oda

Nettverksmøte: Personvern og Informasjonssikkerhet

Agenda - Schrems-II evaluations in Oda

1. Privacy in Oda
2. Case - Iterable (CRM)
3. Summary and some reflections
4. What’s next?

Privacy in Oda

Personvern i Oda

Privacy team (Product & Tech)

Martin Ervik
Privacy lead

Karoline Alnes
Project manager

To be hired H2021
Privacy legal counsel

To be hired H2022
Project manager

To be hired V2022
Privacy legal counsel

To be hired H2022
Privacy engineer

Communication: Slack-channel for Privacy

Stakeholders and support

CTO, Product & Tech
CFO, Finance & Strategy
CPO, People

Legal counsel, Finance & Strategy

Data Protection Officer, Finance & Strategy
To be hired H2021

Privacy Champions, All teams processing

Security Team, Product & Tech

Schjødt law firm
External legal advice

What does the privacy team do?

- Privacy Awareness
- Privacy Champions in every team
- Privacy Assessments and Documentation
- Privacy Guidance for every Oda Team
- Incident and Deviation Handling
- Overall responsibility: Making sure we stay compliant and apply good practices in current and new regions

Challenges ahead and current focus areas

- Schrems-II evaluations
- Compliance-aspects in new markets
- Switch from intellectual property to structured way-of-working, processes and policies
- Raise privacy awareness - Privacy Champions
- Build and recruit a scalable privacy organization

oda

Case - Iterable (CRM)

oda

Background

- Spring 2021: A newly established marketing-team was planning to acquire a CRM-tool, *Iterable*, to replace our old internal built system

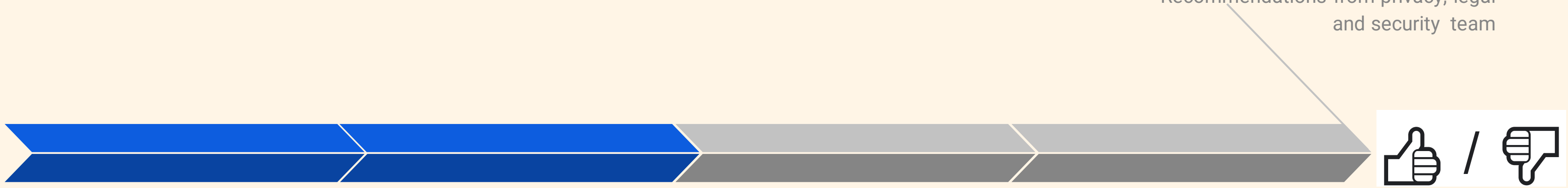
- Why: Critical business acquirement for us, to be prepared for launch in Finland and Germany. Old system required a developer to manually filter on customers before sending out communication

- Timeline:
  - 21.06.21: EDPB provide new guidelines
  - 22.06.21: Marketing team informs privacy and legal team that they need guidance on assessing a new CRM-tool/system
  - 23.06.21: Decision on Iterable was made, MSA signed (!!)

- So... what happened in this (rather short) time period?

oda

Desired process in Oda for privacy evaluations of data transfers outside of EU/EEA



Involve privacy, legal and security team

Pre-screening of alternatives

Questionnaire of y/n questions to understand initial risk level

Acquire documentation

Privacy policy, security overview, MSA draft, Privacy Addendum, etc.

DPIA

PII involved, legal basis, data retention, access control, DPA read-through etc

Data transfer assessment

Use of EDPB guidelines, documentation of org., tech. & contractual measures, walk-through with reps. From provider

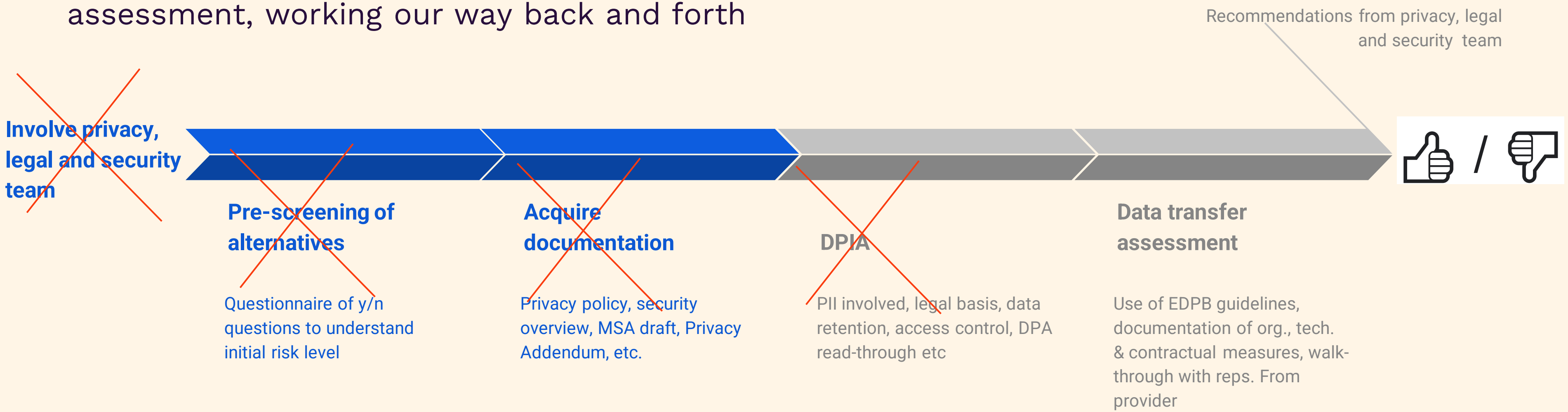
Recommendations from privacy, legal and security team

