DIGITALEUROPE

DIGITALEUROPE response to public consultation on Article 29 Working Party draft guidelines on Article 49 of Regulation 2016/679

Brussels, 26 March 2018

INTRODUCTION

DIGITALEUROPE is pleased to provide its comments on the Article 29 Working Party's (WP29) draft guidelines on derogations for transfers of personal data to third countries or international organisations under Art. 49 of the General Data Protection Regulation (GDPR).

Ensuring the viability of international data transfers in a way that preserves effective protection of fundamental rights under EU law is a top priority of DIGITALEUROPE members. In line with the current Directive, the GDPR sets out a strict set of conditions for such transfers, but also a number of instruments to enable them. It is vital that these instruments remain effective as established by law and that organisations can rely on sufficient flexibility to implement them subject to the relevant legal safeguards.

In this vein, we would like to submit our comments in areas where we feel the draft guidelines go beyond the letter of the GDPR or where we'd like to put forward different interpretations of the text.

GENERAL FRAMEWORK AND CONSISTENT INTERPRETATION

As an overarching comment, we believe that the draft guidelines incorrectly identify some general principles applicable to all international data transfers based on Art. 49. They do so by extending principles and conditions that are applicable only to specific derogations to all derogations.

For instance, p. 4 of the draft guidelines is devoted to the occasional and not repetitive nature of the transfers, implying this is one essential principle that should apply throughout Art. 49. However, the term 'occasional' (closely linked to the term 'necessary', which is the term used in Art. 49(1)(b), (c), (d), (e) and (f)) is only used in Recital 111 in relation to the contract and legal claim derogations; similarly, the term 'not repetitive' is used in Art. 49(1)(2) specifically in relation to the compelling legitimate interest derogation. We are concerned that this approach will unduly restrict organisations' ability to use some of the instruments made available by the GDPR.

The GDPR sets out various ways in which organisations can transfer personal data outside the Union. These comprise: adequate level of protection under adequacy decisions (Art. 45); the provision of appropriate safeguards, including binding corporate rules (BCRs), standard contractual clauses (SCCs) and approved codes of conducts or certification mechanisms (Arts. 46-47); and derogations including explicit consent, performance of a contract, important reasons of public interest and compelling legitimate interests (Art. 49).

As stated in the draft guidelines (p. 3), the GDPR provides for a 'layered approach' to transfers whereby adequacy should be preferred to appropriate safeguards, which in turn should be preferred to derogations. However, within this matrix and the general principles of Art. 44, each of the derogations is subject to specific conditions that should be considered individually. From this perspective, the statement in the draft guidelines (p. 4) that derogations should be an exception applicable when adequacy or appropriate safeguards are not in place should not be linked to the occasional or not repetitive nature of the transfer – a derogation acts as an exception when

DIGITALEUROPE
Rue de la Science, 14 – 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

the other two mechanisms are not available, and only when the conditions for the specific derogation require transfers to happen occasionally and not repetitively should such conditions apply.

DEROGATIONS AND LEVEL OF PROTECTION

Although Recital 101 and Art. 44 enshrine the general principle that the Chapter V provisions should be applied in a manner that ensures the GDPR's level of protection is not undermined, the derogations from letter (a) to letter (g) in Art. 49(1) always refer to situations where appropriate protection *cannot* be guaranteed, given the lack of an adequacy decision or appropriate safeguards, but the transfer can nevertheless occur under particular conditions.

The very fact that adequate protection cannot be guaranteed informs the structure and elements of Art. 49 so that appropriate counterbalances are in place to minimise negative impacts on the data subject's fundamental rights, in line with Art. 44. Such counterbalances normally consist in the fact that the transfer is related to specific purposes that are deemed to be worthy of consideration, including: the fact that the data is necessary for a contract (letters b and c); the existence of important reasons of public interest (letter d); the relevance of the data to legal claims (letter e); the protection of vital interests (letter f); or providing information to the public under conditions laid down in EU or Member State law (letter g).

