rute spoke of the network of critical infrastructure protection experts that has been established. It more than 200 members and 120 organisations.

Continuing the theme, Mrs. Rute explained that the JRC's broad research is being restructured into knowledge centres through which specialised data and information would flow. The centre should thus become platforms for discussion. Recently, a Knowledge Centre for Migration and Demography was inaugurated to enable closer collaboration with researchers, policy makers and practical end users, she noted.

Reflecting on the interventions of the previous speakers, she agreed that some IT systems in place at the EU's external borders are outdated. Thus, she highlighted the JRC's work to find better solutions. Biometrics are a key factor for this, she suggested.

Work is ongoing at the JRC on biometric video technologies that would enable assessment of threats from a distance, for example. Societal impacts, such as impacts on personal data are of high importance in this work. She also expressed satisfaction that the afore-mentioned High Level Expert Group's work is already paying off, with the elaboration of guidelines for end users on how to apply solutions one relevant example provided. Capacity building and awareness raising related to these guidelines must proceed, she said.

SESSION 2

Tomorrow's technology today: Technological Development as a Driving Force for Change in the Home Affairs Field

The panel session was chaired by Ciaran Carolan, eu-LISA.

The panellists were:

Laurent Beslay, European Commission,
Joint Research Centre

Piotr Malinowski, Frontex Situation Centre

Zsolt Szolnoki, Ministry of Interior, Hungary

The panel session was opened by Mr. Ciaran Carolan, who introduced the panellists and the topic. He expressed an intention to discuss new and innovative technologies that could bring benefits in the Justice and Home Affairs field while also examining the role that technology plays as a force for change in the domain. He began by posing a question on this second point, asking the panellists to provide some introductory words for the panel generally and to specify their opinions on whether technology is merely an enabler of policy development or rather a driver for change.

Mr. **Laurent Beslay** from the European Commission, JRC spoke first. He introduced himself and his work in Directorate E of the JRC, generally focusing on migration and security and specifically on project activities related to law enforcement as part of the Digital Citizen Security Unit that he heads. He has previously worked as a scientific advisor with the European Data Protection Supervisor.

Addressing several technological topics in turn, he spoke initially about cyber-security, focussing on methods and tools for the detection and takedown of mobile botnet activities. He emphasised the need to see technology as a key enabler for policy development. Nevertheless, as highlighted by the topic under discussion, it is also a key enabler for criminals, he noted. Criminal activity is fuelled by three parameters: motive, opportunity and vulnerability. If the value of a target is high enough, he suggested, it triggers the motive. Technology is of high relevance in the cases of the two remaining parameters, he argued. Unfortunately, criminals adapt to technology very quickly. He continued by noting that technology is also a key enabler for law enforcement. The JRC, in its work, aims to provide tools to enable faster, smarter and more solid investigations, improved collection of digital evidence and ultimately successful prosecutions.

Mr. Beslay turned briefly to the fight against organised crime, again an area that he considered highly dependent on innovative and creative technologies. On the interaction between technology and policy, he suggested that in this domain technology is a key enabler for the policy yet it doesn't define it. Rather, the goal in all technological development must be to provide the functional tools that are key for everyday users.

He continued his analysis by referencing a third topic, namely the fight against sexual abuse of children online and in particular the utilisation of video analytics. In this field, biometric technology is key, he suggested, and the future is video analytics. He also mentioned complementary tools and methods – standards for localisation such as GPS and GSM and electrical frequency analysis. He cited the latter as particularly interesting, elaborating that electric grids have fluctuations, noticeable through the flickering of lights, for example. Analysis of these fluctuations in video could lead to localisation. He also spoke briefly about sensor pattern noise analysis. Every time a picture is taken with a mobile device, the sensor leaves a unique fingerprint on the picture, he noted. This fingerprint can be extracted to see whether it can be matched against another picture, perhaps comparing holiday snaps against illicit pictures. Video content can be similarly analysed, he noted.

Biometrics are also important in the field of security and border management, he noted, and he continued with some more in-depth discussion on this matter. If one seeks to consider tomorrow's technological solutions, he suggested that one must consider deep learning techniques for content-based data recognition. He elaborated that it should be possible to identify people by their tattoos yet this isn't possible with today's text based technology. Image-based deep learning techniques should bring improvements.

Moderator: Ciaran Carolan, eu-LISA
Panellists:
Laurent Beslay, European Commission, Joint Research Centre
Piotr Malinowski, Frontex Situation Centre
Zsolt Szolnoki, Ministry of Interior, Hungary

Photo: Rene Suurkaev
Copyright: eu-LISA

As an overriding conclusion to his initial intervention, Mr. Beslay suggested that extra emphasis needs to be placed on 3 key elements: quality of data as part of a stronger private data and privacy framework; assessment of system performance; and domestication of technology.

The second panellist to speak was **Piotr Malinowski**, Head of the Frontex Situation Centre. He also introduced himself, noting that he had a long history in the armed forces before beginning work on various information exchange tasks within Frontex.

Given the timing of the conference, he suggested an obvious expectation to reference the fact that Frontex had taken on a new mantle as the European Border and Coast Guard Agency just a few days previously. Within the new Agency, his tasks will be to build a comprehensive situational picture of the EU's external borders as well as the pre-frontier area.

Mr. Malinowski emphasised the turbulent times in which we live. At the same time as the conference took place, he noted that there were 13 ongoing search and rescue operations on the Mediterranean Sea with almost 1000 migrants involved. He added that there were 10 vessels with almost 1400 rescued migrants on board going to Sicily and within the past 24 hours, there had been 35 casualties among people trying to get to Europe.

Mr. Malinowski added that technology plays a critical role in assuring security, but it has also helped to reduce the number of casualties among people trying to cross the Mediterranean Sea. In addition, technology helps in the fight against cross border crime.

