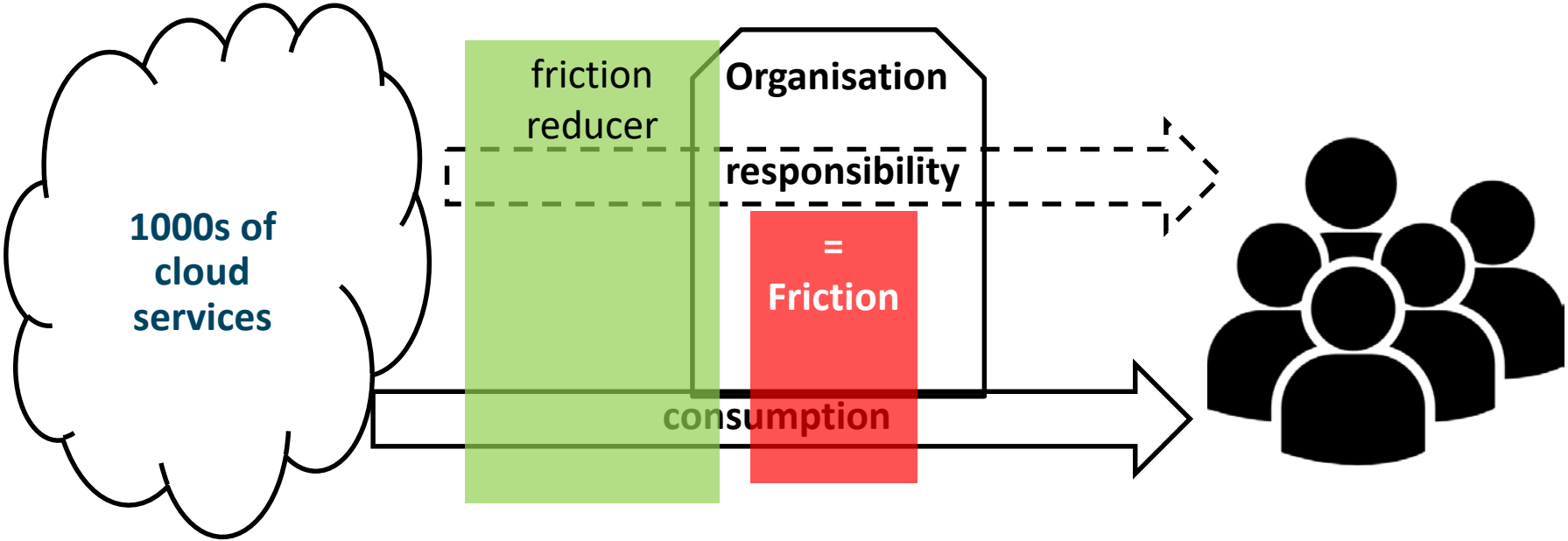
GDPR compliance assessment accalerator

For cloud services

Jan Meijer
Task leader GEANT JRA4 - T2
UNINETT

TF-DPR meeting Dublin
27 February 2018

The general cloud services challenge



Make a (group) of services accessible to HE&R in a compliant way, within reasonable time, playing nicely with existing services, infrastructure and data

GEANT cloud activity - goal

- Aggregating demand, joining forces
  - Do together that which is hard to do alone (e.g. concessions from big providers)
- Do once, use many times
  - Activities that are repeated by most NRENs and/or HE&R institutions
  - Save massive effort at community scale: 5 hours of work saved 5.000 times = 25 FTE saved
- Scope: cloud services

Key achievements and KPI status of JRA4

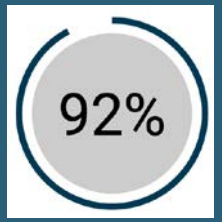
- **Completed a pan-European tender for IaaS solutions:**
  20 services available

- **Co-organised a second tender, for videoconferencing:**
  3 services available

- **Created a first version of a delivery ecosystem:**
  Service management operations
  Channel outreach to the community,
  supporting 26 NRENs

Thus, establishing **a Digital Single Market** of cloud services, for the European Research and Education Community

KPI 1: Make 25 services available
Status: 23 services available



KPI 2: Support 15 NRENs
Status: Supporting 26 NRENs

GDPR related work in cloud activity

- IaaS framework agreement
  - Update DPR clauses: make contract GDPR compliant
- Educational quotations and improved T&Cs
  - Standard contractual clauses (G18)
  - Bolt on to supplier's T&C
  - Has GDPR clauses
- GDPR compliance assessment accelerator

General Data Protection Regulation

1. *Institution's use of service X must be GDPR compliant*
2. *Institution must set internal data protection processes.*
3. *Institution must ensure it's use of services provided by service providers is compliant*
4. *25 May is only the end of the beginning*

GDPR compliance assessment accelerator

Institution (data controller) must assess
contractual relationship and risk associated
with service providers (data processors)

Institution is always responsible,

but the process can be easier, faster, cheaper

to make the institution's use of a service
GDPR compliant.

