Transfer Impact Assessment (TIA)

VISMA IMS A/S
Søren Frichs Vej 44D
8230
Åbyhøj
Denmark
Company registration number:
25862015 (the "**Organization**)"

Regarding transfers of personal data

To Zendesk
1019 Market Street, San Francisco, CA
94103, USA
Company registration number: 26-4411091
(the "**Receiving Organization**")

1. Purpose and scope

1.1 This Transfer Impact Assessment (the "**TIA**") is prepared in order to assess and document the Organization's risks and compliance related to international transfers of personal data pursuant to the EU General Data Protection Regulation (2016/679 of 27 April 2016) (the "**GDPR**") to the Receiving Organization.

1.2 Based on the accountability principle in article 5(2) of the GDPR, the Organization has prepared this TIA in order to document its analysis of the level of data protection in the Receiving Organization's country, including the technical, organizational and contractual measures put in place, and the likelihood of harm to affected data subjects. Taking into account all these parameters, the data transfer is assessed by the Organization to document if the threshold set out in the GDPR and the European Court of Justice are met, and if the transfer can take place or continue to take place.

2. Assessment and structure

2.1 The TIA is based on the Organization's assessment which is scoped in accordance with the requirements set forth in the following:

2.1.1 Chapter V of the GDPR.

2.1.2 The European Court of Justice's judgment in the "Schrems II" case (C-311/18).

2.1.3 The guidelines in the European Data Protection Board's "Recommendations 01/ 2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (R01/2020) and "Recommendations 02/ 2020 on the European Essential Guarantees for surveillance measure" (R02/ 2020).

2.1.4 The European Data Protection Supervisor, "Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling" from 29 October 2020.

2.2 The following icons are used in this TIA in order to indicate the Organization's level of compliance with specific requirements in connection with the transfer:

✅ The parameter is identified as a circumstance that <u>does not negatively affect</u> the compliance of the international transfer that is either contemplated or already takes place.

⚠️ The parameter is identified as a circumstance that will <u>potentially result in the prohibition</u> of the international transfer that is either contemplated or already takes place.

❗ The parameter is identified as a circumstance that will <u>most likely result in the prohibition</u> of the international transfer that is either contemplated or already takes place.

⊘ The parameter has resulted in a sub-conclusion that is highlighted for information purposes.

2.3 The TIA is structured to primarily include and follow the steps described in the guidelines R01/2020 and R02/2020.

3. The Receiving Organization

3.1 The Receiving Organization is subject to this TIA is a data processor to the Organization and a sub-processor to the Organization's end-users and/or customers.

3.2 The Receiving Organization is itself from a third country i.e., outside the EU/EEA as specified on the front page of this TIA.

4. Circumstances of the transfer

4.1 In the following section, the circumstances of the transfer are assessed in order to identify potential high-risk circumstances.

Categories of personal data and data subjects

4.2 The transfer includes processing of the following types of non-sensitive personal data by the Receiving Organization:

a) the users first and last name or nickname
b) email-address
c) content from emails, including attachments
d) telephone number

✅ The processing made by the Receiving Organization does not include processing of any sensitive (special categories of) personal data as described in article 9(1) of the GDPR.

4.3 The transfer of personal data includes personal data concerning the following types of data subjects:

⊘ B2B customers and their employees. This type of data subject is categorized as a data subject type with a low score.

⊘ End-user customers. This type of data subject is categorized as a data subject type with a low score.

⊘ Current and former employees. This type of data subject is categorized as a data subject type with a low score.

⊘ Suppliers or affiliates and their employees. This type of data subject is categorized as a data subject type with a low score.

4.4 Processing activities and purposes

In the following section, the processing activities performed or contemplated along with the purpose for the same are outlined to identify any potential high-risk circumstances.

In the relationship between the Organization and the Receiving Organization, the following processing activities are or will be performed by the Receiving Organization: Hosting of support ticket system

4.5 In the sections below, the Organization has assessed if high-risk processing activities occur. The high-risk processing activities have been identified in accordance with the Article 29 Working Party guidelines no. 248 (WP248 rev. 01).

