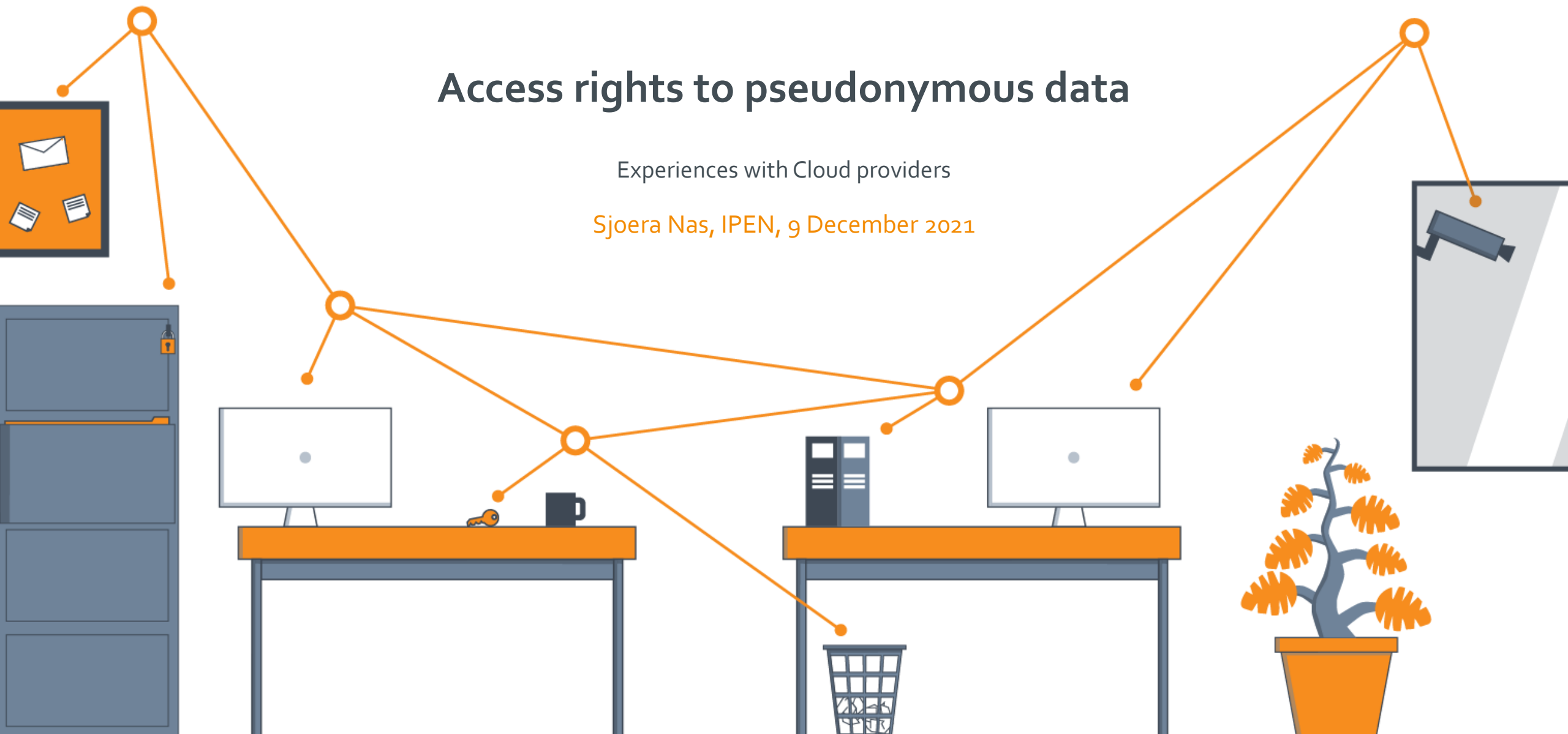


Access rights to pseudonymous data

Experiences with Cloud providers

Sjoera Nas, IPEN, 9 December 2021



Agenda


- Experiences with many cloud providers
- Different categories of pseudonymous personal data
- Processor or joint controller
- Claimed exceptions on access rights

What cloud providers en services?



<https://slmmicrosoftrijk.nl/downloads-dpias/>

DPIA approach Privacy Company: legal and technical



The large print
giveth, but the
small print taketh
away.