He continued by emphasising the need for interoperability in the work of FRONTEX, a point particularly pertinent given that the Agency's work demands contact with different Member States and other stakeholders. The amount of data to be analysed in or close to real time is vast, a fact that inevitably creates technical issues. Mr. Malinowski also briefly mentioned future technological developments, including the further development of satellite technology for monitoring of the external sea borders. On this matter, he specifically referenced the Copernicus Programme to enhance the capabilities of the EU to conduct satellite observations. He also alluded to Frontex's interest in the use of Unmanned Aerial Vehicles to observe and monitor pre-frontier areas. In this area policy development is lagging behind while the technology is available, he suggested, such that technological development must drive policy evolution.

Mr. **Zsolt Szolnoki** provided some opening words subsequently. Mr. Szolnoki is the Senior High Counsellor for the Deputy State Secretary of EU Affairs in the Hungarian Ministry of the Interior. He also fulfils the role of Program Manager for large scale IT systems at the Ministry, and has been working intensively on the national PNR project. He is a member of the eu-LISA Management Board.

Mr. Szolnoki took some time to look back at the previous decade and some notable developments in the domain of Home Affairs. He spoke of various waves of technological development and innovation in Europe, the first of which began with the accession of 10 new Member States in 2004 and their implementation of new technologies to deal with Schengen related legislation. This wave, he suggested, was completed in 2013 with the go-live of the second Schengen Information System. A second wave discernible relates to the proliferation of biometric solutions, firstly in EURODAC and extending later to other systems for border management. A third wave is ongoing, he suggested, focussed on several new systems being developed.

While technology evolves in the Justice and Home Affairs domain, he chose to emphasise the topic of data usage within the framework of IT and systems that is already in place. He thus continued by speaking about the necessity to find the best ways to utilise existing data. The amount of data collected is vast yet it is frequently not shared with other authorities that could utilise it. Within the Hungarian national PNR project, Mr. Szolnoki mentioned that he coordinates deals on how the Passenger Information Unit can share PNR data. Sharing requires specific solutions, both technical and legal, meaning that some Member States don't even share PNR data within their own country. He emphasised the need for a thorough discussion and a common understanding of data sharing and the requirements for it to take place.

Reflecting on the previous interventions, he alluded to the fact that the human resource aspect of technological evolution is often overlooked. Technologies must be accepted by the users to be successful, he suggested. He provided the example of the Hungarian border guard acquiring a new drone, which all staff sought to pilot. Yet such examples of easy acceptance and implementation are rare.

Finally, considering technologies of the future, he briefly mentioned mobile technology, data mining and artificial intelligence as areas in which developments could be of particular interest.

Mr. Carolan followed up on the final point made and enquired whether Mr. Szolnoki could provide any perspectives on the application domains for future developments, particularly related to biometrics and deep learning techniques.

He suggested that biometric system developments could play a significant role in traveller facilitation, enhancing experiences. He particularly cited touchless systems as being capable of facilitating travel while improving security. He continued by speaking about deep learning techniques, such as tattoo recognition systems, which demand immense amounts of data. Repeating the point made earlier, he stated that this requires reflection on how such data that can be collected, stored and shared.

On the topic of biometrics, the views of Mr. Malinowski on the applicability of biometric solutions to surveillance activities were sought.

He explained biometrics are used in migration hotspots in Sicily and Greece. Every migrant is registered and fingerprinted – a time-consuming process especially in case of ships with more than a thousand migrants on board, he noted. He added that often the usefulness of technology is impacted by external factors, such as slow internet speeds.

Otherwise, Mr. Malinowski suggested that the use of biometrics is limited in the context of surveillance of pre-frontier areas. Sensors used are typically very far from the subjects, he noted. The situation is thus quite different from border crossing points on the external borders where existing advanced technologies are already used.

Mr. Carolan followed up on Mr. Beslay's previous emphasis on the need for high data quality in systems. Given that the capabilities of data analytics have increased substantially in recent years and continue to advance, enabling examination of both structured and unstructured data, he queried whether the need for better data quality mentioned might be overemphasised?

Mr. Beslay restated his case that high data quality remains of fundamental importance in large-scale IT systems. In the future Entry-Exit System, he noted that there will be millions of fingerprints being compared; in such instances, there are multiple causes for potential misreads and these must be mitigated to ensure accuracy in databases of this size. Even something as simple as wiping the scanners after each reading can help accuracy. He added that the JRC has discussed whether to establish best practices or even perhaps worst practices lists for fingerprint enrolment in various situations.

Photo: Rene Suurkaev
Copyright: eu-LISA

Mr. Malinowski concurred, adding that there has been a lot of discussion about social media monitoring and the issues connected with it. Today's technology doesn't offer the possibility of reliably analysing unstructured data, he stated. A lot of time and effort goes into structuring data and such efforts are crucial as data must be available to operational actors immediately. Open source data analysis is problematic furthermore as there are countries and groups of criminals that are masters of misinformation, capable of creating millions of fake accounts to spread invalid information. He proposed that open source data should nevertheless be used alongside data from structured sources such as national databases.

Mr. Szolnoki further added to the pleas for continuous emphasis on high quality data being input to systems, noting that continuous efforts are being made in Hungary in this regard. He provided an example of how such efforts can bring benefits, explaining that 50% of biometric datasets enrolled in Hungary at the beginning of biometric systems rollout were missing at least one fingerprint whereas that figure is now about 6%. He did note that an open source analytics system has been added in addition to the PNR system. In cases where additional investigation is needed, this system will enable analysis of open source information relevant to the subject in the manner put forward by Mr. Malinowski.

Mr. Carolan opened the floor to questions from the audience.

A representative of the Estonian administration wondered how technology could become a driver of policy development in the Justice and Home Affairs area.