👍 / 👎

oda

How it actually worked in this case

Due to time pressure and new guidelines* → Ended up starting straight away with the data transfer assessment, working our way back and forth



Recommendations from privacy, legal and security team

~~Involve privacy, legal and security team~~

~~Pre-screening of alternatives~~

Questionnaire of y/n questions to understand initial risk level

~~Acquire documentation~~

Privacy policy, security overview, MSA draft, Privacy Addendum, etc.

~~DPIA~~

PII involved, legal basis, data retention, access control, DPA read-through etc

Data transfer assessment

Use of EDPB guidelines, documentation of org., tech. & contractual measures, walk-through with reps. From provider

👍 / 👎

*Quite common that this happens in a rapid-growing scale-up like Oda...

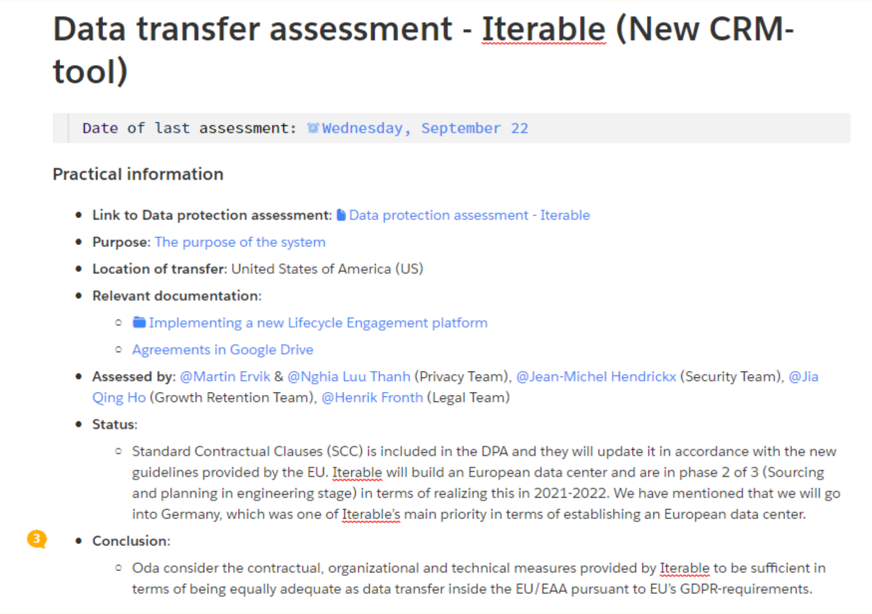
Data transfer assessment - Initial work from the privacy team

- It was quite clearly explained that there was no better fit for the marketing team than the tool Iterable could provide us with
- We quickly understood that this was to be considered as a data transfer outside of EU/EEA → More specific: To the U.S.
- Prioritize focus area: Had basically 1 day to familiarize ourselves with the new updated guidelines
- Created a template for evaluation/assessment of Iterable based on the guidelines
- Had to go with a pragmatic approach as we understood the deal was gonna be signed the next day no matter the recommendations
- Bought time: Agreed that **NO DATA SHOULD BE TRANSFERRED** until we are comfortable with the documentation and supplementary measures

oda

Data transfer assessment

- Step “zero”: Initial meeting with provider
- Step 1: Know your transfers
- Step 2: Identify the transfer tools you are relying on
- Step 3: Assess whether the article 46 GDPR transfer tool you are relying on is effective in the light of all circumstances of the transfer
- Step 4: Identify and addopt supplementary measures
- Step 5: Procedural steps if you have identified effective supplementary measures (a checklist of what we need to do)
- Step 6: Re-revaluate at appropriate intervals (defining a follow-up process)



Data transfer assessment - Iterable (New CRM-tool)

```
Date of last assessment: Wednesday, September 22
```

Practical information

- **Link to Data protection assessment:** Data protection assessment - Iterable
- **Purpose:** The purpose of the system
- **Location of transfer:** United States of America (US)
- **Relevant documentation:**
  - Implementing a new Lifecycle Engagement platform
  - Agreements in Google Drive
- **Assessed by:** @Martin Ervik & @Nghia Luu Thanh (Privacy Team), @Jean-Michel Hendrickx (Security Team), @Jia Qing Ho (Growth Retention Team), @Henrik Fronth (Legal Team)
- **Status:**
  - Standard Contractual Clauses (SCC) is included in the DPA and they will update it in accordance with the new guidelines provided by the EU. Iterable will build an European data center and are in phase 2 of 3 (Sourcing and planning in engineering stage) in terms of realizing this in 2021-2022. We have mentioned that we will go into Germany, which was one of Iterable’s main priority in terms of establishing an European data center.
- **Conclusion:**
  - Oda consider the contractual, organizational and technical measures provided by Iterable to be sufficient in terms of being equally adequate as data transfer inside the EU/EAA pursuant to EU’s GDPR-requirements.

