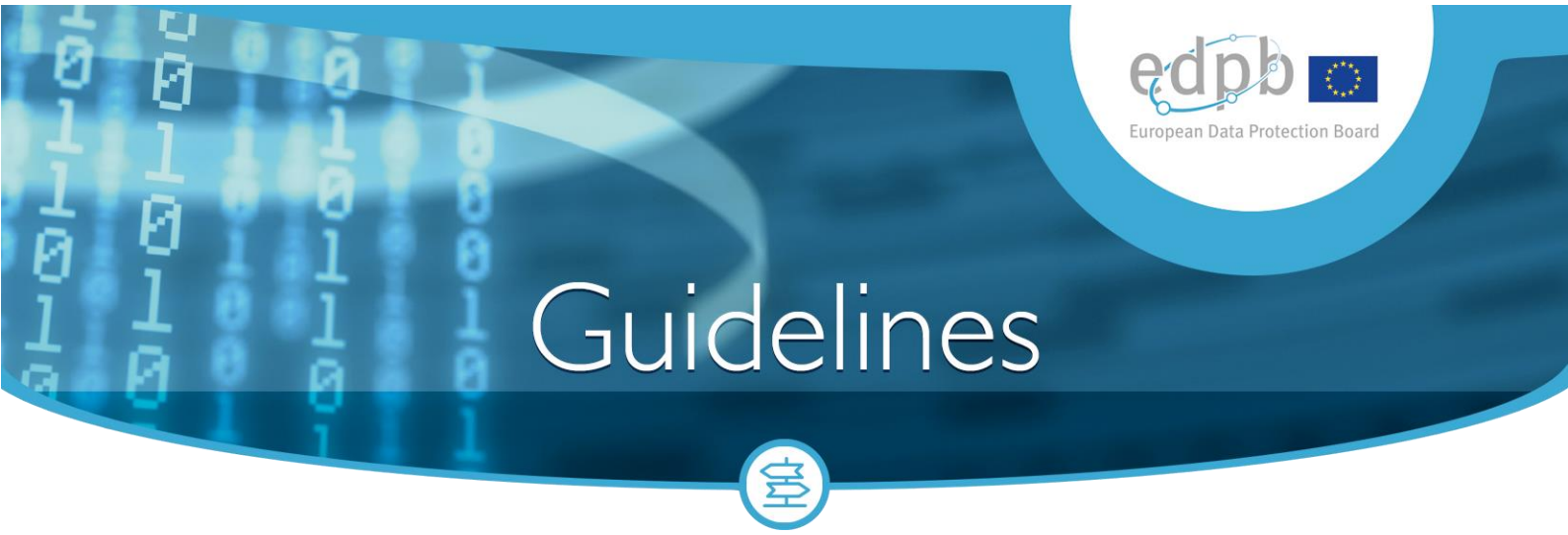

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

Adopted on 25 May 2018

Contents

The European Data Protection Board

Having regard to Article 70 (1j) and (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED FOLLOWING GUIDELINES:

1. GENERAL

This document seeks to provide guidance as to the application of Article 49 of the General Data Protection Regulation (GDPR)[1] on derogations in the context of transfers of personal data to third countries.

The document builds on the previous work[2] done by the Working Party of EU Data Protection Authorities established under Article 29 of the Data Protection Directive (the WP29) which is taken over by the European Data Protection Board (EDPB) regarding central questions raised by the application of derogations in the context of transfers of personal data to third countries. This document will be reviewed and if necessary updated, based on the practical experience gained through the application of the GDPR.

When applying Article 49 one must bear in mind that according to Article 44 the data exporter transferring personal data to third countries or international organizations must also meet the conditions of the other provisions of the GDPR. Each processing activity must comply with the relevant data protection provisions, in particular with Articles 5 and 6. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V must be complied with.

Article 49 (1) states that in the absence of an adequacy decision or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only under certain conditions. At the same time, Article 44 requires all provisions in Chapter V to be applied in such a way as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. This also implies that recourse to the derogations of Article 49 should never lead to a situation where fundamental rights might be breached.[3]

The WP29, as predecessor of the EDPB, has long advocated as best practice a layered approach[4] to transfers of considering first whether the third country provides an adequate level of protection and ensuring that the exported data will be safeguarded in the third country. If the level of protection is not adequate in light of all the circumstances, the data exporter should consider providing adequate

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Article 29 Working Party, Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, November 25,2005 (WP114)
[3] Article 29 Working Party, WP 114, p.9, and Article 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), p.39.
[4] Article 29 Working Party, WP114, p.9

safeguards. Hence, data exporters should first endeavor possibilities to frame the transfer with one of the mechanisms included in Articles 45 and 46 GDPR, and only in their absence use the derogations provided in Article 49 (1).

Therefore, derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.[5] Due to this fact and in accordance with the principles inherent in European law,[6] the derogations must be interpreted restrictively so that the exception does not become the rule.[7] This is also supported by the wording of the title of Article 49 which states that derogations are to be used for specific situations ("Derogations for specific situations").

When considering transferring personal data to third countries or international organizations, data exporters should therefore favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data once this data has been transferred. As derogations do not provide adequate protection or appropriate safeguards for the personal data transferred and as transfers based on a derogation are not required to have any kind of prior authorisation from the supervisory authorities, transferring personal data to third countries on the basis of derogations leads to increased risks for the rights and freedoms of the data subjects concerned.

Data exporters should also be aware that, in the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly limit transfers of specific categories of personal data to a third country or an international organization (Article 49 (5)).

Occasional and not repetitive transfers

The EDPB notes that the term "occasional" is used in recital 111 and the term "not repetitive" is used in the "compelling legitimate interests" derogation under Article 49 par. 1 §2. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive. Besides, a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.

Recital 111 differentiates among the derogations by expressly stating that the "contract" and the "legal claims" derogations (Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to "occasional" transfers,

[5] Recital 114

[6] Article 29 Working Party, WP114, p.7

[7] See already Article 29 Working Party, WP114, pg. 7. The European Court of Justice repeatedly underlined that "the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary" (judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C 73/07, paragraph 56; of 9 November 2010, Volker und Markus Schecke and Eifert, C 92/09 and C 93/09, paragraph 77; the Digital Rights judgment, paragraph 52, and of 6 October 2015, Schrems, C 362/14, paragraph 92, and of 21 December 2016, Tele2 Sverige AB, C 203/15, paragraph 96). See also report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data, Article 2(2) (a), p.6 accessible at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181.1)

while such limitation is absent from the "explicit consent derogation", the "important reasons of public interest derogation", the "vital interests derogation" and the "register derogation" pursuant to Article 49 (1) subpar. 1 (a), (d), (f) and, respectively, (g).

Nonetheless, it has to be highlighted that even those derogations which are not expressly limited to "occasional" or "not repetitive" transfers have to be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place.[8]

Necessity test

One overarching condition for the use of several derogations is that the data transfer has to be "necessary" for a certain purpose. The necessity test should be applied to assess the possible use of the derogations of Articles 49 (1) (b), (c), (d), (e) and (f). This test requires an evaluation by the data exporter in the EU of whether a transfer of personal data can be considered necessary for the specific purpose of the derogation to be used. For more information on the specific application of the necessity test in each of the concerned derogations, please refer to the relevant sections below.

Article 48 in relation to derogations

The GDPR introduces a new provision in Article 48 that needs to be taken into account when considering transfers of personal data. Article 48 and the corresponding recital 115 provide that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries. Therefore, a transfer in response to a decision from third country authorities is in any case only lawful, if in line with the conditions set out in Chapter V.[9]

In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.

This understanding also closely follows Article 44, which sets an overarching principle applying to all provisions of Chapter V, in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

[9]See Recital 115 sentence 4

2. SPECIFIC INTERPRETATION OF THE PROVISIONS OF ARTICLE 49

2.1 The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards - Article (49 (1) (a))

The general conditions for consent to be considered as valid are defined in Articles 4 (11)[10] and 7 of the GDPR[11]. The WP29 provides guidance on these general conditions for consent in a separate document, which is endorsed by the EDPB.[12] These conditions also apply to consent in the context of Article 49 (1) (a). However, there are specific, additional elements required for consent to be considered a valid legal ground for international data transfers to third countries and international organizations as provided for in Article 49 (1) (a), and this document will focus on them.

Therefore, this section (1) of the present guidelines shall be read in conjunction with the WP29 guidelines on consent, endorsed by the EDPB, which provide a more detailed analysis on the interpretation of the general conditions and criteria of consent under the GDPR.[13] It should also be noted that, according to Article 49 (3), public authorities are not able to rely on this derogation in the exercise of their public powers.

Article 49 (1) (a) states that a transfer of personal data to a third country or an international organization may be made in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, on the condition that '*the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards'*.

2.1.1 Consent must be explicit

According to Article 4 (11) of the GDPR, any consent should be freely given, specific, informed and unambiguous. On this very last condition, Article 49 (1) (a) is stricter as it requires "explicit" consent. This is also a new requirement in comparison to Article 26 (1) (a) of Directive 95/46/EC, which only required "unambiguous" consent. The GDPR requires explicit consent in situations where particular data protection risks may emerge, and so, a high individual level of control over personal data is required, as is the case for the processing of special category data (Article 9 (2) (a)) and automated decisions (Article 22 (2) (c)). Such particular risks also appear in the context of international data transfers.

For further guidance on the requirement of explicit consent, and for the other applicable requirements needed for consent to be considered valid, please refer to the WP29's Guidelines on Consent which are endorsed by the EDPB.[14]

[10] According to Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
[11] Also recitals 32, 33, 42 and 43 give further guidance on consent
[12] See Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259)
[13] Idem
[14] Idem

2.1.2 Consent must be specific for the particular data transfer/set of transfers

One of the requirements of valid consent is that it must be specific. In order to constitute a valid ground for a data transfer pursuant to Article 49 (1) (a), hence, consent needs to be specifically given for the particular data transfer or set of transfers.

The element "specific" in the definition of consent intends to ensure a degree of user control and transparency for the data subject. This element is also closely linked with the requirement that consent should be "informed".

Since consent must be specific, it is sometimes impossible to obtain the data subject's prior consent for a future transfer at the time of the collection of the data, e.g. if the occurrence and specific circumstances of a transfer are not known at the time consent is requested, the impact on the data subject cannot be assessed. As an example, an EU company collects its customers' data for a specific purpose (delivery of goods) without considering transferring this data, at that time, to a third party outside the EU. However, some years later, the same company is acquired by a non-EU company which wishes to transfer the personal data of its customers to another company outside the EU. In order for this transfer to be valid on the grounds of the consent derogation, the data subject should give his/her consent for this specific transfer at the time when the transfer is envisaged. Therefore, the consent provided at the time of the collection of the data by the EU company for delivery purposes is not sufficient to justify the use of this derogation for the transfer of the personal data outside the EU which is envisaged later.

Therefore, the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made. This requirement is also related to the necessity for consent to be informed. It is possible to obtain the specific consent of a data subject prior to the transfer and at the time of the collection of the personal data as long as this specific transfer is made known to the data subject and the circumstances of the transfer do not change after the specific consent has been given by the data subject. Therefore the data exporter must make sure that the requirements set out in section 1.3 below are also complied with.

2.1.3 Consent must be informed[15] particularly as to the possible risks of the transfer

This condition is particularly important since it reinforces and further specifies the general requirement of "informed" consent as applicable to any consent and laid down in Art. 4 (11).[16] As such, the general requirement of "informed" consent, requires, in the case of consent as a lawful basis pursuant to Article 6(1) (a) for a data transfer, that the data subject is properly informed in advance of the specific circumstances of the transfer, (i.e. the data controller's identity, the purpose of the transfer, the type of data, the existence of the right to withdraw consent, the identity or the categories of recipients).[17]

In addition to this general requirement of "informed" consent, where personal data are transferred to a third country under Article 49 (1) (a), this provision requires data subjects to be also informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented. The provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer and therefore if it is not supplied, the derogation will not apply.

[15] The general transparency requirements of Articles 13 and 14 of the GDPR should also be complied with. For more information see Guidelines on transparency under Regulation 2016/679 (WP 260)

[16] See Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259)

[17] Idem, page 13

The information provided to data subjects in order to obtain consent for the transfer of their personal data to third parties established in third countries should also specify all data recipients or categories of recipients, all countries to which the personal data are being transferred to, that the consent is the lawful ground for the transfer, and that the third country to which the data will be transferred does not provide for an adequate level of data protection based on a European Commission decision.[18] In addition, as mentioned above, information has to be given as to the possible risks for the data subject arising from the absence of adequate protection in the third country and the absence of appropriate safeguards. Such notice, which could be standardized, should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country.

In the specific case where a transfer is performed after the collection of personal data from the data subject has been made, the data exporter should inform the data subject of the transfer and of its risks before it takes place so as to collect his explicit consent to the "proposed" transfer.

As shown by the analysis above, the GDPR sets a high threshold for the use the derogation of consent. This high threshold, combined with the fact that the consent provided by a data subject can be withdrawn at any time, means that consent might prove not to be a feasible long term solution for transfers to third countries.

2.2 Transfer necessary for the performance of a contract between the data subject and the controller or for the implementation of precontractual measures taken at the data subject's request - (49 (1) (b))

In view of recital 111, data transfers on the grounds of this derogation may take place "*where the transfer is **occasional** and **necessary** in relation to a contract (…)*"[19]

In general, although the derogations relating to the performance of a contract may appear to be potentially rather broad, they are being limited by the criterions of "*necessity*" and of "*occasional transfers*".

Necessity of the data transfer

The "*necessity test*" [20] limits the number of cases in which recourse can be made to Article 49 (1) (b).[21] It requires a close and substantial connection between the data transfer and the purposes of the contract.

This derogation cannot be used for example when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country as there is no direct and objective link between the performance of the employment contract and such transfer.[22] Other grounds for transfer as provided for in Chapter V such as standard contractual clauses or binding corporate rules may, however, be suitable for the particular transfer.

[18] The last mentioned requirement also stems from the duty to inform the data subjects (Article 13(1)(f), Article 14(1)(e))

[19] The criterion of "occasional" transfers is found in recital 111 and applies to the derogations of Article 49 (1) (b), (c) and (e).

[20] See also Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)

[21] The "necessity" requirement also can be found in the derogations set forth in Article 49 (1) (c) to (f).

[22] In addition it will not be seen as being occasional (see below).

On the other hand, the transfer by travel agents of personal data concerning their individual clients to hotels or to other commercial partners that would be called upon in the organization of these clients' stay abroad can be deemed necessary for the purposes of the contract entered into by the travel agent and the client, since, in this case, there is a sufficient close and substantial connection between the data transfer and the purposes of the contract (organization of clients' travel).

This derogation cannot be applied to transfers of additional information not necessary for the performance of the contract or, respectively, for the implementation of precontractual measures requested by the data subject[23]; for additional data other tools would hence be required.

Occasional transfers

Personal data may only be transferred under this derogation when this transfer is occasional.[24] It would have to be established on a case by case basis whether data transfers or a data transfer would be determined as "*occasional*" or "*non-occasional*".

A transfer here may be deemed occasional for example if personal data of a sales manager, who in the context of his/her employment contract travels to different clients in third countries, are to be sent to those clients in order to arrange the meetings. A transfer could also be considered as occasional if a bank in the EU transfers personal data to a bank in a third country in order to execute a client's request for making a payment, as long as this transfer does not occur in the framework of a stable cooperation relationship between the two banks.

On the contrary, transfers would not qualify as "occasional" in a case where a multi-national company organises trainings in a training centre in a third country and systematically transfers the personal data of those employees that attend a training course (e.g. data such as name and job title, but potentially also dietary requirements or mobility restrictions). Data transfers regularly occurring within a stable relationship would be deemed as systematic and repeated, hence exceeding an "occasional" character. Consequently, in this case many data transfers within a business relationship may not be based on Article 49 (1) (b).

According to Article 49(1) (3), this derogation cannot apply to activities carried out by public authorities in the exercise of their public powers.

2.3 Transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person - (49 (1) (c))

The interpretation of this provision is necessarily similar to that of Article 49 (1) (b); namely, that a transfer of data to a third country or an international organization in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, can only be deemed to fall under the derogation of Article 49(1) (c), if it can be considered to be "*necessary for the conclusion or performance of a contract between the data controller and another natural or legal person, in the interest of the data subject*".

Aside from being necessary, recital 111 indicates that, data transfers may only take place "*where the transfer is **occasional** and **necessary** in relation to a contract (...)*" Therefore, apart from the "*necessity*

[23] More generally, all derogations of Article 49(1) (b) to (f) only allow that the data which are necessary for the purpose of the transfer may be transferred.

[24] As to the general definition of the term « occasional » see page 4

test", personal data here as well may only be transferred under this derogation only when the transfer is occasional.

Necessity of the data transfer and conclusion of the contract in the interest of the data subject

Where an organization has, for business purposes, outsourced activities such as payroll management to service providers outside the EU, this derogation will not provide a basis for data transfers for such purposes, since no close and substantial link between the transfer and a contract concluded in the data subject's interest can be established even if the end purpose of the transfer is the management of the pay of the employee.[25] Other transfer tools provided in Chapter V may provide a more suitable basis for such transfers such as standard contractual clauses or binding corporate rules.

Occasional transfers

Moreover, personal data may only be transferred under this derogation, when the transfer is occasional as it is the case under the derogation of Article 49 (1) (b). Therefore, in order to assess whether such transfer is occasional, the same test has to be carried out[26].

Finally, according to Article 49(1) (3), this derogation cannot apply to activities carried out by public authorities in the exercise of their public powers.[27]

2.4 Transfer is necessary for important reasons of public interest - (49 (1) (d))

This derogation, usually referred to as the "important public interest derogation", is very similar to the provision contained in Directive 95/46/EC[28] under Article 26 (1) (d), which provides that a transfer shall take place only where it is necessary or legally required on important public interest grounds.

According to Article 49 (4), only public interests recognized in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.

However, for the application of this derogation, it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law. Where for example a third country authority requires a data transfer for an investigation aimed at combatting terrorism, the mere existence of EU or member state legislation also aimed at combatting terrorism is not as such a sufficient trigger to apply Article 49 (1) (d) to such transfer. Rather, as emphasized by the WP29, predecessor of the EDPB, in previous statements,[29] the derogation only applies when it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation. The existence of an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest pursuant to Article 49 (1) (d), as long as the EU or the Member States are a party to that agreement or convention.

[25] In addition it will not be seen as being occasional (see below).
[26] As to the general definition of the term "occasional" please see page 4
[27] For more information please refer to section 1, page 5 above.
[28] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[29] Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), p. 25

Although mainly focused to be used by public authorities, Article 49 (1) (d) may also be relied upon by private entities. This is supported by some of the examples enumerated in recital 112 which mention both transfers by public authorities and private entities[30].

As such, the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organization (public, private or international organization) that transfers and/or receives the data.

Recitals 111 and 112 indicate that this derogation is not limited to data transfers that are "occasional"[31]. Yet, this does not mean that data transfers on the basis of the important public interest derogation under Article 49 (1) (d) can take place on a large scale and in a systematic manner. Rather, the general principle needs to be respected according to which the derogations as set out in Article 49 shall not become "the rule" in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.[32]

Where transfers are made in the usual course of business or practice, the EDPB strongly encourages all data exporters (in particular public bodies[33]) to frame these by putting in place appropriate safeguards in accordance with Article 46 rather than relying on the derogation as per Article 49(1) (d).

2.5 Transfer is necessary for the establishment, exercise or defense of legal claims - (49 (1) (e))

Establishment, exercise or defense of legal claims

Under Article 49 (1) (e), transfers may take place when "*the transfer is necessary for the establishment, exercise or defense of legal claims*". Recital 111 states that a transfer can be made where it is *"occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies*". This covers a range of activities for example, in the context of a criminal or administrative investigation in a third country (e.g. anti-trust law, corruption, insider trading or similar situations), where the derogation may apply to a transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen e.g. in anti-trust investigations. As well, data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation. It can also cover actions by the data exporter to institute procedures in a third country for example commencing litigation or seeking approval for a merger. The derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

This derogation can apply to activities carried out by public authorities in the exercise of their public powers (Article 49 (3)).

The combination of the terms "legal claim" and "procedure" implies that the relevant procedure must have a basis in law, including a formal, legally defined process, but is not necessarily limited to judicial or administrative procedures ("or any out of court procedure"). As a transfer needs to be made **in** a

[30] "*international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport."*

[31] As to the general definition of the term « occasional » see page 4

[32] See also page 3

[33] For example financial supervisory authorities exchanging data in the context of international transfers of personal data for administrative cooperation purposes

procedure, a close link is necessary between a data transfer and a specific procedure regarding the situation in question. The abstract applicability of a certain type of procedure would not be sufficient.

Data controllers and data processors need to be aware that national law may also contain so-called "blocking statutes", prohibiting them from or restricting them in transferring personal data to foreign courts or possibly other foreign official bodies.

Necessity of the data transfer

A data transfer in question may only take place when it is **necessary** for the establishment, exercise or defense of the legal claim in question. This "*necessity test*" requires a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position.[34] The mere interest of third country authorities or possible "good will" to be obtained from the third country authority as such would not be sufficient.

Whilst there may be a temptation for a data exporter to transfer all possibly relevant personal data in response to a request or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In relation to litigation proceedings the WP29, predecessor of the EDPB, has already set out a layered approach to the question of whether the personal data should be transferred, including the application of this principle. As a first step, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its relevance to the particular matter should be assessed before the transfer – so only a set of personal data that is actually necessary is transferred and disclosed.

Occasional transfer

Such transfers should only be made if they are occasional. For information on the definition of occasional transfers please see the relevant section on "occasional and "non-repetitive" transfers.[35] Data exporters would need to carefully assess each specific case.

2.6 Transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent – (49 (1) (f))

The derogation of Article 49 (1) (f) obviously applies when data is transferred in the event of a medical emergency and where it is considered that such transfer is directly necessary in order to give the medical care required.

Thus, for example, it must be legally possible to transfer data (including certain personal data) if the data subject, whilst outside the EU, is unconscious and in need of urgent medical care, and only a exporter (e.g. his usual doctor), established in an EU Member State, is able to supply these data. In such cases the law assumes that the imminent risk of serious harm to the data subject outweighs data protection concerns.

[34] Recital 111: "necessary in relation to a contract or a legal claim."
[35] Page 4

The transfer must relate to the individual interest of the data subject or to that of another person's and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, this derogation cannot be used to justify transferring personal medical data outside the EU if the purpose of the transfer is not to treat the particular case of the data subject or that of another person's but, for example, to carry out general medical research that will not yield results until sometime in the future.

Indeed, the GDPR does not restrict the use of this derogation to the physical integrity of a person but also leaves room for example to consider the cases where the mental integrity of a person should be protected. In this case, the person concerned would also be incapable - physically or legally - of providing his/her consent for the transfer of his/her personal data. In addition, the concerned individual whose personal data are the subject of the transfer specifically must not be able to give his/her consent – physically or legally - to this transfer.

However, whenever the data subject has the ability to make a valid decision, and his/her consent can be solicited, then this derogation cannot apply.

For example, where the personal data is required to prevent eviction from a property, this would not fall under this derogation as, even though housing be considered as a vital interest, the person concerned can provide his/her consent for the transfer of his/her data.

This ability to make a valid decision can depend on physical, mental but also legal incapability. A legal incapability can encompass, without prejudice to national representation mechanisms, for example, the case of a minor. This legal incapability has to be proved, depending on the case, through either a medical certificate showing the mental incapability of the person concerned or through a governmental document confirming the legal situation of the person concerned.

Data transfers to an international humanitarian organization, necessary to fulfil a task under the Geneva Conventions or to comply with international humanitarian law applicable in armed conflict may also fall under Article 49 (1) (f), see recital 112. Again, in such cases the data subject needs to be physically or legally incapable of giving consent.

The transfer of personal data after the occurrence of natural disasters and in the context of sharing of personal information with entities and persons for the purpose of rescue and retrieval operations (for example, relatives of disaster victims as well as with government and emergency services), can be justified under this derogation. Such unexpected events (floods, earthquakes, hurricanes etc.) can warrant the urgent transfer of certain personal data to learn for example, the location and status of victims. In such situations it is considered that the data subject concerned is unable to provide his/her consent for the transfer of his/her data.

2.7. Transfer made from a public register - (49 (1) (g) and 49 (2))

Article 49 (1) (g) and Article 49 (2) allow the transfer of personal data from registers under certain conditions. A register in general is defined as a "*(written) record containing regular entries of items or details*" *or as "an* official list or record of names or items » [36], where in the context of Article 49, a register could be in written or electronic form.

The register in question must, according to Union or Member State law, be intended to provide information to the public. Therefore, private registers (those in the responsibility of private bodies) are

[36] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/register (22.01.2018); Oxford Dictionary https://en.oxforddictionaries.com/definition/register (22.01.2018).

outside of the scope of this derogation (for example private registers through which credit-worthiness is appraised.

The register must be open to consultation by either:

(a) the public in general or

(b) any person who can demonstrate a legitimate interest.

These could be, for example: registers of companies, registers of associations, registers of criminal convictions, (land) title registers or public vehicle registers.

In addition to the general requirements regarding the set-up of the registers themselves, transfers from these registers may only take place if and to the extent that, in each specific case, the conditions for consultation that are set forth by Union or Member State law are fulfilled (regarding these general conditions, see Article 49 (1) (g).

Data controllers and data processors wishing to transfer personal data under this derogation need to be aware that a transfer cannot include the entirety of the personal data or entire categories of the personal data contained in the register (Article 49 (2)). Where a transfer is made from a register established by law and where it is to be consulted by persons having a legitimate interest, the transfer can only be made at the request of those persons or if they are recipients, taking into account of the data subjects' interests and fundamental rights[37]. On a case by case basis, data exporters, in assessing whether the transfer is appropriate, would always have to consider the interests and rights of the data subject.

Further use of personal data from such registers as stated above may only take place in compliance with applicable data protection law.

This derogation can also apply to activities carried out by public authorities in the exercise of their public powers (Article 49 (3)).

2.8. Compelling legitimate interests – (49 (1) § 2)

Article 49 (1) § 2 introduces a new derogation which was not previously included in the Directive. Under a number of specific, expressly enumerated conditions, personal data can be transferred if it is necessary for the purposes of compelling legitimate interests pursued by the data exporter.

This derogation is envisaged by the law as a last resort, as it will only apply where "*a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation is applicable*".[38]

This layered approach to considering the use of derogations as a basis for transfers requires consideration of whether it is possible to use a transfer tool provided in Article 45 or 46 or one of the specific derogations set out in Article 49 (1) § 1, before resorting to the derogation of Article 49 (1) §2. This can only be used in residual cases according to recital 113 and is dependent on a significant number of conditions expressly laid down by law. In line with the principle of accountability enshrined in the GDPR[39] the data exporter must be therefore able to demonstrate that it was neither possible to frame the data transfer by appropriate safeguards pursuant to Article 46 nor to apply one of the derogations as contained in Article 49 (1) § 1.

[37] Recital 111 of the GDPR
[38] Article 49 (1) § 2 GDPR
[39] Article 5 (2) and Article 24 (1)

This implies that the data exporter can demonstrate serious attempts in this regard, taking into account the circumstances of the data transfer. This may for example and depending on the case, include demonstrating verification of whether the data transfer can be performed on the basis of the data subjects' explicit consent to the transfer under Article 49 (1) (a). However, in some circumstances the use of other tools might not be practically possible. For example, some types of appropriate safeguards pursuant to Article 46 may not be a realistic option for a data exporter that is a small or medium-sized company.[40] This may also be the case for example, where the data importer has expressly refused to enter into a data transfer contract on the basis of standard data protection clauses (Article 46 (2) (c)) and no other option is available (including, depending on the case, the choice of a different "data importer") – see also the paragraph below on 'compelling' legitimate interest.

Compelling legitimate interests of the controller

According to the wording of the derogation, the transfer must be necessary for the purposes of pursuing compelling legitimate interests of the data controller which are not overridden by the interests or rights and freedoms of the data subject. Consideration of the interests of a data exporter in its capacity as data processor or of the data importer are not relevant.

Moreover, only interests that can be recognized as "compelling" are relevant and this considerably limits the scope of the application of the derogation as not all conceivable "legitimate interests" under Article 6 (1) (f) will apply here. Rather a certain higher threshold will apply, requiring the compelling legitimate interest to be essential for the data controller. For example, this might be the case if a data controller is compelled to transfer the personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business.

Not repetitive

According to its express wording, Article 49 (1) § 2 can only apply to a transfer that is not repetitive[41].

Limited number of data subjects

Additionally, the transfer must only concern a limited number of data subjects. No absolute threshold has been set as this will depend on the context but the number must be appropriately small taking into consideration the type of transfer in question.

In a practical context, the notion "limited number of data subjects" is dependent on the actual case in hand. For example, if a data controller needs to transfer personal data to detect a unique and serious security incident in order to protect its organization, the question here would be how many employees' data the data controller would have to transfer in order to achieve this compelling legitimate interest.

As such, in order for the derogation to apply, this transfer should not apply to all the employees of the data controller but rather to a certain confined few.

Balancing the "compelling legitimate interests of the controller" against the "interests or rights and freedoms of the data subject" on the basis of an assessment of all circumstances surrounding the data transfer and providing for suitable safeguards

As a further requirement, a balancing test between the data exporter's (compelling) legitimate interest pursued and the interests or rights and freedoms of the data subject has to be performed. In this

[40] For example binding corporate rules may often not be a feasible option for small and medium-sized enterprises due to the considerable administrative investments they imply.
[41] For more information on the term « not repetitive » see page 4

regard, the law expressly requires the data exporter to assess all circumstances of the data transfer in question and, based on this assessment, to provide "suitable safeguards" regarding the protection of the data transferred. This requirement highlights the special role that safeguards may play in reducing the undue impact of the data transfer on the data subjects and thereby in possibly influencing the balance of rights and interests to the extent that the data controller's interests will not be overridden.[42]

As to the interests, rights and freedoms of the data subject which need to be taken into consideration, the possible negative effects, i.e. the risks of the data transfer on any type of (legitimate) interest of the data subject have to be carefully forecasted and assessed, by taking into consideration their likelihood and severity.[43] In this regard, in particular any possible damage (physical and material, but also non-material as e.g. relating to a loss of reputation) needs to be taken into consideration[44]. When assessing these risks and what could under the given circumstances possibly be considered as "suitable safeguards" for the rights and freedoms of the data subject, the data exporter needs to particularly take into account the nature of the data, the purpose and duration of the processing as well as the situation in the country of origin, the third country and, if any, the country of final destination of the transfer.[45]

Furthermore, the law requires the data exporter to apply additional measures as safeguards in order to minimize the identified risks caused by the data transfer for the data subject.[46] This is set up by the law as a mandatory requirement, so it can be followed that in the absence of additional safeguards, the controller's interests in the transfer will in any case be overridden by the interests or rights and freedoms of the data subject.[47] As to the nature of such safeguards, it is not possible to set up general requirements applicable to all cases in this regard, but these will rather very much depend on the specific data transfer in question. Safeguards might include, depending on the case, for example measures aimed at ensuring deletion of the data as soon as possible after the transfer, or limiting the purposes for which the data may be processed following the transfer. Particular attention should be paid to whether it may be sufficient to transfer pseudonymized or encrypted data.[48] Moreover, technical and organizational measures aimed at ensuring that the transferred data cannot be used for other purposes than those strictly foreseen by the data exporter should be examined.

Information of the supervisory authority

The duty to inform the supervisory authority does not mean that the transfer needs to be authorized by the supervisory authority, but rather it serves as an additional safeguard by enabling the supervisory

[42] The important role of safeguards in the context of balancing the interests of the data controller and the data subjects has already been highlighted by the Article 29 Working Party in WP 217, p. 31.
[43] See Recital 75: "*The risk to the rights and freedoms of natural persons, of varying likelihood and severity (…)"*
[44] See Recital 75: "*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage."*
[45] Recital 113
[46] While in the context of an "ordinary" balancing test foreseen by the law such (additional) measures might not be necessary in each case (see Article 29 Working Party Working document on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP 214), p. 41), the wording of Art. 49 (1) § 2 suggests that additional measures are mandatory in order the data transfer to comply with the "balancing test" and therefore to be feasible under this derogation.
[47] While in the context of an "ordinary" balancing test foreseen by the law such (additional) measures might not be necessary in each case (see Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 41), the wording of Art. 49 (1) § 2 suggests that additional measures are mandatory in order the data transfer to comply with the "balancing test" and therefore to be feasible under this derogation.
[48] For other examples of possible safeguards see Article 29 Working Party Working document on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP 214), p. 41-43

authority to assess the data transfer (if it considers it appropriate) as to its possible impact on the rights and freedoms of the data subjects affected. As part of its compliance with the accountability principle, it is recommended that the data exporter records all relevant aspects of the data transfer e.g. the compelling legitimate interest pursued, the "competing" interests of the individual, the nature of the data transferred and the purpose of the transfer.

Providing information of the transfer and the compelling legitimate interests pursued to the data subject

The data controller must inform the data subject of the transfer and of the compelling legitimate interests pursued. This information must be provided in addition to that required to be provided under to Articles 13 and 14 of the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)