Mr. Beslay suggested that this would be difficult and perhaps inappropriate, suggesting that one must always understand business needs before identifying technological needs.

Citing a belief that the world is facing a big change in terms of how technology defines certain elements of life, **Mr. Malinowski** disagreed. The internet has created a society where data is not assessed by whether it is trustworthy or not, or the source of the data, but rather by other criteria. This is the post-fact society, he stated. In this society, he suggested that technology is already a driving force for policy development. This results from developments in the business sector. Nevertheless, he did express a feeling that technology is often not seen as one of the main factors that will shape future policies, not only in terms of border management but for the society as a whole.

Mr. Szolnoki expressed a view that technologies need to be better understood if they are to influence policy making in an appropriate manner. Thus, he emphasised the need for better understanding to be prioritised ahead of political discussions on technological developments. He referred to the example of PNR once more, noting that it was blocked for years, with at least some of the reasoning for delays being misplaced. It is important to show what the results of implementation of new technologies will be and how such implementation can best be done, he argued. Common understanding is key.

Mr. Frank Smith, chairman of the ENLETS Mobile EU working group on mobile solutions for law enforcement alluded to Mr. Szolnoki's reference to mobile devices previously.

He expressed a view that mobile solutions for law enforcement will be a game changer and ever faster development is needed compared to current work. Yet the current development model, he suggested, seems to be that immense amounts of money and time are spent developing systems that remain reasonably static until they're replaced 5 years later. He wondered whether development models should be altered considering the fast pace of change of technologies such as mobile devices nowadays.

Mr. Malinowski disagreed with the suggestion that systems remains relatively static, pointing to the EURODAC system that makes use of state of the art, modern technology despite its implementation many years ago. He did concur with the suggestion that development and implementation processes are often too longwinded, however. Considering that one generally waits for demonstration of a technology's applicability and usefulness in a business environment, before writing specifications and waiting for the results of procurement assessments, it can often take more than 5 years from the time of technology identification to implementation. He suggested that the approach needs to change, proposing that one might look towards creation of self-financed systems that sustain their maintenance, even perhaps though selling certain data in some instances.

Mr. Beslay suggested that strengthening of the link between researchers and operators is key to reducing the time between technology development and implementation. The JRC is doing this as much as possible, he noted, working with operational entities such as EUROPOL on an almost daily basis when developing new solutions.

Moderator: Ciaran Carolan, eu-LISA
Panellists:
Laurent Beslay, European Commission, Joint Research Centre
Piotr Malinowski, Frontex Situation Centre
Zsolt Szolnoki, Ministry of Interior, Hungary

Photo: Rene Suurkaev
Copyright: eu-LISA

Agreeing that the time factor in implementation is crucial, **Mr. Szolnoki** placed much of the blame on the bureaucratic environments in which we live and work. Somehow a solution needs to be found to implement new systems very quickly if the need arises, obviating such obstacles, he suggested.

An industry representative wondered whether the implementation of ETIAS alongside PNR will be a stepping-stone for automated risk assessment of visitors using information from multiple databases, including those at national level. He also wondered about the timeframe for systems interconnectivity as spoken about frequently at events around the conference.

Mr. Szolnoki emphasised that development of national PNR systems are perhaps some way off, and hence discussion on interconnection of PNR systems with other systems may be premature. He elaborated that there is the EU Directive guiding all Member States in the same direction yet levels of development nationally differ greatly. Harmonisation of systems implementation across 28 Member States and facilitation of data exchange is a big challenge, he noted.

From the operational viewpoint, it is crucial that results are available when needed, stated **Mr. Malinowski**. When considering interconnectivity of systems, it must be considered carefully what triggers automatic alerts in order to ensure that there is enough time for operational personnel to react and check alerts against other databases, he argued.

Another industry representative enquired about the extent of data and knowledge sharing on-going with tax and customs authorities.

Mr. Szolnoki indicated that, at least in Hungary, customs authorities are key contributors to PNR data.

As a final point, Mr. Carolan sought short indications from each panellist about the technologies that they would be keeping the closest eye on within the next few years with a view to their applicability in the Justice and Home Affairs domain.

Refraining from putting forward any particular technology, **Mr. Beslay** chose to emphasise the horizontal theme of fundamental rights, highlighting that any technological development will need to consider such rights. He insisted that technologies can always be developed with such considerations in mind - communication interception can be conducted in a privacy friendly way, in compliance with EU regulations, for example.

Mr. Malinowski also refrained from naming any specific technology, but emphasised that new technologies must benefit not only EU and national agencies but also EU society, providing for improved quality of life and also financial benefits.

Mr. Szolnoki mentioned mobile technologies as a specific category of interest while also noting an interest in any technology that can improve data quality in IT systems.

SESSION 3

Enabling Interoperability to Enhance Cross-border Cooperation amongst Law Enforcement Authorities.

Presentation by Richard Rinkens, Coordinator for Biometrics and Identity Management, DG Home affairs, European Commission.

Panel discussion chaired by Raluca Peica, eu-LISA

with

Olivier Burgersdijk, Europol

Richard Rinkens, European Commission, DG HOME

Jan Segerberg, Police Authority, Sweden

Thomas Sommerfeld, Interpol

The session began with a presentation by Mr. Rinkens on Stronger and Smarter Information Systems for Borders and Security.

The presentation was based on the Commission communication of the same name published on 6th of April 2016. Mr. Rinkens suggested that EU citizens expect that border control and law enforcement are done correctly, in a way whereby life in the Schengen area will remain safe and comfortable, noting that the Communication was prepared with this spirit in mind. While it may not set a full basis for truly standardised solutions that can be perfectly implemented, it should be seen as a starting point for working towards better systems utilisation by everyone, he said. The document outlines approaches to making systems work better, individually and together to provide for a seamless experience for all user groups. Examination of all systems in context is crucial, he noted, as data is currently collected and stored separately for each system, with interconnectivity completely lacking.

