Designing With Privacy in Mind

David Sietz

Solutions Architect

www.linkedin.com/in/davidsietz

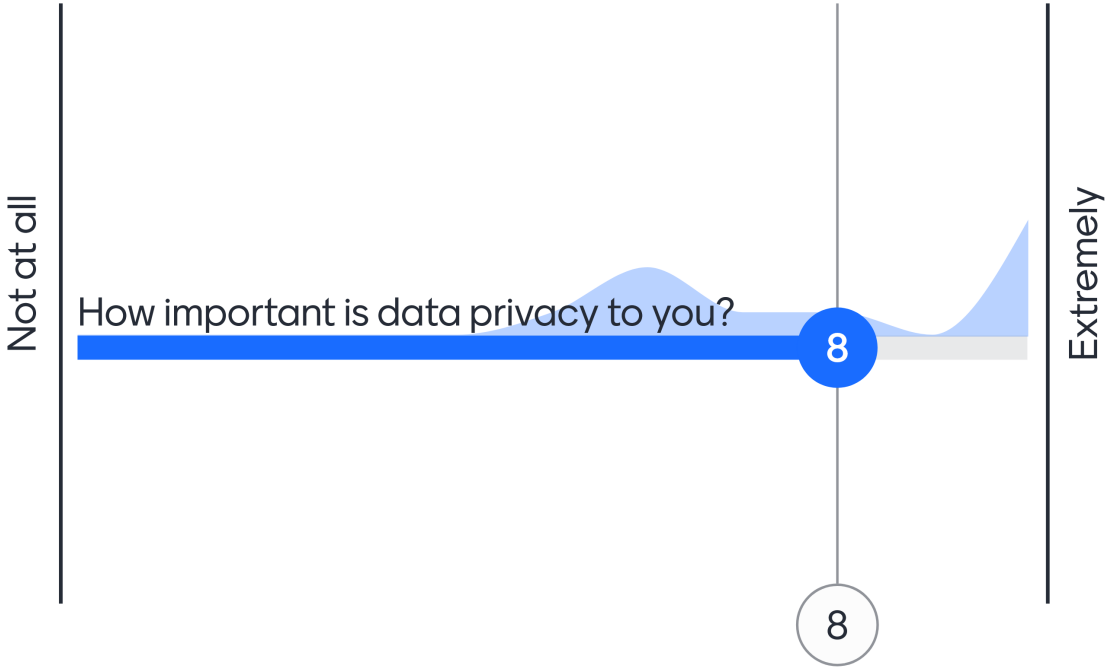
1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

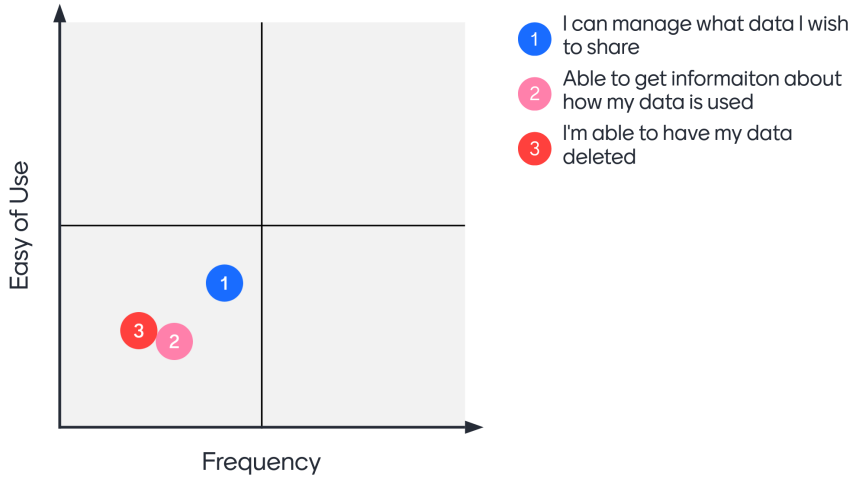


Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

How well do online companies manage your privacy?