Analysing framework agreement
often many separate documents

DPIA approach Privacy Company: legal and technical

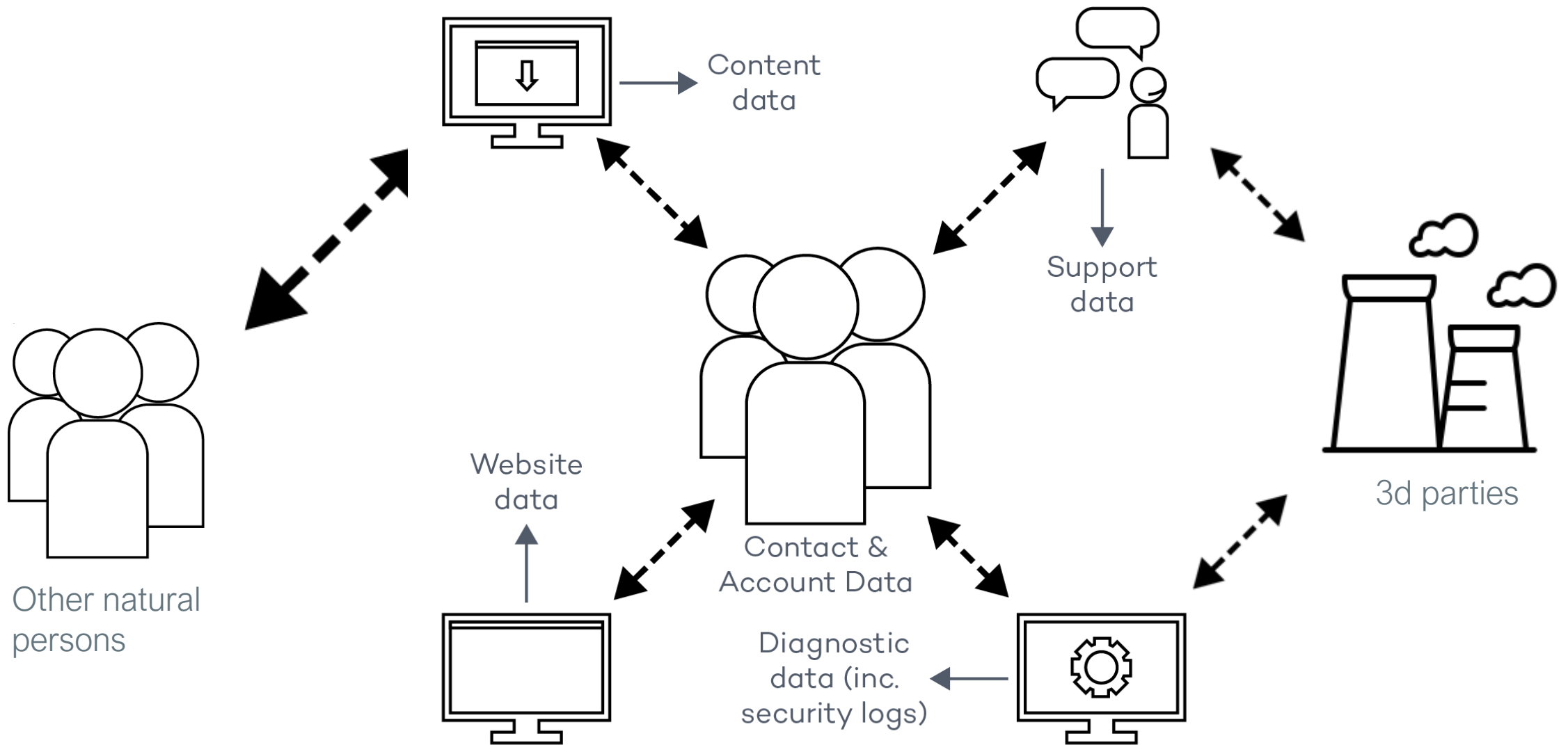




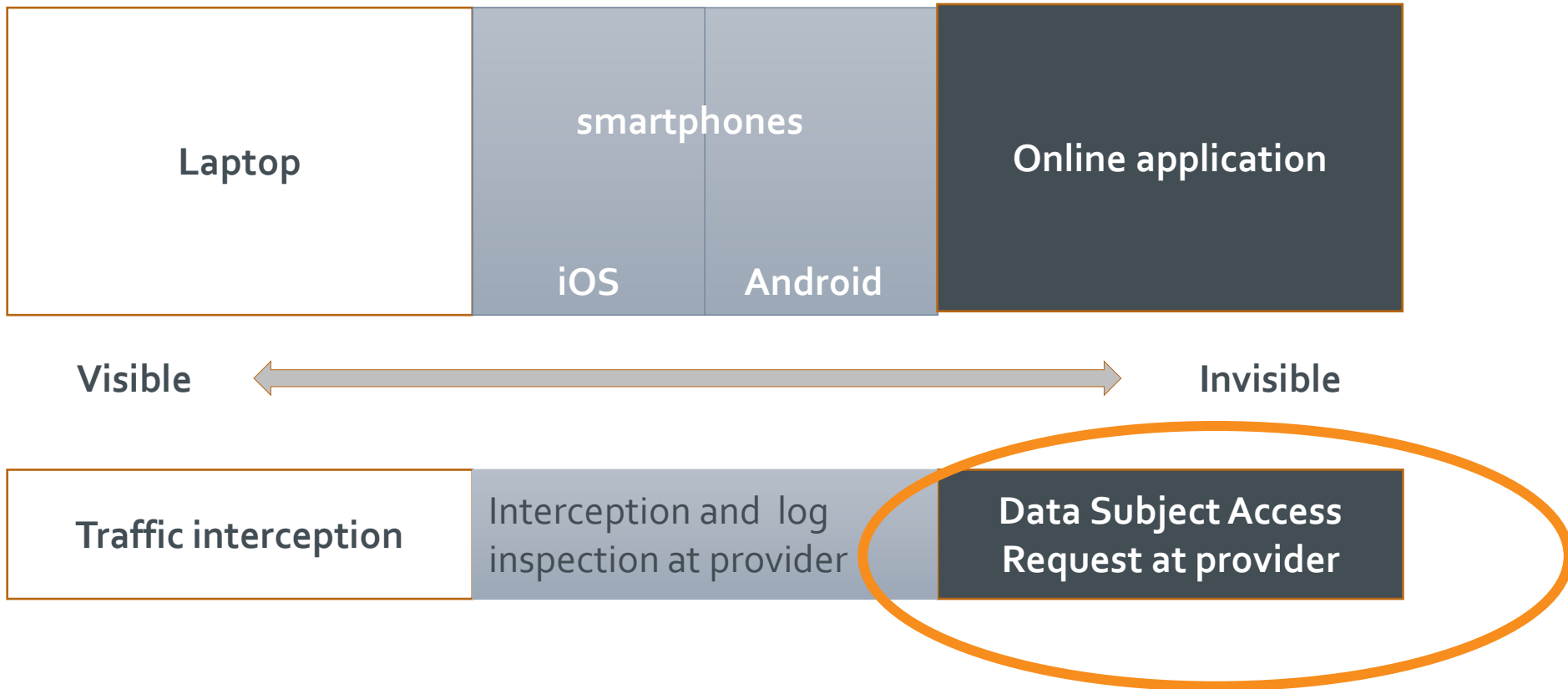
Different kinds of Diagnostic Data

- Telemetry data: installed software applications and browsers collect and send data about the individual use of the services to the mothership
- Service generated server logs: cloud providers register all end user activities in their own logs
- SIEM logs: some personal data such as IP addresses in SIEM (security) logs
- Webserver access logs: restricted and public access webpages
- Traffic to third parties: cookies, support tickets, sometimes even Content Data (crash logs, spam/malware/CSAM scanning)

6 types of personal data



Inspection methods processing at cloud providers



Pseudonymous data are personal data

- Artikel 4(5) GDPR: pseudonymisation' means the processing of personal data in such a manner (...)
- Diagnostic data with unique identifiers are personal data
- Most cloud providers store diagnostic data for a long period of time in a single database. Hashing or other kinds of pseudonymisation do not help as companies can attach new information to the existing data with the same formula.

