

Complaint re: Cross Border Data Transfers
by the International Association of Privacy
Professionals (IAPP) and failure to meet
obligations under Article 13(1)(f).

Contents

Background to Complaint	1
Establishment in the Union.....	1
Substance of Complaint	2
Article 41 GDPR.....	2
Article 44 GDPR.....	2
Relevant Law and Guidance regarding Cross Border Transfer	3
Article 49 Derogations	3
Transfer based on Explicit Consent (Article 49(1)(a))	4
Transfer based on the Compelling Legitimate Interest Derogation	8
Transfer Necessary for Conclusion or performance of a contract between data subject and Controller (Article 49(1)(b)).....	10
Failure to meet obligations under Article 13 GDPR.....	11

Background to Complaint

The IAPP is a professional membership organisation headquartered in the United States and operating as a 501(c)(3) non-profit organisation.

They offer membership of a professional association, certification, and a variety of other services. The primary means of accessing and engaging with the IAPP is via their website at www.iapp.org

The primary focus of the International Association of Privacy Professionals is the development of the data protection and data privacy profession. They have in excess of 50,000 members worldwide.

I am a member of the IAPP and hold multiple certifications from the Association. I also attend events which require registration via the IAPP website and am required to maintain a CPE (Continuing Privacy Education) register via the IAPP website in order to maintain my accreditations.

Due to the market dominance of the IAPP as a professional body and the dominance of their certifications in the industry it has been necessary for me to join and maintain my membership and certification for the purposes of carrying out my professional functions and operating my business.

This is particularly true in the context of tenders for work with public or private sector organisations which allocate scoring based on the ability to demonstrate professional competence.

Establishment in the Union

The IAPP operates a series of geographic and sectoral oriented “knowledge nets” which offer training, networking, and events for IAPP members.

Each “KnowledgeNet” has a country chair who acts in a volunteer capacity and but is not an agent or employee of the IAPP and do not have authority to act on their behalf.
(<https://iapp.org/connect/communities/chapters/knowledgenet-chapter-chair/>)

The IAPP operates a KnowledgeNet in the Republic of Ireland. Registration is required to attend KnowledgeNet events and information about KnowledgeNet events is communicated to IAPP members.

In addition to KnowledgeNet activities, the IAPP specifically targets the European Union with events, membership recruitment and the development and maintenance of a certification in European Data Protection. Furthermore, the IAPP engages in the monitoring of behaviour of people in the Union through the automated recording of Continuous Privacy Education Credits whenever a member attends an IAPP hosted event by registering through their website and also through the provision of an online process for the recording of CPE points against a certification in order to maintain that accreditation.

Finally, the IAPP maintains an office in Brussels that is identified on their website as their EMEA headquarters.

Substance of Complaint

The IAPP has not established an adequate lawful basis for transfers of personal data to the United States in the information provided in its Privacy Notice

(<https://web.archive.org/web/20210127161221/https://iapp.org/about/privacy-notice/>).

The IAPP asserts that it collects and transfers personal data to the United States on the basis of consent or on the basis of a “compelling legitimate interest”.

Transferring personal data from the EU to the US

The IAPP has its headquarters in the United States. Information we collect from you will be processed in the United States, and by using the IAPP's services you acknowledge and consent to the processing of your data in the United States. The United States has not sought nor received a finding of “adequacy” from the European Union under Article 41 of the GDPR. The IAPP relies on derogations for specific situations as set forth in Article 44 of the GDPR. In particular, the IAPP collects and transfers to the U.S. personal data only: with your consent; to perform a contract with you; or to fulfill a compelling legitimate interest of the IAPP in a manner that does not outweigh your rights and freedoms. The IAPP endeavors to apply suitable safeguards to protect the privacy and security of your personal data and to use it only consistent with your relationship with the IAPP and the practices described in this Privacy Statement. The IAPP also enters into data processing agreements and model clauses with its vendors whenever feasible and appropriate.

[↑ BACK TO TOP](#)

Figure 1 Screenshot of IAPP Data Privacy Notice section re: Cross Border Data Transfers

In doing so, they reference Article 41 of GDPR and seek to rely on derogations set out in Article 44 of GDPR.

Article 41 GDPR

Article 41 of GDPR relates to the monitoring of approved Codes of Conduct under the GDPR. It bears no relation to the protection of personal data in respect of transfers outside the Union.

Article 44 GDPR

Article 44 of GDPR states:

“Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.”

No derogations are set out in this Article which can be relied upon. Article 44 does require the application of the provisions in Chapter V of GDPR to be applied to ensure the level of protection for natural persons is not undermined.

Relevant Law and Guidance regarding Cross Border Transfer

As the Supervisory Authority will be aware, data transfers to third countries can take place on the basis of either:

- 1) An adequacy decision under Article 45 of GDPR.
- 2) The implementation of appropriate safeguards as set out in Article 46
- 3) The operation of Binding Corporate Rules under Article 47, or
- 4) Specific derogations under Article 49.

The IAPP acknowledges that no adequacy decision exists between the EU and the US. Therefore, this does not apply.

Of the appropriate safeguards identified under Article 46:

- 1) The IAPP is not a public authority or public body;
- 2) The IAPP does not make reference to the existence of or operation of Binding Corporate Rules under Article 47;
- 3) The relationship in question is not a Controller to Processor relationship, therefore Standard Contractual Clauses do not apply in respect of either a Commission adopted form of clauses or any form of clauses which may be adopted by a Supervisory Authority under Article 93(2);
- 4) The IAPP is not subject to an approved code of conduct under Article 40;
- 5) There is no approved certification mechanism under Article 42 in place which might apply to this transfer.

Article 49 Derogations

The IAPP seeks to rely on derogations under Article 49. In this context, it is inferred from the IAPP's Data Protection Notice that they are specifically relying on Article 49(1)(a) and on the provision in respect of compelling legitimate interests set out in the second paragraph of Article 49(1) GDPR.

These derogations should be interpreted in line with the guidance of the European Data Protection Board in respect to Derogations under Article 49 ([edpb guidelines 2 2018 derogations en.pdf](#) ([europa.eu](#))). This requires that the derogations "must be interpreted restrictively so that the exception does not become the rule".

The EDPB also notes in these guidelines that the use of the terms "occasional" in Recital 111 and "not repetitive" in respect of the "compelling legitimate interests" derogation indicate that 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".

While Recital 111 does distinguish between the different categories of derogation, the EDPB guidance on this matter explicitly highlights that "even those derogations that 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 being exceptions to 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".

As such, it is submitted that the operation of a membership organisation with an annual membership renewal cycle, the operation of a certification scheme and associated training and continuous professional development activities, and the management and maintenance of a formal register of Continuous Professional Education credits for the purposes of maintaining professional

certifications and accreditations constitutes a non-occasional and repetitive set of data transfers and, as such, the application of derogations must be interpreted restrictively.

Transfer based on Explicit Consent (Article 49(1)(a))

Article 49(1)(a) can be relied upon when a data subject has *explicitly* consented to the proposed transfer. It also requires that the data subject is informed of the “possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards”.

Under Article 4(11) GDPR the conditions for consent are clearly set out. To be valid, consent must be

- Informed
- Specific
- Unambiguous
- Freely Given

The concept of consent in GDPR has further been elaborated on by the EDPB in their guidelines on consent (Guidelines 05/2020).

Informed

It is submitted that the information provided in the IAPP’s Data Protection Notice does not provide any information, or at a minimum provides insufficient information, to data subjects to enable them to make a fully informed choice in respect of the transfer of their data to the United States.

It is submitted that it is insufficient to merely reference the absence of an Adequacy Decision but that further information must be provided to ensure that the data subject is informed as to the specific nature of the processing that they are consenting to.

No information is provided as to the safeguards or other supplemental measures which might be employed by the IAPP for the purposes of ensuring “appropriate safeguards are put in place”.

Paragraph 64 of the EDPB’s guidelines on consent sets out the minimum content requirements for consent to be informed. In respect of transfers to the United States it is submitted that these minimum requirements are not met as no information has been provided about:

- The types of data that will be collected and used/transferred.
- The existence of a right to withdraw consent.
- The possible risks of data transfers due to the absence of an adequacy decision and of appropriate safeguards as described in Article 46

It is further submitted, therefore, that the Data Protection Notice of the IAPP does not meet these minimum requirements for consent.

The EDPB Guidelines on the application of derogations under Article 49 highlights the importance of data subjects being informed as to the possible risks of the data transfer.

“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.”

It is submitted that the IAPP's Data Protection Notice does not meet the standard set out in the EDPB Guidelines as it fails to provide any information as to the specific risks resulting from the fact of transfer to a third country that does not provide adequate protection.