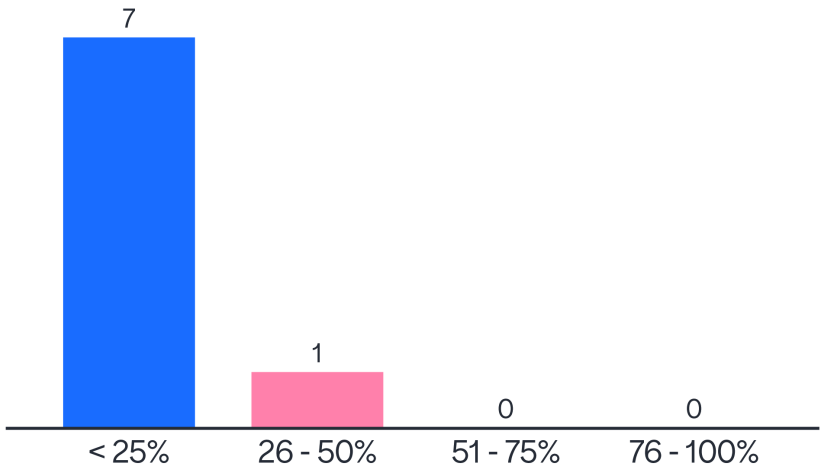
9

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

What percentage of your business requirements (or acceptance criteria) are privacy related?



8

Security vs Privacy

Our customers' data is secured, so we're okay. No one unauthorized can access it.

We have a privacy notice on our website. It's all explained in there.

We follow company policies.

```
In order to comply with GDPR, no data shall be stored outside the USA.
```

Our security architecture covers that.

Security

- Encryption
- Access Controls
- Audit Logs
- Multi-Factor Authentication

You built yourself a secured home and feel safe.

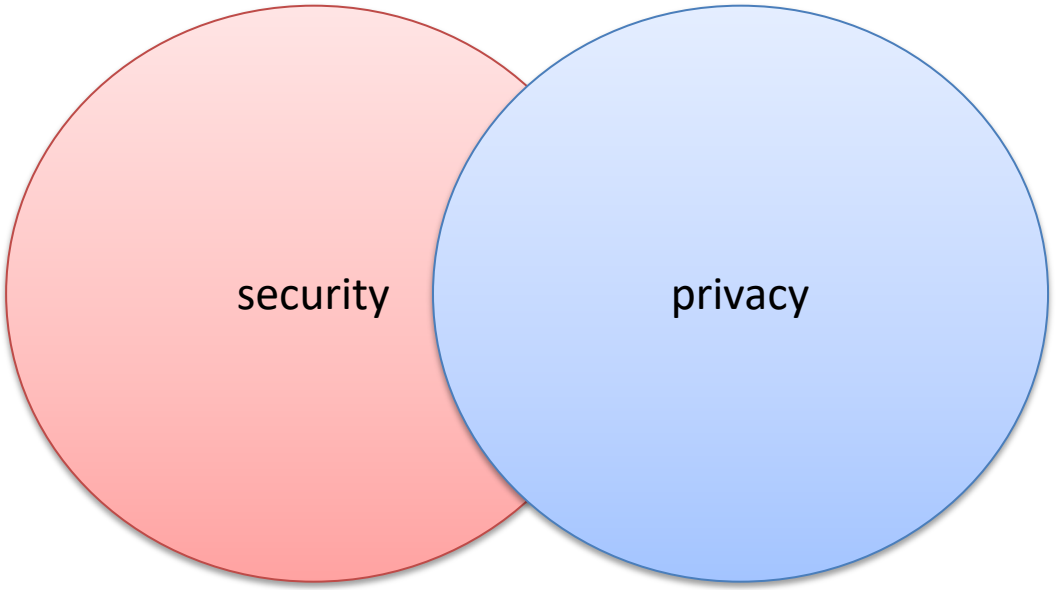
Privacy

- Do you enforce how data is used?
- Are you fully transparent with what data you have and how it is being used?
- Do you track where data is located in the system
- Do you minimize data collection based on immediate need?
- Are the data owners still in control of their data?