The communication begins by listing existing systems used for both law enforcement and border control. The Schengen Information System is used in both domains. Mr. Rinkens described the system as the cornerstone for all other interconnected Europe-wide systems. It is large, containing significant amounts of data. It was searched 3 billion times in 2015.

Thanks to eu-LISA, Mr. Rinkens noted, the system works very well. Yet he noted several possible improvements that could be identified. One vulnerability alluded to relates to the fact that passports are used as proof of identity while changes can be made to such identities rather easily in some countries, perhaps even by using someone else's passport. Verification of biometric data in the passport and within the SIS II databases is necessary to detect such simple cases of identity fraud, he argued. He continued by noting that asylum denial decisions aren't stored anywhere, meaning that border guards and police may not be aware that a presenting person has been ordered to leave. Likewise, information on when and where any given person crossed the external border is not stored. Finally, the current information landscape lacks accessible forensic information, he noted. While the Prüm system is in operation, it is an exchange system requiring requests to be sent to partner states in a rather outdated manner.
He wondered, therefore, whether the Schengen Information System might be one system to store such information.

Mr. Rinkens mentioned some improvements proposed in the communication that related to the Visa Information System and Eurodac system. One change put forward was the lowering of the age

Photo: Rene Suurkaev
Copyright: eu-LISA

for fingerprinting. Currently, children older than 12 have their fingerprints enrolled in VIS. In Eurodac, those aged 14 and older are fingerprinted. The aim, he suggested, should be to lower the threshold to 6 years of age across the board. Such a threshold would also apply for enrolment of fingerprints into European e-passports. Such a change would contribute to the fight against illegal smuggling of children into the EU.

On issues related to systems usage, Mr. Rinkens added that EUROPOL has access to SIS, VIS and EURODAC but, for various reasons, doesn't make use of them. One goal, he indicated, must be to further develop strategies to utilise the enormous wealth of information in the EUROPOL information systems.

He continued with some words on the EU Entry-Exit System, reflecting on some of the issues that the system should address. Current procedures imply that during the border crossing, the official has to consider a traveller's previous travel history and to calculate whether he/she has complied with the duration of stay permitted on such previous visits based on stamps from the traveller's passport. This procedure is time consuming and prone to errors, he argued, while also creating a situation whereby people can hide the fact they've overstayed in the Schengen area by simply throwing away their passports. He stated, therefore, that entry records need to be saved in a centralised database that is easily and quickly checked by all operators, regardless of the country in which they are located or the countries that the traveller has entered and exited the Schengen area through previously.

Switching focus to systems interoperability, he described the concept as one that has been shunned for a long time at the European level. Yet interconnectivity between certain systems is of paramount importance, he argued. He asked the audience to consider the hypothetical situation an American traveller presenting at an EU external border. His or her details should be checked against SIS II, national databases, the Interpol SLTD, in case of visa holders the VIS, and perhaps other system. Considering the amount of information that could possibly be retrieved across the various databases queried, it is clear, he said, that a single search interface would make decision-making for the border guard easier. While many national single search interfaces are in operation, all of them work with alphanumeric information, he noted, i.e. none utilise biometrics. Within the communication, the single search interface is introduced as a concept rather than any particular solution that will address the mentioned points and make sure that available information is given in a timely, correct and complete manner to those who need it.

Interconnectivity of systems is one aspect of interoperability described in the Communication and Mr. Rinkens spoke about this briefly. Systems such as the Entry-Exit System and VIS need to be interconnected, he suggested, in order to avoid situations in which a traveller's data will have to be added to two systems separately. Such an interconnection is already proposed in the EES legislative documentation, he noted.

He also emphasised the need for a shared biometric matching service. Fingerprint data is stored in EURODAC and VIS and will soon be searchable in the EES and SIS II, he noted. According to current system development paradigms, this would imply implementation and maintenance of 4 separate AFIS solutions. Rather, it makes sense to use one physical IT service to search for fingerprints in all databases, he argued.

Much of the resistance to creating interoperability is based on misinformation, he suggested, which creates a false image of what is being shared and how such sharing is being accomplished. Interconnectivity, he stressed, does not mean that all data is stored on one server and every stakeholder automatically has access to everything.

Mr. Rinkens concluded by bringing the speech full circle. He again emphasised that the Communication is just a starting point for work going forward. Hard work is underway to bring about change to ensure that European freedom and security will not hit a brick wall, he said.

Reflecting on the presentation provided and the points put forward, Mrs. Peica began the panel discussion by enquiring about law enforcement needs, wondering what needs particularly might be addressed by interoperability.

Mr. Segerberg noted that interoperability facilitates information sharing. Failure to share information that could be used to prevent or solve crimes is a crime in and of itself, he wryly stated. In his response, he focused on so-called business interoperability. In order to successfully share data, one must be sure that only proper and accurate data is sent and that the received data is understandable and usable. Implementation of interoperability will have to be pursued with these thoughts in mind,

He went on to describe the intersection of business processes at border crossing points. Processes include border surveillance, visa processes, facilitation, logistics, resource planning, document identification, fraud prevention, migration –related processing, public security and state security are some that he mentioned. All of the people involved in these processes need to share data, he suggested. When considering interoperability, Mr. Segerberg urged that one must take a holistic view and look at the big picture.

Mr. Burgersdjik stated that interoperability, the need for strengthening of law enforcement cooperation and the need to better use information have been discussion points for some time already. However, only recently has there been new impetus to ensure that we benefit from interoperability and data sharing. He suggested that this is due to changes in crime. For EUROPOL, crucial areas in which better tools need to be provided are terrorism, migration, and cybercrimes, he intimated. These crimes are all detached from a physical location, he noted, meaning that there is more reliance on other entities than ever before when attempting to crimes associated to these areas. While, historically, cooperation in law enforcement has meant police exchanging data, one must nowadays cooperate with coast guards, border guards, customs, and others. Cooperation with private partners is increasingly relevant, he noted. He provided the example of teams taking down botnets, which necessarily includes interaction with telecom providers and internet security companies.