It is submitted that, as this information is not supplied, it is not possible for the IAPP to rely on the derogation in Article 49(1)(a) as, in the opinion of the EDPB:

"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.**" (emphasis added).

Specific

The consent in question effectively acts to bundle consent for transfers for multiple processing activities. It does not set out clearly what functions, services, or operations of the IAPP require transfers of personal data to the United States.

In paragraph 42 of the EDPB Guidelines on Consent, the EDPB states:

"A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR"

It is submitted that the IAPP's Data Protection Notice does not provide the several consents required for the multiple processing operations and purposes for which the transfers of personal data are required.

It is noted that the EDPB Guidelines on the application of Derogations under Article 49 references the requirements for specific consent in section 2.1.2 of that document, wherein it is stated that:

"The element "specific" in the definition of consent intends to ensure a degree of user control and transparency for the data subject."

As such it is submitted that the IAPP has failed to meet the "specific" requirement for valid consent under Article 4(11) of GDPR and cannot therefore rely on Article 49(1)(a) as a basis for transfers to a third country.

Unambiguous

Consent under GDPR requires a statement or a "clear affirmative act". Paragraph 77 of the EDPB Guidelines on consent state that:

"A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing.⁴³ Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means."

The EDPB's Example 14 in their guidance provides the vignette of software installation that requires the obtaining of consent for reporting. They specifically indicate that actively ticking an optional box stating "I consent" provides the mechanism for that "clear and affirmative act".

It is submitted that no such clear and affirmative act is recorded by the IAPP.

Paragraph 79 of the EDPB Guidelines on consent is clear:

“Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.”

Paragraph 81 of the EDPB Guidelines on consent is equally explicit:

“A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data”

It is submitted that merely proceeding with an application for membership or purchase of products or services from the IAPP “cannot be regarded as an active indication of choice” regarding transfers of personal data to the United States.

Freely Given

Paragraph 13 of the EDPB Guidelines on Consent informs us that the “freely given” element of consent “implies a real choice and control for data subjects”.

It is submitted that the consent relied upon by the IAPP for data transfers to the United States is not freely given as the data subject has no real choice. Furthermore, as the IAPP arguably enjoys a quasi-monopoly position in respect of professional membership organisations and mass-market accepted certifications for professionals working in the data protection disciplines, it is increasingly the case that career entry or progression in the field requires certification from the IAPP.

This is not intended as a criticism of the IAPP and their success as a professional organisation and their valuable work in developing and promoting baseline professional standards of competency and professionalism in the data protection field. However, it has been my personal experience that, as a result of the organisation’s success, being “IAPP Certified” is an increasingly important metric that is used by contracting authorities in various sectors in the evaluation of tenders or professional competencies of contractors.

