GDPR ACCOUNTABILITY PRINCIPLE AND EU POLITICAL STRATEGY ON CYBERSECURITY: THE CYBERSECURITY ACT.

EMILIANO TROISI

Key-words: privacy - Cybersecurity

Category: Legal Area

It will be approved soon the EU Regulation on Cybersecurity, and it is already promising to mark a radical change in perspective in this field, in the same line as GDPR did.

Thanks to GDPR, security indeed became a basic regulating principle of data processing: according to Article 5.1, letter f) of the Regulation, Personal Data has to be processed in a manner that ensures their appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Moreover, the new GDPR accountability principle requires a data processor's different approach to data security. In particular, the general provision of minimum standard measures and best practices is replaced by the requirement of a case by case risk-based approach to security that needs the adoption of those technical or organisational measures which are appropriate to prevent data breaches and to ensure a level of security adequate to the risk (Article 32 GDPR).

This flexible regime, rather than the previous merely-prescriptive one, promotes the development of new market opportunities in the field of technological goods and services (above all, artificial intelligence). At the same time, it stimulates a higher degree of competitiveness in the market supply of professional cybersecurity services and technological solutions designed to optimise the costs connected with customer's data privacy compliance.

Therefore, cybersecurity is going to be the biggest business of the near future and the EU Cybersecurity Act, that's about to be adopted, has to set up the objective for the development and the deep digitalisation of society.

It will introduce a community-level framework for certifying the security degree of ICT products, processes, and services. This could be useful both for producers, by giving them minimum security standards to follow in designing their computer systems and services (security by design), and for users, by giving them a definite benchmark they can use to consciously assess the reliability of products and services they are about to buy.

More precisely, the regulation will set up a 3-levels certification system whose technical parameters will have to be established and monitored in accordance with a centralised procedure run by the EU Agency ENISA and a network of national public bodies specifically (and nationally) responsible for both certifying the products which so request, and then, monitoring compliance with certificate.

Source: opinion of Giuseppe d'Acquisto, official of Italian DPA and lecturer of the Italian Master Course on Tatodpr 'Data Protection Officer and Privacy Law' at Suor Orsola Benincasa University of Naples

Link:https://www.agendadigitale.eu/sicurezza/privacy/la-nuova-strategia-europea-di-cybersecurity-e-il-gdpr-quali-sinergie/
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0151+0+DOC+XML+V0//EN&language=EN#title2