

Transfer Impact Assessment (TIA)

Prepared by

INNOMATE A/S
Ørestads Boulevard 73
2300 København S

Company registration number: 15882271
(the "**Organization**")

regarding transfers of personal data to

[PartName]
[PartAdresse]
[PartZipCity]
[PartCountry]
Company registration number: [PartCVR]
(the "**Receiving Organization**")

Table of contents

1. Purpose and scope	(link)
2. Assessment method and structure	(link)
3. The Receiving Organization	(link)
4. Circumstances of the transfer	(link)
5. General risk assessment	(link)
6. The transfer tool	(link)
7. Assessment of the Receiving Country's legislation	(link)
8. Assessment of authority practices	(link)
9. Supplementary measures	(link)
10. Assessment conclusion	(link)
11. Applicable procedural steps	(link)
12. Re-evaluation of the TIA	(link)
13. Changes to the TIA	(link)
14. Contact and questions	(link)

1. **Purpose and scope**


- 1.1 This Transfer Impact Assessment (the “**TIA**”) is prepared in order to assess and document the Organization’s 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 The purpose of the TIA is to determine if there, considering the specific circumstances of the transfer, is reason to believe that local legislation and practices in the Receiving Country prevent the Receiving Organization from fulfilling its obligations regarding the protection of the fundamental rights of the data subjects. This is especially important where such legislation and practices authorize public authorities to access the transferred personal data.
- 1.3 The Organization has taken account of the following when preparing the TIA: (1) Relevant circumstances of the specific transfer; (2) legislation and practices of the receiving country, which might interfere with the safeguards of the transfer tool; and (3) the level of protection afforded within the EEA, as well as any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards of the transfer tool.
- 1.4 Since the Receiving Organization is the European based subsidiary of a parent company incorporated outside the EEA in USA, the subject of this TIA is the legislation and practices in place said country which may henceforth be referred to as the “**Receiving Country**”. The reader should be aware that this does not indicate that the Organization exports personal data to the Receiving Country, or that personal data transferred between the parties will necessarily be processed in the Receiving Country. The TIA is solely prepared in order to ensure the highest possible degree of confidence in the compliance of the inter-European transfers between the parties, and to demonstrate the Organizations observance of the accountability principle in article 5(2) of the GDPR, as to onward transfers by the Receiving Organization to its parent entity which may under article 46 transfer tools in place between them.
- 1.5 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 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. Version 2.0. Adopted on 18 June 2021." (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 does not negatively affect the compliance of the international transfer that is either contemplated or already takes place.
 - ⚠ The parameter is identified as a circumstance that increases the risks posed to the rights of the data subjects following the international transfer that is either contemplated or already takes place.
 - ❗ The parameter is identified as a circumstance that raises significant questions as to the risk posed to data subject rights, and the effectiveness of the transfer tool in providing adequate protection of data subject rights following 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 a processor to the Organization and a sub-processor to the Organization's end-users and/or customers.
- 4. Circumstances of the transfer**
- 4.1 In order to document circumstances regarding the transfer that may be relevant for the effective protection or lack thereof of the chosen transfer tool.
- 4.2 Categories of personal data**
- a) Basic personal data (for example place of birth, street name and house number)

- (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth)
- b) Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details)
 - c) Authentication data (for example user name, password or PIN code, security question, audit trail)
 - d) Unique identification numbers and signatures (for example social security number, bank account number, ID card number, vehicle registration data, IP addresses, unique identifier in tracking cookies or similar technology)
 - e) Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness)
 - f) Photos, video and audio
 - g) HR and recruitment data (for example recruitment information, job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, and location and organizations);
 - h) Education data (for example education history, current education, grades and results, highest degree achieved, learning disability)

 The transfer includes processing of the following types of sensitive personal data as defined in article 9(1) of the GDPR, by the Receiving Organization: information concerning health of one or more persons (health, illness, diagnosis, etc.), information about trade union membership

4.3 Categories of data subjects

- a) Employees, contractors and temporary workers (current, former, prospective)
- b) Users (e.g., customers, clients, patients, visitors, etc.)

4.4 Nature and purpose of the processing activities

INNOMATE makes the cloud-based HR solution 'INNOMATE HR' available to the data controller, so that the data controller can thereby store and access personal information that is registered about the data controller's employees in connection with HR processes ranging from recruitment to resignation.

Via INNOMATE HR, the data controller collects, registers and organizes e.g., personal information about the data controller's employees. The data processing also includes changes and deletion of personal data as well as ongoing transmission of the personal data between the data controller, the data processor and its sub-data processors.

The data processor's processing primarily concerns the loading, registration, storage, systematization, processing and deletion of the data controller's personal data and to ensure that the data controller's handling of personal data takes place in accordance with the GDPR Regulation.