But is there privacy?

Security vs Privacy

You need security to ensure privacy. But you don't need privacy to ensure security.



Privacy Design Strategies

Strategy	Description
Minimize	Limit as much as possible the processing of personal data.
Separate	Separate the processing of personal data as much as possible.
Abstract	Limit as much as possible the detail in which personal data is processed.
Hide	Protect personal data, or make it unlinkable or unobservable. Make sure it does not become public or known.
Inform	Inform data subjects about the processing of their personal data in a timely and adequate manner.
Control	Provide data subjects adequate control over the processing of their personal data.
Enforce	Commit to processing personal data in a privacy-friendly way, and adequately enforce this.
Demonstrate	Demonstrate you are processing personal data in a privacy-friendly way.

Privacy Design Strategies (The Little Blue Book)
Jaap-Henk Hoepman
Agusut 23, 2019

Privacy by Design SDK

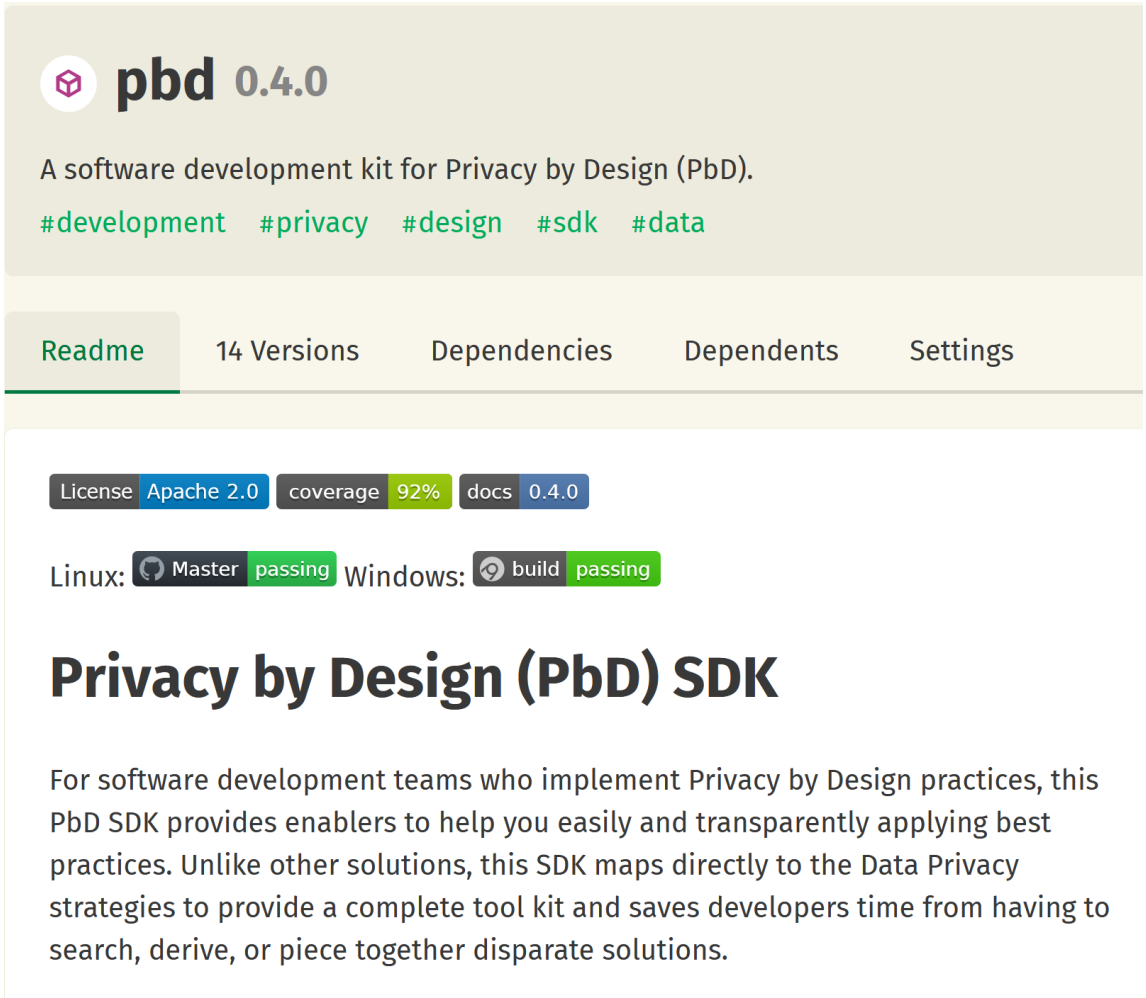
PbD SDK

Data Usage Agreement (DUA)
Management of how data is allowed to be used

Data Tracker Chain (DTC)
Auditing of the data lineage

Data Privacy Inspector (DPI)
Dynamically identify data based on privacy characteristics

Privacy by Design SDK

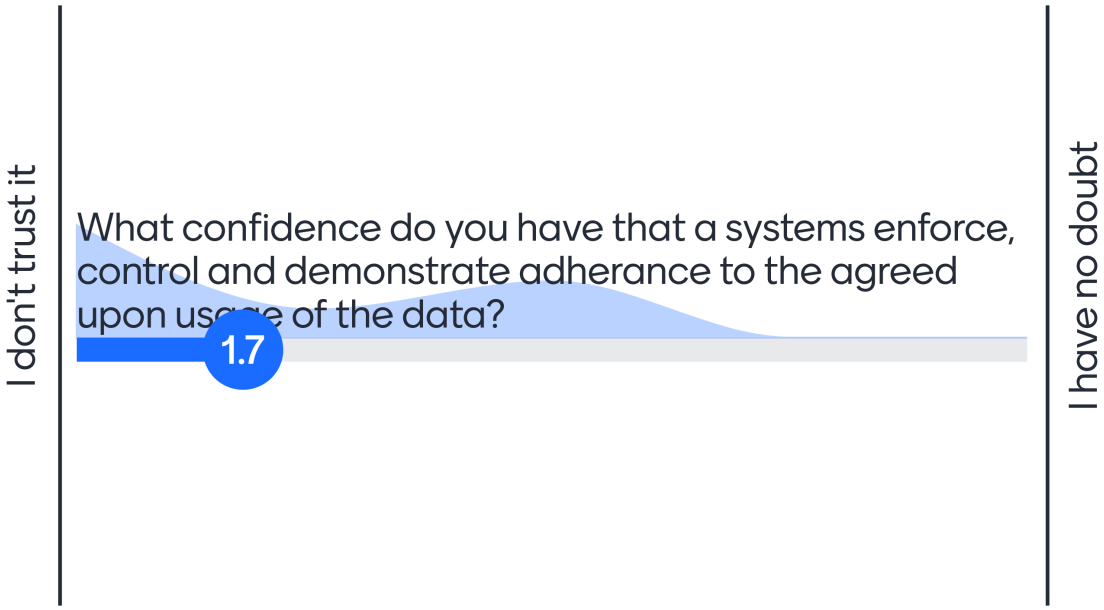


1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter



7

Data Usage Agreement

The cashier always asks for my phone number. I just wink and tell him, "Only if you'll call me."

