

Brussels, 16 June 2020

Moritz Körner,
Member of the European Parliament

By email only

Ref: OUT2020-0061

Dear Mr Körner

Thank you for your letter of 23 January 2020 as regards the relevance of encryption bans in third countries for assessing the level of protection in accordance with the GDPR when personal data are transferred to countries where these bans exist.

Encryption (cryptography, more in general) is a technology, which, if implemented in the right way, provides for the effective protection of the security of personal data and is a building block for many other privacy-enhancing technologies. The GDPR mentions it explicitly as a possible technical measure to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons and takes it explicitly into account in assessing certain compliance obligations.

Security (“integrity and confidentiality”) is one of the principles relating to the processing of personal data¹, which uniquely contributes to the compliance and protection of individuals’ fundamental rights in all processing activities. Article 32 GDPR gives to encryption, together with pseudonymisation, the rank of a measure that, yet as appropriate, may not be neglected when identifying security protection measures.

As the Working Party 29 already highlighted², the EDPB considers the availability of strong and trusted encryption as a “*necessity in the modern digital world*” and a technology contributing in “... *an irreplaceable way to our privacy and to the secure and safe functioning of our societies*”. They state that encryption “... *must remain standardized, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys*”.

Any ban on encryption or provisions weakening encryption would undermine the GDPR obligations on the concerned controllers and processors for an effective implementation of both data protection principles and the appropriate technical and organisational measures. Similar considerations apply to transfers to controllers or processors in any third countries adopting such bans or provisions.

Security measures are therefore specifically mentioned among the elements the European Commission must take into account when assessing the adequacy of the level of protection in a third

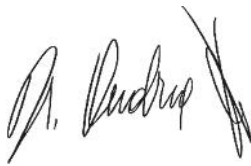
¹ See Article 5(1)(f) GDPR.

² “Article 29 WP Statement on encryption”: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229

country.³ In the absence of such a decision, transfers are subject to appropriate safeguards⁴ or may be based on derogations⁵ ; in any case the security of the personal data has to be ensured at all times.

The EDPB is of the opinion that any encryption ban would seriously undermine compliance with the GDPR. More specifically, whatever the instrument used, it would represent a major obstacle in recognising a level of protection essentially equivalent to that ensured by the applicable data protection law in the EU, and would seriously question the ability of the concerned controllers and processors to comply with the security obligation of the regulation.

Yours sincerely,



Andrea Jelinek

³ See Article 45(2)(a) GDPR.

⁴ See Article 46 GDPR.

⁵ See Article 49 GDPR.