In conclusion, he emphasised that interoperability is increasingly one of the key drivers of progress and success in the JHA field.

Mr. Sommerfeld agreed that a definite change in the needs of the law enforcement community has arisen in the last few years based on the strong terror threat and migration issues. This has led to a common understanding that information must be brought together. Nevertheless, as a former police officer, he also suggested that data sometimes has to be kept separate. In all instances, data should only ever be used for the purposes that it was initially recorded for.

It has become clear in recent years, he stated, that the decentralised model doesn't work anymore. Yes overcoming this model going forward presents challenges. Noting that interconnecting domestic national systems can often be problematic, he surmised that doing so for systems of different member states is even more complicated. While the ideal solution in some ways might be to create huge centralised systems that store all relevant information related to identity, this is not feasible. Therefore, interoperability of already existing data in systems is paramount, he argued. When it comes to persons identification as an example of a typical transaction run against systems, he suggested that the key to implementation will be to set common rules for how a person is modelled in an information system, providing for what data belongs to the entity of a person.

Mr. Rinkens expressed his belief that interoperability will improve the availability and quality of data. Interoperability is all around us already, he noted, being exemplified on the proliferation of mobile phones that heavily rely on data exchange between different systems. Yet when it comes to interoperability of systems, he reiterated, people have unfounded misconceptions.

Mrs. Peica continued by asking HOW interoperability will be achieved.

Once again making a plea for a more holistic view on data utilisation and sharing, **Mr. Segerberg** noted a wish that some legal obstacles to such usage and sharing be removed. He cited a need for law enforcement authorities to use EURODAC more directly as an example, emphasising that such relaxation of requirements can be done while keeping modern data protection rules and standards in mind. He also suggested that a common rule when implementing interoperability must be that if a particular item of data is used often, it must be stored so that it is commonly accessible. PNR is a prime example of this, he suggested. Thirdly, a key element of implementation will involve education, he suggested. Systems that are not used at all or to their full extent become useless, he argued.

He added that an education program is needed at the policy level as well so that policy makers fully understand what can and cannot be done, particularly with regards to data protection access levels and similar.

Mr. Burgersdjik agreed with Mr. Segerberg on the need for a holistic view. He emphasised the need for standards that facilitate cooperation between parties while each party can still work in his/her own environment in accordance with his/her own needs and operational realities.

Mr. Sommerfeld stated that a prerequisite for operational functionality is to assure that information is stored and available where that information is needed. Thus, a first step towards fully functional interoperability is making sure that tools already in place are fully used. In the case of Interpol's tools, he noted, multiple stakeholders utilise them heavily, but others either fail to use them at all or do so only to a limited extent. He elaborated that Interpol is conducting an exercise to find out which police relevant databases exist that are shared between at least two countries. The first partner for the project is eu-LISA, he noted. The aim is to provide a picture of what the realities are, to identify gaps that need filling and additionally to elucidate any unnecessary overlaps in data.

In the domain of standardisation already referenced, Mr. Sommerfeld added that law enforcement is lagging quite far behind. Adoption of standardised solutions is the basis for creating true interconnectivity, he argued. While the process of standardisation adoption may be slow and involve many steps, he argued that it's worthwhile to proceed with such efforts, providing the example of firearms interoperability as evidence for his conviction. There is firearms information in SIS II and the Interpol iARMS and hence a natural desire to create a one-stop solution for border guards and law enforcement officers in the field. The first necessary step in creation of such a solution is the elaboration of a common definition of the firearms data model – work that is currently ongoing, he noted.

Mrs. Peica proceeded to ask the panel for their opinions on what mix of identifiers (alphanumeric and biometric) could provide us with one trusted identity across future interoperable systems.

Mr. Rinkens explained that currently, biometric data present in any large-scale IT system is linked to an identity in that system. Fingerprints alone do not identify a person, he noted; this data must be linked to a reference point, i.e. to some repository where the data is linked to an identity. The most common example of this repository is the passport, he stated, as it details the person's identity and links it to some biometric data stored therein. On the topic of a single trusted identity, he suggested that the identifiers to be used can then vary. For travelling, he postulated that use of a facial image and one fingerprint should be enough but in cases of suspicion of criminal activity, use of 10 fingerprints may be warranted as several databases may need to be searched. He suggested that a key task is to identify the minimal set of data needed to perform the tasks that one has set out to do.

Photo: Rene Suurkaev
Copyright: eu-LISA

Mrs. Peica asked the panellists to name one challenge that needs to be overcome in order to achieve interoperability.

Reiterating and emphasising some points already made, **Mr. Segerberg** referenced requirements to fully utilise the technology that is available, to ensure that policy makers understand how technology can be used in a proper way and to ensure that the operators of any given technology are educated on its usage.

Mr. Burgersdjik highlighted the need to incorporated interoperability needs into the design and development processes for new systems and databases. Early definition of the requirements for interoperability is paramount to ensure the long-term functionality of these systems, he argued. While investments in interoperability are unavoidable, he felt it crucial to emphasise that they are just one of a multitude of investments undertaken at the same time. They also take a long time to finally pay off, he added, noting that all parties need to be aware of this at the outset. In all of this work, the scattered nature of the parties involved makes it harder to achieve results. Each stakeholder has their own interests and priorities that need to be recognised, he suggested.

Mr. Sommerfeld suggested that the biggest challenge is to retain the discipline required. Proposals for new systems normally arise from a concrete need, he noted. Yet having the discipline to slow down and display patience is a necessary skill.

The panel turned to the audience for some brief questions.