oda

Step "zero": Initial meeting with provider

- The same day as the deal was signed, we managed to get a meeting with Iterable's General Counsel and Security Team

- Some red flags discovered in the meeting:
    - Referred to Privacy Shield all the time
    - Schrems-II seemed to be of no worry. "*We have everything under control, we have a lot of customers in Europe already. We are compliant within the requirements of Privacy Shield*"
    - Data hosting/storage and support in the U.S., but with plans on moving to the EU by end of 2022
    - "Old" SCC's
    - Restrictive on access to detailed documentation of encryption method and security details

- Based on this meeting, we had enough details to finalize the DPIA of Iterable

Step 1: Know your transfers

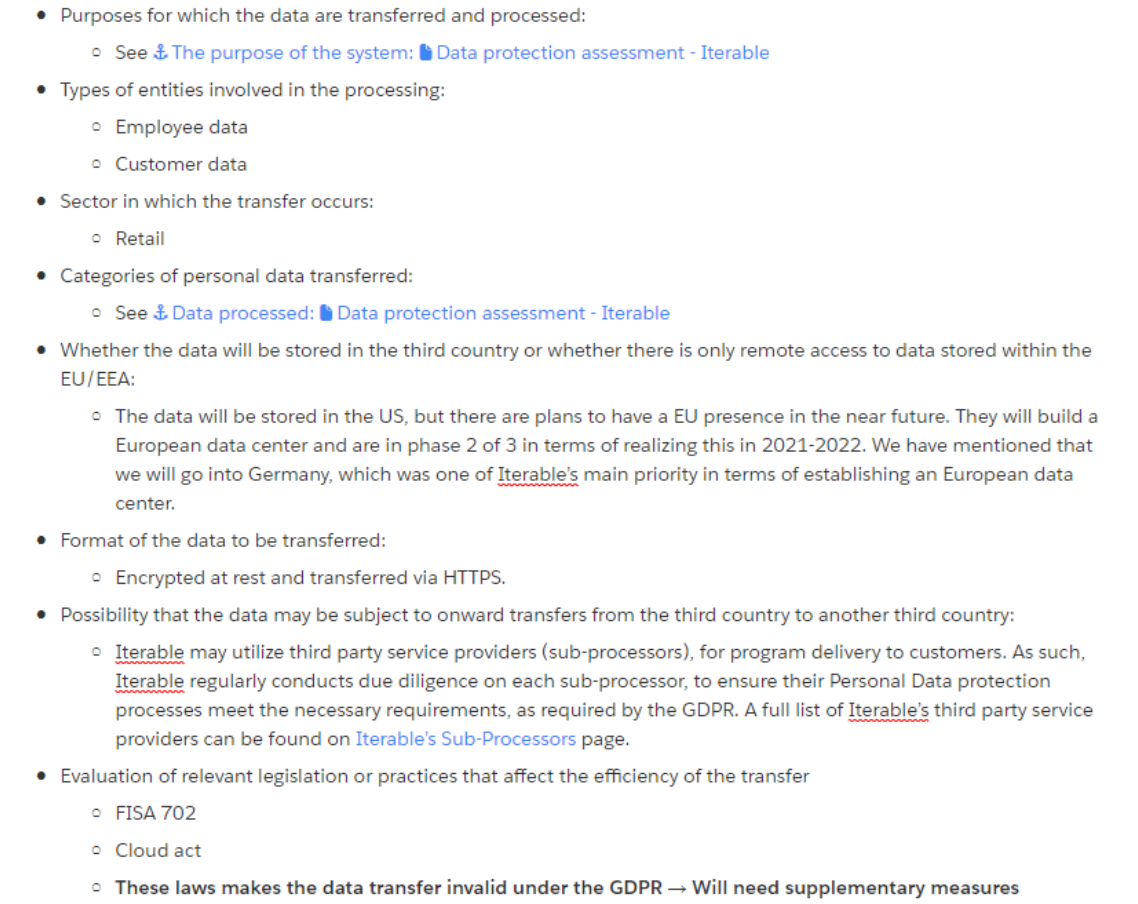
- Summary from DPIA
    - Purpose of processing
    - Description of provider
    - Data categories involved in the processing
    - Legal basis covered by...
    - Data storage/deletion
    - Access control
    - Description of why this is considered a data transfer to a third country
- Link to Data Processing Agreement (old “SCC”)