Contracts and Agreements

User Requirements
Acceptance Criteria

Security Standards
and Audits

OpenAPI

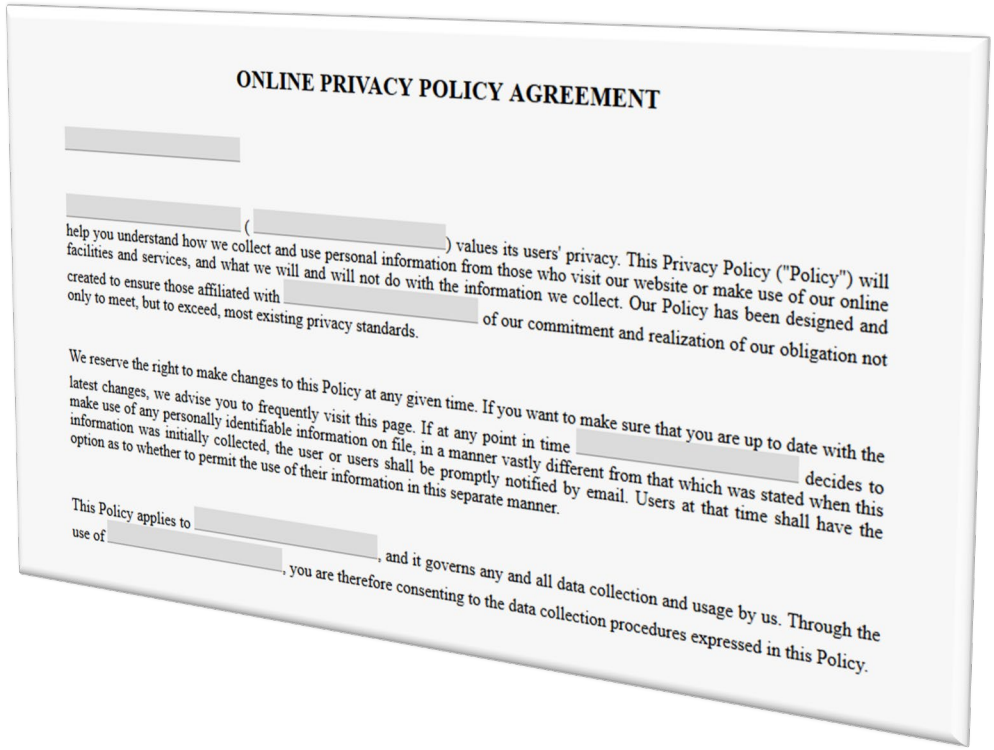
Contract Driven
Development

Testing

Contracts and Agreements

Data Usage ?

Contracts and Agreements



ONLINE PRIVACY POLICY AGREEMENT

[redacted] ([redacted]) values its users' privacy. This Privacy Policy ("Policy") will help you understand how we collect and use personal information from those who visit our website or make use of our online facilities and services, and what we will and will not do with the information we collect. Our Policy has been designed and created to ensure those affiliated with [redacted] of our commitment and realization of our obligation not only to meet, but to exceed, most existing privacy standards.

We reserve the right to make changes to this Policy at any given time. If you want to make sure that you are up to date with the latest changes, we advise you to frequently visit this page. If at any point in time [redacted] decides to make use of any personally identifiable information on file, in a manner vastly different from that which was stated when this information was initially collected, the user or users shall be promptly notified by email. Users at that time shall have the option as to whether to permit the use of their information in this separate manner.

This Policy applies to [redacted], and it governs any and all data collection and usage by us. Through the use of [redacted], you are therefore consenting to the data collection procedures expressed in this Policy.

How do you enforce this?

How do you control this?

How do you demonstrate this?

Data Usage Agreement

Inform : Inform data subjects about the processing of their personal data in a timely and adequate manner.

Control : Provide data subjects adequate control over the processing of their personal data.