GDPR compliance assessment accelerator

Proposed shared materials (license: CC-BY-NC)

1. Contract clause map – find your GDPR way in contract spaghetti
2. Risk map – assist in risk discovery

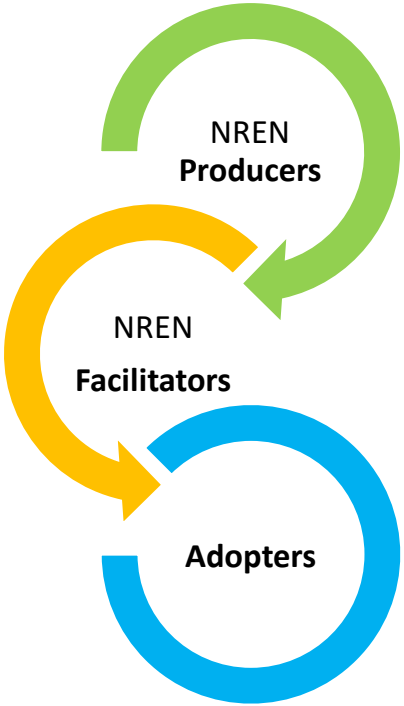
Future:

3. *Data processor agreement template*
4. *Single channel to provider – distribution updated security audit reports*
   – central point to aggregate common questions

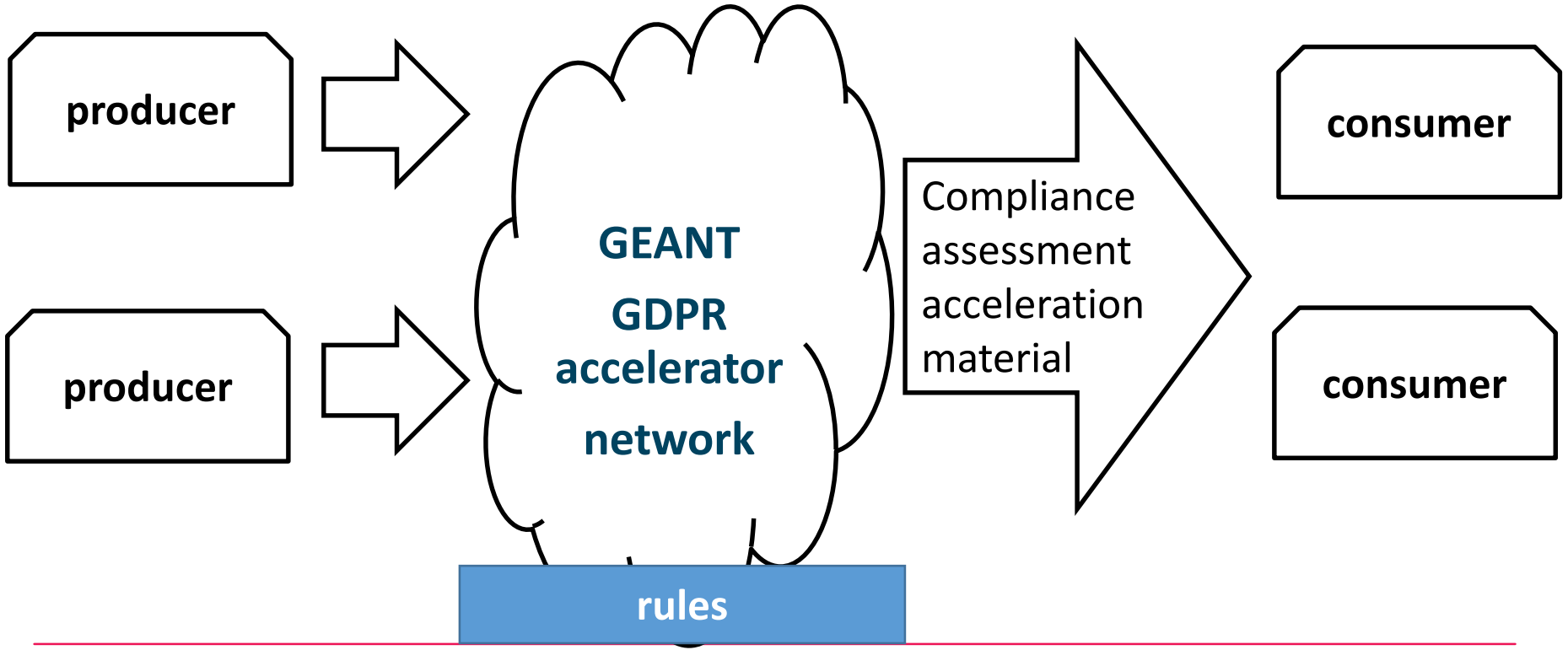
GDPR compliance accelerator

Sharing network** - done **ONCE**, use by **MANY:

