Brussels, 07 October 2022

CoESS-Euralarm Joint Declaration

The European Security Industry, represented by CoESS and Euralarm, expresses its serious concerns about the present proposal for an EU Data Act and calls on European Parliament and Council to exclude data related to the provision of security services from the scope of the proposal.

- We understand the value of data-driven innovation for the EU economy and support initiatives that promote the secure, free flow of non-personal data, if it benefits citizens and businesses.
- Holding security-related data generated by security systems is subject to specific criteria and safeguards and in certain cases, legislation, no matter whether it is held by public or private entities, and the same should prevail for the exchange of such data.
- We note that security-sensitive data held by public authorities is excluded from the present proposal's scope as per Art. 1.4. This should be extended to security-related data held by security services in general.

CoESS and Euralarm believe that the proposal for an EU Data Act extensively lifts barriers for the sharing of security-sensitive data that is generated by security systems and held by private entities, creating serious security risks.

- Security-sensitive data generated by security systems that is covered by the scope of the proposal includes video surveillance recordings, screening images, alarm signals, and operational data in case of an incident or ongoing alarm and crime prevention response, among others.
- Such security-sensitive data is not only held and processed by public authorities, but also our members, including security technology manufacturers, security service companies and private security companies.
- Our members have adequate frameworks in place to share such data with clients, including specific safeguards (e.g. legitimate interest during and after an incident, security clearances).
- The provisions of the proposal legally challenge these safeguards and oblige our members to share security-sensitive data on electronic request without undue delay with clients and third parties as per Chapter II.

Consequently, the proposal creates severe vulnerabilities in cyber and physical security without legitimate benefits to the client, putting at risk citizens, businesses and perimeters that we are committed to protect (see cases in Annex II).

CoESS and Euralarm therefore recommend the amendment outlined in detail in the Annex I to this Joint Statement.

CoESS *is recognised by the European Commission as the European representative of the private security services – a labour-intensive sector with 45.000 companies and 2 million security officers. CoESS is actively engaged in EU Sectoral Social Dialogue and member of diverse EU Expert Groups, such as the EU Operators Forum for the Protection of Public Spaces. (www.coess.eu)*

Euralarm *represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our Members make society safer and more secure through systems and services for fire detection, extinguishing systems, security systems and alarm receiving centers. (www.euralarm.org)*

ANNEX I – PROPOSAL FOR AN AMENDMENT TO THE EU DATA ACT PROPOSAL

Main arguments

Allowing access to data related to security activities without proper safeguards may compromise customers' security and, in fact, the whole performance of the security system/infrastructure itself. Thus, any access to data related to the provision of security services should be exempted from this regulation as it is the case for those data related to security linked to public activities.

Main arguments to consider:

1. As data related to security activities are related to critical and very sensitive operations and procedures, access to this Data would allow a very high level of knowledge of the installation and performance of the service. This would result in a very high risk of security breach not only for a given customer installation but could also can compromise the whole security system itself.

2. Moreover, access to pure operational data/metadata does not provide any benefit to the end customer, nor does it allow for a smoother switching of providers. Therefore, there is no benefit in allowing/imposing any requirement in the way the data have to be accessed, exchanged or managed.

   In the same sense, and as it is covered by Recital 34: "*In line with the data minimisation principle, the third party should only access additional information that is necessary for the provision of the service requested by the user. Having received access to data, the third party should process it exclusively for the purposes agreed with the user, without interference from the data holder.*"

   In case of a security service, no data is necessary for the provision of the service by other providers in case the user switches his security provider.

3. In addition, there is a need to harmonize the EU Data Act with the security obligations laid out in GDPR (specifically Art 32),

   Recognizing the fact that sharing detailed communication data of a system might cause compromising the security and integrity of that system. As such, the EU Data Act should contain a provision acknowledging the obligations of the data holder (controller) to maintain security of processing (GDPR Art. 32) when transferring data **and exempt data** that could compromise the security of the system and risk the rights and freedoms of other people using such system.

   Thus, it is proposed that the EU Data Act exempts sharing of data that could compromise the integrity of a system and by extension, forcing the data holder to breach the security provision in GDPR Art. 32 of other data subjects using the same system.

4. Directive 2006/123/EC on services in the internal market, also exempt private security services form its application (art. 2.2 k), and the same arguments should apply in this case.

Proposal:

In this sense we would propose the following AMs to exempt data related to the provision of security services:

Recital 60:

"For the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes, public sector bodies and Union institutions, agencies and bodies should rely on their powers under sectoral legislation. This Regulation accordingly does not affect instruments for the sharing, access, and use of data in those areas.

In this sense, access to data related to security or for the protection of customers are not covered by this regulation, especially those that can create a breach of security for a given security system.

Therefore, this Regulation should not apply to situations concerning national security or defence, and shall neither affect the collection, sharing, access to and use of data for the sole purpose of providing security services."

In this sense we would propose a **new Art. 1.4a:**

"Except for Chapter V, this Regulation shall not apply to the collection, sharing, access to and use of data generated by security systems or for the sole purpose of providing security services to the user."

And a definition of "security systems" and "security services" **in Art. 2.:**

(21) 'security systems' interconnected series of electronic equipment and devices which is designed to discourage crime. It may include intrusion detection, access control, audio and video equipment, other electronic systems which emit or transmit an audible, visual or electronic signal warning of security violation and provide notification of events that jeopardize the safety of life or property.

(22) 'security services' services aimed at preventing, detecting and protecting against criminal acts or unlawful interferences, without prejudice to national legislation, also including installation and maintenance of security systems.

ANNEX II – CASE EXAMPLES

Case #1: Aviation Security Services

Aviation security services handle a large range of data on behalf of private and public airport operators – including alarms and assessments on hazardous and prohibited items, or video recordings of security check and other areas – just to name a few. The provisions in Chapters II-IV of the EU Data Act would open a loophole for wider sharing of such security-sensitive material, leading to substantial security threats at airports – e.g. by revealing to criminals operational response data, security check procedures and crime prevention tactics.

Example #2: Critical Infrastructure Protection Services

Data that is handled by security companies, which are protecting privately operated Critical Infrastructure, can include video surveillance records of protected perimeters, alarm signals and operational data in case of an alarm response. If such data falls into the hands of organised criminals or terrorist networks due to the lack of adequate safeguards, either through insider threats within the operator or by sharing of such data with third parties, this could lead to a substantial threat to public security. In its current form, Chapters II-IV of the EU Data Act would unnecessarily faciliate the sharing of such senstive data if it is held by private security companies without real benefit to the client itself.

Example #3: Remote Monitoring and Alarm Response Services

Remote monitoring and alarm response services are provided for a large range of clients, including diverse supply chain facilities. Data handled in these services include alarms and video recordings. If clients receive the right to have access to this data, and request the sharing with third parties, this could lead to substantial security loopholes at the protected perimeters. We also note that there are shortcomings in the definition of "data processing services" as per Art. 2.12. As it stands, remote monitoring could be covered by the scope of this definition, although security companies in remote monitoring do much more than processing data. They assess the adequacy of alarms and video footages, and set in place operational response, if needed. This additional issue reinforces our conclusion that the present proposal is inadequate to the security industry in various aspects.