Position Paper

Euralarm Position Paper on proposed Data Act – 7 October 2022

1. Introduction

Euralarm, the European association representing the electronic fire safety and security industry, welcomes the initiatives from the European Commission towards legislations promoting the data economy. This Position Paper addresses a particular concern regarding the draft Data Act as published on 14 March 2022. We would like to stress on specific provisions that, if enforced as intended in the present draft, would generate security risks.

2. Our concern

Chapter II of the proposal makes mandatory the sharing of data with third parties. Allowing access to data related to security activities without necessary technical and organisational measures (e.g. ensuring proper qualification - expertise and/or authorisations) can compromise customer´s security and the whole performance of the security system itself without any benefit for the user.

Data related to security activities are linked to critical and very sensitive operations and procedures. With access to this data, it would be possible to gain a very deep understanding of the installation and performance of the system or service. This would result in a very high risk of security breaches, including cybersecurity breaches, not only in the case of a given customer installation but also with regard to the whole security system itself. The annex to the present Position Paper provides some illustrative examples.

Furthermore, the criticality of data generated by security systems (e.g. video surveillance systems) is already recognized by national laws regulating private security and the installation of video surveillance systems. These laws limit the right to share information related to or generated by these systems. We therefore would like to stress that the data sharing provisions of the draft Data Act are in conflict with these national laws.

Finally, access to pure operational data/metadata does not provide any benefit to the end-user, neither allows a smoother switching of provider. Therefore, there is no benefit in allowing/imposing any requirement in the way the data have to be accessed or managed.

3. Our proposal

Euralarm proposes the following amendments to the draft Regulation in order to exempt security-related data from the obligation of sharing.

The existing Recital 60 should be complemented as proposed here (bold characters):

"*(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 addition, acknowledging the sensitive character of data related to security systems or for the sole purpose of providing security systems service or private security activities, access to data related to

security or for the protection of users are not covered by this regulation, especially those that can create a breach of security, including cybersecurity, for a given security system.

Therefore, this Regulation shall 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 to the user."

In order to implement this intention, Euralarm proposes a new Article 1(4a) as follows:

"This Regulation shall not affect the collection, sharing, access to and use of data generated by security systems or for the sole purpose of providing security systems service or private security activities to the user."

and the following definition for each of the two key terms to be added to Article 2:

"(14) Security system: interconnected series of electronic equipment and devices which is designed to protect the safety of life or property. It may include intrusion detection, access control, audio and video equipment, fire detection and fire alarm systems, other electronic systems which emit or transmit an audible, visual or electronic signal warning of security or safety incidents and provide notification of such events.

(15) Security systems service: monitoring or remote monitoring of electronic security alarm systems, such as burglar and fire alarms, including their installation and maintenance. (NACE Rev. 2 80.2)"

3. Conclusion

Euralarm has stressed a security concern regarding the mandatory sharing of data related to security systems and services.

We have put forward proposals supported by specific arguments to avoid security breaches potentially generated by these provisions for mandatory data sharing.

Services Directive 2006/123/EC excludes private security services from its scope via Article 2(2)(k). We therefore believe that a similar exemption in the Data Act should be feasible.

We remain available to further discuss these proposals.

About Euralarm

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 secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm members are national associations and individual companies from across Europe.

Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

DISCLAIMER

This document is intended solely for guidance of Euralarm members, and, where applicable, their members, on the state of affairs concerning its subject. Whilst every effort has been made to ensure its accuracy, readers should not rely upon its completeness or correctness, nor rely on it as legal interpretation. Euralarm will not be liable for the provision of any incorrect or incomplete information.

Note: The English version of this document, [document number], is the approved Euralarm reference document.

Annex

Practical examples illustrating the need to exempt private security systems and services from the requirements of the EU Data Act

B2C example: residential alarm system

A private customer wants to protect his home by means of a security system such as an intruder alarm system. The private security company provides this security system which consists of physical components at the premises of the customer (e.g. control panel, sensors, window contacts) that are connected to a digital platform. This allows to monitor the status of the security system remotely, evaluate the data and take action as needed, either by the customer himself or by a service provider through a security alarm centre.

The data collected and handled in this case is obviously very sensitive as it contains information about the premises, their occupants and the way in which both are protected. Misuse of this kind of data can lead to security threats, including cyber threats and danger to the wellbeing of people and integrity of property. For this reason, security service providers are taking very serious measures to ensure the confidentiality and integrity of the data on the basis of contractual obligations. Any requirement to share this data with the customer or third parties, as envisaged under the EU Data Act under Chapter II, poses the risk of data being exposed, intentionally or unintentionally, and consequently the risk of data being misused.

Furthermore, such systems are designed and installed according to specific customer needs and requirements that can vary considerably from case to case. A security service provider's business model is based on its digital platform and the way it processes the data to provide an added value to the customer. Such data can be used to reconstruct business-critical information about the working and technical aspects of the security system and platform. Sharing such information with the user increases significantly the risk to see this data being divulgated which would result in competitive losses and makes it unsustainable, especially for small providers, to invest in developing a security solution.

B2B example: protection of critical infrastructure

Video surveillance, access control systems and fire detection systems are used in a wide variety of public environments to protect people as well as property either inside buildings or as part of perimeter protection measures. This includes critical infrastructure such as airports, train stations, hospitals and power plants. In many instances, these systems are operated by private companies and the data is being handled by the operator or a private security company. Data that is usually generated in these cases contains sensitive information, including video surveillance records, alarm signals and biometric data of employees for access control.

In its current form, the Data Act draft would facilitate the sharing of this sensitive data being handled by private security companies or operators, even though it is directly related to public security. Sharing the data, e.g. with third parties, would create manifold risks for public security, given that the data allows to fully understand the technical aspects of the system and the way it is operated. This could mean that organized crime, cyber crime or terrorist networks, once they gain access to this information, can find ways to circumvent the security measures in place. At the same time and in comparison, the benefit of sharing the data is neglectable.