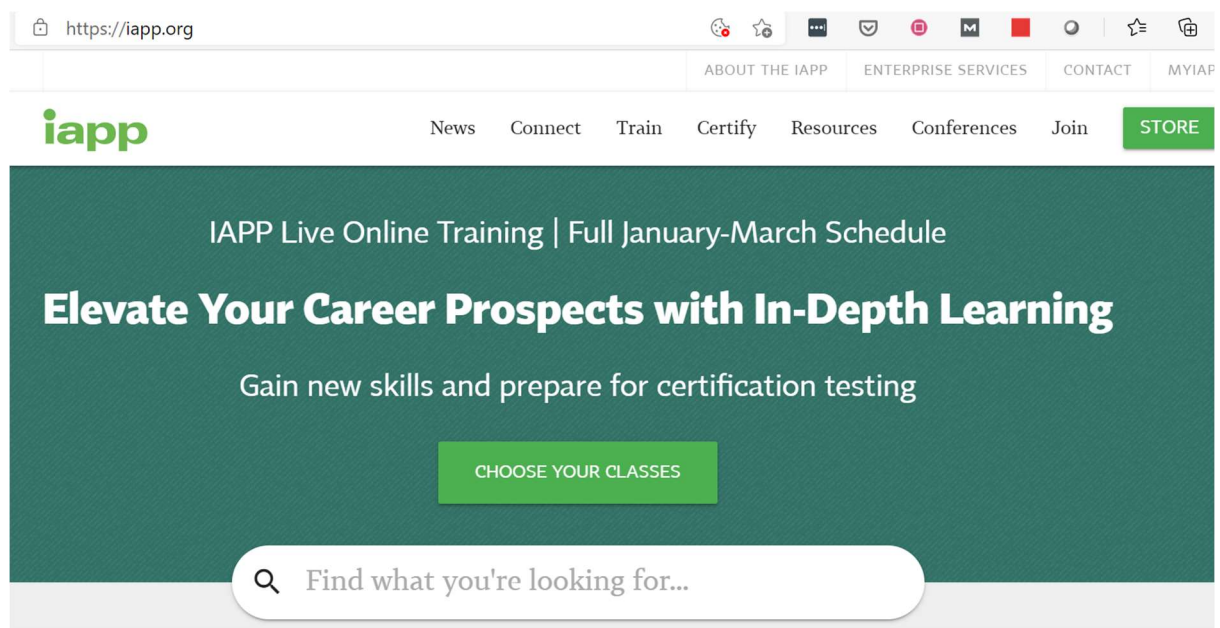


Figure 2 Screenshot from IAPP Homepage highlighting the perceived value of IAPP membership and education.

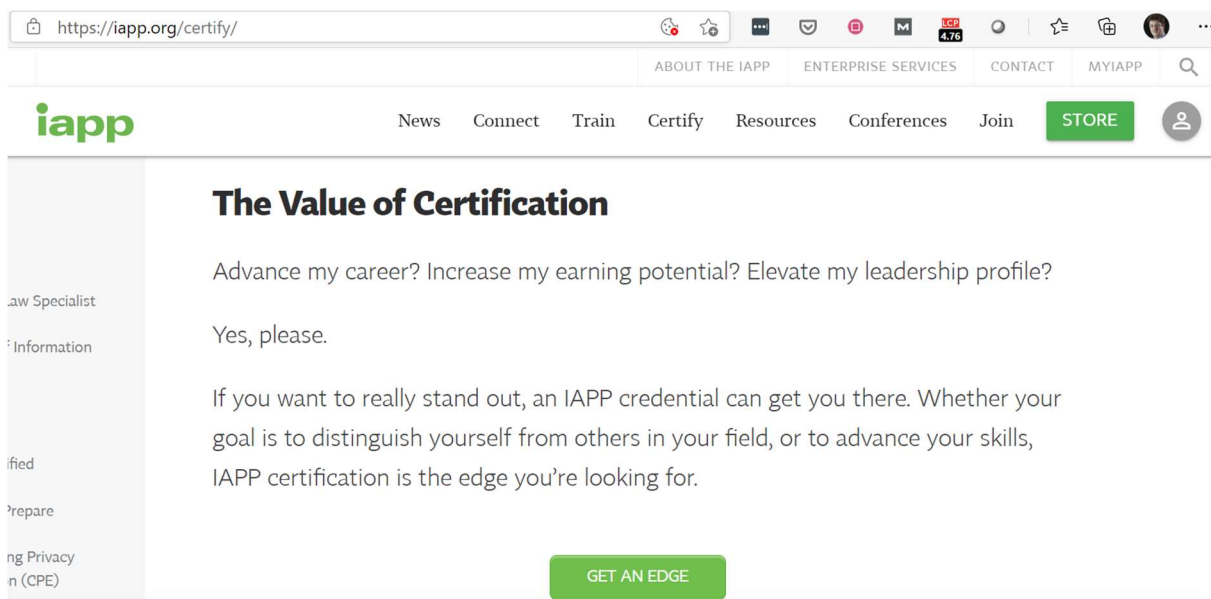


Figure 3 Screenshot from IAPP Certification page highlighting the value of IAPP Certification to career progression

Data subjects are unable to engage with the IAPP or obtain any of its certifications without their personal data being transferred to the United States. Therefore, it is submitted, data subjects feel compelled to consent or may perceive that by not consenting they may “endure negative consequences” as a direct or indirect result of not being able to hold IAPP membership or obtain or maintain IAPP certification and accreditation.

It is also submitted that the dominance of the IAPP in the market as the most recognised and recognisable professional body for data protection and data privacy practitioners and the certifying body for what is possibly the most widely recognised and best-known data protection certification examinations creates an imbalance of power between the IAPP and data subjects which renders it impossible for consent to be freely given in this context.

Again, this is not a criticism of the IAPP and its undisputed successful growth over the last twenty years, but it is a direct consequence of that success that an imbalance of power exists.

In paragraph 20 of the EDPB Guidelines on consent the example is given of a school requesting consent for the use of photographs. The guidance advises that:

“Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment”.