Example of Microsoft Windows 10 telemetry event

```
{
  "ver": "3.0",
  "name": "Census.Enterprise",
  "time": "2019-01-23T07:12:19.6354125Z",
  "cV": "OHkC3yxxkkqfwQc.0",
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "flags": 514,
  "ext": {
    "utc": {
      "pgName": "WINCORE",
      "flags": 908067332,
      "epoch": "1108672",
      "seq": 17 },
    "os": {
      "bootId": 11,
      "name": "Windows",
      "ver": "10.0.17763.195.amd64fre.rs5_release.180914-1434" },
    "app": {
      "id": "W:000f519feec486de87ed73cb92d3cac80240000000!000064cd6dc111ba59b11923e2ec26825c75ee6ab7aa!devicecensus.exe",
      "ver": "2096/05/22:02:17:09!12DE0!devicecensus.exe",
      "asId": 147 },
    "device": {
      "localId": "s:0694CCC4-88C9-4A58-AD5D-7905553CE3E9",
      "deviceClass": "Windows.Desktop" },
    "protocol": {
      "devMake": "VMware, Inc.",
      "devModel": "VMware Virtual Platform" },
    "user": { "localId": "w:B04E2543-63EB-D3C6-4722-FBFE64FA31C0" },
    "loc": { "timeZone": "+01:00" } },
  "data": {
    "IsCloudDomainJoined": "0",
    "IsMDMEnrolled": "0",
    "CDJType": 4294967295,
    "ServerFeatures": "#",
    "CommercialId": "#",
    "AzureVMType": "#",
    "AzureOSIDPresent": false,
    "IsDomainJoined": "1",
    "HashedDomain": "fcd5c26eb73477b14760d9b21464c355ee2f682243ce5907cd356cf54f935467.6f9478eb2551c0756bdb6eed6710764fa4ccd44bef780537b09c655169674db.cc1962a142a7828f7ec3013845b510522f71d67983758ecd61b5aefe38e18479",
    "SystemCenterID": "6GR0BPiesP/bl6jXJlbCxr88J1k5n581gDY/FC5m8nU=",
    "MPNId": "#",
    "SCCMClientid": "#",
    "IsDeviceProtected": "DEVICE_NOT_PROTECTED",
    "IsDERequirementMet": "DEVICE_REQ_NOT_MET|HW_TPM_NOT_CONFIGURED|SW_GP_MISCONFIGURED",
    "IsEDPEnabled": "EDP_NOT_ENABLED",
    "AADDeviceId": "#",
    "ContainerType": 4294967295,
    "EnrollmentType": 4294967295 }
}
```

Standard header

Event specific data

All kinds of unique identifiers in telemetry events

```
{
  "ver": "3.0",
  "name": "Census.Enterprise",
  "time": "2019-01-23T07:12:19.6354125Z",
  "cV": "OHkC3yxxkkqvfwQc.0",
  "iKey": "o:0a89d516ae714e01ae89c96d185e9ae3",
  "flags": 514,
  "ext": {
    "utc": {
      "pgName": "WINCORE",
      "flags": 908067332,
      "seq": "1108672",
      "seq": 17
    },
    "os": {
      "bootId": 11,
      "name": "Windows",
      "ver": "10.0.17763.195.amd64fre.rs5_release.180914-1434"
    },
    "app": {
      "id": "W:0000f519fec486de87ed73cb92d3cac80240000000!000064cd6dc111ba59b11923e2ec26825c75ee6ab7aa!devicecensus.exe",
      "ver": "2096/05/22:02:17:09!12DE0!devicecensus.exe",
      "bootId": 11
    },
    "device": {
      "localId": "s:0694CCC4-88C9-4A58-AD5D-7905553CE3E9",
      "deviceClass": "Windows.Desktop"
    },
    "protocol": {
      "devMake": "VMware, Inc.",
      "devModel": "VMware Virtual Platform"
    },
    "user": {
      "localId": "w:B04E2543-63EB-D3C6-4722-FBFE64FA31C0",
      "timeZone": "+01:00"
    },
    "data": {
      "IsCloudDomainJoined": "0",
      "IsMDMEnrolled": "0",
      "CDJType": 4294967295,
      "ServerFeatures": "#",
      "CommercialId": "#",
      "AzureVMType": "#",
      "AzureOSIDPresent": false,
      "IsDomainJoined": 1,
      "HashedDomain": "fcd5c26eb73477b14760d9b21464c355ee2f682243ce5907cd356cf54f935467.6f9478eb2551c0756bdb6eed6710764fa47ccd14bef780537b09c655169674db.cc1962a142a7828f7ec3013845b510522f71d67983758ecd61b5aefe38e18479",
      "SystemCenterID": "6GR0BPiesP/bl6jXlBcXr88J1k5n581gDY/FC5m8nU=",
      "MPNId": "#",
      "SCCMClientId": "#",
      "IsDeviceProtected": "DEVICE_NOT_PROTECTED",
      "IsDERequirementMet": "DEVICE_REQ_NOT_MET|HW_TPM_NOT_CONFIGURED|SW_GP_MISCONFIGURED",
      "IsEDPEnabled": "EDP_NOT_ENABLED",
      "AADDeviceId": "#",
      "ContainerType": 4294967295,
      "EnrollmentType": 4294967295
    }
  }
}
```



