Position Paper
European Commission Proposal for an EU Data Act

Brussels, 08 August 2022

The Confederation of European Security Services (CoESS) welcomes EU initiatives that promote the data economy, but is wary in this paper of the EU Data Act's impact in public and private security. Concretely, CoESS calls on the EU legislator to exclude private security services, similar to the field of public security, from the scope of all Chapters except for Chapter V – hence all Chapters except the sharing of data with public authorities in case of an emergency.

While there is manifold potential in empowering businesses and citizens of the data they produce, it can also be highly detrimental to the legitimate need to protect citizens, infrastructure, and information from organised crime. Where the data is sensitive and can impact security, public or private, CoESS believes that a balance needs to be struck by closing a loophole in the proposal: excluding private security services its scope, similar to the field of public security.

The private security industry provides a wide range of services, both for private and public clients, ranging from Critical Infrastructure to public spaces, supply chains and government facilities. Traditional services include aviation security, on-site surveillance and access control, remote monitoring and alarm response. While supplying these services, security companies handle different data, which are covered by Art. 2.1 of the EU Data Act, and which are hence subject to the proposal's data sharing obligations – including alarm signals, sound, visual recording or audio-visual recording.

This data is collected for different public and private clients – ranging from law enforcement to private operators of Critical Infrastructure and industrial sites of supply chain operators. Lifting barriers for sharing such sensitive data, as foreseen by the EU Data Act proposal with the client and, upon request, with third parties, can lead to considerable security threats, including insider threats, organised crime and terrorism. It can put at risk the security and safety of the persons, organisations and infrastructure, supply chains and the general public.

CoESS welcomes that Art. 1.4 of the proposal excludes the sharing, access and use of data for the prevention, investigation and detection of crime in the field of public security. Recital 60 further clarifies that the proposal does not affect the competencies of public bodies in this field. It is however not clear whether this includes private security activities, although their mission is the same.

It is thus necessary to clearly exclude private security activities from the scope of all Chapters except for Chapter V to ensure that the proposal does not create challenges to public security.

Example #1: Aviation Security

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, video recordings of security check and other areas, and AI-enabled video surveillance recordings that detect suspicious behaviour – 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 security check procedures and crime prevention tactics.

Example #2: Critical Infrastructure Protection

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 biometric data of employees for the verification of their identity at access control. If such data falls into the hands of organised criminals or terrorist networks, 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

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,

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

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. It is therefore key that private security activities are also excluded from the scope of Chapters VI-VIII.

About CoESS

CoESS acts as the voice of the private security industry, covering 23 countries in Europe and representing 2 million security officers as well as over 45,000 companies. The private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure facilities to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the only European employers' organisation representative of the private security services. Representing a labour-intensive sector, CoESS is actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups – including SAGAS, SAGMAS, LANDSEC, RAILSEC and the EU Operators Forum for the Protection of Public Spaces.

EU Transparency Register Number: 61991787780-18

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**