Step 2: Identify transfer tools

- Art 45: Is the U.S. a country with adequate protection? **No**
- Art 42/46: Certification mechanisms? **No**, but could be used as an assurance for quality in addition to supplementary measures
- Art 49: Exceptions? **No,** wouldn't dare it…
- Art 46: Could BCC's, codes of conduct or ad-hoc contractual clauses be a fit for us? **No**
- Art 46: SCC's? **Yes,** closest to our "normal" use of data processing agreements. Felt "safe"
- PS! In heinzeit, at the time of the first assessment, we clearly didn't understood what the new SCC's actually meant for us

oda

Step 3: Evaluate effectiveness of transfer tools



- Purposes for which the data are transferred and processed:
    - See ⚓ The purpose of the system: 📄 Data protection assessment - Iterable
- Types of entities involved in the processing:
    - Employee data
    - Customer data
- Sector in which the transfer occurs:
    - Retail
- Categories of personal data transferred:
    - See ⚓ Data processed: 📄 Data protection assessment - Iterable
- Whether the data will be stored in the third country or whether there is only remote access to data stored within the EU/EEA:
    - The data will be stored in the US, but there are plans to have a EU presence in the near future. They will build a European data center and are in phase 2 of 3 in terms of realizing this in 2021-2022. We have mentioned that we will go into Germany, which was one of Iterable's main priority in terms of establishing an European data center.
- Format of the data to be transferred:
    - Encrypted at rest and transferred via HTTPS.
- Possibility that the data may be subject to onward transfers from the third country to another third country:
    - Iterable may utilize third party service providers (sub-processors), for program delivery to customers. As such, Iterable regularly conducts due diligence on each sub-processor, to ensure their Personal Data protection processes meet the necessary requirements, as required by the GDPR. A full list of Iterable's third party service providers can be found on Iterable's Sub-Processors page.
- Evaluation of relevant legislation or practices that affect the efficiency of the transfer
    - FISA 702
    - Cloud act
    - **These laws makes the data transfer invalid under the GDPR → Will need supplementary measures**

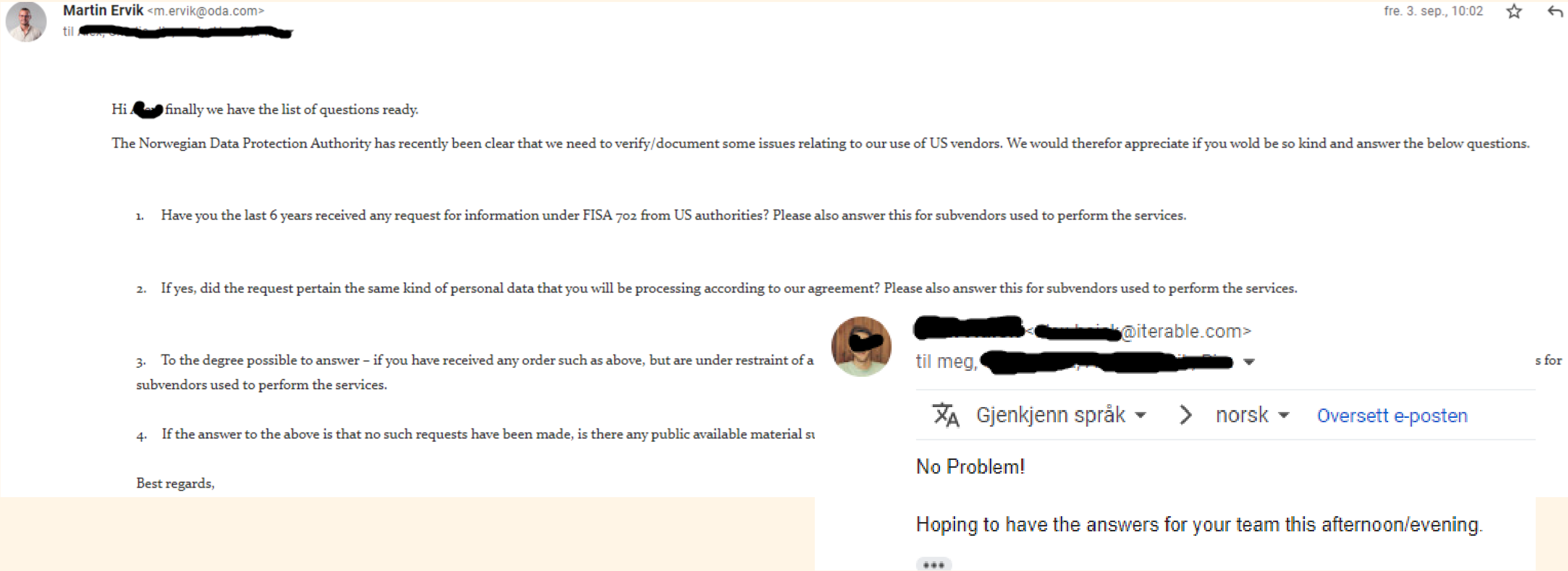
Step 3: Evaluate effectiveness of transfer tools

- Okay, but what about the relevance of the data we plan to transfer?
  - Will the data we transfer be relevant to a potential audit extraction request from U.S. authorities?

- “Schrems-Questionnaire” sent to Iterable (Thank you Eva!!)
  - *Have you the last 6 years received any request for information under FISA 702 from US authorities? Please also answer this for sub-vendors used to perform the services.*
  - *If yes, did the request pertain the same kind of personal data that you will be processing according to our agreement? Please also answer this for sub-vendors used to perform the services.*
  - *To the degree possible to answer – if you have received any order such as above, but are under restraint of a gag-order – are you free to report the number of such orders on a larger scale (gag-order-deal)? Please also answer this for sub-vendors used to perform the services.*
  - *If the answer to the above is that no such requests have been made, is there any public available material supporting that this is true that you could send us? This may be sector-relevant documentation*

Step 3: Evaluate effectiveness of transfer tools

- Dialogue with Iterable started 3. sept:



Martin Ervik <m.ervik@oda.com>

til [redacted]

fre. 3. sep., 10:02

Hi [redacted] finally we have the list of questions ready.

The Norwegian Data Protection Authority has recently been clear that we need to verify/document some issues relating to our use of US vendors. We would therefor appreciate if you wold be so kind and answer the below questions.

1. Have you the last 6 years received any request for information under FISA 702 from US authorities? Please also answer this for subvendors used to perform the services.

2. If yes, did the request pertain the same kind of personal data that you will be processing according to our agreement? Please also answer this for subvendors used to perform the services.

3. To the degree possible to answer – if you have received any order such as above, but are under restraint of a s for subvendors used to perform the services.

4. If the answer to the above is that no such requests have been made, is there any public available material su

Best regards,

[redacted] <[redacted]@iterable.com>

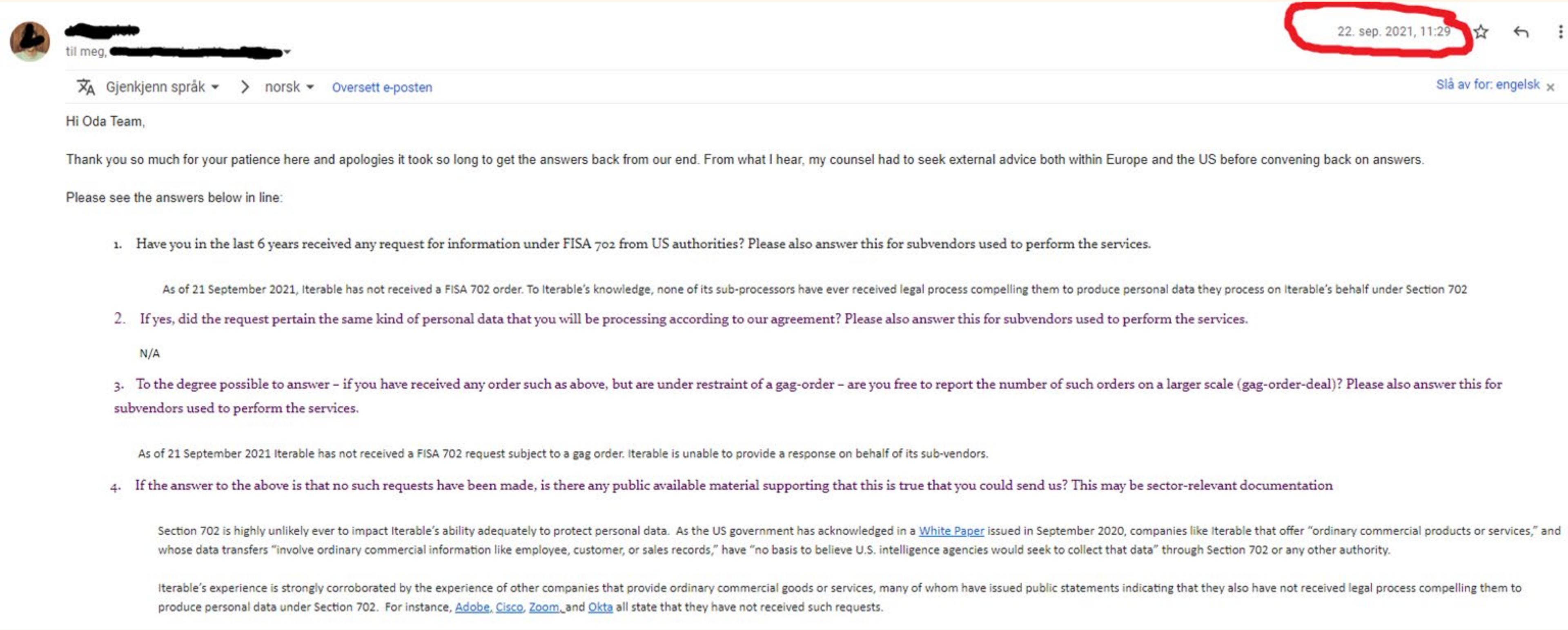
til meg, [redacted]

No Problem!

Hoping to have the answers for your team this afternoon/evening.

Step 3: Evaluate effectiveness of transfer tools

- And finally, 3 weeks later!!



[redacted]

til meg, [redacted]

22. sep. 2021, 11:29

Hi Oda Team,

Thank you so much for your patience here and apologies it took so long to get the answers back from our end. From what I hear, my counsel had to seek external advice both within Europe and the US before convening back on answers.

Please see the answers below in line:

1. Have you in the last 6 years received any request for information under FISA 702 from US authorities? Please also answer this for subvendors used to perform the services.

   As of 21 September 2021, Iterable has not received a FISA 702 order. To Iterable's knowledge, none of its sub-processors have ever received legal process compelling them to produce personal data they process on Iterable's behalf under Section 702

2. If yes, did the request pertain the same kind of personal data that you will be processing according to our agreement? Please also answer this for subvendors used to perform the services.

   N/A

3. To the degree possible to answer – if you have received any order such as above, but are under restraint of a gag-order – are you free to report the number of such orders on a larger scale (gag-order-deal)? Please also answer this for subvendors used to perform the services.

   As of 21 September 2021 Iterable has not received a FISA 702 request subject to a gag order. Iterable is unable to provide a response on behalf of its sub-vendors.

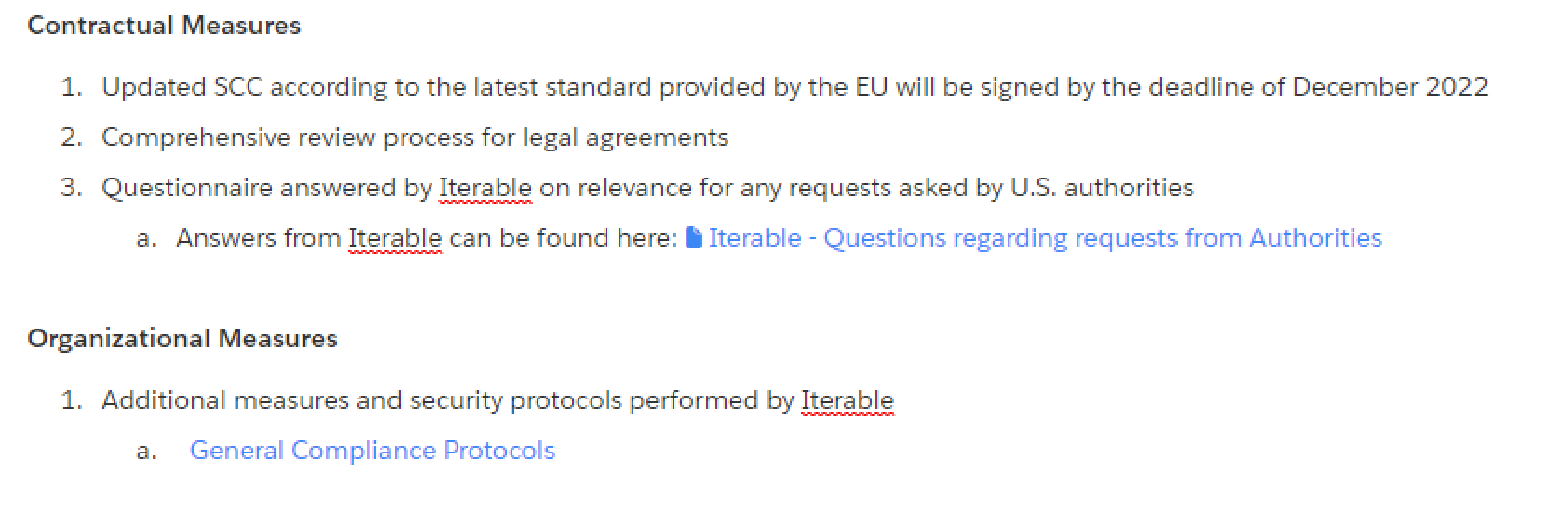
4. If the answer to the above is that no such requests have been made, is there any public available material supporting that this is true that you could send us? This may be sector-relevant documentation

   Section 702 is highly unlikely ever to impact Iterable's ability adequately to protect personal data. As the US government has acknowledged in a White Paper issued in September 2020, companies like Iterable that offer "ordinary commercial products or services," and whose data transfers "involve ordinary commercial information like employee, customer, or sales records," have "no basis to believe U.S. intelligence agencies would seek to collect that data" through Section 702 or any other authority.

   Iterable's experience is strongly corroborated by the experience of other companies that provide ordinary commercial goods or services, many of whom have issued public statements indicating that they also have not received legal process compelling them to produce personal data under Section 702. For instance, Adobe, Cisco, Zoom, and Okta all state that they have not received such requests.

Step 4: Identify and adopt supplementary measures

- From the documentation:



Contractual Measures

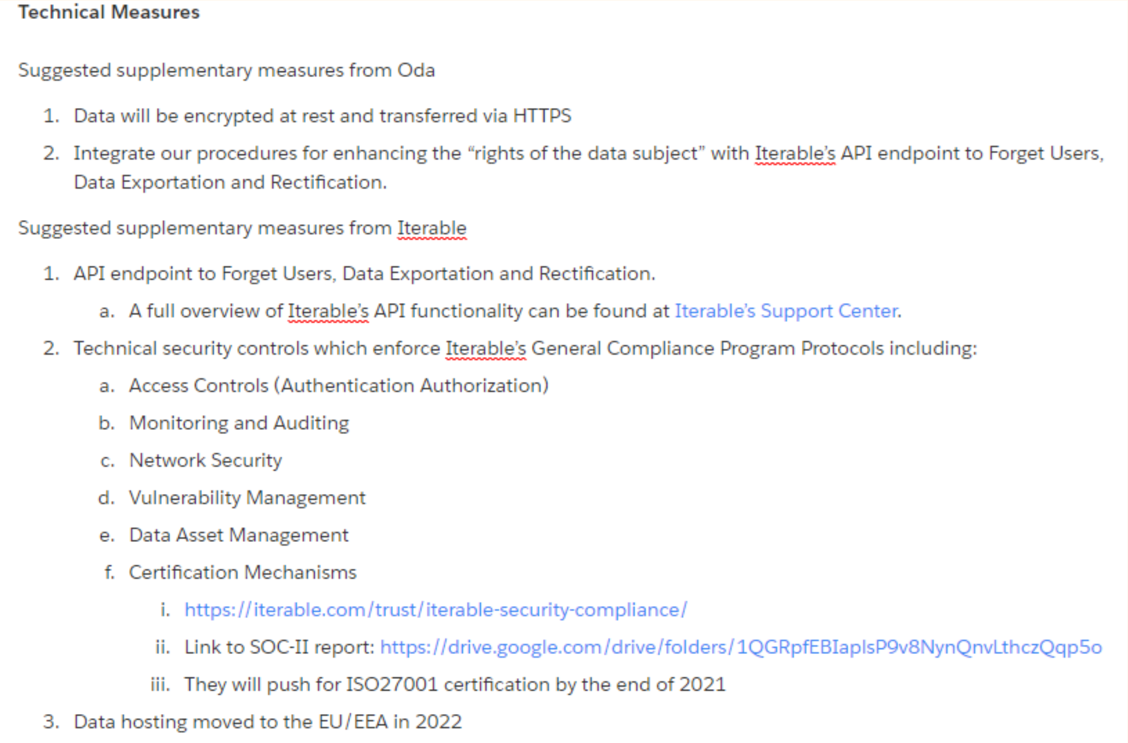
1. Updated SCC according to the latest standard provided by the EU will be signed by the deadline of December 2022
2. Comprehensive review process for legal agreements
3. Questionnaire answered by Iterable on relevance for any requests asked by U.S. authorities
   a. Answers from Iterable can be found here: Iterable - Questions regarding requests from Authorities

Organizational Measures

1. Additional measures and security protocols performed by Iterable
   a. General Compliance Protocols

Step 4: Identify and adopt supplementary measures

- From the documentation:



Technical Measures

Suggested supplementary measures from Oda

1. Data will be encrypted at rest and transferred via HTTPS
2. Integrate our procedures for enhancing the "rights of the data subject" with Iterable's API endpoint to Forget Users, Data Exportation and Rectification.

Suggested supplementary measures from Iterable

1. API endpoint to Forget Users, Data Exportation and Rectification.
    a. A full overview of Iterable's API functionality can be found at Iterable's Support Center.
2. Technical security controls which enforce Iterable's General Compliance Program Protocols including:
    a. Access Controls (Authentication Authorization)
    b. Monitoring and Auditing
    c. Network Security
    d. Vulnerability Management
    e. Data Asset Management
    f. Certification Mechanisms
        i. https://iterable.com/trust/iterable-security-compliance/
        ii. Link to SOC-II report: https://drive.google.com/drive/folders/1QGRpfEBIapIsP9v8NynQnvLthczQqp5o
        iii. They will push for ISO27001 certification by the end of 2021
3. Data hosting moved to the EU/EEA in 2022

Step 4: Identify and adopt supplementary measures

- What about “encryption in use”, you may ask? From security review:

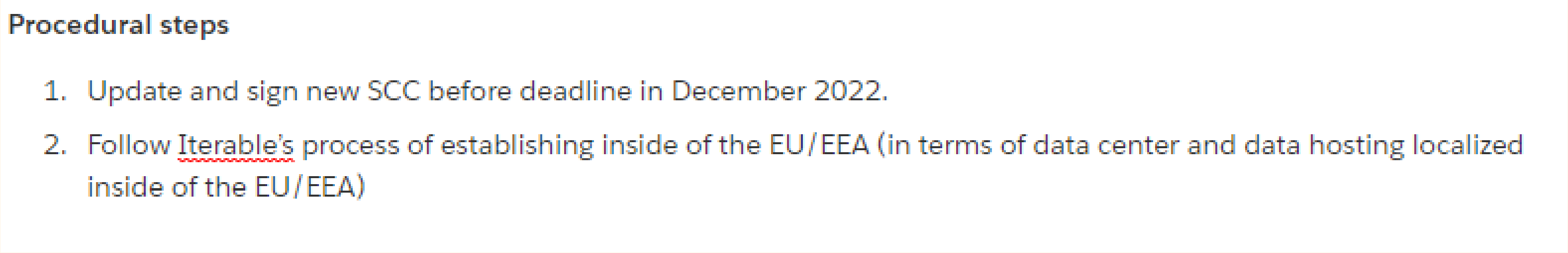
- *Access to customer data is granted based on employee roles and is only granted to those roles which require access to fulfill their job duties.* ***Only internal Admins have the ability to export customer data when necessary, and all exports are tracked and closely monitored.All customer data access is logged and monitored.***