A representative of industry asked about the timeline for interoperability.

Mr. Rinkens spoke on behalf of the High Level Expert Group on Information Systems and Interoperability when noting that an interim report on the Group's activities will be released in December 2016 and a final report in June 2017. The reports, he suggested, will include some significant and necessary ideas. Obviously work on these ideas will proceed thereafter, implying that many developments will likely not be ready by the end of 2017. Nevertheless, work on some initiatives has started, he noted. The SIS II AFIS is well on its way to being implemented, while progress on the legislative process for the Entry-Exit System continues. He did acknowledge that, although work is underway and concrete plans are being formulated, there is no answer to the question of when interoperability issues will be solved.

Mrs. Peica concluded that the work underway represents the first steps of a long journey. Yet we should be satisfied that these first steps have been taken and there will be more to follow, she suggested.

Another audience member wondered how one can engage citizens in order to improve the quality of data in large-scale IT systems?

Mr. Burgersdjik expressed his belief that normal EU citizens don't really need to be involved in efforts to improve data quality. What is rather needed, he argued, is to have common criteria on how information is used and evaluated.

Mrs. Peica summarised the main conclusions of the panel. The panellists had agreed that interoperability is achievable but only if legislative and technical challenges are overcome and only if all involved parties agree to work together towards common positive goals. Furthermore, interoperability assumes a common language, she noted, which means more than a common dictionary. In fact, it implies common usage of information by all, she said. Standards are important in this regard, being crucial for harmonisation of the information collected and shared, technology and data exchange.

Olivier Burgersdijk, Europol
Richard Rin ns, European Commission, DG
H E
Poli Auth Sweden
ol

Photo: Rene Suurkaev
Copyright: eu-LISA

SESSION 4
Information Sharing in Border Control: One Stop Shop and Related Concepts

The panel session was chaired by Ciaran Carolan, eu-LISA

The panellists were:

Aleksandrs Gromovs, JHA Counsellor, Latvia

Zahouani Saadaoui, European Commission, DG TAXUD

Frank Smith, ENLETS Mobile

Paul Sturm, Ministry of Security and Justice, the Netherlands

Mr. Carolan noted that the main aim of the panel was to look at interoperability in general, but with a particular focus on the concept of the single search interface introduced earlier in the conference and its usefulness in the border control context.

He also introduced the panellists, looking forward to their contributions based on expertise in customs border checks and mobile devices and their various national and European perspectives.

Mr. Saadaoui began by noting that many of the key issues discussed earlier in the day – data quality, harmonisation, interoperability with legacy systems and big data – are also of utmost importance in customs work and relevant in terms of how customs interfaces with other authorities at the border.

He elaborated on the one stop shop solution that the European Commission have developed, the so-called customs 'single window' solution that he considered may be considered in all work on interoperability going forward. He described the great volume of customs-relevant documents presented at EU borders, the considerable variation in terms of agencies operating and standards in place, and the variability in certificates, permits and licenses as some of the challenges presenting in his domain of work. Legislation often provides authorities with certain competencies for checking documents at the border, leading to a paper-based process that is inefficient and a burden on trade. The single window solution was designed to solve these communication issues and facilitate trade by providing for electronic facilitation of customs procedures. It interfaces various agencies, providing them with the information they require. It is based on international standards and recommendations, among them, for example, the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) recommendation number 33.

To further define the single window from the customs standpoint, he explained that it is a facilitating system that allows the parties involved with trade and transport to standardise information. There is one entry point to fulfil all import and export requirements. The single window provides business-to-government (B2G) and government-to-government (G2G) components for facilitation and information access. Benefits related by Mr. Saadaoui included (for governments) improved risk management and improvement in the collection of revenue and (for traders) reduced paperwork, higher productivity and more transparency.

He continued by noting that at policy meetings, it is clear that there is political will amongst Member States to implement these kinds of interfaces at the borders. The implementation of the EU customs single window itself then leads to harmonisation of national policies across the EU.

On the topic of data quality, Mr. Saadaoui mentioned that the single window adheres to international standards and, in sending and receiving information flows and messages, is in compliance with the World Customs Organisation data model. Furthermore, he explained that an EU customs data model has been prepared for EU needs that is in line with the WCO customs model, thereby ensuring interoperability with other relevant systems.

Some functionalities provided by the single window mentioned during the presentation included validity checks on certifications in terms of their reference numbers and consistency checks against information declared by economic operators.

Mr. Saadaoui went on to note that in 2008, the EU Electronic Customs Decision was made. Furthermore, the Union Customs Code provides the legal basis for the completion of the computerisation of customs and applied from May 2016. Interestingly, he noted, it outlines full dematerialisation with the aim of having a fully digital customs service in the EU by 2020. With this in mind, the single window will be evolved further. It already has business and government elements while there are local and regional variances. Its functionalities will be rolled out in stages as it evolves while always retaining focus on the key concepts of interoperability and data quality.

Speaking briefly about DG TAXUD itself, Mr. Saadaoui noted that that they offer a service for customs, providing information from the back end. There are a number of EU level certificates, for example, for phytosanitary imports issued by DG SANTE, which are connected to databases where the certificates are stored. In such a manner, DG TAXUD seeks to transform data and make it understandable for each authority that operates in the field. Among others, there are liaisons being put in place with the European Chemical Agency (ECHA) to connect with their databases and provide information for customs about ECHA-certified products.

Summarising, it was noted that general benefits of the single window include interoperability with a high level of data quality, real resource savings for operators as well as administrators on account of reduced administrative burden, facilitation of customs controls and reduced risks of human error and fraud. It was suggested that the single window may, to some extent, be seen as analogous to the single search interface, in that its development faces the same challenges, some related to the same legacy systems and the fact that an overarching solution is sought to provide end users with the necessary information in a timely manner. Thus, as efforts towards increasing interoperability in border management systems proceed, lessons learned should be borne in mind.

