EUROPEAN COMMISSION

Brussels, 1.8.2013
C(2013) 5058 *final*

Dear President,

The Commission would like to thank the Bundesrat for its Opinion on the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security ("NIS") across the Union {COM(2013) 48 final}.

The Commission welcomes the fact that the Bundesrat supports the aim of the Directive, considers that common network and information security (NIS) standards help to improve the internal market by dismantling obstacles to trade and eliminating distortions of competition, and that EU legislation in the field of NIS is largely justified given that central, regional and local NIS measures alone are not sufficient.

The Commission does not share the view of the Bundesrat that the proposed provisions on the national authority and the risk management requirements for public administrations are contrary, respectively, to the principle of proportionality and the internal market legal base.

On the first point, the Commission finds that Article 4 of the Proposal leaves the Member States sufficient flexibility to decide on the powers and structure of the authorities. In this context, the Commission wishes to highlight that, contrary to the data protection authorities under Article 47 of the Proposal for an EU General Data Protection Regulation of 25 January 2012 {COM(2012) 11 final}, Article 4 of the NIS proposed Directive does not require the NIS authorities to be independent. The Commission has taken careful note of the suggestion of the Bundesrat to refer to "one or more" authorities responsible for NIS in the proposed Directive. It is nevertheless important to maintain a single focal point to ensure coordination of the various NIS activities within a Member State as well as effective cooperation within the NIS cooperation network.

On the second point, the Commission considers that the requirements for all public administrations to take security measures and report incidents comply with Article 114(1) of the Treaty.

Public administrations' e-government and e-participation services are increasing, with citizens and businesses demanding timely and cost-effective services. Public administrations have a central role to play in the implementation of the Digital Agenda. To this end they must be able to rely on a resilient ICT infrastructure to deliver their on-line services while preserving and promoting citizens' trust in e-government.

Mr Winfried KRETSCHMANN
President of the Bundesrat
Leipziger Straße 3 - 4
D – 10117 BERLIN

Resilient on-line public administration services are essential for the smooth functioning of the internal market. They allow the free movement of goods, services and people across the European Union since they can be accessed from abroad and taken advantage of remotely.

For instance, a well-functioning Internet site of a fiscal administration is essential to allow tax payers to fill in their tax forms from abroad. The same applies to social security services which have an essential role to play in facilitating the free movement of people.

Secure IT systems are prerequisites for carrying out judicial proceedings at a distance and for the administration of justice across the EU.

The disruption of the network and information system of even a small regional entity can have a direct impact on cross-border movement of goods, services and people. This would be the case where a small municipality experiences such disruption after launching a call for tender, with the effect of preventing EU companies located abroad from participating in the tender.

Furthermore, public networks are strongly interconnected and an incident affecting one entity can easily spread to another entity. As a result, an incident affecting the network and information system of a public service which is not directly related to the internal market can spread to a service whose proper functioning is essential for the internal market. In addition, due to this strong interconnection, a network effect, resulting from incidents affecting a number of similar administrations, even small and local, is more likely in the context of public administrations. Such an effect carries the risk of NIS incidents spreading within or between administrations, which could disrupt or paralyse vast fields of local and national public activities.

This risk is increased by the fact that state and local administrations are often targeted by cyber-attacks and are facing very significant and rising NIS risks. Criminals can in particular use a local administration as an entry point to attack other sectors of the administration. An employee portal used exclusively by Member State public administrations to handle internal matters with its staff is a typical example of a network that would be targeted by criminals to get an internal entry point to other better protected or critical IT systems of an administration.

In this regard, notwithstanding the precise activity concerned and its specific nature, it is essential to cover the public administration generally because of the overall vulnerability of its network and information systems, its interdependence and the heavy risk of propagation and/or network effect.

The Commission hopes that these clarifications address the concerns raised by the Bundesrat and looks forward to continuing the political dialogue in the future.

Yours faithfully,

Maroš Šefčovič
Vice-President