- *Iterable uses AWS managed cryptographic keys and does not have access. Encryption keys are managed by AWS Instance Store (for hardware based encryption), AWS Secrets Manager, AWS S3, or AWS Key Management Service depending on the type of key or cert. As customer data is stored in Amazon S3 buckets, Iterable utilizes Amazon’s S3 encryption (a description of this can be found here). The keys cannot be distributed per customer as Iterable is a multi-tenant platform and the encryption is applied across customers.*

- Most likely **not sufficient(?)**, but a “risk level” internal stakeholders found comfortable in combination with the answers from the Schrems-questionnaire

Step 5: Procedural steps for supplementary measures

From the documentation:



Procedural steps

1. Update and sign new SCC before deadline in December 2022.
2. Follow Iterable's process of establishing inside of the EU/EEA (in terms of data center and data hosting localized inside of the EU/EEA)

Step 6: Re-evaluate steps (3-5) at appropriate intervals

- Until procedural steps mentioned in last slide is finalized, we’ve agreed on a check-in every 2nd month with Iterable KAM and General Counsel

- Full review by the end of 2022 (“Schrems-deadline”)

What's next?

- "Schrems-II project" - Deadline H2022

- Project split in two:
    a. Evaluation and documentation of data transfers outside of EU/EEA already happening
    b. Create policy for evaluation of new data transfers outside of EU/EEA

- **Data transfers already "happening"**
    - "Core systems" prioritized
    - Review DPA's and update with new SCC's
    - Document data transfer assessment with the EDPB 6-step guideline (Step 1-4 minimum)
    - Provide recommendations for system owners

- **Evaluation of new data transfers**
    - Document data transfer assessment with the EDPB 6-step guideline (Step 1-6)
    - Schrems-questionnaire sent to providers
    - Put pressure on providers
    - Follow-up meetings with providers of "core systems"

oda

Summary and reflections

Summary and reflections - Iterable

- It swallows a lot of resources doing these assessments
  - Time consuming effort, especially the first time
  - Cross-functional training of relevant teams is needed
  - Not very correlant with a company like Oda, where most decisions are made on team level
  - Dialogue with providers takes time as well - They are probably not mature enough on Schrems-2 considerations...yet!

- It ended up being “risk-based” after all?
  - Encryption method probably not sufficient
  - Schrems-questionnaire and the resulting answers could be seen as a “false” safety measure

- It ended up being a decision for stakeholders on “how compliant” do we want to be at this stage?
  - “We do as much as we can!”

- Paradox: We needed this system as it actually is a measure to provide better control of compliance-aspects in market communication
  - Remove “human” error from the former manual process
  - Better control of filtering on consent for marketing communication

oda

Summary and reflections - In general

- Use of EDPB’s guidelines
  - Could be hard to use at first try
  - What are good and sufficient documentation?
  - Not implicit how to evaluate relevant legislation or practices that affect the efficiency of the transfer - Schrems-questionnaire helpful tool
  - “Over Documenting”, just to be on the safe side
  - Technical supplementary measures will be hard to solve
  - Feels like a “risk-based” approach
  - **But luckily for us, it gets easier for every time!**

- Use of updated SCC’s
  - Seems like stuff is happening after the summer → American-based companies pro-actively reaches out
  - A lot of American-based companies still refers to Privacy Shield “compliance”
  - More pressure and dialogue with a broad spectrum of providers will make them take more of the responsibility
  - If they don’t have the SCC ready, make sure to agree on deadlines and follow-up meetings to finalize it

oda

Summary and reflections

- Communicating Schrems-II consequences internally is not always easy!
    - (Especially in a fast growing company where decisions are being made quite rapidly)
    - Training and awareness will be necessary. On top level as well

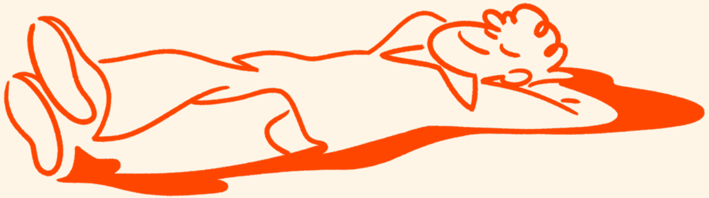
- Waiting a bit with spending a lot of time and resources could be a good idea?

- Things are getting better!
    - Next assessment we did, for a new HR-system (Workday), was much more satisfying.
    - Seems to be a lag in time for American companies to raise their awareness on the topic

- One thing is big companies with large resources, smaller businesses on the other hand….

Summary and reflections

- Finally.. We did as much as we could!
- But the question will still be: **Is this sufficient?**



What’s next?

oda