Paul Sturm followed with some thoughts from a national perspective. He stated at the outset that systems are useful only when they can be of assistance to actual users. In this regard, appropriate governance structures must be in place to provide the ideal solutions to these users, he noted. Within the Netherlands, as depicted in an organisational chart presented on screen, the large-scale IT systems used at borders are managed at the ministerial level through a separate Migration Coordination Department that works with relevant organisations in the field such as the police, the INS, the Royal Dutch Border Control and reception organisations on questions of migration. Thus, the central IT structure supports the needs of these customers in the field of migration. The central structure includes a database with personal identification information, fingerprints and photos, information about rights of stay in the country, related information about a person (e.g. whether they are an asylum seeker, student or worker), and one unique central ID number of each person that is used by all organisations in the Netherlands. The system is accessible to all stakeholders and thus eliminates the need for paper-based solutions.

He continued by arguing that the unique central identification number and the biometric information stored are both key elements, the former for data organisation and connection and the latter for verification purposes. Thus, these data items are stored in a central system that is queried by other system instances. In order to avoid storage information that would be irrelevant in the future, only basic information is stored at the central level, he noted. Structured information exchanges with the central system can proceed rendering processes fast, efficient and accurate. Interfaces with the data system are tailor-made for each organisation to best suit their needs. Benefits of this architecture include easy system expansion and convenient generation of management information and statistics that guide day-to-day work in the migration field.

This way of organising work also makes the one-stop-shop solution possible, he noted, demonstrating the system with the example of an asylum seeker coming to the Netherlands. He guided the audience through an animation of the reception process involving fingerprinting, registration and data matching through a one-stop-shop solution.

Considering a European single search interface and interoperability, Mr. Sturm put forward some thoughts based on the Dutch experiences. He stated unequivocally that any EU single search interface should not disrupt processes already in place nationally and must be able to accommodate national technical solutions. Currently, there are different central interfaces for the SIS, EURODAC and VIS systems and he suggested that there would be definite benefits arising from standardisation based on biometrics. Standardisation also means more interoperability and ease of use, he said. The path ahead is not fully clear, he suggested – at the process level, there are still issues to work out in terms of what should be connected. What is very clear, he stated, is that at the operational level, business needs should be evaluated before all systems are connected. He concluded with a plea to look more at the user processes, and to base solutions on these evaluations rather than technical solutions alone.

Photo: Rene Suurkaev
Copyright: eu-LISA

Frank Smith presented his views based on his experiences working in border management in the UK before continuing with some points specifically on the relevance of mobile solutions to discussions on interoperability.

He first presented the system for processing advanced passenger information in the UK as relevant to discussions on interoperability facilitating border checks. The UK built a system that is similar to that used the Netherlands although passenger traffic is particularly high – the UK receives around 100 Million arrivals per year – implying significant amounts of data and hence a long process for system development. To deal with this, the UK built rolled the system out gradually. Liaison with carriers during preparation work was critical but undertaken successfully, meaning that over 100 different airlines are now connected. The system is now functioning well and enables advance risk analysis on arriving passengers.

Considering biometric systems in the UK, he noted that the police's automated fingerprinting system is in its 3rd generation police. The second generation national migration system connects to it and has expanded exponentially with the introduction of biometric passports. UK authorities, now considering the ageing of the solutions, are considering whether to recreate the systems or rather establish a new biometric system on top of those systems existing. The latter, in fact, appears to be the likeliest choice at this point. Mr. Smith clarified that in this case, as in many, the solutions appear simple yet in technical terms it is highly complicated work.

He switched his attention to mobile solutions, speaking in depth about the MEOS system in the Netherlands as an example of a comprehensive and cleverly integrated solution. He demonstrated its usefulness by providing the example of a speeding driver who is pulled over. The mobile device's camera scans the licence plate and recalls the appropriate records based on automated number plate recognition, enabling recall and presentation of the driver's photo from the national license database for verification. All data from the license is recalled along with information from the event so that, with the push of a button, the officer can send the information to the server that issues the penalty message. The system is a huge improvement in terms of accuracy and efficiency, he argued.

Reflecting on some benefits of interoperability and some of the challenges of implementation, he finally mentioned his previous experiences with the personnel and financial planning system developed within the Home Office. Within this system, instead of just updating the personnel system and payroll system separately, personnel changes would be sent to payroll automatically, essentially halving the human workload. Yet the implementation was erroneous, with it soon being noted that that the HR system had not been updated sufficiently.

Critical data items subsequently had to be realigned and corrected, requiring 18 more months until the joining interface could be switched on once more. Mr. Smith emphasised that the systems in question had just 20000 records. Considering that Europe speaks of interfacing systems with millions of items, the challenges are profound, he suggested. If data isn't properly aligned, he warned, full systems might fail. He encourages, therefore, consideration of middle-way solutions that may not require absolute alignment and that are more tolerant towards deviations. These solutions may be necessary as full alignment might not be possible, he argued.

The final intervention was delivered by **Aleksandrs Gromovs**, who noted that Latvia has been considering interoperability and interconnections for some 10-15 years now. Back then, registries had been built separately, contained different information and were accessible to different users and authorities. Indeed some registries were still paper-based. Interoperability of law enforcement systems was seen as a cost-saving measure and was therefore undertaken leading to the go-live of an integrated system for home affairs in 2000. That system, he noted, is still in use today. Despite the age of that system, he suggested that it is advanced, although upgrades are being actively considered. As it would not be feasible to rebuild the system, he argued, an interim solution being pursued involves the use of virtual IT solutions.

Referring to its IT infrastructure for border control, Mr. Gromovs mentioned that like other Member States along the periphery, Latvia has developed a national Entry-Exit System (EES) that went live in 2000. It has more recently been upgraded and continues to operate. Further upgrades are planned in 2017 that take into account the outcomes of the Smart Borders pilot and the discussions at EU level on the current EES proposal.