- Some NRENs / Géant can produce reusable materials to assist GDPR compliance assessments
- NRENs can facilitate distribution of the compliance assessment accelerating materials to their community
- Institutions can adopt the materials in their GDPR compliance assessment process on par with other external documentation



GDPR compliance assessment accelerator



Example contractual clauses map

Data processing agreements – checklist (https://www.uninett.no/infosikkerhet/databehandleravtaler)	**Vendor DPA/ T&C:** **Slack Data Processing Addendum v170828** **(https://slack.com/terms-of-service/data-processing)** This Data Processing Addendum ("DPA") forms a part of the Customer Terms of Service found at https://slack.com/terms-of-service, unless Customer has entered into a superseding written master subscription agreement with Slack, in which case, it forms a part of such written agreement (in either case, the "Agreement"). By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (…). **HOW THIS DPA APPLIES TO CUSTOMER AND ITS AFFILIATES** If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Slack entity that is party to the Agreement is party to this DPA.
Division of responsibility between the service provider and the institution: The service provider confirms that any processing of personal data as part of the service is done on behalf of the institution.	**2.1 Roles of the Parties.** *"The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Slack is the Processor and that Slack or members of the Slack Group will engage Sub-processors pursuant to the requirements set forth in Section 4 ["Subprocessors" below."* **2.3 Slack's Processing of Personal Data.** *"As Customer's Processor, Slack shall only Process Personal Data for the following purposes:* *i. Processing in accordance with the Agreement and*

- Live document in .no
- www.uninett.no/slack "avtale speil"
- Institutions report back the documents are useful
- NL has similar

Example risk discovery map

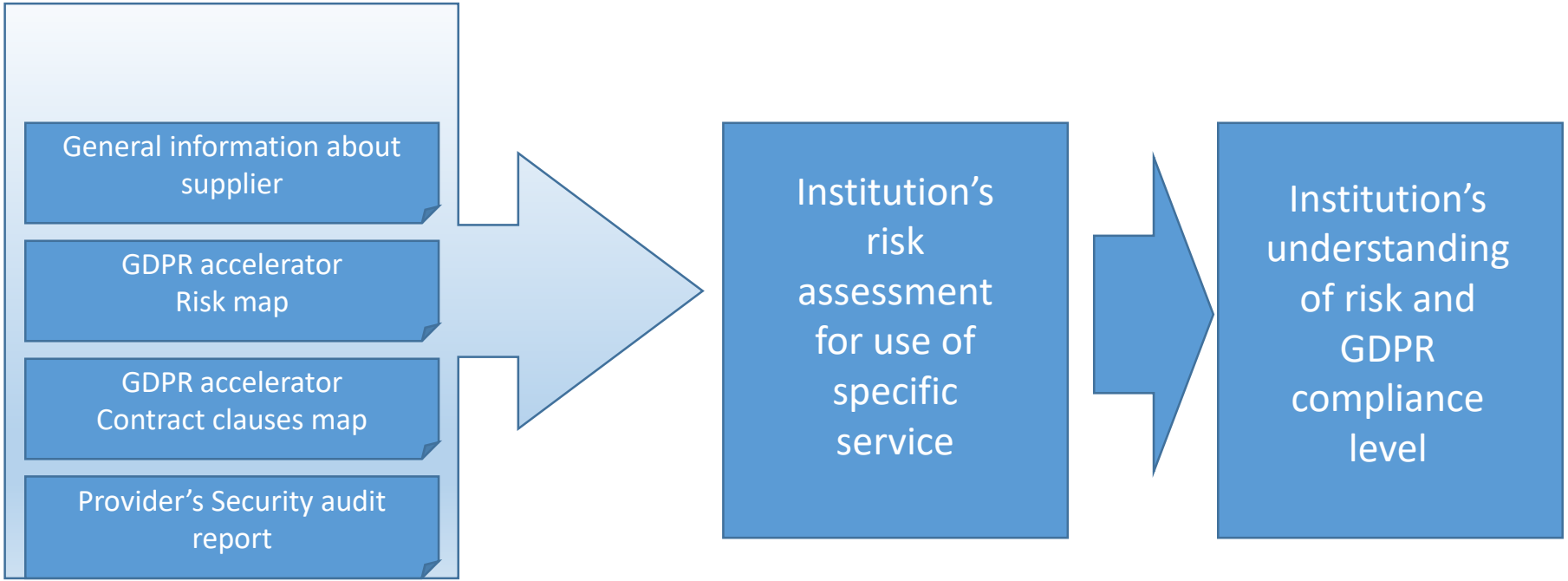
Risk discovery map

Service/System: Slack

#	Risk element	Vulnerability/ weakness	Existing security measures	Existing control measures	Assessment			Suggestions for measures
					P	C	Risk	
1	An unauthorised person gains access to another user's account: Data that should be protected may fall into the wrong hands. Examples include sensitive personal data, important trade secrets or research data. These data can also be erased or changed without the user him/herself finding out.	Poor security habits, for example keeping your password on a post-it note, being exposed to malware such as keyloggers, or a users account information being obtained in other ways.					0	- Procedures and training in what you can put in the cloud. - Two-factor authentication - Review and follow-up of logs
2	Incorrect access control to research data: With a cloud solution, it is easy to share research data with external users. In principle, the cloud solution is accessible from the internet, and this allows for the possibility of sharing research data with external users. If you share research data with the wrong external user, and forget to remove access, data can fall into the wrong hands.	- Human error/weakness - Inadequate training					0	- Procedures and training in what you can put in the cloud. - training - Awareness-raising work - Review and follow-up of logs
3	A cyberattack against the solution is not stopped in time: When the institution uses a cloud service provider, it often depends on the provider implementing countermeasures to combat a cyberattack. This is especially the case if you have been subjected to a DDoS (Distributed Denial of Service) attack or a Phishing campaign. In such cases, the institution may find that the provider's response time is too long for their liking. A security breach like this can therefore become more extensive than necessary.	The institution is not prioritised by the cloud service provider.					0	- Enter into an agreement on response times - Perimeter security, logging, monitoring - Penetration testing - The SLA should set out sanctions for breaches - Investigate the possibility of using a separate management server at the cloud service provider's so that it is possible to handle the incident yourself.
4	A cyberattack against the solution is not stopped in time: When the institution uses a cloud service provider, it often depends on the provider implementing countermeasures to combat a cyberattack. This is especially the case if you have been subjected to a DDoS (Distributed Denial of Service) attack or a Phishing campaign. In such cases, the institution may find that the provider's response time is too long for their liking. A security breach like this can therefore become more extensive than necessary.	The institution is not prioritised by the cloud service provider.					0	- Enter into an agreement on response times - Perimeter security, logging, monitoring - Penetration testing - The SLA should set out sanctions for breaches - Investigate the possibility of using a separate management server at the cloud service provider's so that it is possible to handle the incident yourself.
5	Security breach by exploiting vulnerabilities in systems: If any necessary security updates are not carried out, the institution's cloud solution may be subjected to cyberattacks. This vulnerability can be exploited by internal, external or other tenants in the same 'rig' (installation).	When the institution puts its computer systems in the cloud, it nevertheless has to ensure that security updates are carried out. When using cloud solutions, it can vary who is responsible for carrying out security updates of the systems. This division of responsibility must be clear. If it is unclear, known vulnerabilities can be exploited.					0	- Enter into agreements that clearly describe who is responsible for what - Check regularly whether the security updates have been completed - Carry out vulnerability scanning
6	Data are unavailable in the cloud solution: If a cloud service provider must change or take down parts of its system to correct errors with some of its customers, it may also affect the quality of the service for its other customers. Among other things,	The need for economies of scale leads to complex cloud solutions. If the cloud service provider does not have a complete overview of the complexity, more customers than planned and notified may be					0	- The cloud service provider must support 'live migration'. - The SLA must set out requirements for necessary

- Live document in .no
- www.uninett.no/slack (RoS mal)
- Institutions report back the documents are useful

Institution's GDPR compliance assessment – based on material



Early feedback from NRENs

- Can be used as benchmark by institutions
- Share risk assessment result and use as benchmark against other institutions: how big a risk does instution X feel a risk element is
- A review and feedback mechanism would be good
- Build community with multiple producers!
- Good idea!

GDPR compliance assessment accelerator: summary

- Toolset to help institutions use less time on assessing GDPR compliance with cloud service use
  - Contract clause map
  - Risk map
- Main benefits:
  - Save time/money/resources
  - Shorten time-to-market for new services
  - Help institution to scale GDPR compliance efforts for cloud services

- Mechanisms in use for years in NL and NO
- Sharing network to let those who produce share their results with those who can consume
- Once done, apply to set of common services used in EU HE&R
- Future: on-demand

Public PoC

- UNINETT will work on list of services until summer:
  - Google G Suite, Socio, Prezi, Slack, Plot.ly, Kahoot, Piazza, Asana, Autorea, Overleaf
- PoC: put contract clause and risk discovery maps from UNINETT in archive & make available through cloud service delivery managers @ NRENs
- Other elements in archive:
  - methodology document (risk assessment guide for cloud services)
  - Explanatory text
  - Explanatory podcast
- Start in March
- Add services as they become available
- Interested?