It is submitted that the IAPP’s consent for transfer of personal data to the United States is analogous to this example scenario and the same criteria for assessing the valid nature of the consent should be applied. In the context of the IAPP’s data transfers the consent relied upon cannot be considered a genuine choice as the population of affected data subjects (IAPP members, certification holders, prospective members, non-members attending events) will be denied “education or services” and are not in a position to refuse the transfer of personal data “without any detriment”.

Paragraph 24 of the EDPB Guidelines on Consent states unambiguously that:

“Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.”

It is submitted that, due to the dominance of the IAPP in the market as a professional body and as a provider of education and certifications which are increasingly considered minimum benchmark standards for competence in the data protection profession, and which are advertised and promoted by the IAPP on that basis, there is an inability on the part of data subjects to exercise free will in respect of the processing of their data by the IAPP, specifically with regards to the transfer of personal data outside the EU/EEA on the basis of Article 49(1)(a).

Explicit Consent

Section 4 of the EDPB Guidelines on Consent deal with the question of explicit consent, including in the context of data transfers in the absence of adequate safeguards under Article 49. Paragraph 93 states that:

“The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent”.

In paragraph 94 the EDPB guidelines suggest that a data subject may be able to provide the required express statement of consent through an online form or other electronic means.

It is submitted that this condition is not met as there is no express statement of consent obtained specifically to the transfer of personal data outside of the EU/EEA. As such, it is submitted that the explicit consent requirement of Article 49(1)(a) is not met.

Conclusion of analysis of this basis for transfer

In summary, it is submitted that the IAPP has failed to meet one or more of the conditions necessary to establish valid consent under Article 4(11) GDPR.

Furthermore, it is submitted that they have failed to meet the criteria necessary to establish explicit consent. As such, it is submitted that the IAPP does not meet the explicit consent requirement of Article 49(1)(a).

As either some or all of the required elements of the explicit consent derogation for cross border data transfer under Article 49(1)(a) are not met, it is submitted that transfers on this basis do not have any lawful basis under Article 44 GDPR.

Furthermore, as the IAPP has failed to provide any information in respect of the risks associated with the transfer of data to a third country, they have failed to meet the minimum standard set out by the EDPB with respect to the criteria for the application of the Article 49(1)(a) derogation and it cannot be applied.

Transfer based on the Compelling Legitimate Interest Derogation

The IAPP seeks to rely also on the “compelling legitimate interests” basis under Article 49(1) §2.

The information provided in respect of this derogation by the IAPP is as follows:

“In particular, the IAPP collects and transfers to the U.S. personal data only: with your consent; to perform a contract with you; or to fulfill a compelling legitimate interest of the IAPP in a manner that does not outweigh your rights and freedoms.”

No further information is provided in respect of the nature of these compelling legitimate interests.

It is submitted that this derogation only applies where a number of restrictive conditions and obligations are met.

- 1) The transfer is not repetitive, i.e. is occasional in nature.,
- 2) It concerns only a limited number of data subjects,
- 3) The compelling legitimate interests do not override the interests or rights and freedoms of data subjects,
- 4) The Controller must have assessed all circumstances surrounding the transfer and, on the basis of that assessment, provided suitable safeguards,
- 5) The processing is necessary for the purposes of those compelling legitimate interests,
- 6) The Controller must, in addition to their obligations under Article 13 and Article 14, inform the data subject of the transfer and of the compelling legitimate interests pursued.

The EDPB Guidelines on derogations under Article 49 highlights the tenuous nature of this derogation.

“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.”

The Guidelines also stat that:

“In line with the principle of accountability enshrined in the GDPR 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.”

It is submitted that the information provided in the Data Protection Notice of the IAPP does not meet the standard required to demonstrate that this derogation actually applies.

Provision of information about Compelling Legitimate Interests

Furthermore, it is submitted that no information is provided as to the compelling legitimate interests that are being pursued by the IAPP which would necessitate the transfer of personal data from the EU to the United States. The EDPB guidelines on the application of Article 49 derogations is clear that

“The data controller must inform the data subject of the transfer and of the compelling legitimate interests pursued.”

Repetitive nature of transfers

It is submitted that the management of membership and the operation of certification schemes constitute repetitive processing necessitating non-occasional transfers of data.

On that basis it is submitted that Article 49(1) §2 cannot be relied upon.

Scale of Transfers

It is submitted that the transfers relate to the entire membership of the IAPP in the Union. This is not a limited number of data subjects. Therefore this derogation cannot be applied.