Zahouani Saadaoui,
DG TAXUD
Frank Smith, ENLETS Mobile
Paul Sturm, Ministry of Security and Justice,
The Netherlands

Photo credit: Rene Suurkaev
Copyright: eu-LISA

Mr. Gromovs also expressed a desire to focus on people and specifically end users in discussions. He noted that within work to centralise ICT services around 2008, procedures and processes, including those for secure administration and IT infrastructure, had to be defined in accordance with best practices. Thus, it was necessary to conduct extensive interviews concerning systems and services to identify gaps and to ensure user perspective and expectations were taken into account. The aim was to treat the user as a client. It was not a simple task, he said, as practitioners tend not to be selective about their needs, expressing a need for almost everything. Yet upon detailed investigation, fast access, provision of reliable and usable information, the possibility to request information for cross-border investigations, convenient access and good technical support were clearly the most important demands, along with the requirement that all work could be undertaken through a single window on one work station.

Concluding, he suggested that this experience, along with similar work undertaken, indicated that when speaking about a single search interface and interoperability, end users have to be consulted to find out their actual needs. He also mentioned the importance of carefully considering what data is collected, where and how it is stored, who has access and how such access is managed and when and how data is shared.

Mr. Carolan followed up requesting some national perspectives on what the EU could include in a single search interface for border control to enable efficiencies while avoiding replication with existing national systems.

Mr. Gromovs proposed that uniform standards and message formats need to be looked at – work that would also be useful for a future EES, he noted. He suggested that one could consider support for fallback in case of failures at the central EU or national level. Without a paper visa sticker to carry out manual comparisons, could IT provide the necessary information, he wondered. With this in mind, he wondered whether an SSI or the EES NUI, with temporary data storage could play a role. On the topic of data quality and using the EES as an example, he wondered whether control of data input could help to avoid mistakes in the registration of entries and exits.. The aim would be to enforce some minimal data for the border guards and to ensure that there are no negative effects on travellers.

Mr. Carolan put forward some other possible benefits of an EU single search interface solution, including work flow improvements, facilitation of interrogation of new data systems and the introduction of standardized analytics and asked the national representatives about their interest towards such solutions.

Mr. Gromovs suggested that a common data repository would definitely be something to think about as it would help with data quality and deficiencies in the data entered. Whether it would be possible, he queried, is another issue.

Mr. Carolan connected the question of feasibility to what Mr. Sturm had said earlier about the inclusion of an individual ID and biometrics in a central system and wondered whether this was a paradigm that could be pursued.

Mr. Smith added that operational borders need to keep functioning at a fast pace. Thus he questioned whether an EU interface should display queried background information or have a simple green light/red light solution with forwarding of any red lights to the second line of control. All possible solutions have to be hands-on, lab tested and proven to be optimal before any national rollouts, he stated.

Mr. Carolan asked Mr. Saadaoui to elaborate his thoughts on targeted and intelligent use of data. Different end users, to some extent, will need different things and thus shouldn't a 'single' search interface have customized interfaces for different instances, he wondered.

Mr. Saadaoui agreed, noting that the customs single window was presented as a business transformation with information being provided on a need basis enabling its variable exploitation by different partners. He reiterated the need for early identification and engagement of users and partners. IT interoperability can only facilitate business interoperability, he argued, an early assessment of required services is crucial. On the topic of a common repository, he noted that there is an important project underway within the customs domain aimed at upgrading import control systems at EU level that will have a common repository handling millions of declarations. He suggested that this could present an opportunity for collaboration.

On the question of big data, Mr. Saadaoui referenced first the need to consider who owns the data and how it is handled. In the customs case, the end user data is only held at Member State level or by economic operators. Any use of that data thus needs to be agreed with each Member State or other data owner individually. Nevertheless, he stated that there is now some reflection at EU level on the matter of data analytics. The first goal is to understand the different concepts, after which consideration may be given to application of solutions in the community with different owners of data.

Closing words

Mr. Krum Garkov, Executive Director, eu-LISA

Photo: Rene Suurkaev
Copyright: eu-LISA

Although the conference was drawing to an end, **Mr. Garkov** urged the audience not to think of it as an end but rather as the beginning of the next steps in a common journey on the way towards interoperability, more efficient information systems, and more and better use of IT in the Justice and Home Affairs domain. He said it was clear from the interventions of the Commissioner and the Minister in the morning that there is now a widespread recognition that technology is very important today and will continue to be crucial tomorrow as developments continue in this policy area.

He expressed hope that everyone drew some new information or insights from the exchanges and panels. He also wished that everyone present would continue together on the journey towards implementation of some of the concepts discussed at the conference. At the end of the day, he said, technology is just a tool and it has to support practical policy development.

To conclude, Mr. Garkov thanked the panellists and facilitators for contributing to the conference and ensuring its added value. He hoped and believed that the exchanges would sharpen the axe for future challenges and formally closed the conference.

Conference Organiser:

eu-LISA,
European Agency for the operational
management of large-scale IT
systems in the area of freedom,
security and justice

EU House
Rävala 4
10143 Tallinn
Estonia
E-mail: communication@eulisa.europa.eu

eu-LISA is the European Agency that ensures 24/7 operational management of the European Union's (EU) largest IT systems and their respective communication infrastructure in the area of freedom, security and justice: Eurodac, SIS II and VIS.
With information technology, eu-LISA safeguards the EU's internal security and supports the implementation of asylum, migration and border management policies for the benefit of citizens.

www.eulisaconference.eu
www.eulisa.europa.eu

ISBN 978-92-95208-47-6
doi:10.2857/837842
Catalogue n°: EL-01-17-042-EN-N