The processing includes the following categories of data subjects:

- Employees who are or have been employed by the data controller
- Persons who apply or have previously applied for a position with the data controller
- Other persons, without employment, but who assist the data controller.
- The data controller - in connection with the administration and management of

financial balances and customer care.

INNOMATE processes both general and sensitive personal data for the data controller.

- 4.5 Industry: INNOMATE's business area is HR-Tech - we develop and implement web-based solutions for HR.
- 4.6 Scope: We process personal data for approx. 17,000 employees spread over approx. 60 companies.
- 4.7 Format: The data processor processes the following categories of personal data about the data controller and his / her employees / end users:

General personal information

- Name, telephone number, address, email, employee photo, position, CPR no., Next of kin, Job application, CV, Employment contract, Salary information / deduction percentage and tax deduction, courses / educations, competencies, agreements, free text and the like.

Sensitive personal information

- Trade union affiliation, non-disclosure, sick days, health information, service conditions.

- ✓ Personal data covered by the transfer under this TIA will not be transferred onwards to sub-processors.
- ✓ Personal data covered by the transfer under this TIA will not be transferred onwards to public authorities.
- ✓ Personal data covered by the transfer under this TIA will not be transferred onwards to other controllers.

5. **General risk assessment**

- 5.1 A general risk assessment has not been included in this TIA as it is of no relevance to the effectiveness of the transfer tool with regard to the protection of the data subject rights under the specific conditions of the transfer.

6. **The transfer tool**

- 6.1 Standard data protection clauses adopted by the European Commission in accordance with the examination procedure referred to in article 93(2) of the GDPR, cf. article 46(2)(c).

7. **Assessment of the Receiving Country's legislation**

- 7.1 **Legislation establishing rights of privacy and/or data protection**
-

- 7.1.1 The Receiving Country protects privacy as a right, in a manner which precludes public authorities from accessing the transferred data, as the main rule.

This conclusion is reached based on the following:

- 7.1.2 The U.S. Constitution asserts a set of rights, subject to judicial review, protecting the individual against the actions of public authorities. For government access to personal data held by the private sector, the Fourth Amendment plays a particularly important role.
- 7.1.3 In brief Fourth Amendment applies to searches and seizures within the U.S. territory such as when data is transferred to and stored within the U.S., as well as to searches against U.S. persons that take place outside of the United States.
- 7.1.4 For foreign intelligence collected in the U.S., the Fourth Amendment continues to apply, as searches must meet the fundamental standard of reasonability found in the Fourth Amendment. See *In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).
- 7.1.5 When the U.S. government collects personal data inside the U.S., statutory protections apply in addition to the Fourth Amendment, including the Wiretap Act, 18 U.S.C. 119 §§ 2510-2522 and the Stored Communications Act, 18 U.S.C. 121 §§ 2701-2712.
- 7.1.6 The Fourth Amendment states: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*
- 7.1.7 Jurisprudence on Fourth Amendment protection has adapted to the rapid changes in technology, so as to cover electronic data held by the private sector.
- 7.1.8 See among others: *Riley v. California* (warrant needed to search cell phones), *United States v. Jones* (warrant needed when attaching a GPS device to a car), *Kyllo v. United States* (warrant needed for high-technology search of home conducted from the street), *United States v. Warshak* (warrant needed to access email), and *Carpenter v. United States*, (warrant needed to access cellphone location data).
- 7.1.9 Notably *Carpenter* holds that, personal data does not lose Fourth Amendment protections merely because it is stored on a "third party" server, amending the "third party doctrine" previously in place (See *United States v. Miller and Smith v. Maryland*).
- 7.1.10 Although non-U.S. persons, are not directly protected under the Fourth Amendment, the personal data transferred is indirectly protected because it, almost always, will be in the custody or form part of the protected communications of a U.S. person.
-

- 7.1.11 The term “U.S. person” extends to legal persons such as private companies established in the U.S. as well as subsidiaries abroad.
- 7.1.12 Notably, the indirect protection of non-U.S. persons, under the Fourth Amendment is comparable to that offered surveillance targets of The Danish Defense Intelligence Service (FE), insofar as these are not Danish or Danish residents.
- 7.1.13 FE processing is exempt from the GDPR and the implemented data protection mechanisms only apply to Danish citizens and persons permanently resident in Denmark. (See The Danish Defence Intelligence Act (Lov om Forsvarets Efterretningstjeneste §§ 4 – 6, 11), and “Sikkerhedsbekendtgørelsen vedrørende Forsvarets Efterretningstjeneste” § 1).
- 7.1.14 *Source(s):*
- The U.S. Constitution IVth Amendment
 - U.S. Supreme Court practice: *Riley v. California*, *United States v. Jones*, *Kyllo v. United States*, *United States v. Warshak*, *Carpenter v. United States*
 - *In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002)
 - Independent expert testimony by: Professor Peter Swire submitted before the Irish High Court in the original Schrems case. Available at: <https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony>
 - Lov om Forsvarets Efterretningstjeneste. Available at: <https://www.retsinformation.dk/eli/lta/2017/1287>
 - Sikkerhedsbekendtgørelsen vedrørende Forsvarets Efterretningstjeneste § 1

7.2 Interferences with the right to privacy

- 7.2.1 U.S. legislation allows for certain regulated interferences with the right to privacy, authorizing public authorities to access personal data held by the private sector, as specified below.

The interferences with the right to privacy identified by the Organization are specified as follows:

- 7.2.2 U.S. law allows for several specified interferences with the established rights to privacy. When assessing the “Privacy Shield” framework in *Schrems I* and *II* (C-311/18 and C-362/14) the Court of Justice of the European Union (“CJEU”) identified two regulated interferences of particular concern: Section 702 of the Foreign Intelligence Surveillance Act (Procedures for targeting certain persons outside the United States other than United States Persons) (“FISA 702”) and Executive Order 12333 (United States intelligence activities) (“EO 12333”). The organization therefore considers an analysis of these to be sufficient. No other problematic legislation has been identified explicitly by the court, nor by the Organization’s research of the U.S. legal regime.
- 7.2.3 FISA 702, authorizes the U.S. government to issue orders requiring companies

in the United States to disclose communications data of specific non-U.S. persons located outside the United States. The purpose is to obtain specified types of foreign intelligence information. Historically, foreign intelligence on non-U.S. persons gathered overseas, was processed under the regulatory framework of EO12333. However, with the advent of the internet a small number of U.S. companies came to be central to the global communications infrastructure. This situation meant that communications of interest to the intelligence community, for example sent between foreign targets in Russia and Bangladesh, was now located within U.S. borders. Under the previous FISA framework the government would be required to get individual warrants, as though surveilling U.S. citizens. As is entirely standard among national intelligence agencies, the standards of protection offered citizens and residents, differs from that afforded to foreign nationals on foreign territory.

- 7.2.4 Thus, the scope and applicability of FISA 702 is to target (1) specific non-U.S. persons, (2) not currently located within the U.S., whose (3) communications (4) are reasonably believed to contain foreign intelligence information, (5) by compelling electronic communication service providers to query and deliver communications from specific selectors. Selectors must be specific, e.g., usernames, emails or phone numbers, not names or general search terms ("bomb").
- 7.2.5 There are no indications that the U.S. government engages in indiscriminate or bulk collection under FISA 702. Collections are limited to information that relates to or is necessary to: protect against actual or potential attacks; protect against international terrorism and proliferation of weapons of mass destruction; conducting counterintelligence; and collecting information with respect to a foreign power or territory that concerns U.S. national defense or foreign affairs. See 50 United States Code (U.S.C.) § 1801(e).
- 7.2.6 Two programs conducted under FISA has raised particular attention of the CJEU namely "PRISM" and "UPSTREAM" collection.
- 7.2.7 "PRISM" concerns targeted collection of foreign intelligence communications through the compelled assistance of internet service providers, "UPSTREAM" targets communications infrastructure "backbone", including internet and telephone cable providers within the United States. In either case the target of surveillance is communications to and from non-U.S. persons currently outside the U.S., as identified by specific selectors.
- 7.2.8 "About" queries under the "UPSTREAM" program whereby any mention of a selector may cause a communication to be targeted are no longer practiced, (See FISC Memorandum Opinion and Order at 11-25 (26 April 2017)).
- 7.2.9 Secondly, the CJEU examined the NSA's gathering of signals intelligence (SIGINT) outside U.S. borders under EO12333. Particularly when surveilling submarine cables carrying internet communications as they cross the Atlantic. The interception and processing of foreign SIGINT is common practice among national intelligence agencies, both within an outside the territory of the EEA.

(See "Betænkning nr. 1529, om FE og PET", page 54).

- 7.2.10 EO 12333 does not in fact authorize any interferences with the right to privacy, as surveillance of foreign nationals on foreign territory does not fall within jurisdiction of the U.S. constitution, and statutory privacy laws. It does however circumscribe the processing of SIGINT data, for U.S. persons as well as non-U.S. persons.
- 7.2.11 The Organization recalls that no such regulation exists with regard to FE's processing of non-Danish non-resident SIGINT data, and while enforceable rights may be inferred from EU- or international law, there is no oversight with such processing. (See "FE-lovens" designation of applicability to in Denmark "hjemmehørende personer").
- 7.2.12 Furthermore, unlike FISA 702, EO 12333 does not authorize the U.S. government to compel any U.S. company to disclose data. Any requirement of disclosure to the government for intelligence purposes must be authorized by statute, such as through FISA 702 orders as discussed above.
- 7.2.13 Whereas U.S. governments may unilaterally acquire access to transferred personal data through clandestine operations, targeting of undersea cables, it is not clear that a hypothetical risk of such processing, impedes the continuation of the protection guaranteed within the EEA.
- 7.2.14 Personal data in transfer is potentially subject to SIGINT collection by a great number of state actors. This is also the case when the transfer is internal to the EEA. Many countries around the world, including the United States and EU Member States, collect bulk raw data for intelligence purposes.
- 7.2.15 This occurs both extraterritorially and within the country as the data transfers through.
- 7.2.16 No country currently acknowledges the specific locations and operational details of its clandestine operations concerning SIGINT collection. As such there is no way to determine the extent to which a data transfer might lead to processing by foreign intelligence services in violation of the data subjects' fundamental rights. This is the case whether, or not, the transfer occurs within the territory of the EEA.
- 7.2.17 The extend and ubiquity of bulk processing in connection with SIGINT, is evidenced in the recent "Big Brother Watch Judgement" (BIG BROTHER WATCH AND OTHERS, v. THE UNITED KINGDOM, 25th may, 2021).
- 7.2.18 The European Court of Human Rights held that bulk processing of SIGINT is not inherently disproportionate and expressly recognized a wide margin of appreciation for the States in deciding what type of interception regime was necessary to protect national security.
- 7.2.19 It should be noted that processing of personal data for national security purposes is usually exempt from the GDPR by virtue of Article 23 (1), and

subject to national legislation.

- 7.2.20 EU-member state intelligence agencies have not consistently implemented the standard of regulatory limitations and safeguards, put forth by the CJEU in Schrems I and II. This is the case regardless of the potential EU citizenship of the data subject.
- 7.2.21 For example, the national security processing of FE is exempted from the GDPR and “The Danish Data Protection Act” (see Databeskyttelsesloven § 3(2)). Aside from a storage limitation on raw SIGINT data for 15 years, the limitations on processing personal data contained in FE-loven, do not apply to non-resident, non-nationals (see FE-loven §§ 4 – 6, and § 10).
- 7.2.22 As such, there is in fact no national statutory limitations imposed on FE as to the processing of the personal data of non-Danish EU-citizens, insofar as these are not Danish residents.
- 7.2.23 Processing by third country intelligence services is also a risk. Recent media stories on NSA access to fiber cables on Danish territory, with the participation of FE, demonstrate that data subjects are not insulated from non-member states accessing personal data in transfer, even within the EEA.
- 7.2.24 There is no reason to believe only Danish authorities has allowed such access, and as all such programs are classified there is no way to determine their extend. Furthermore, intelligence is routinely exchanged between allied intelligence services, whether both parties are EU member states or not.
- 7.2.25 As noted by the CJEU in Schrems II (para. 92 and 93) the purpose of the transfer tools contained in GDPR Chapter 5, is to ensure the continuity of the high level of protection guaranteed within the EEA.
- 7.2.26 It follows that law and practices of the Receiving Country, can only impede the protection of the transfer tool, insofar as the data subject, by virtue of the transfer, loses the benefit of protections guaranteed by the legal framework of the EEA.
- 7.2.27 The intended function of the transfer tools contained in Chapter V of the GDPR, is not to add protections in addition to those guaranteed within the EEA, but to ensure the continuation of an essentially equivalent level of protection.
- 7.2.28 It follows, that a risk of clandestine SIGINT collection, could only possibly impede the effectiveness of the transfer tool, where protections limiting such processing are guaranteed within the EEA.
- 7.2.29 The Organization considers that, transfers of personal data occurring within the territory of the EEA might be subjected to SIGINT processing by foreign intelligence services, as signals may be collected directly by third countries or member states, operating clandestinely.
- 7.2.30 As demonstrated, EU citizens are not guaranteed enforceable rights, when

subjected to SIGINT surveillance within the EEA by foreign EU member state governments. Nor are EEA intelligence services consistently subjected to effective and independent oversight, especially when processing non-resident, non-citizen personal data.

- 7.2.31 Thus, the Organization does not consider the risk of unilateral clandestine SIGINT activities of the U.S. government, without the compelled co-operation of the Receiving Organization, occurring outside the territory of the United States, to be capable of affecting the Receiving Organizations ability to comply with the guarantees of the transfer tool. For the following reasons:
- 7.2.32 As the risk of clandestine SIGINT operations is present even within the EEA, it is not suitable to be remedied under Chapter 5 of the GDPR, which concerns the continuation of the protections guaranteed within the EEA as data is exported.
- 7.2.33 As EU-citizens, are not consistently guaranteed enforceable rights in this regard within the EEA, there is no clear basis of comparison when assessing the protection offered by the laws and practices of the Receiving Country.
- 7.2.34 As any number of third country governments may be engaged in clandestine SIGINT surveillance, which could hypothetically target any given transfer, it is not clear why only the practices of the Receiving Country should be assessed.
- 7.2.35 Even if the hypothetical SIGINT collection of the United States was to impede the protection of the transfer tool, the Organization considers that there is no reason to believe the U.S. government would target the specific transfer. As discussed below.
- 7.2.36 Thus, subject to the reservations described above Organization considers FISA 702 and SIGINT collection under EO 12333, as potentially capable of impeding the effective protections of the transfer tool.
- 7.2.37 *Source(s):*
- Section 702 of the Foreign Intelligence Surveillance Act (Procedures for targeting certain persons outside the United States other than United States Persons) Executive Order 12333 (United States intelligence activities)
 - CJEU practice: SCHREMS I and II (C-311/18 and C-362/14)
 - Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield
 - President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies 179 (dec. 12, 2013) Available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
 - Yearly Review of Danish Defence Intelligence Agency 2019 by Tilsynet med Efterretningstjenesterne. Available at: https://www.tet.dk/wp-content/uploads/2020/11/FE_2019.pdf
 - EU Agency for Fundamental Right Rapport: Surveillance by intelligence
-

services: fundamental rights safeguards and remedies in the EU

- Volume II: field perspectives and legal update. Available at <https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu>
- Privacy and Civil Liberties Oversight Board Report on Executive Order 12333
- Privacy and Civil Liberties Oversight Board Report on FISA 702
- U.S. Department of Commerce White Paper: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II
- Lov om Forsvarets Efterretningstjeneste (FE) med senere ændringer (FE-loven)
- European Union Agency for Fundamental Rights: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015. Available at:
 - <https://www.statewatch.org/media/documents/news/2015/nov/eu-fra-2015-surveillance-intelligence-services.pdf>

7.3 **Applicability of identified legislation interfering with the right to privacy**

7.3.1 As only legislation applicable to the transfer, can authorize public authorities to access it, the theoretical applicability of the interferences identified above will be discussed below.

7.3.2 The Organization estimates that legislation allowing for authority access, are applicable to the specific transfer, or cannot determine with certainty that they are not.

The conclusion is reached based on the following:

7.3.3 Above FISA 702 and overseas SIGINT collection was identified as possible interferences.

7.3.4 For the reasons discussed above, the Organization does not consider the hypothetical overseas SIGINT activities of the U.S. government to be capable of interfering with the protections of the transfer tool.

7.3.5 However, the organization recognizes that this view may conflict with the positions expressed by the CJEU and EDPB. As such, in order to provide the greatest possible confidence as to the compliance of the transfer, overseas SIGINT collection under EO12333, will nonetheless be considered a possible interference.

7.3.6 FISA 702 permits the government to conduct targeted surveillance of foreign persons located outside of the U.S. with the compelled assistance of electronic communications service providers, to acquire foreign intelligence information. The information is collected to protect the U.S. and its allies from hostile foreign adversaries, incl. terrorists and spies. Thus, the U.S. government can, through electronic communication service providers, use FISA 702 to targets non-U.S. Persons located abroad, who are expected to possess, receive or

communicate foreign intelligence information.

- 7.3.7 The Organization cannot determine with certainty that the transferred data would be considered communications between U.S. persons and not fall within the theoretical scope of FISA 702.
- 7.3.8 As concluded above, the Organization finds that legislation allowing for interference with the right to privacy might be applicable to the specific transfer. It follows from R01/2021 section 37 that interferences restricting the fundamental rights of data subjects must be limited to what is necessary and proportionate in a democratic society; they may not impinge on the commitments contained in the transfer tool relied upon.
- 7.3.9 Following the Schrems II judgement, the EDPB published guidelines on assessing whether surveillance measures are essentially equivalent to the level of protection guaranteed within the EU, under the title European Essential Guarantees for surveillance measures. The four guarantees are as follows:
- A. Processing should be based on clear, precise and accessible rules
 - B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
 - C. An independent oversight mechanism should exist
 - D. Effective remedies need to be available to the individual
- 7.3.10 In the following section the interferences with the right to privacy and data protection discussed above will be assessed in the light of the guarantees.

7.4 **Guarantee A: Processing should be based on clear, precise and accessible rules**

- 7.4.1 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 down by the law. Furthermore, under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter within the EU must be provided for by law. This is elaborated in R02/2020, paragraph 26 ff.
- 7.4.2 The potential access to personal data by the authorities in the country of the Receiving Organization, interfering with the fundamental rights of the data subject, is based on "clear, precise and accessible rules". The Organization therefore considers Guarantee A to be fulfilled.

This conclusion is based on the following:

- 7.4.3 Processing under FISA 702 clearly limits government access to transferred data to specified purposes, acquired based on specific selectors of individual non-U.S. persons. The legislation lays down procedures by which the categories of people that might be subjected to surveillance are defined. It limits the duration of the measures and defines the procedures to be followed when examining, using and storing the data obtained. All processing is subjected to a general standard

of reasonability, and the additional minimum safeguards discussed above.

- 7.4.4 Personal data gathered extraterritorially as SIGINT under EO12333, is subject so the safeguards specified in PPD-288. The Organization recognizes the hesitation of the CJEU, regarding SIGINT collection under EO12333, but does not consider it to provide an essentially inferior protection when compared with equivalent regulation within the EEA, see for example the regulation on the German SIGINT program (Act on the Federal Intelligence Service, Sections 1 (1) and 2(1)9, the regulation on Italian Intelligence Activities (Law No. 124 of 3 August 2007 “Intelligence System for the Security of the Republic and new Provisions governing Secrecy”, Section 26), or the Danish Defence Intelligence Act §1.
- 7.4.5 The legislation allowing the national security agencies of the EEA to gather intelligence extraterritorially, does not consistently ensure data subjects enforceable rights, regardless of their potential status as EU citizens.
- 7.4.6 Nor does it consistently provide a definition of the categories of people that might be subject to surveillance, a limit on the duration of the measure, the procedure to be followed for examining, using and storing the data obtained, and the precautions to be taken when communicating the data to other parties, as referenced in R02/2021, section 39.
- 7.4.7 Moreover, the assessment must also take into consideration recent ECtHR practice on bulk intelligence processing for national security purposes, asserting the wide margin of appreciation given to States in determining national security measures.
- 7.4.8 *Source(s):*
- EO 12333
 - FISA 702
 - Presidential Policy Directive 28 (PPD-28)
 - German, Act on the Federal Intelligence Service. Available at: <http://www.gesetze-im-internet.de/bndg/BJNR029790990.html>
 - European Union Agency for Fundamental Rights: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015
 - Law No. 124 of 3 August 2007 “Intelligence System for the Security of the Republic and new Provisions governing Secrecy”
 - BIG BROTHER WATCH AND OTHERS, v. THE UNITED KINGDOM, 25th may, 2021

7.5 **Guarantee B: Necessity and proportionality need to be demonstrated with regard to the legitimate objectives pursued**

- 7.5.1 In accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised 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 recognised

by the EU or the need to protect the rights and freedoms of others. This is elaborated in R02/2020, paragraph 32 ff.

- 7.5.2 For the reasons specified below, the Organization does not consider Guarantee B to be fulfilled, meaning that 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” with regard to the legitimate objectives pursued.

This conclusion is based on the following:

- 7.5.3 The CJEU clearly stated in Schrems II (para. 180-184) that it did not consider access to personal data by U.S. government agencies pursuant to FISA 702 and EO12333 to be “necessary and proportionate” measures, even considering the protections offered by PPD-28.
- 7.5.4 The Organization takes note, that some of the considerations of the Court, based on the “Privacy Shield Decision”, could be challenged namely:
- 7.5.4.1 That the “FISA Court” (FISC) does not cover the issue of whether individuals are properly targeted by FISA 702. (para. 179.) Though it is true that individual targeting is not subject to FISC review, FISC indirectly oversees the individual targeting practices, as every targeting assessment and rationale made by NSA analysts and every selector tasked for data acquisition is reviewed by independent intelligence oversight attorneys in the Department of Justice (DoJ). The DoJ review board is legally obligated to report any non-compliance to the FISC.
- 7.5.4.2 That there is no limitation to the power FISA 702 conveys to surveil non-U.S. persons for the purpose. (para. 180) As discussed above, surveillance under FISA 702 is subject to a general standard of reasonableness and is subject to procedural rules which circumscribe the range of surveillance, both in terms of targeting and content of the targeted communications.
- 7.5.4.3 Although the court remarks that PPD-28 does not confer the data subjects’ actionable rights (para. 181-182), the Organization recalls that, at present, no equivalent rights are necessarily secured by EU member states, even within the EEA, as discussed above.
- 7.5.5 Furthermore, the Organization has included in the assessment relevant changes to U.S. law implemented since the deciding facts of Schrems II, were recorded in the “Privacy Shield Decision” of July 2016.
- 7.5.6 These include inter alia a prohibition on “about” queries in the UPTREAM program, more vigorous review of FISA 702 targeting practices, increased oversight, notably through the passing of the FISA Amendments Reauthorization Act of 2017.
-

- 7.5.7 As stated, when member states process personal information for national security purposes within the EEA, the data subjects are not consistently guaranteed actionable rights, nor are there consistently clear rules imposing limitations on the processing. It is therefore not evident to the Organization that the interferences specified above render the level of protection essentially inferior to that guaranteed within the EEA.
- 7.5.8 However, in order to provide the highest degree of confidence in the compliance of the transfer. The Organization will align its assessment with the general positions of the European legal bodies and conclude that the interferences are not “proportional and necessary” measures.
- 7.5.9 *Source(s):*
- Schrems II (C-311/18)
 - EO 12.333
 - FISA 702
 - Presidential Policy Directive 28 (PPD-28)
 - CCBE Recommendations on the Protection of Fundamental Rights in the Context of ‘National Security’ 2019. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf
 - Privacy and Civil Liberties Oversight Board Report on Executive Order 12333
 - Privacy and Civil Liberties Oversight Board Report on FISA 702
 - U.S. Department of Commerce White Paper: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II
 - Lov om Forsvarets Efterretningstjeneste (FE) med senere ændringer (FE-loven)
 - European Union Agency for Fundamental Rights: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015

7.6 **Guarantee C: Independent oversight mechanism**

- 7.6.1 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.
- 7.6.2 Based on the reasoning below, the Organization does not consider Guarantee C to be fulfilled, meaning that the potential processing of personal data made by the authorities in the country of the Receiving Organization is not considered subject to an “independent oversight mechanism”.

This conclusion is based on the following:

- 7.6.3 In Schrems II the CJEU held that the oversight mechanisms in place regarding

FISA 702 and SIGNIT collection under EO12333 did not constitute sufficient independent oversight.

- 7.6.4 However, it is not clear that the targeting and minimization reviews conducted by the DOJ's National Security Division ("NSD") and the Office of the Director of National Intelligence ("ODNI"), the reports issued by the inspectors general and The Privacy and Civil Liberties Oversight Board ("PCLOB") as well as additional oversight activities conducted by the FISC and the Congressional Committees, were fully considered in the decision.
- 7.6.5 When surveying the equivalent oversight mechanisms in place for member state intelligence activities, there is no evidence of consistent independent oversight mechanism superior to those of the U.S.
- 7.6.6 For example, the Danish Intelligence Oversight Authority ("TET"), does not extend oversight with FE activities, where the rights of non-resident, non-Danish nationals are implicated.
- 7.6.7 In France, the recently instituted oversight mechanism, is to ex ante review the proportionality of national security surveillance measures against individual targets, reporting its recommendations to the Presidential office.
- 7.6.8 Between October 2015 and October 2016, the office reviewed 66 584 requests, with a staff of 16 people. Today it staffed by 26.
- 7.6.9 It is thus reasonable to assume that the review process is not in fact individual, and that the oversight body is not "vested with sufficient powers and competence to exercise and effective and continuous control" (R02/2021, section 42).
- 7.6.10 Notably, the French model received praise by European Union Agency for Fundamental Rights in their 2015 report on surveillance measures and safeguards.
- 7.6.11 The insufficient level of independent oversight within the EU was explicitly recognized by the European parliament in 2013 stressing that:
- 7.6.12 The majority of current EU oversight bodies dramatically lack both democratic legitimacy (strong legal framework, ex ante authorisation and ex post verification) and adequate technical capability and expertise. (Motion 2013/ 2188(INI) following Snowden revelations).
- 7.6.13 As such the Organization considers it doubtful if the independent oversight mechanisms in place in the U.S. concerning FISA 702 and EO12333 processing by public authorities, in fact impede the continuation of the high level of protection guaranteed within the EEA.
- 7.6.14 However, to ensure full confidence with the compliance of the transfer the Organization will follow the assessments of the CJEU, and consider there not to be sufficient independent oversight in place.

7.6.15 Source(s):

- Schrems II (C-311/18)
- EO 12333
- FISA 702
- Presidential Policy Directive 28 (PPD-28)
- CCBE Recommendations on the Protection of Fundamental Rights in the Context of 'National Security' 2019. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf
- Privacy and Civil Liberties Oversight Board Report on Executive Order 12333
- Privacy and Civil Liberties Oversight Board Report on FISA 702
- U.S. Department of Commerce White Paper: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II
- Lov om Forsvarets Efterretningstjeneste (FE) med senere ændringer (FE-loven)
- European Union Agency for Fundamental Rights: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015
- 2013/2188(INI) - U.S. NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs
- Information of the French oversight mechanism: <https://thesecuritydistillery.org/all-articles/reform-of-the-french-intelligence-oversight-system>

7.7 **Guarantee D: Effective remedies need to be available to the individual**

7.7.1 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.

7.7.2 As stated by the European Court of Justice in Schrems I: "*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.”

7.7.3 This is elaborated in the European Data Protection Board’s “Recommendations 02/2020 on the European Essential Guarantees for surveillance measure” and “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, para. 43 ff.

7.7.4 Based on the above, the Organization does not consider that Guarantee D is fulfilled, meaning that the remedies available to the individuals in the Receiving Country that are not considered effective.

This conclusion is based on the following reasons:

7.7.5 As found in the ruling in the Schrems II case, the PPD-28, although placing specific requirements on the U.S. intelligence authorities, does not grant data subjects actionable rights before the courts against the U.S. authorities. Similarly, EO 12333 confers no rights which are enforceable against the U.S. authorities in the courts. (para. 183 ff).

7.7.6 The Organization does not find reason to deviate from the positions expressed by the CJEU in this matter. Though, it should be noted that it is questionable if effective legal remedies are in fact available within the EEA when national security agencies of member states violate data subject rights.

7.7.7 The legal remedies available within the EEA does not consistently correspond to the requirements specified in R02/2021, unless the right to pursue rectification with the ECtHR and possibly CJEU, under the relevant international human rights instruments, is considered effective legal remedies in of themselves. The Organization considers this doubtful.

7.7.8 Within the EEA, there is no consistent requirement Within the of notice or means of access to information as to existing or past processing. See for example FE measures for access, managed by TET only apply to Danish nationals and residents.

7.7.9 *Source(s):*

- Schrems II (C-311/18)
- EO 12333
- FISA 702
- Presidential Policy Directive 28 (PPD-28)
- CCBE Recommendations on the Protection of Fundamental Rights in the Context of ‘National Security’ 2019. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf
- European Union Agency for Fundamental Rights: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015
- 2013/2188(INI) - U.S. NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on

transatlantic cooperation in Justice and Home Affairs

7.8 Other legislation not concerning authority access

7.8.1 Aside from the legislation identified above granting authority access to the transferred personal data, no other legislation has been identified, which would interfere with the effective protection of the transfer tool.

7.9 Conclusion on the U.S. and its legal regime

7.9.1 Based on The Organization's interpretation of the above, The Organization concludes the following with respect to each of the four European essential guarantees:

7.9.2 The legal regime of the U.S. may interfere with the effectiveness of the transfer tool in protecting the fundamental rights of the data subject. The Organization notes that this assessment is heavily influenced by the positions of the CJEU in Schrems II, as the Organization has not been able to establish that the safeguards of the four guarantees are in fact ensured within the territory of the EEA.

7.9.3 Followingly, the data subject is not ensured an essentially equivalent protection of his or her rights when compared to that afforded within the EEA, unless it can be established that there is no reason to believe the problematic legislation will be applied to the transferred data in practice.

7.9.4 The sources listed above have been verified on the following date: 14/09/2021

8. Assessment of authority practices

8.1 As has been established above, the legal regime of the country of the Receiving Organization does not offer an essentially equivalent protection of the rights of the data subject.

Followingly, sufficient supplementary measures must be put in place, unless it can be demonstrated that there is no reason to believe that the transferred personal data would be targeted by the identified problematic legislation and/or practices.

Though generally problematic legislation and/or practices, that could in principle target the transferred data, has been identified, the Organization considers that there is no reason to believe the transferred personal data would be targeted by the problematic legislation and/or practices for the documentable reasons specified below.

8.2 Information from the importer

<https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098>

<https://docs.microsoft.com/da-DK/compliance/regulatory/offering-ISO-27018?view=o365-worldwide>

Information about other actors or similar transfers in the same sector

Not relevant

- 8.3 Based on the above assessment of the relevant legislation, its interpretation and practical application, the Organization has not found any reason to believe that problematic legislation and/or practices, will interfere with effectiveness of protections offered by the transfer tool.

The Organization therefore considers the country of the Receiving Organization to offer an essentially equivalent protection of the rights of the data subject, as that of the EU, in the context of the specific transfer.

8.4 *Source(s):*

1. Answering Europe's Call: Storing and Processing EU Data in the EU", Brad Smith - President and Chief Legal Officer, may 6, 2021. Microsoft Blogs/eupolicy/2021/05/06/eu-data-boundary/

2. "EU Data Boundary for the Microsoft Cloud | Frequently Asked Questions", Kacey Lemieux, May 06 2021 (updated on may 5, Compliance, and Identity Blog.

3. "ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud", Microsoft website/ Dokumentation, november 2021.

Find links under 7.5

9. Supplementary measures

- 9.1 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.

- 9.2 No supplementary measures are implemented.

10. Assessment conclusion

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

- ✓ The Organization has identified problematic legislation and/or practices in place in the country of the Receiving Organization which would impede on the effectiveness of the transfer tool to guarantee an essentially equivalent protection of the rights of the data subject as they would be entitled to in the EEA. However, the Organization considers it demonstrated that there is no reason to believe that the problematic laws and/or practices in the country of the Receiving Organization, which in principle could impede the protections of the transfer tool, will target the specific personal data transferred. In the context of the specific transfer the data subjects are therefore afforded a level of protection of their rights which is essentially equivalent to that in the EEA. The Organization therefore finds that the transfer complies with the requirements laid down in Chapter V of the GDPR.

11. **Applicable procedural steps**

- 11.1 The Organization will use its best endeavours and reasonable measures to initiate and implement all procedural steps identified above.

12. **Re-evaluation of the TIA**

- 12.1 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 every two years as part of the Organizations' annual cycles of self-assessments and audits.

13. **Changes to the TIA**

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

14. **Contact**

- 14.1 If you have questions or comments to this TIA, you can always direct them to DPO Anne Margrethe Madsen, amm@innomate.com, direkte +45 30 33 39 93.