✅ The Receiving Organization does not process nor contemplate to process biometric data for the purpose of uniquely identifying one or more natural persons in the context of at least one additional criterion as mentioned in the Article 29 Working Party guidelines (WP 248 rev. 01). The Organization should however be aware that this scenario is just one of several examples where it is likely that there is always a high risk for the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not process nor contemplate to process genetic data for the purpose of uniquely identifying one or more natural persons in the context of at least one additional criterion as mentioned in the Article 29 Working Party guidelines (WP248 rev. 01). The Organization should be aware that this scenario is just one of several examples where it is likely that there is always a high risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not process nor contemplate to process location data for the purpose of uniquely identifying one or more natural persons in the context of at least one additional criterion as mentioned in the Article 29 WorkingParty guidelines (WP248 rev. 01). The Organization should be aware that this scenario is just one of several examples where it is likely that there is always a high risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not process or contemplate to process personal data by using new technologies in the context of at least one additional criterion as mentioned in the Article 29 Working Party guidelines (WP248 rev. 01). The Organization should be aware that this scenario is just one of several examples where it is likely that there is always a high risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not process nor contemplate to process personal data that leads to decisions about a data subject's right to a product, service, potential opportunity or favor based on any form of automated decision making (including profiling). The Organization should be aware that this scenario is just one of several examples where it is likely that there is always a high risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not carry out nor contemplate to carry out large- scale processing of personal data that includes profiling of natural persons as defined in the Article 29 Working Party guidelines (WP 248 rev. 01). The Organization should be aware that this scenario is just one of several examples where it is likely that there is always a high risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not carry out nor contemplate to carry out processing of personal data about vulnerable persons or where sensitive data (special categories) is being processed and where profiling or other automated decisions are being used. The Organization should be aware that this scenario is just one of several examples where it is likely that there is always a high risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

✅ The Receiving Organization does not process nor contemplate to process personal data where a personal data breach can have a direct effect on the protection of the physical health of a natural person. The Organization should be aware that this scenario is just one of several examples where it is likely that there is always ahigh risk to the rights and freedoms of the data subjects according to the Danish Data Protection Agency and the former Article 29 Working Party.

⚠️ The Receiving Organization will transfer personal data onwards to one or more sub-processors. The Organization will prepare a transfer impact assessment or collect a document with the same content from the Receiving Organization or its sub- processors.

⚠️ The Receiving Organization will transfer personal data onwards to one or more public authorities. The Organization will prepare a transfer impact assessment or collect a document with the same content from the Receiving Organization or the receiving public authorities.

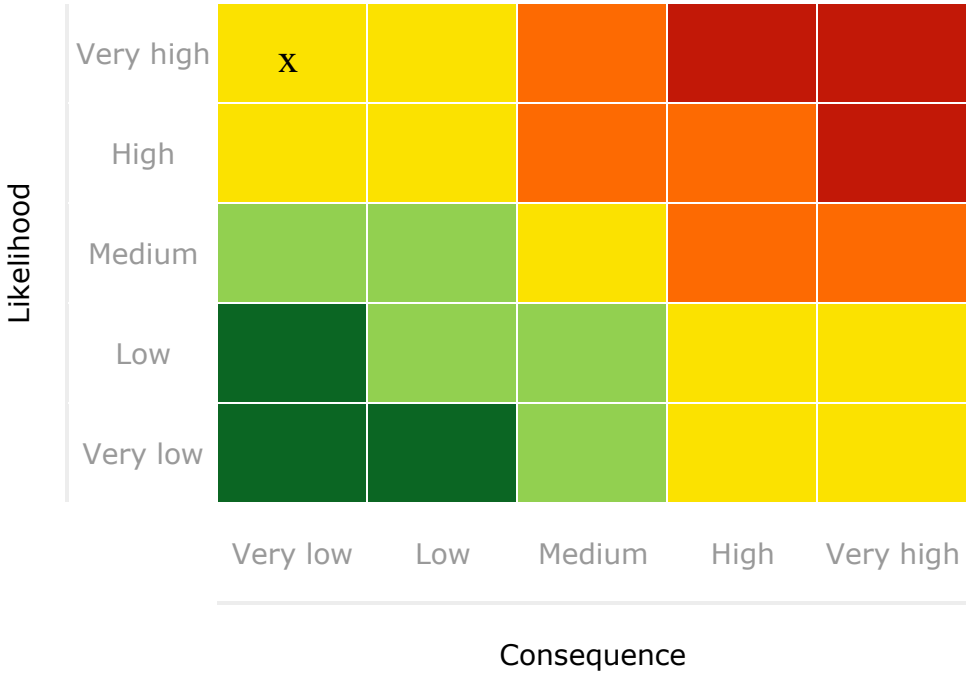
✅ Personal data covered by the transfer under this TIA will not be transferred onwards to other controllers.