Conclusion of analysis of this basis for transfer

It is submitted that the IAPP fails to meet the requirements necessary to rely on Article 49(1) §2 on the basis that:

- 1) No information has been provided to Data Subjects regarding the nature of these “compelling legitimate interests”,
- 2) Transfers are repetitive and non-occasional,
- 3) Transfers relate to a large number of data subjects.

It is not possible in the scope of this submitted complaint to evaluate or assess the existence of or appropriateness of any balancing tests or other evaluations which the IAPP are required to have done and which should have informed the safeguards in respect any proposed reliance on the derogation in Article 49(1) §2. However, it is noted that the EDPB Guidelines on the application of derogations under Article 49 explicitly requires the completion of such a balancing test:

“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.”

Transfer Necessary for Conclusion or performance of a contract between data subject and Controller (Article 49(1)(b))

Article 49(1)(b) can be relied upon as a derogation in specific limited circumstances that are constrained by necessity and the occasional nature of the transfers.

It is not in dispute in this complaint that the provision of member services, the operation of certification, and the management of the membership association aspects of the IAPP are done on the basis of contractual or quasi-contractual relationships between the data subject and the Controller. The purchase of reference materials and the annual renewal of membership are two examples where the conditions of a contract will exist.

Necessity Test

Within the context of the IAPP’s centralised business model where there are no IAPP legal entities at national or regional and given the centralisation of operating functions of the IAPP in the United States, this complaint does not contest the necessity of data transfers to the United States.

It is noted however that similar organisations such as DAMA International operate different and disparate operating models which allow for regional and geographic representative subsidiaries to be created which process membership information locally at the local “chapter” level (for example there is a DAMA Belgium Chapter which holds its own membership database).

Occasional Transfers

Transfers of personal data from the EU to the US are a regular and systemic aspect of the IAPP’s operations.

It is submitted that the IAPP’s operating model does not meet the requirement for “occasional transfers” under the Article 49(1)(b) derogation. It is noted that the EDPB Guidelines on derogations under Article 49 give the following example of a scenario where transfers would not be “occasional”.

“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).”

In the context of the IAPP's transfers, it is submitted that the IAPP systematically transfers the personal data of members, prospective members, event attendees, and certification examination candidates to the United States.

These transfers occur regularly within a stable relationship, specifically the existence of the IAPP as an entity that provides defined services and requires data to be submitted to them for the purposes of establishing and maintaining professional certification and accreditation as part of an ISO 17024:2012 accredited certification scheme.

The EDPB Guidelines on the application of derogations under Article 49 is explicit in its assessment of the application of the Article 49(1)(b) derogation in circumstances such as these:

"Data transfers regularly occurring within a stable relationship would be deemed as systematic and repeated, hence exceeding an "occasional" character."

Conclusion of Analysis of this basis for transfer

It is submitted that the IAPP, by reason of the regularly occurring transfers taking place within a stable relationship which are of their essence systemic and repeated, does not meet the criteria for the application of the "occasional" characteristic necessary for the application of Article 49(1)(b) to their data transfers from the EU to the United States.

Failure to meet obligations under Article 13 GDPR

Article 13(1)(f) GDPR requires Data Controllers, where applicable, to provide reference to the appropriate or suitable safeguards which have been implemented in respect of the transfer of personal data to a third country on the basis of the second paragraph of Article 49(1). Information must also be provided as to the means by which to obtain a copy of them or where they are made available.

It is submitted that the IAPP has failed to meet their obligation in this regard.

It is submitted that no information is provided in respect of the appropriate or suitable safeguards, other than the following:

"The IAPP endeavors to apply suitable safeguards to protect the privacy and security of your personal data and to use it only consistent with your relationship with the IAPP and the practices described in this Privacy Statement."

It is submitted that no information is provided in the Data Protection Notice as to the means by which details of the appropriate and suitable safeguards which are applied to the transfers of personal data from the EU to the United States may be obtained.

Furthermore, it is reiterated that, in the context of compelling legitimate interests which may apply to the transfers of personal data from the EU to the United States, no information is provided in the context of the Article 13 information relating to those compelling legitimate interests, as required under Article 49(1) §2.

Furthermore, it is submitted that the failure to disclose the consequences of failing to provide personal data to the IAPP through, for example, seeking to withdraw consent for transfers to the United States, constitutes an infringement of Article 13(2)(e).

Finally, it is submitted that the references to Article 41 and Article 44 in the Data Protection Notice have resulted in a technical breach of Article 13(1)(c) as the legal basis for processing has not actually been identified.