Zoom telemetry events

```
{
  "client_os":"mac",
  "client_type":"Zoom Main Client",
  "client_version":"5.3.52877.0927",
  "event":"Tap Security",
  "event_loc":"In Meeting",
  "event_time":"9/30/2020 12:19:40",
  "in_sharing":"o",
  "meeting_id":"focAptkITTSfHTiULJWSlw=",
  "sub_event": "",
  "user_id":"6n1pCAW4TT2qj5tmnGoKSg",
  "uuid":"3bdDCvtUdtgM7X
uLZf79WIDlu7jTmLQ2YNzdDLgl7A="
}
```

```
{
  "client_os":"mac",
  "client_type":"Zoom Main Client",
  "client_version":"5.3.52877.0927",
  "event":"Recording",
  "event_loc":"In Meeting",
  "event_time":"9/30/2020 12:20:51",
  "meeting_id":"68460188777",
  "record":"toolbar-button",
  "sub_event":"Cancel",
  "user_id":"6n1pCAW4TT2qj5tmnGoKSg",
  "uuid":"3bdDCvtUdtgM7X
uLZf79WIDlu7jTmLQ2YNzdDLgl7A="
} ....
```



`l,null,null,\"en\",null,null,null,null,null,[\"Trek het aandacht van uw lezers met een veelzeggend citaat uit dat dokumen
t of gebruik dit ruimte om \",\"veelzeggend\",40,50,[],3,0,18,0,[null,18,3,0],0,null,[\"0\\\", \"0\\\"],[],[],null,null,9
,null,
null,null,null,null,null,null,null,null,null,[],1,4,null,null,null,null,null,true,null,null,null,null,null,null,`

Key problem: cloud provider as data controller



Joint controllership cloud providers with Enterprise customers

- Cloud providers often claim to act as data processor, but formal roles and contracts are not leading
- If a processor allows itself to determine processing purposes in its own interest, such as marketing or product innovation, it factually behaves as controller
- Most cloud providers omit to provide public documentation about the Diagnostic and Website Data
- The risk of factual, unintended joint controllership for the Diagnostic Data is that end users cannot exercise their data protection rights



Microsoft DSAR tools: audit logs, DDV and DSAR tool for diagnostic data

- (Query on) audit logs: always contain directly identifiable data, such as user ID, Organisation ID, IP address, subject header and addressees of mails, type of action + exact time
- Diagnostic Data Viewer Tool: shows very limited amount of telemetry events per app (less than 10%)
- New DSAR tool for Diagnostic Data: hodgepodge of undocumented files. Mostly with pseudonymised identifiers for the user and the tenant, such as "UserId": "b2814ab7-ocdb-4b7c-98fe-26deea388bb3"
- No access to *Required Service Data*
- No access to controller data (Windows, Edge)



Microsoft Diagnostic Data Viewer

Windows 10 Enterprise (Configured Proxy and installed wireshark) [Running]

Viewer voor diagnostische gegevens

Zoeken (Ctrl+E)

userbi
7-12-2021 12:19:39

userbi
7-12-2021 12:19:37

scenario
7-12-2021 12:17:16

scenario
7-12-2021 12:17:16

scenario
7-12-2021 12:17:04

Product- en servicegebruik

```
{
  "complianceEnvironmentType": 0,
  "isDataCategorizationEnabled": true,
  "userpdcllevel": 2,
  "processMemory": 27963552,
  "freeMemory": 102535168,
  "clientType": "desktop",
  "batterylevel": 1,
  "pluggedin": true,
  "Window": {
    "Focus": "foreground",
    "Status": "systray",
    "Type": "main"
  },
  "windowIsVisible": true,
  "UserInfo": {
    "TimeZone": "+01:00",
    "Id": "234783b6-e703-4ba2-9772-69042325bab7",
    "TenantId": "439f91bd-ed3a-49cf-b758-9e0d41fe7520",
    "Ring": "general",
    "ETag": "\\gOKvIcD6jBWOGa15XZiOqRPAwnmUNI4t8Db7tZbxBYg=\\",
    "Region": "emea",
    "LicenseType": "SmbNonVoice"
  },
  ...
}
```



Microsoft DSAR tool for Diagnostic Data

`./a42a5d8foc984421955do1a4e24b5336/c814ff83c1324f809ff3d7fa05a821f7/3517510.json`

This file contains 39 events recorded during the tests performed for this report. Example:

```
{
  "time": "",
  "correlationId": "",
  "properties": {
    "Browser": "Firefox",
    "BrowserVersion": "91",
    "env_time": "2021-08-24 13:23:11.5473232",
    "IpAddress": "185.213.106.92",
    "ObjectId": "b2814ab7-ocdb-4b7c-98fe-26deea388bb3",
    "OfferId": "MS-AZR-0044P",
    "operationName": "SectionCompleted-PhoneVerification",
    "OriginalEventTimestamp": "Tue, 24 Aug 2021 13:23:11 GMT",
    "Platform": "Unknown",
    "Puid": "1003200138BoD6A3"
  }
},
```

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365#part-3-responding-to-dsrs-for-system-generated-logs>

AWS, Oracle, Microsoft Azure, Google Cloud VMs and databases

- Documentation and access for admins to detailed audit logs, but -generally- no individual take-out of end user data (system administrators)
- No access to data exchanged via market places (app stores)
- No access to cookies and data in webserver access log
- No access to all security logs that the provider creates behind the screens.



Claimed exceptions on access rights

- company confidential / non relevant internal information
- privacy of other data subjects
- technically too difficult
- not in a position to reliably identify the data subject
- referral to third parties



Dissection of refusal arguments

- Company confidential: If you can intercept personal data such as telemetry events in the network traffic, they cannot be company confidential (already made public). *Interception and access did reveal sensitive contents of telemetry data.* With regard to detailed security logging: the provider should provide access in the context of a DPIA to the customer's own data, and publish the results of an independent audit of the contents, retention periods and possible onward transfers to 3d parties. *Access did reveal unknown 3d parties (malware scanning)*
- Cannot reliably identify: must accept means such as identification in person, combination of timestamps with unique identifiers, bring along test device, provide full network capture, including identifiers



Dissection of refusal arguments

- Too difficult to identify: if the core business of a provider is to sell targeted ads based on these data, the categorical refusal to provide access is untenable. The provider must build the logs in such a way that access can be provided upon request without disclosing other individuals' personal data (Art 11 + Art 25 design)
- Referral to third parties: Customer/controllers must be able provide to access to traffic exchanged with third parties via their website. If they are joint controllers with for example Facebook for a Facebook Page, they must design a mechanism to provide access to these data



Conclusions

- Cloud providers must provide complete answers to DSAR, as controller and as processor (Art. 28(3) under e, f and h of the GDPR)
- If access to pseudonymous data is denied, the customer/controller cannot assess the scale and impact of the data processing
- Risk of factual joint controllership without division of responsibilities
- Lack of transparency about diagnostic data may be intentional or accidental: DSARs are necessary to assess accuracy of public documentation
- In view of the dynamic nature of telemetry data, end users should be able to get semi realtime access



Questions?

Contact me via www.linkedin.com/in/sjoera

www.privacycompany.eu
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
Den Haag