5. Risk assessment

5.1 In this section, the Organization has conducted a general data protection risk assessment of the Receiving Organization's processing of personal data.

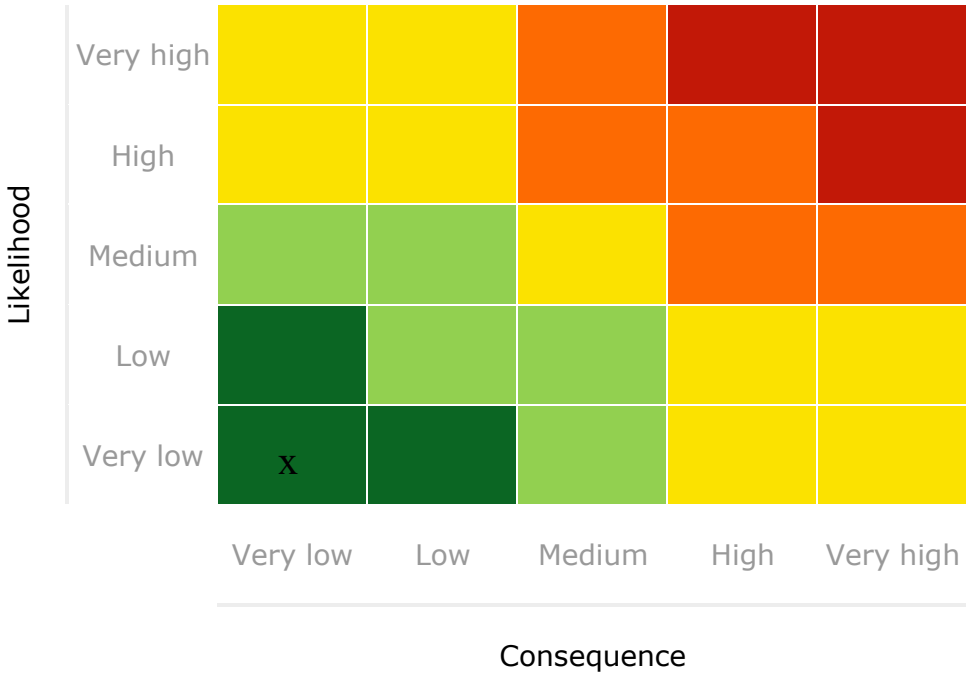
5.2 Confidentiality

In the heat map below, the Organization has assessed the overall risk to the confidentiality of the transferred personal data subject to this TIA. The risk assessmentis based on a score of the potential negative consequences for the data subjects if the confidentiality to the personal data is breached and on a score of the likelihood of the confidentiality being breached. When assessing the likelihood, the Organization has considered the known factors and threats along with the Organization's implemented security measures. The transfer itself and the third country subject to this TIA is not covered by the risk's assessment below as the assessment of the adequacy of the security measures in this respect will be assessed below under "Supplementary measures". The risk assessment is therefore conducted to give a full picture of the circumstances surrounding the transfer.



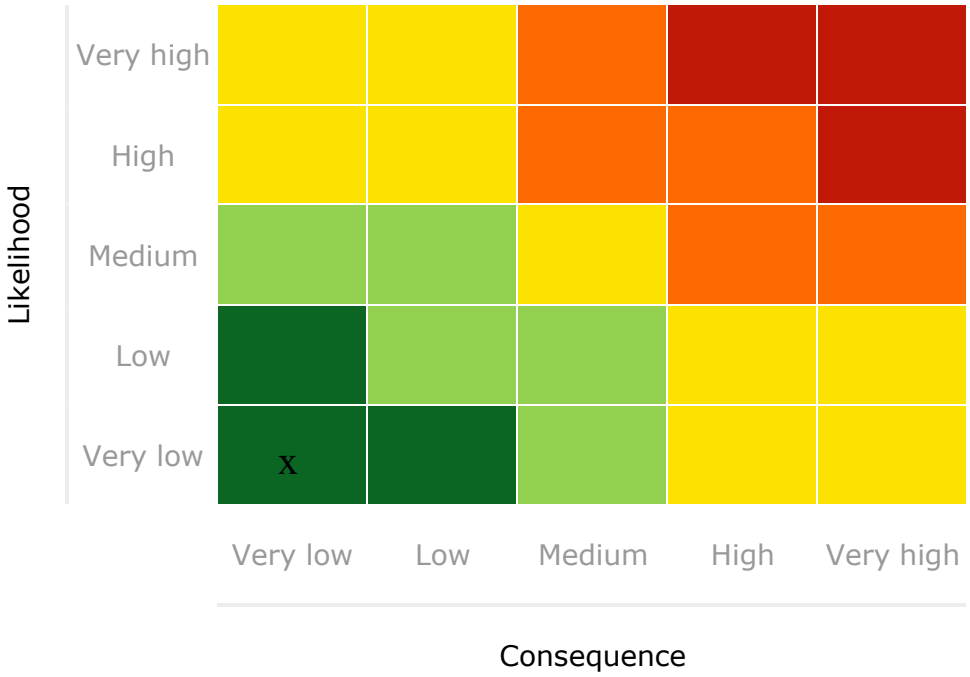
5.3 Integrity

In the heat map below, the Organization has assessed the overall risk to the integrity of the transferred personal data subject to this TIA. The risk assessment is based on a score of the potential negative consequences for the data subjects if the integrity in the personal data is breached and on a score of the likelihood of the integrity being breached. When assessing the likelihood, the Organization has considered the known factors and threats along with the Organization's implemented security measures. The transfer itself and the third country subject to this TIA is not covered by the risk assessment below as the assessment of the adequacy of the security measures in this respect will be assessed below under "Supplementary measures". The risk assessment is therefore conducted to give a full picture of the circumstances surrounding the transfer.



5.4 Availability

In the heat map below, the Organization has assessed the overall risk to the availability of the transferred personal data subject to this TIA. The risk assessment is based on a score of the potential negative consequences for the data subjects if the availability to the personal data is breached and on a score of the likelihood of the availability being breached. When assessing the likelihood, the Organization has considered the known factors and threats along with the Organization's implemented security measures. The transfer itself and the third country subject to this TIA is not covered bythe risk assessment below as the assessment of the adequacy of the security measures in this respect will be assessed below under "Supplementary measures". The risk assessment is therefore conducted to give a full picture of the circumstances surrounding the transfer.



5.5 Taken the supplementary organizational safeguard, i.e., VISMA IMS´ company policy that forbids processing outside the provide instruction from the Customers and forbids including personal data of the end users if requesting for support from the receiving company into account, the residual risk is low.
Therefore, the overall risk is low, but seeing as there still is a risk of breach of confidentiality, it cannot be ignored or labeled unimportant, and therefore, further attention is still required.

5.6 The risk assessments above will be considered when assessing the potential need for "supplementary measures" below.

Implemented security measures

The security measures listed below concern the data security at the Receiving Organization and does not relate to the transfer of personal data. The Receiving Organization has implemented the following security measures:

a) **Information Security Program.** Zendesk will maintain an information security program (including the adoption and enforcement of internal policies and standards of administrative, technical, physical and organisational safeguards) designed to protect the confidentiality and integrity of service data, appropriate to the nature, scope, context and purposes of processing and the risk involved in the processing for the data subjects. Zendesk maintains a globally distributed security team on call 24/7 to respond to security alerts and events.

b) **Physical Security**

Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

c) **Limited Employee and Contractor Access.** Zendesk takes reasonable measures to prevent Service Data from being used without authorisation. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its Affiliates.

d) **Physical Security Protections.** Zendesk benefits from the impressive organisational measures implemented by AWS. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All

physical access to the Facilities by employees and contractors is logged and routinely audited.

e) **Continued Evaluation.** Zendesk´s network is protected through the use of key AWS security services. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews

See also:
- https://www.zendesk.com/trust-center/
- aws.amazon.com/products/security/?nc=sn&loc=2

Residual risk

5.7 Considering the identified risks and the implemented data security measures (described in further detail elsewhere and for data processors in the data processing agreement), the Organization has concluded the below with regard to the residual risk associated with the processing at the Receiving organization. Please note that this residual risk does not include the risks associated with the transfer or the third country, but only includes the residual risk associated with the processing itself.

☑ The risk is assessed to be low and acceptable after comparing the identified risks with the implemented security measures. Although this residual risk assessment does not consider the risks associated with the international transfer of personal data, the present risk assessment does, however, play an important role when concluding whether the transfer is legal in the assessment conclusion, reference is made hereto.

6. The transfer tools

6.1 In this section, the Organization has outlined which transfer tool(s) is/are in use to ensure compliance with Chapter V of the GDPR.

☑ a) The EU Commission's Standard Contractual Clauses, cf. article 46(2)(c) of the GDPR, are used as a transfer tool. The Standard Contractual Clauses constitute a legitimate basis for the performed or contemplated transfer of personal data to the Receiving Organization, provided that the Receiving Organization's country provides a level of data protection essentially equivalent to that guaranteed within the EU by the GDPR, read considering the Charter of Fundamental Rights. Please refer to the sections below, namely the sections concerning the country in question and the implemented supplementary measures.

b) Binding Corporate Rules is used as the transfer tool, cf. article 46(2)(b) and 47 of the GDPR. Binding Corporate Rules constitute a legitimate basis for the performed or contemplated transfer of personal data to the Receiving Organization, provided that the Receiving Organization's country provides a level of data protection essentially equivalent to that guaranteed within the EU by the GDPR, read considering the Charter of Fundamental Rights. Please refer to the sections below, namely the sections concerning the

country in question and the supplementary measures.

c) There is no transfer tool in place as the Receiving Organization is located within the EU and the EEA, and a transfer tool is therefore not needed.

7. The country and its legal regime

7.1 In this section, the Organization has assessed the legal regime in the Receiving Organization's country: USA.

⚠ As the Receiving Organization is from USA, the transfer will be subject to the Presidential Executive Order no. 12.333 enabling US agencies and authorities to conduct unspecific surveillance of data transferred from EU and to the US via the "Upstream" program initiated under the Presidential Executive Order no. 12.333. It is not specifically decided by legal authorities whether this surveillance issue in itself prohibits the transfer unless "supplementary measures" are implemented. The current use cases from the European Data Protection Board do, however, indicate that the potential surveillance issue represents a circumstance that will prohibit the transfer unless "supplementary measures" are implemented. The potential surveillance issue is therefore identified as a "gap" that has to be filled and closed with "supplementary measures". If such "Supplementary measures" cannot be implemented, the transfer shall be stopped. This is the case, regardlessof the conclusion made under the European essential guarantees processed below.

❗ In addition to the above-mentioned surveillance issue under Presidential Executive Order no. 12.333, the Receiving Organization is categorized as an "Electronic Communication Service Provider" that is subject to section 702 of Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (called FISA 702). This entails that the Receiving Organization is subject to the surveillance program "Prism" and that US agencies and authorities can make specific requests in order to obtain data in connection with surveillance. The requests from US agencies and authorities can be directed both at US companies and EU subsidiaries to US companies. This surveillance issue is therefore identified as a "gap" that has to be filled with "supplementary measures". If such "supplementary measures" cannot be implemented, the transfer shall be stopped. This is the case, regardless of the conclusion made under the European essential guarantees set forth below.

Based on this, despite any review the essential European guarantees below, the Organization cannot for certain conclude that the Receiving Organization's country's legal regime and data protection level is essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter of Fundamental Rights. This is based on the European Data Protection Board's opinion that all essential guarantees must be fulfilled both individually and whenassessed as a whole. The transfer tool used is therefore not considered effective when considered individually. This will be taken into account when assessing theneed for "supplementary measures" below.

7.2 The Receiving Organization's country's legal regime and data protection level has beenassessed against the threshold of the European Essential Guarantees in accordance with R02/2020. The assessment of the European Essential Guarantees follows below.

7.3 **Guarantee A: Processing should be based on clear, precise and accessible rules** Pursuant to Article 8(2) of the Charter of Fundamental Rights of the European Union (the "Charter"), personal data should be processed for specified purposes and on the
basis of the consent of the person concerned or some other legitimate basis laid downby the law. Furthermore, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognized by the Charter within the EU must be provided for by law. This is elaborated in R02/2020, paragraph 26 ff.

The Organization is unsure of whether the potential processing of personal data made by the authorities in the country of the Receiving Organization can be considered to be based on “clear, precise and accessible rules”. Based on this and the essential European guarantees, the Organization cannot for certain conclude that the Receiving Organization’s country’s legal regime and data protection level is essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter of Fundamental Rights. This is based on the European Data Protection Board’s opinion that all essential guarantees must be fulfilled both individually and when assessed as a whole. The transfer tool used is therefore notconsidered effective when considered individually. The Organization must take this into account when assessing the need for “supplementary measures” as described below. The Organization will in any event re-evaluate this parameter onthe next occasion and no later than after a year, see section regarding re- evaluation.

Comment: FISA 702 is based on clear, precise, and accessible rules, but the practice of this law is not, and there is no possibility of obtaining information on the reason and proportionality of the processing, as well as no legal remedies for the data subjectwhose personal data is processed.

7.4 Guarantee B: Necessity and proportionality need to be demonstrated withregard to the legitimate objectives pursued

In accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognized by the Charter must respect the essence of those rights and freedoms. According to the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. This is elaborated in R02/2020, paragraph 32 ff.

The authorities in the country of the Receiving Organization are not able to demonstrate that the potential processing of personal data made by the authorities is “necessary and proportionate” regarding the legitimate objectives pursued. The Organization does therefore not consider Guarantee B to be fulfilled. Based on this and the essential European guarantees, the Organization cannot for certain conclude that the Receiving Organization’s country’s legal regime and data protection level is essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter of Fundamental Rights. This is based on the European Data Protection Board’s opinion that all essential guarantees must be fulfilled both individually and when assessed as a whole. The transfer tool used is therefore not considered effective when considered individually. This will be considered when assessing the need for “supplementary measures” below.

7.5 Guarantee C: Independent oversight mechanism

The European Court of Human Rights has specified multiple times that any interference with the right to privacy and data protection should be subject to an effective, independent, and impartial oversight system that must be provided for either by a judge or by an independent body (e.g., an administrative authority or a parliamentary body). This is elaborated in R02/2020, paragraph 39 ff.

✅ The potential processing of personal data made by the authorities in the country of the Receiving Organization is subject to an "independent oversight mechanism".The Organization therefore considers Guarantee C to be fulfilled.

Comment: There is an independent oversight mechanism, which, though, is unavailable for non-US citizens.

7.6 Guarantee D: Effective remedies need to be available to the individual

The final European Essential Guarantee is related to the redress rights of the individual. (S)he must have an effective remedy to satisfy his/her rights when (s)he considers that they are not or have not been respected. The European Court of Justice explained in Schrems I that

"*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the EU are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article*".

This is elaborated in R02/2020, paragraph 43 ff.

❗ There are not measures available to the individuals in USA that are considered effective. The Organization does therefore not consider Guarantee D to be fulfilled. The Organization must take this into account when assessing the need for "supplementary measures" as described below. The Organization will in any event re-evaluate this parameter on the next occasion and no later than after a year, see section regarding re-evaluation.

Comment: There are effective remedies, which, though, are unavailable for non-US citizens.

⚠️ Based on the above review of the third country in question and the essential European guarantees, the Organization cannot for certain conclude that the Receiving Organization's country's legal regime and data protection level is essentially equivalentto that guaranteed within the EU by the GDPR, read in light of the Charter of Fundamental Rights. This is based on the European Data Protection Board's opinion that all essential guarantees must be fulfilled both individually and when assessed as a whole. The transfer tool used is therefore not considered effective when considered individually. This will be taken into account when assessing the need for "supplementary measures" below.

8. Supplementary measures

8.1 Based on the accountability principle in article 5(2) of the GDPR and on R01/2020, the Organization has assessed the need for "supplementary measures" that – when added to the safeguards contained in the chosen transfer tool – could ensure that the data transferred to the third country is afforded a level of protection essentially

equivalent to that guaranteed in EU.

Necessity of supplementary measures

⚠ The Organization has concluded that the Receiving Organization's country does not provide a data level protection level that is essentially equivalent to the EU. Therefore, and in compliance with the Schrems II case and the recommendations from the European Data Protection Board, the transfer subject to this TIA is prohibited and shall be stopped, unless the Organization below concludes that the necessary supplementary measures are implemented.

8.2 In the sections below, the Organization has assessed which supplementary measures are necessary based on the processing activities and characteristics of the transfer and whether such supplementary measures are implemented.

Hosting or otherwise "at rest"

✅ The Organization has concluded that the personal data covered by the transfer subject to this TIA is encrypted after the transfer to the Receiving Organization's country. Even though the European Data Protection Board has not identified encryption after the transfer as a sufficient security measure to document adequate supplementary measures, the Organization considers the security measure relevant when assessing the collective circumstances relating to the transfer.

✅ The Organization can conclude that the encryption key is provided for and stored with a different supplier than the Receiving Organization and in an EU/EEA country. The European Data Protection Board has identified this security measure as necessary to document adequate supplementary measures in situations where data is hosted or otherwise "at rest" in the Receiving Organization's country. The Organization will either take this into account when identifying other supplementary measures below or remedy the gap by implementing this security measure.

Transit

🚫 Some or all of the personal data covered by this TIA and the occurring or contemplated transfer will be in transit in the Receiving Organization's country. This entails that the Receiving Organization must be subject to supplementary measures that corresponds to the risks associated herewith.

✅ The Organization has concluded that some or all of the personal data is encrypted and thereby pseudonymised before transit and that the pseudonymisation is performed with the effect that none of the personal data can be attributed to a person by other parties than the Organization. The European Data Protection Board has identified this security measure as a possible security measure and adequate supplementary measure in a specific situation regarding statistical research (use case no. 2, paragraph 80-83 in "Recommendations 01/2020 on measures that supplement transfer tools to

ensure compliance with the EU level of protection of personal data"). As the use case made by the European Data Protection Board is very specific, it is not certain that pseudonymization will be considered to suffice as a supplementary measure to fill in the gaps. For now, and unless otherwise specified below in the conclusion, the pseudonymization performed is considered to be an adequate supplementary measure with respect to the personal data in question. The Organization will take into account the development in the applicable guidance when the TIA is updated.

Other technical supplementary measures

8.3 In this section, the Organization will outline additional technical supplementarymeasures, if any, that has been implemented by the Receiving Organization.

All data is stored within the EU/EAA. Personal data is protected and stored safely in rest by AES 256-bit CBC data encryption. Transport encryption is used and for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of this third country using TLS 1.2 or higher. The customer agrees that AES 256-bit CBC data encryption and TLS 1.2 are considered as specific protective and state-of-the-art measures to be used against active and passive attacks on the sending and receiving systems. VISMA IMS ensures the transport encryption, including tests for software vulnerabilities and possible backdoors, Using AES 256-bit CBC data encryption and TLS 1.2 the customers agrees that the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities if data are forced to third countries taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them and the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved. VISMA IMS guarantees that the encryption algorithm has been flawlessly implemented by properly maintained software. The keys are reliably managed by VISMA IMS. This means that the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organization for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured. The core setup is built around the AWS Key Management Service (KMS). Masterkeys are generated per customer and rotated regularly. The frequency for rotation of keys can be defined per customer need. For every object (file or text) stored in VISMA IMS, we use the Masterkey to generate an object key and a cipher (an encrypted version of the object key). In combination with a user/customer-specific context, we have secured the data in the best way. The Masterkeys are safely stored in VISMA IMS MasterKey Vault (CMV) and the cipher and the id of the Masterkey is saved together with the object for use together with the Masterkey when decrypting the data. To be able to protect the Masterkeys, we have an Unseal Vault placed outside AWS. The VISMA MasterKey Vault is only accessible by having access to the

Unseal Vault. The communication is protected by the use of TLS to encrypt the communication.

The AWS SES uses client-side encryption before sending it to Amazon Simple Storage Service (Amazon S3). It is necessary to decrypt the content after retrieving the mail from Amazon S3. Amazon does not have permission to decrypt and cannot decrypt encrypted email messages on our behalf.

Further description on technical supplementary measures can be forwarded upon request.

Contractual supplementary measures

8.4 In this section, the Organization will outline contractual supplementary measures, if any, that have been implemented by the Receiving Organization.

8.5 The Organization has established Contractual supplementary measures with the receiving company that generally consist of unilateral contractual commitments.
These measures are combined with the above-mentioned technical measure and the below mentioned organizational measures to provide the level of data protection required.

- Providing for the contractual obligation to use specific technical measures
- Transparency obligations
- Obligations to take specific actions
- Empowering data subjects to exercise their rights

Organizational supplementary measures

8.6 In this section, the Organization will outline organizational supplementary measures, ifany, that have been implemented by the Receiving Organization.

8.7 Internal policy and awareness on the prohibition of using Support when the support case includes personal data. Thorough background checking of all employees and additional security clearance of employees with access to customer data. Procedures are in place for overall IT-security and handling of personal data. Access to IT-systems and customer data is conditional, and only selected persons has access to the information in accordance with their company role and work-related need for such access. All employees are legally bound by their employment contract and policies to adhere to:

- §§7 and 14 in their employment contract
- Declaration of confidentiality
- It-security and personal data policy

Employees are kept updated and trained on GDPR and handling of personal data, and compliance measures have been put in place.

9. Assessment conclusion

9.1 Taking into account the assessments conducted in the above sections, the Organization has concluded the following about the transfer in scope of this TIA:

Given the technical, organizational, and contractual security measures, VISMA IMS assesses that the use of the receiving company secure and following most essential guarantees stemming from the aforementioned rights. In addition, ceteris paribus, there will not be much difference in how these cases are enforced in Denmark. Although we cannot determine the proportionality and necessity, as well as challenge decisions on monitoring in connection with intelligence, in our view there will be an assurance that data will be used for exactly this purpose: intelligence matters. Therefore, it is considered that the possibility of secret illegal sharing of data with US intelligence services is contrary to EU law, but that possible termination of the cooperation relationship with the receiving company would not fully solve the problem. In addition, as we do not have confirmation that the receiving company pulls, has pulled, or will pull Visma IMS data. With the current technical measures implemented we also consider it as impossible for the receiving company to pull data from Visma IMS and the customers using the Visma IMS platform. Also as stated in written from Datatilsynet the receiving company would be viewed as an independent data controller for the transfer of personal data from the EU to the US. We are awaiting developments in relation to the EDPB's adopted Recommendations 01/2020 as well as the political developments between the US and the EU. We will also examine additional encryption options and privacy settings. In addition, we will update our Transfer Impact Assessments parallel with new developments in the area, both politically, legally, technically, etc., and according to risks involved.

10. Applicable procedural steps

10.1 The Organization will use its best endeavors and reasonable measures to initiateand implement all procedural steps identified in the above.

11. Re-evaluation of the TIA

11.1 Based on the accountability principle in article 5(2) of the GDPR and on R01/2020, the Organization will re-evaluate this TIA and the Receiving Organization at least once a year as part of the Organizations' annual cycle of self-assessments and audits.

12. Changes to this TIA

12.1 The Organization may change this TIA and prepare it in several versions. If it is changed, the Organization will maintain copies of all versions.

13. Contact

13.1 If you have questions or comments to this TIA, you can always direct them to

Søren Skou Jessen, senior legal advisor Phone: +45 29 36 51 64 Email: soren.jessen@visma.com.