In other words, as a rule Art. 49 ensures GDPR protections are not undermined by attaching strict conditions to the derogations, so that these are only available in cases when risks for data subjects are minimal or justified by specific purposes. In those circumstances where this is not possible, because the derogation is less specific as to the nature of the data at hand, Art. 49 ensures coherence with the rest of the GDPR by: 1) specifying a duty of transparency about the potential risks of the transfer necessary to receive an informed, explicit consent from the data subject (letter a); and 2) setting stricter conditions around non-repetitiveness, limited number of data subjects and the provision of 'suitable' (not 'appropriate') safeguards for compelling legitimate interests, including an obligation to inform the supervisory authority (second subparagraph of Art. 49(1)).

The above structure and conditions are put in place to ensure that risks to fundamental rights are mitigated and the GDPR protections are not undermined. However, given the rationale and purpose of the derogations, in no way can this guarantee that data subjects will continue to benefit from the same safeguards to which they are entitled under Arts. 45-47.

EXPLICIT CONSENT

The extension of specific requirements to all instruments is particularly problematic when it comes to the explicit consent derogation. While we agree that organisations will as a rule want to rely on adequacy, SCCs or BCRs, in some cases consent may be the only viable instrument for transfers; therefore, it is important that the rationale for consent and its specific meaning under Art. 49(1) be correctly interpreted.

In addition to the general conditions for consent, the only (albeit fundamental and rigorous) condition attached to such derogation under Art. 49(1)(a) is that the data subject be informed of the possible risks of transfers based on explicit consent, given that: a) the data will be moved to a third country or organisation that does not ensure an adequate level of protection; and b) no appropriate safeguards are in place.

The specific language for the explicit consent derogation is clear on the fact that this derogation applies to transfers that *by their very nature* do not provide an adequate level of protection nor appropriate safeguards. In light of the inherent risk posed by such transfers, Art. 49(1)(a) requires additional transparency for the data subject on such possible risks and the data subject's explicit informed consent to the transfer to occur in spite of such risks.

DIGITALEUROPE
Rue de la Science, 14 – 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

Put differently, the explicit consent derogation aims to give data subjects the option of consenting to transfers that expose them to risks compared to the level of fundamental rights protection ensured by the GDPR, provided the 'high threshold' (p. 8 of the draft guidelines) of being informed of the implications of doing so is met. An interpretation of this derogation that would 'never lead to a situation where fundamental rights might be breached' (p. 3 of the draft guidelines) would defeat the very logic of the derogation, which does not seek to eliminate risks but to allow data subjects to make an informed choice.

INFORMATION NECESSARY TO OBTAIN CONSENT

We welcome the WP29's clarification concerning the necessary information to be provided to data subjects so as to enable them to express their informed consent. In particular, we welcome the indication that such information could be standardised. It is important that the information provided be clear about the basic implications of the transfer compared to the GDPR provisions, and data controllers or processors should have sufficient flexibility to ensure the right balance is achieved between ensuring transparency and the actual relevance of the information presented.

COMPELLING LEGITIMATE INTERESTS

In the context of the compelling legitimate interest derogation, the draft guidelines include the existence of 'suitable safeguards' within the balancing test between the controller's compelling legitimate interests and the interests, rights or freedoms of the data subject. While the existence of suitable safeguards is essential for the derogation to apply, we believe it should be considered as a separate requirement attached to the derogation rather than included in the balancing test itself. While some of the elements may be the same for both, e.g. nature of the data, purpose for processing or situation in the third country, when applied to suitable safeguards they serve the purpose of identifying relevant protective measures for the specific situations; conversely, such elements serve to assess the legitimacy of the controller's interests in wanting to move the data when applying the balancing test. Although linked, the two levels are logically different and shouldn't be confused.

ARTICLE 48 AND DEROGATIONS

DIGITALEUROPE welcomes the WP29's reinstatement of the relationship between Chapter V and requests from foreign law enforcement. Our association has been actively engaged in the defence of transfers based on MLATs or similar international agreements, including in relevant court cases in third-country jurisdictions.[1]

--

For more information please contact:
Alberto Di Felice, DIGITALEUROPE's Senior Policy Manager for Infrastructure, Privacy and Security
+32 2 609 53 10 or alberto.difelice@digitaleurope.org

[1] See brief for DIGITALEUROPE, Bitkom, TECH IN France, Syntec Numérique, and other European national trade organisations as *amici curiae* supporting respondent in *United States v. Microsoft Corporation*. In the same case, see also brief of the European Commission on behalf of the European Union as *amicus curiae* in support of neither party.

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.`

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK