Lietuvos duomenų apsaugos pareigūnų asociacija

DUOMENŲ TEIKIMAS Į TREČIĄSIAS VALSTYBES

Liudas Karnickas

Rutina

Adekvatumas, BCR→SCC (+teikimo/tvarkymo)→leidimas, sutikimas, kodeksas +Minimizavimas+Informavimas+A28 tvarkytojo pareigos+ADTVĮ

https://i.ntnu.no/documents/portlet_file_entry/1305837853/0920+Data+Transfer+Agreement+between+two+Data+Controllers.docx/7e2f64d1-f298-2d0e-4cdb-082e6827bc4a?status=0&download=true

VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS DIREKTORIAUS ĮSAKYMAS

DĖL PAVYZDINĖS ASMENS DUOMENŲ TEIKIMO SUTARTIES FORMOS PATVIRTINIMO

2015 m. vasario 25 d. Nr. 1T-9 (1.12.E.)
Vilnius
(įsakymas **netenka galios nuo 2018 05 25** pagal VDAI 2018 04 18 įsakymą Nr. 1T-39(1.12.E); TAR, 2018-04-18, Nr. 6180)

Vadovaudamasis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 40 straipsnio 13 punktu ir atsižvelgdamas į Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 6 straipsnį,

t v i r t i n u pavyzdinę Asmens duomenų teikimo sutarties formą (pridedama).

DIREKTORIUS ALGIRDAS KUNČINAS

Forma patvirtinta
Valstybinės duomenų apsaugos inspekcijos direktoriaus
2015 m. vasario 25 d. įsakymu Nr. 1T-9 (1.12.E.)

(Pavyzdinė asmens duomenų teikimo sutarties forma)

ASMENS DUOMENŲ TEIKIMO SUTARTIS Nr. _____

20____ m. _____ d.

NTNU

AGREEMENT FOR TRANSFER OF PERSONAL DATA

(DATA TRANSFER AGREEMENT)

BETWEEN INDEPENDENT DATA CONTROLLERS

According to applicable Norwegian personal data legislation and EUs General Data Protection Regulation 2016/679 of 27 April 2016 ("GDPR")

[*Sub-title related to the concrete project*]

between

[*Name of institution/company*]

[*org.no.*]

("Transferor")

and

[*Name of institution/company*]

[*org.no.*]

("Transferee")

https://www.seagullscientific.com/media/1652/intra-group-sharing-agreement.pdf

Seagull Scientific

Intra-group data sharing agreement

DATE

..... 2018

PARTIES

(1) **SEAGULL SCIENTIFIC, INC** of 15325 SE 30th Place, Suite 100, Bellevue, WA 98007-6597, USA;

(2) **SEAGULL SCIENTIFIC LATAM, INC** of 15325 SE 30th Place, Suite 100, Bellevue, WA 98007-6597, USA;

(3) **SEAGULL SCIENTIFIC CHINA, INC** of 15325 SE 30th Place, Suite 100, Bellevue, WA 98007-6597, USA;

(4) **SEAGULL SCIENTIFIC EUROPE, INC** of Paseo de la Castellana, 18, 5º A, 28046 Madrid, Spain;

(5) **SEAGULL SCIENTIFIC ASIA-PACIFIC, INC** of 14F., No.39, Sec. 2, Dunhua South Rd., Daan District, Taipei City 106, Taiwan; and

(6) **SEAGULL SCIENTIFIC CHINA, LTD** of Room 601-13, Block 1, MeiNian International Square, West Nanhai Avenue, Zhaoshang Jiedao, Nanshan District, Shenzhen, China.

BACKGROUND

(A) The Parties are Affiliates; and the Parties share Personal Data in the course of the operation of their businesses.

(B) The sharing of Personal Data is subject to data protection law (including the General Data Protection Regulation (EU) 2016/679); in particular, the transfer of Personal Data from a place within the European Economic Area to a place outside the European Economic Area is subject to legal restrictions.

(C) To ensure the protection of Personal Data that is shared, and to ensure that the sharing and transfer of Personal Data between the Parties is lawful, the parties have entered into this intra-group data sharing agreement.

AGREEMENT

1. Definitions

1.1 In this Agreement:

"Accession Agreement" means an agreement between the Lead Party and an Additional Party under which, upon and from the date of execution that agreement, the Additional Party agrees to become a Party;

SCC

- Pasirašymas
- Keitimas
- Teikimas DS
- A28 sąlygos įtrauktos į M2 ir M3
- Ekstra susitarimai
- M3 (p-p) specifika
- M4 (p-c) specifika
- Netinka neEEE importuotojui, kuriam taikoma A3.2 (SP2P)
  - https://edpb.europa.eu/system/files/2021-10/20210914plenfinalminutes_54thplenary_public.pdf
- TIA
- Prieigos užklausų valdymo procesas

SCC: tolesnis perdavimas

https://www.linkedin.com/posts/renzomarchini_flow-down-obligations-in-the-new-sccs-activity-6813356383203819520-O7F6/

Module	Exporter	Importer	Transferee	Flow-down requirements*
1	Controller	Controller	Controller	Either sign the clauses with **exporter** or put in place "same level of ... protection" (Module 1) – copy to exporter.
1	Controller	Controller	Processor	Either sign the clauses (Module 2) with **exporter** or put in place "same level of ... protection" (Module 2) – copy to exporter.
2	Controller	Processor	Controller	Sign the clauses (Module 1) with the **exporter**
2	Controller	Processor	Processor	Impose "same obligations" (Module 3)
3	Processor	Processor	Processor	Impose "same obligations" (Module 3)
4	Processor	Controller	Any	None

Note*: some of these are softened if the recipient is in an adequate country or there are other "appropriate safeguards" in place (eg BCRs or Codes of Conducts/Certifications). Derogations (legal claims, vital interest, data subject consent) also apply.

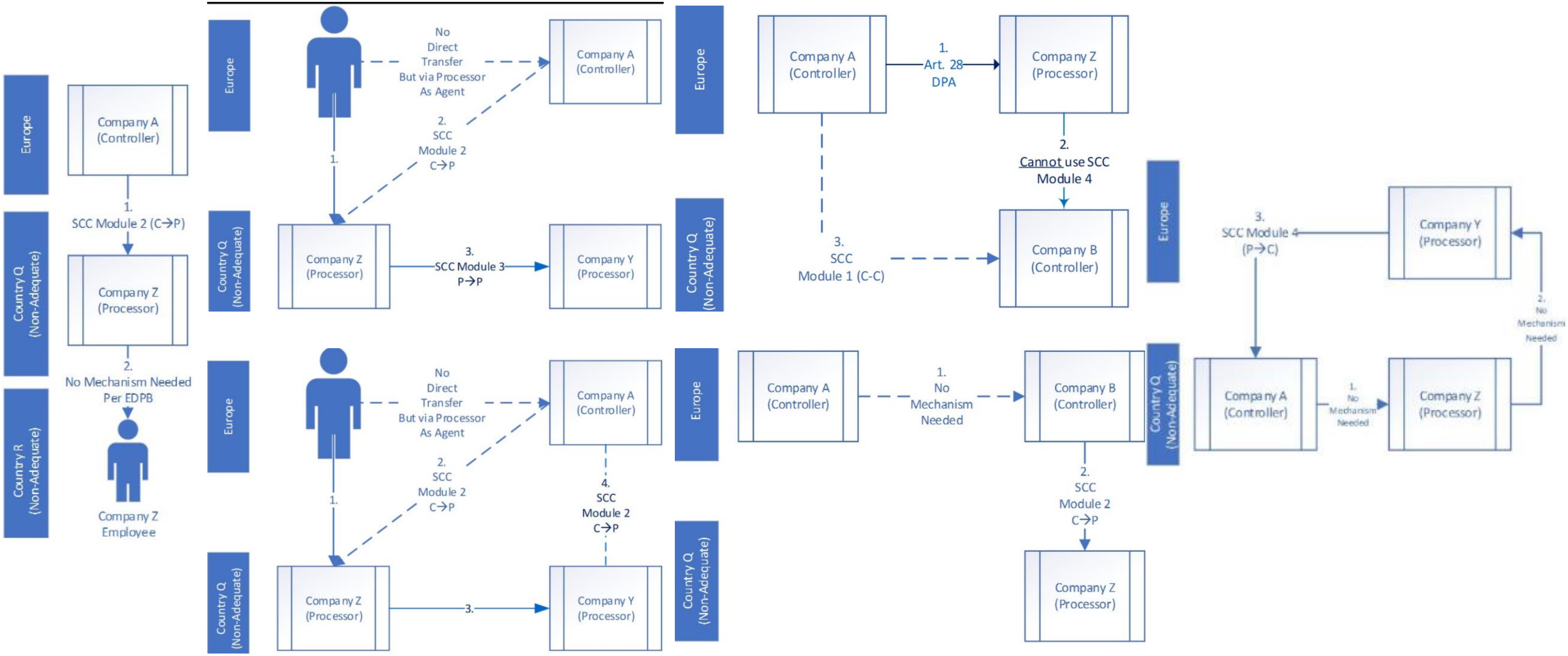
SCC: Terminas

Deadline
EU: 27.12.2022
CH: 31.12.2022

https://www.rosenthal.ch/downloads/VISCHER-EU-SCC-Updatecheck.pdf

SCC: Audito būtinumas

https://www.gtlaw-dataprivacydish.com/



SCC

mySCCcreator

Step by step: How do you proceed now?

- Download the document: DOWNLOAD - SCC
- You should carefully read and understand the provisions within the SCCs before entering into them, as the SCCs impose wide-ranging obligations for Data Exporters and Data Importers.
- Complete the Appendix.

If you need any assistance, our data protection team is of course happy to help.

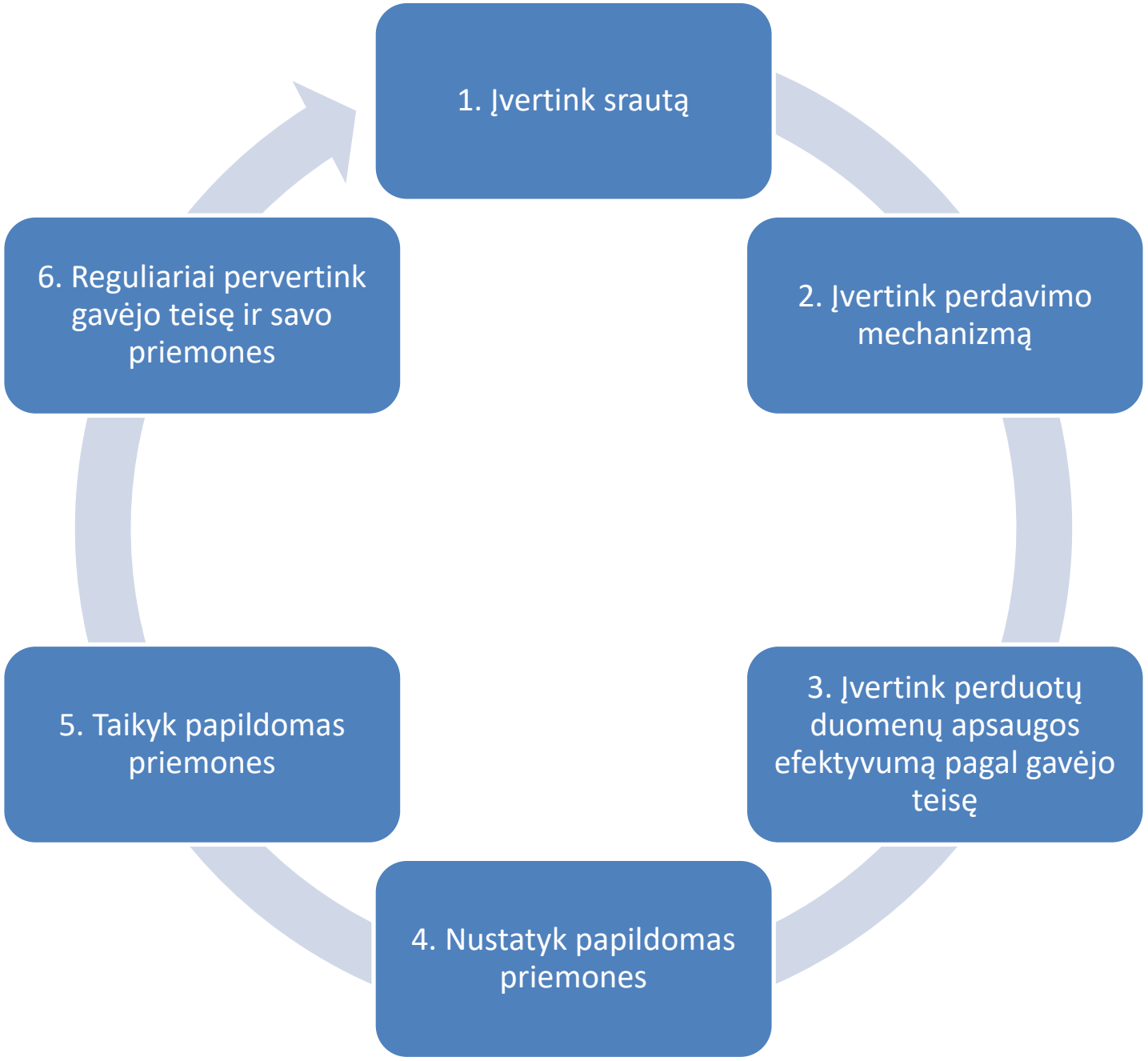
https://www.fieldfisher.com/en/locations/germany/services/data-protection/mysccreator

TIA įrankiai

Rekomendacijos Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui

Versija 2.0

Priimta 2021 m. birželio 18 d.



TIA įrankiai

Rekomendacijos Nr. 02/2020 dėl Europos pagrindinių garantijų taikant stebėjimo priemones

Priimta 2020 m. lapkričio 10 d.

- Aiškus pagrindas gauti duomenis gavėjo valstybėje
- Reikia įrodyti „būtinybę ir proporcingumą“ gauti duomenis?
- Gavėjo teismų nepriklausomumas
- Prieinama ir veiksminga teisių gynyba gavėjo valstybėje subjektui

TIA įrankiai: rizikos vertinimas v 0 tolerancija

Rekomendacijos Nr. 01/2020 dėl priemonių duomenų perdavimo priemonėms papildyti, siekiant užtikrinti atitiktį ES asmens duomenų apsaugos lygiui

Versija 2.0

Priimta 2021 m. birželio 18 d.

[80] Vertindami šifravimo algoritmų sudėtingumą, jų atitiktį pažangiausioms technologijoms ir jų patikimumą atsižvelgiant į kriptoanalizę laikui bėgant, duomenų eksportuotojai gali remtis ES ir jos valstybių narių oficialių kibernetinio saugumo institucijų paskelbtomis techninėmis gairėmis. Žr., pvz., ENISA ataskaitą „Kokie naujausi technikos laimėjimai pasiekti IT saugumo srityje?“, 2019 m. https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; Vokietijos Federalinio informacijos saugumo biuro gaires, pateiktas TR-02102 serijos techninėse gairėse ir „Algoritmų, rakto dydžio ir protokolų ataskaitą (2018 m.)“, H2020-ICT-2014 – projektas 645421, D5.4, ECRYPT-CSA, 2018 m. vasario mėn https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Kriptografinių algoritmų apsauginis pajėgumas ilgainiui mažėja dėl to, kad atrandama naujų kriptoanalizės metodų, atsiranda naujų kompiuterijos paradigmų, pvz., kvantinės kompiuterijos, ir apskritai padidėja turima skaičiavimo galia, nebent įrodoma, kad taikomi algoritmai yra teoriškai saugūs informacijos atžvilgiu. Tai visų pirma pasakytina apie viešojo rakto algoritmus, kurie tuo metu, kai rašomi, yra naudojami bendrai. Todėl duomenų eksportuotojas turi atsižvelgti į tai, kad valdžios institucijos gali įsipareigoti susipažinti su užšifruotais duomenimis 80 punkte aprašytomis aplinkybėmis ir juos saugoti tol, kol jų ištekliai bus pakankami iššifruoti. Papildoma priemonė gali būti laikoma veiksminga tik tuo atveju, jei toks iššifravimas ir tolesnis duomenų tvarkymas tuo metu nebebūtų duomenų subjektų teisių pažeidimas, pvz., dėl to, kad duomenys nebegali būti naudojami siekiant tiesiogiai ar netiesiogiai nustatyti duomenų subjektų tapatybę.

[82] NIST specialusis leidinys Nr. 800-57, Rekomendacija dėl rakto valdymo https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

TIA įrankiai

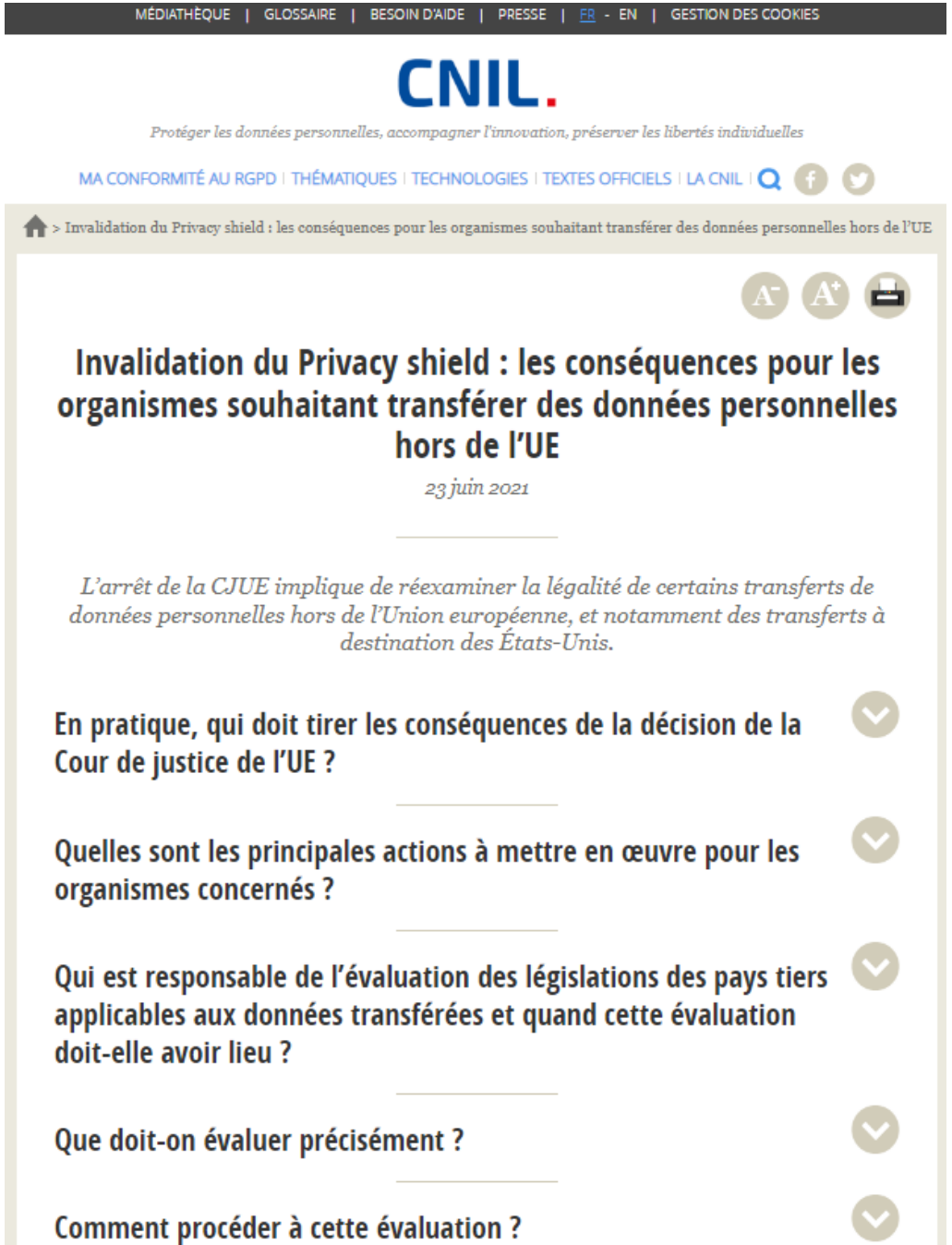
https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf

ICO consultation

Draft International transfer risk assessment and tool

August 2021

https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-consequences-pour-les-organismes-souhaitant-transferer-des



TIA įrankiai: www.difc.ae

Ethical Data Management Risk Index

EDMRI+ Due Diligence Risk Assessment

Thank You!

Risk Assessment Review

The assessment has shown that there is a high risk in exporting Personal Data, as the importing entity does not implement adequate data protection safeguards and mechanisms. You are urged to redo the survey after gathering further information on the questions you answered either "No" or "Don't Know", in order to ensure that the importing entity employs adequate data protection policies. If, despite the above uncertainties, you move forward with the transfer, you have to be satisfied that you have taken proper measures to mitigate any risk arising. Otherwise, you may be liable in case your business partner breaches provisions of the DIFC Data Protection Law or other applicable Laws.

Assessment Review

2.

1. Do you understand and apply Articles 26 and 27 regarding data export from the DIFC to a non-DIFC jurisdiction?
- Yes

2. Do you understand and apply Article 28 of the DIFC DP Law, regarding the requirements when the importing entity (anywhere) is a government authority?
- Yes

3. Does the importing entity have controls in place for onward transfers, i.e., further transfers of the personal data your company has sent the importing entity?
- Yes

4. Is the importing entity aware of Article 28 of the DIFC DP Law, especially where the importing entity is a government authority?
- Yes

5. Has your company been subject to prior instances of requests for disclosures from public authorities?
- No

6. Has the importing entity been subject to prior instances of requests for disclosures from public authorities?
- Don't Know

7. Is the importing entity willing to share security and data protection policies to demonstrate that at least high level technical and organizational measures are in place?

8. Does the importing entity require at least annual data protection and security training?
- Yes

9. Does the importing entity conduct departmental or project / design DPIAs?
- No

10. Has the importing entity conducted data mapping exercises recently, such it can demonstrate where your company's and its own Personal Data are processed?
- Don't Know

11. Does the importing entity provide a privacy notice and / or explanation of individuals' rights on the company website or somewhere easily accessible?
- No

12. Does the importing entity have a breach reporting policy?
- No

13. Does the importing entity have a data protection officer or other sufficiently provisioned person or team responsible for data protection and security?
- No

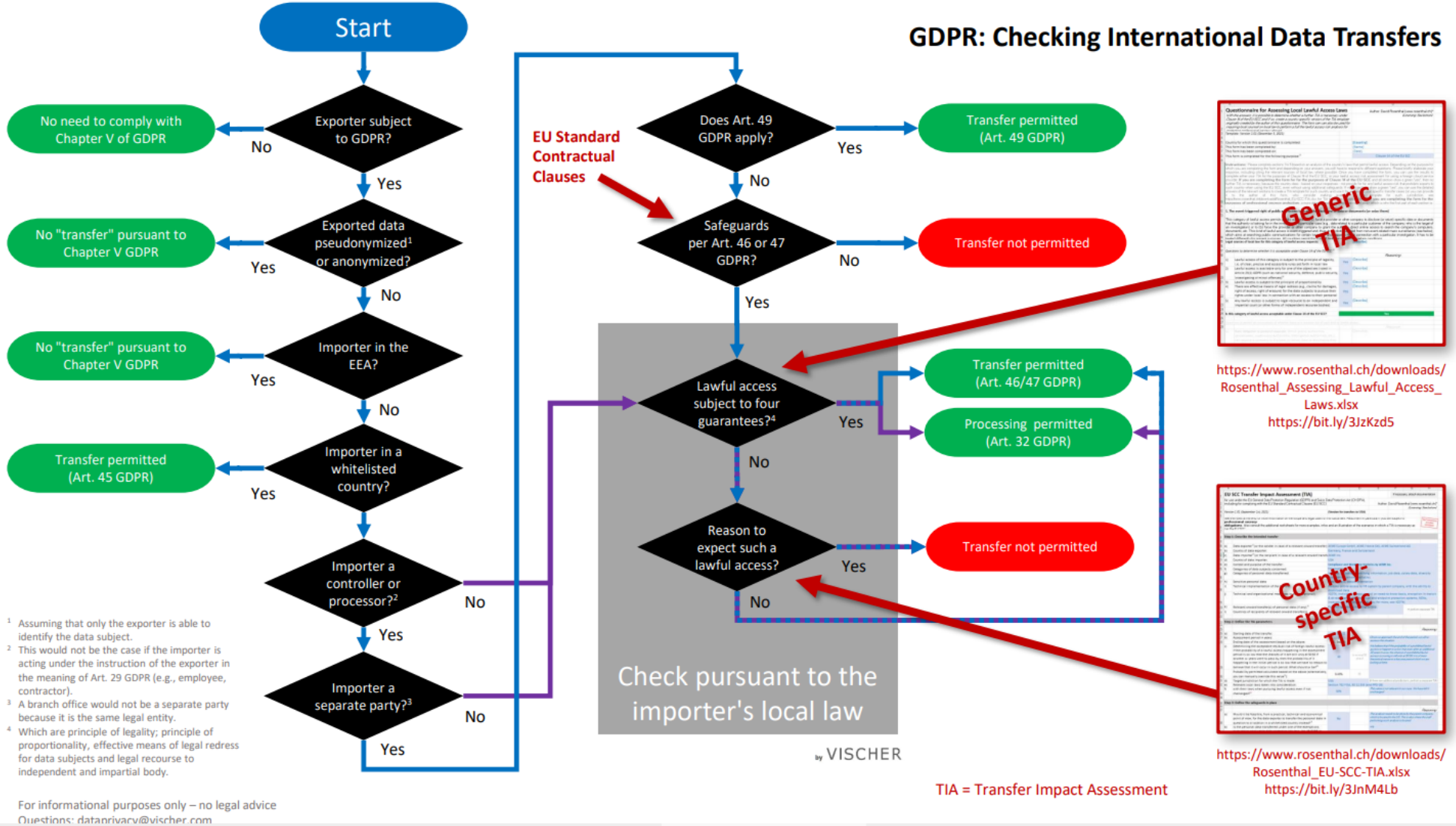
14. Has the importing entity been subject to data protection supervision or enforcement action for non-compliance in any jurisdiction?
- Yes

15. Does the importing entity subscribe to any certification schemes under an applicable arrangement (i.e., local privacy code, CBPRs, etc)?
- Don't Know

16. Are you satisfied that processing by the importing entity will be secure and aligned with the requirements and obligations of the DP Law 2020, specifically Articles 14, 23 to 25, and Articles 26 to 28?
- No

17. Are you satisfied that individuals' rights to access and control their Personal Data will be respected via your instructions to the importing entity or any additional transfer mechanisms (i.e., the DIFC SCCs), especially where requested by a public authority?
- Yes

TIA įrankiai: www.rosenthal.ch



https://www.rosenthal.ch/downloads/Rosenthal_International_Transfers_Charts.pdf

TIA įrankiai: www.rosenthal.ch

David Rosenthal,

EU SCC Transfer Impact Assessment (TIA) Toolbox, with templates/samples for the various jurisdictions and a questionnaire for assessing foreign lawful access laws; the IAPP version

EU SCC Transfer Impact Assessment (TIA) iapp

If necessary, attach documentation

for use under the EU General Data Protection Regulation (GDPR) and Swiss Data Protection Act (CH DPA), including for complying with the EU Standard Contractual Clauses (EU SCC)

Author: David Rosenthal (original version at www.rosenthal.ch)*
(Licensing: See bottom)

The IAPP is publishing this template as one resource to assist privacy professionals in conducting TIAs, with thanks to the contributor. The IAPP does not endorse any specific template.

Version 1.01 (September 1st, 2021) | **(Version for transfers to USA)**

See the notes at the end for more information on the scope and legal basis of this document. Read them in particular if you are subject to **professional secrecy obligations**. Also consult the additional worksheets for more examples, infos and an illustration of the scenarios in which a TIA is necessary as per the EU SCC. The green text is mere sample text; the values and reasoning do *not* necessarily represent the author's opinion and are given for illustration purposes only.

Step 1: Describe the intended transfer

a)	Data exporter[1] (or the sender in case of a relevant onward transfer):	ACME Europe GmbH, ACME France SAS, ACME Switzerland AG	
b)	Country of data exporter:	Germany, France and Switzerland	
c)	Data importer[2] (or the recipient in case of a relevant onward transfer):	ACME Inc.	
d)	Country of data importer:	USA	
e)	Context and purpose of the transfer:	**Compliance and Workforce Statistics by ACME Inc.**	
f)	Categories of data subjects concerned:	Employees	
g)	Categories of personal data transferred:	HR data, including identifying information, job data, salary data, diversity information (where available)	
h)	Sensitive personal data:	data on race, sexual orientation	
i)	Technical implementation of the transfer:	Remote online access to HR system by parent company, with the ability to download data	
j)	Technical and organizational measures in place (optional):	IGDTA, individual access control on need-to-know-basis, encryption in-transit & at-rest, data loss prevention and endpoint protection systems, NDAs, instructions, trainings and audits (for more, see IGDTA)	
k)	Relevant onward transfer(s) of personal data (if any):[3]	Processing done by HostingCo Corp.	→perform separate TIA
l)	Countries of recipients of relevant onward transfer(s):	USA	

Step 2: Define the TIA parameters

				Reasoning
a)	Starting date of the transfer:	01-rugs-21		
b)	Assessment period in years:	5		*Once we approach the end of the period, we will re-assesss the situation.*
	Ending date of the assessment based on the above:	01-rugs-26		

Importo valstybės įvertinimai: EDPB 01/2020

ANNEX 3: POSSIBLE SOURCES OF INFORMATION TO ASSESS A THIRD COUNTRY

144. Your data importer should be in a position to provide you with relevant sources and information relating to the third country in which it is established, including the laws and the practices applicable to the importer and the data transferred. You and the importer may refer to several sources of information, such as the ones non-exhaustively listed below and presented by order of preference:

- Case-law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR)[104] as referred to in the European Essential Guarantees recommendations;[105]
- Adequacy decisions in the country of destination if the transfer relies on a different legal basis;[106]
- Resolutions and reports from intergovernmental organisations, such as the Council of Europe,[107] other regional bodies,[108] and UN bodies and agencies (e.g. UN Human Rights Council,[109] Human Rights Committee[110]);
- Reports and analysis from competent regulatory networks, such as the Global Privacy Assembly (GPA);[111]
- National case-law or decisions taken by independent judicial or administrative authorities competent on data privacy and data protection of third countries;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the importer;
- Warrant canaries of other entities processing data in the same field as the importer;
- Reports produced or commissioned by Chambers of commerce, business, professional and trade associations, governmental diplomatic, trade and investment agencies of the exporter or other third countries exporting to the third country to which the transfer is made;
- Reports from academic institutions, and civil society organizations (e.g. NGOs);
- Reports from private providers of business intelligence on financial, regulatory and reputational risks for companies;
- Warrant canaries of the importer itself;[112]
- Transparency reports, on the condition that they expressly mention the fact that no access requests were received. Transparency reports merely silent on this point would not qualify as sufficient evidence as these reports most often focus on access requests received from law enforcement authorities and provide figures only on this aspect while remaining silent on access requests for national security purposes received. This does not mean that no access requests were received but rather that this information cannot be shared;[113]
- Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period; and with a preference for statements and records engaging the liability of the importer and/or issued by internal positions with some autonomy such as internal auditors, DPOs, etc.[114]

---

[104] See factsheet of the ECtHR jurisprudence on mass surveillance: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] C-311/18 (Schrems II), paragraph 141; see adequacy decisions in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] See for instance country reports of the Inter-American Commission on Human Rights (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[109] See https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] See: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] See e.g. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

Importo valstybės įvertinimai: www.difc.ae

Ethical Data Management Risk Index

3. EDMRI

LOW: No concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights.	**LOW / MEDIUM**: Almost no concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights.	**MEDIUM**: Concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights, but likely to be mitigated if enhanced due diligence is undertaken.	**MEDIUM / HIGH**: Increased concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights, and unlikely to be mitigated unless enhanced due diligence is undertaken.	**HIGH**: Significant degree of concerns about importing entity complying with existing laws, including DP laws, and assuring data subjects' rights, and unlikely to be mitigated.

Data Importer Location(s)	Grey = Adequacy Blue = DPL Only	Risk Index
Spain		Low
Portugal		Low
South Korea		Low
United Kingdom		Low
Jersey		Low
Bermuda		Low
Slovakia		Low / Medium
France		Low / Medium
Czech Republic		Low / Medium
Israel		Low / Medium
Colombia	DIFC	Low / Medium
Ireland		Low / Medium
Austria		Low / Medium
Singapore	DIFC	Low / Medium
Australia		Low / Medium
Japan		Low / Medium
Belgium		Low / Medium
South Africa		Low / Medium
Canada		Low / Medium

Data Importer Location(s)	Grey = Adequacy Blue = DPL Only	Risk Index
New Zealand		Low / Medium
Italy		Low / Medium
Bulgaria		Low / Medium
Mexico		Low / Medium
Malaysia		Low / Medium
Iceland		Low / Medium
Philippines		Low / Medium
Brazil		Medium
Germany		Medium
Morocco		Medium
Romania		Medium
Nigeria		Medium
Kenya		Medium
China		Medium
Slovenia		Medium
Switzerland		Medium
Turkey		Medium
Hong Kong		Medium
Russia		Medium

Data Importer Location(s)	Grey = Adequacy Blue = DPL Only	Risk Index
Indonesia	No law	Medium
UAE		Medium
Ukraine		Medium
USA (with Individual States)	In draft	Medium
Hungary		Medium / High
Saudi Arabia		Medium / High
Bosnia		Medium / High
Egypt		Medium / High
Qatar		Medium / High
Vietnam	In draft	High
Venezuela	No law	High
Tanzania	In draft	High
Pakistan	No law	High
Ethiopia		High
India	In draft	High
Bangladesh	No law	High
Afghanistan	No law	High

Importo valstybės įvertinimai: www.difc.ae

- Ethical Data Management Risk Index


DIFC

DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

United Kingdom 2022

Commissioner of Data Protection


DIFC

DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

Russia 2022

Commissioner of Data Protection

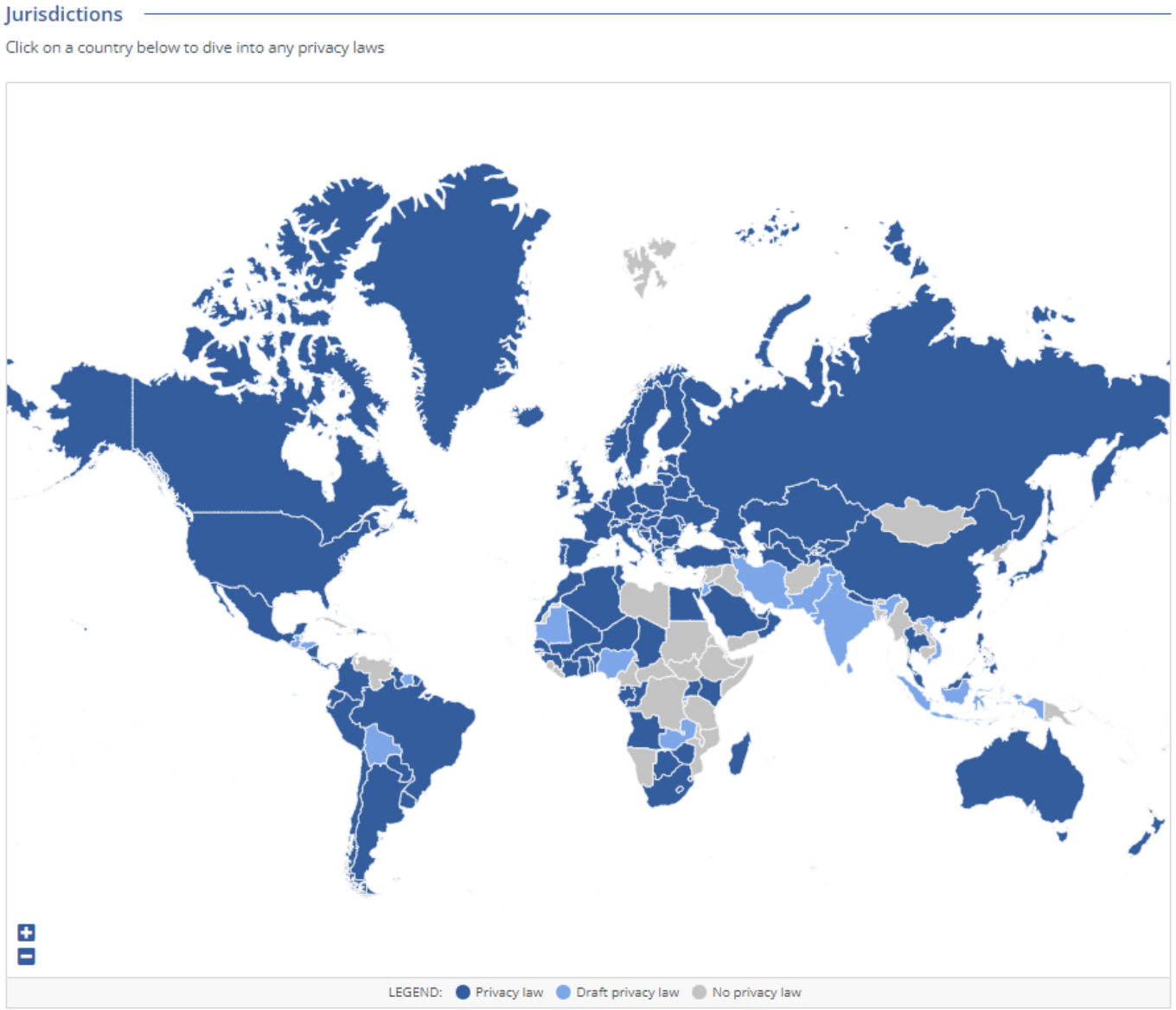

DIFC

DATA IMPORT RISK RATING ASSESSMENT FOR DP LAW COMPLIANCE

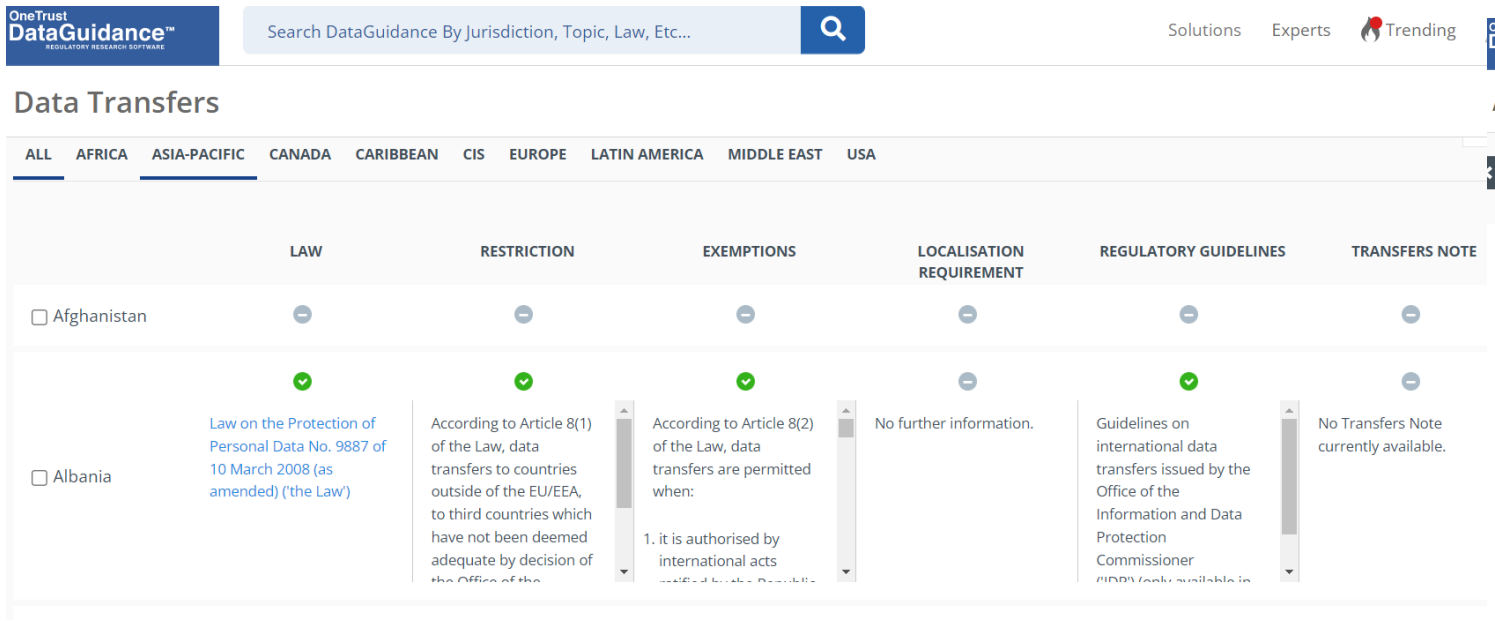
India 2022

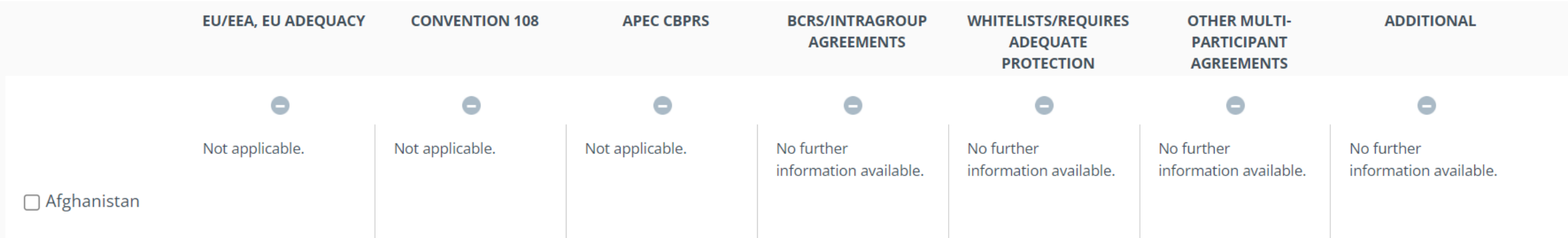
Commissioner of Data Protection

Importo valstybės įvertinimai: dataguidance.com



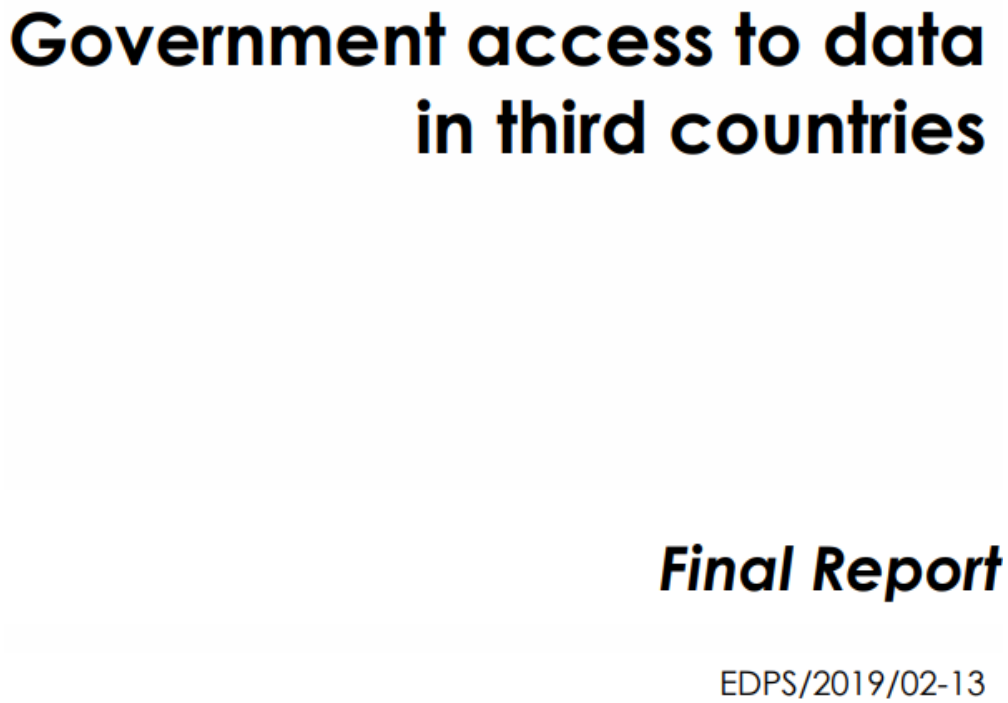
Importo valstybės įvertinimai: dataguidance.com





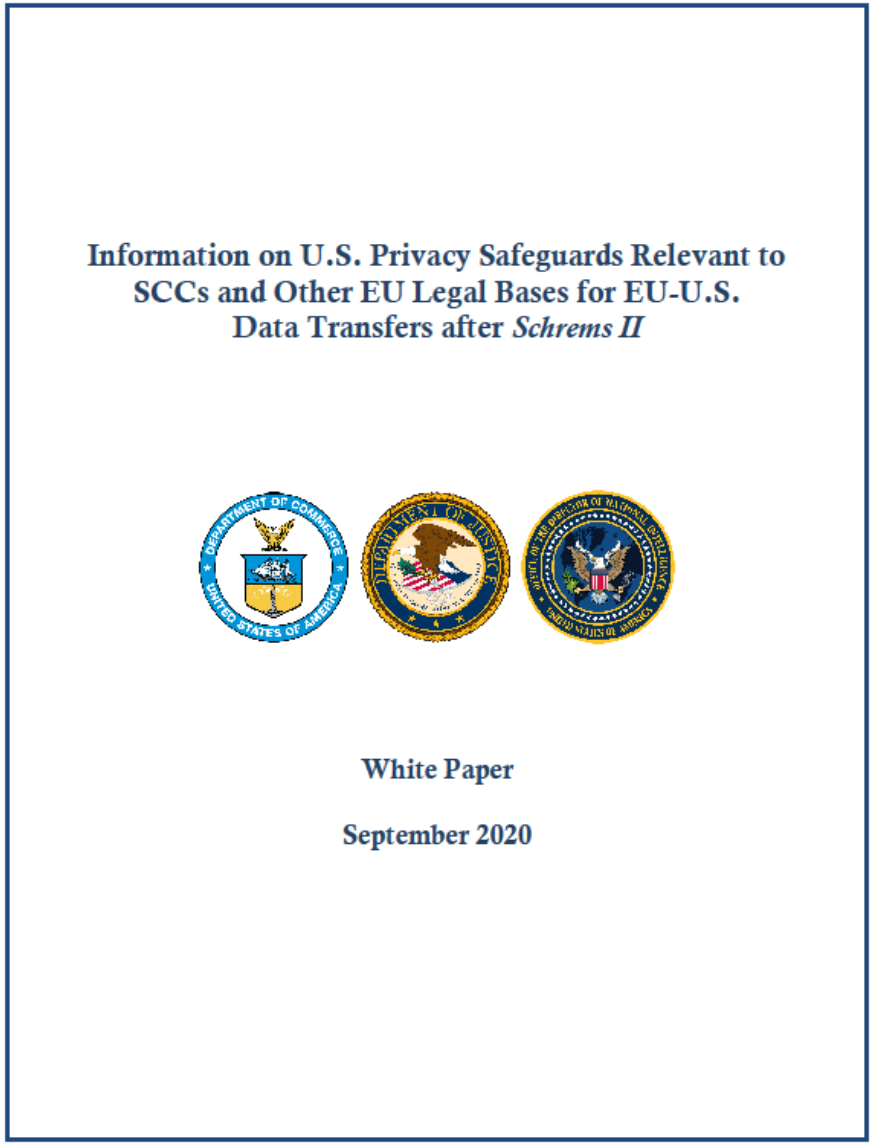
Importo valstybės įvertinimai: kiti

- https://www.dlapiperdataprotection.com/
- https://www.cnil.fr/en/data-protection-around-the-world



https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

Importo valstybės įvertinimai: Valstybės komentarai



Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*

White Paper

September 2020

https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

ES-JAV SHv3

20220930-DataGuidance-PrivacyShield2.0Timeline-Infographic

https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law

Importo valstybės įvertinimai: Paslaugų tiekėjų duomenys

https://www.atlassian.com/legal/data-transfer-impact-assessment

Atlassian's Data Transfer Impact Assessment Guide for Customers

Last updated on: **13 July 2022**

Overview

This document provides information to help Atlassian customers conduct data transfer impact assessments in connection with their use of Atlassian products, in light of the "Schrems II" ruling of the Court of Justice for the European Union and the recommendations from the European Data Protection Board.

In particular, this document describes the legal regimes applicable to Atlassian in the US, the safeguards Atlassian puts in place in connection with transfers of customer personal data from the European Economic Area, United Kingdom or Switzerland ("Europe"), and Atlassian's ability to comply with its obligations as "data importer" under the Standard Contractual Clauses ("SCCs").

For more details about Atlassian's GDPR compliance program please visit this page.

Step 1: Know your transfer

Where Atlassian processes personal data governed by European data protection laws as a data processor (on behalf of our customers), Atlassian complies with its obligations under its Data Processing Addendum available at https://www.atlassian.com/legal/data-processing-addendum ("DPA"). The Atlassian DPA incorporates the SCCs and provides the following information:

- description of Atlassian's processing of customer personal data (Exhibit A); and
- description of Atlassian's security measures (Exhibit B)

Please refer to Exhibit A to the DPA for information on the nature of Atlassian's processing activities in connection with the provision of the Services, the types of customer personal data we process and transfer, and the categories of data subjects.

A list of all of our data subprocessors and an RSS feed subscription where you can stay up-to-date on changes is available at https://www.atlassian.com/legal/sub-processors.

We may transfer customer personal data wherever we or our third-party service providers operate for the purpose of providing you the Services. The locations will depend on the particular Atlassian Services you use, as outlined in the chart below.

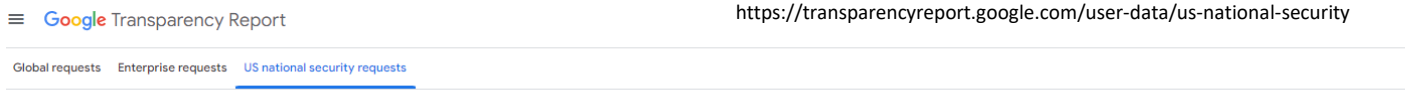
Gavėjo vertinimas: Paslaugų tiekėjų duomenys

Law Enforcement Requests Report 2022

Requests received for all Microsoft Services from January to June 2022

	Total Requests		Some Customer Data Disclosed				No Customer Data Disclosed			
	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests	Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)	
	#	#	%	#	%	#	%	#	%	#
TOTAL	26 365	58 665	3,76%	992	53,26%	14 043	17,94%	4 730	25,03%	6 600
Lithuania	14	41	0,00%	0	71,43%	10	14,29%	2	14,29%	2
United States	5 560	17 337	9,89%	550	43,78%	2 434	33,67%	1 872	12,66%	704

https://transparencyreport.google.com/user-data/us-national-security



https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

United States national security requests for user information

In this US national security requests report, we separately report requests from US authorities using national security laws because these laws restrict how much information companies like us are allowed to share, and when we are allowed to share it. In cases of national security, the US government can use the **Foreign Intelligence Surveillance Act (FISA)** to request non-content and content information, and use **National Security Letters (NSLs)** to request limited information about a user's identity.

Non-content requests under FISA

A FISA request can include non-content metadata—for example, the "from" and "to" fields in an email header and the IP addresses associated with a particular account.

Reporting period	Number of requests	Number of accounts
Jan 2022 – Jun 2022	Data subject to six month reporting delay	Data subject to six month reporting delay
Jul 2021 – Dec 2021	0 – 499	28000 – 28499
Jan 2021 – Jun 2021	0 – 499	27000 – 27499
Jul 2020 – Dec 2020	0 – 499	21500 – 21999

https://surfshark.com/warrant-canary

Warrant canary

We, Surfshark, are committed to being transparent and taking full control of our service. Private information of our users has never been disclosed or seized, nor have we been compromised or suffered a data breach.

As of November 5, 2022 Surfshark has received:

0 National Security letters;
0 Gag orders;
0 Warrants from any government organization;

To ensure your privacy and security, we guarantee a strict no logs policy – we don't monitor, log or store your online activities.

SCC 2 priedas

"more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing… The contract needs to include or reference information as to the security measures to be adopted, an obligation on the processor to obtain the controller's approval before making changes, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The **degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR**…"

Guidelines 07/2020 on the concepts of controller and processor in the GDPR, v2.1

SCC 2 priedas: standarto pagrindu

RISK LEVEL: L/M/H

Security policy and procedures for the protection of personal data (ref. ISO 27001: A.5 - Security Policy)
Roles and responsibilities (ref. ISO 27001: A.6.1.1 - Information security roles and responsibilities)
Access control policy (ref. ISO 27001: A.9.1.1 - Access control policy)
Change Management (ref. ISO 27001: A.12.1 - Operational procedures and responsibilities)
Subcontractors (ref. ISO 27001: A.15 - Suppliers relations)
Incident management/Personal data breaches (ref. ISO 27001: A.16 - Incident management)
Business continuity (ref. ISO 27001: A.17 - Business Continuity Management)
Confidentiality of personnel (ref. ISO 27001: A.7 - Human resource security)
Training (ref. ISO 27001: A.7.2.2 - Information security awareness, education and training)
Access control and authentication (ref. ISO 27001: A.9 - Access control)
Logging and monitoring (ref. ISO 27001: A.12.4 - Logging and monitoring)
Server/Database security (ref. ISO 27001: A.12 - Operations security)
Workstation security (ref. ISO 27001: A.14.1 - Security requirements of information systems)
Network/Communication security (ref. ISO 27001: A.13 - Communications Security)
Back-up (ref. ISO 27001: A.12.3 - Back-Up)
Mobile/Portable devices (ref. ISO 27001: A.6.2 - Mobile devices and teleworking)
Application Lifecycle Security (ref. ISO 27001: A.12.6 - Technical vulnerability management & A.14.2 Security ir development and support processes)
Data deletion/disposal (ref. ISO 27001: A.8.3.2 - Disposal of media & A. 11.2.7 Secure disposal or reuse o equipment)
Physical security (ref. ISO 27001: A.11 - Physical and environmental security)
Extra EU data transfer (ref. EDPB: Recommendations 01/2020)
System Administrators (ref. XYZ Data Protection Authority - System Administrators General Decision)

EXHIBIT A TO THE DATA PROCESSING AGREEMENT

TECHNICAL AND ORGANIZATIONAL MEASURES

This Exhibit A forms part of the DPA. Capitalized terms not defined in this Exhibit A have the meaning set forth in this DPA.

McAfee Enterprise has implemented technical and organisational security measures which remain compliant with industry standards, including ISO 27001, 27017 27018 and 27701[1]. McAfee's Information Security & Privacy Management System (ISMS) ensures continued operation of sure measures, and supports th governance of information security & procession of personal data as a PII processor across all global locations and cloud services and is inclusive of the following sites with primary security operations:

- Musarubra US, LLC. - 6220 America Center Drive, San Jose, CA. 95002 USA;
- Musarubra Ireland Limited - Building 2000, Citygate, Mahon, Cork City, Ireland, T12RRC9

In addition to any data security requirements set forth in the DPA, McAfee shall comply with the following, as derived from industry standards:

Standard	Control Ref/ Title		Control Description
Compliant with ISO 27001 - Information Security Management System (incl. controls amendments compliant with ISO 27017/27018/27701)	***6.1.3 - A.5 Information Security Policy***		
	5.1.1	Policies for information security	A set of policies for information security is defined, approved by management, published and communicated to employees and relevant external parties.
	5.1.2	Review of the policies for information security	The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
	6.1.3 - A.6 Organization of Information Security		
	6.1.1	Information security roles and responsibilities	All information security responsibilities are defined and allocated.
	6.1.2	Segregation of duties	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
	6.1.3	Contact with authorities	Appropriate contacts with relevant authorities are maintained.
	6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.
	6.1.5	Information security in project management	Information security is addressed in project management, regardless of the type of the project.
	6.2.1	Mobile device policy	A policy and supporting security measures is adopted to manage the risks introduced by using mobile devices.
	6.2.3	Teleworking	A policy and supporting security measures is implemented to protect information accessed, processed or stored at teleworking sites.

https://www.mcafee.com/enterprise/en-us/assets/legal/McAfee-DPA-for-Customers-September-23-2021.pdf

SCC 2 priedas: nuoroda į kt. SOP

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

The full text of Twilio's technical and organizational security measures to protect Customer Data is available at https://www.twilio.com/legal/security-overview ("*Security Overview*").

Where applicable, this Schedule 2 will serve as Annex II to the EU Standard Contractual Clauses. The following table provides more information regarding the technical and organizational security measures set forth below.

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	See Section 13 (Encryption) of the Security Overview
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	See Section 18 (Resilience and Service Continuity) and Section 19 (Customer Data Backups) of the Security Overview

https://www.twilio.com/legal/data-protection-addendum

TEIKIMAS IŠ TREČIŲJŲ VALSTYBIŲ Į ES

- Specialūs pranešimai, sutikimai
- Adekvatumo sąrašai
- Privatumo skydai (CH-US)
- Atstovo paskyrimas, registracijos
- Tipinės sutarčių sąlygos (UK, CH, CN)
- Lokalizavimas

Lietuvos duomenų apsaugos pareigūnų asociacija

liudas.karnickas@ldapa.lt

www.ldapa.lt

Lietuvos duomenų
apsaugos pareigūnų
asociacija