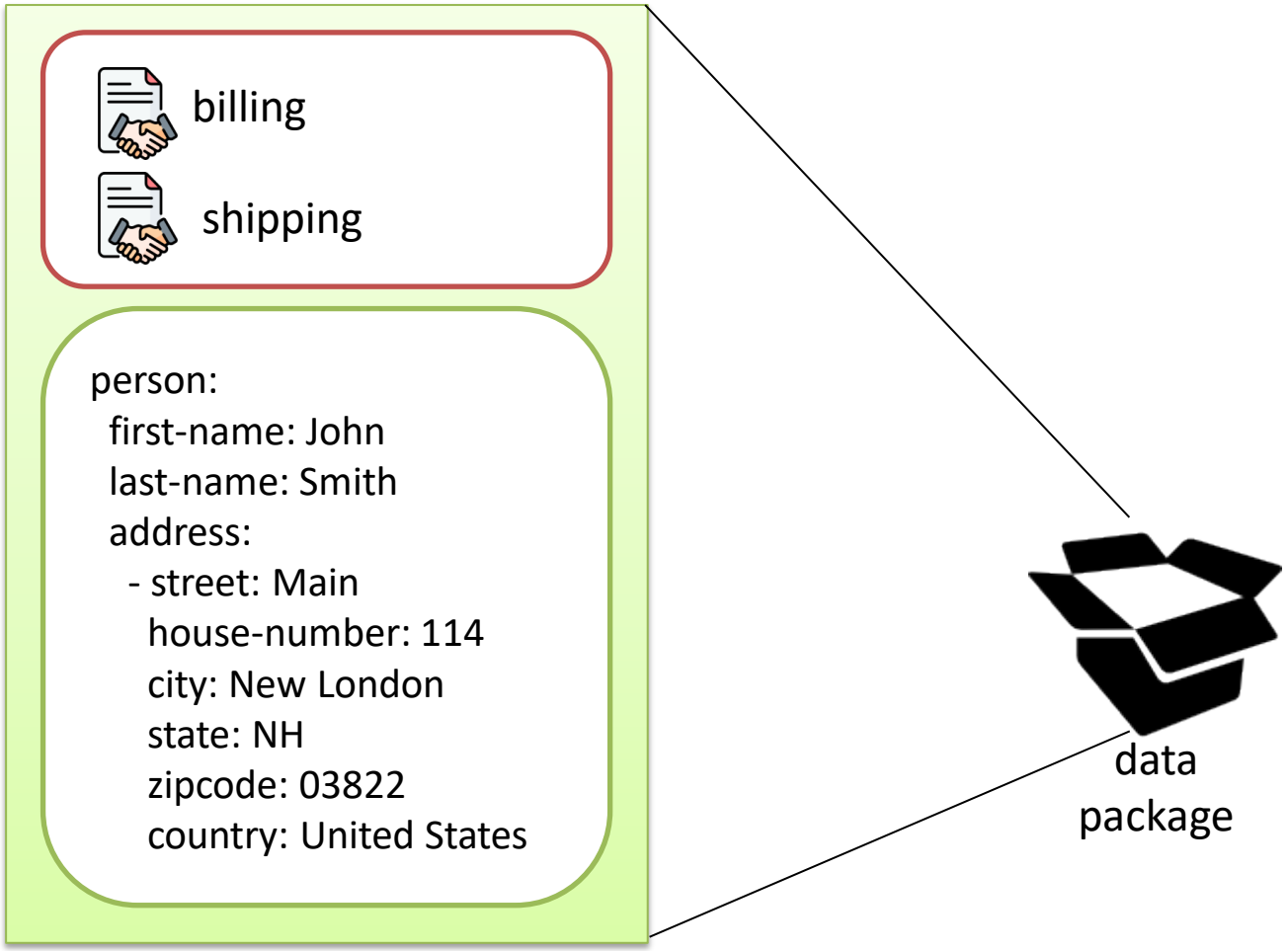
Enforce : Commit to processing personal data in a privacy-friendly way, and adequately enforce this.

Demonstrate : Demonstrate you are processing personal data in a privacy-friendly way.

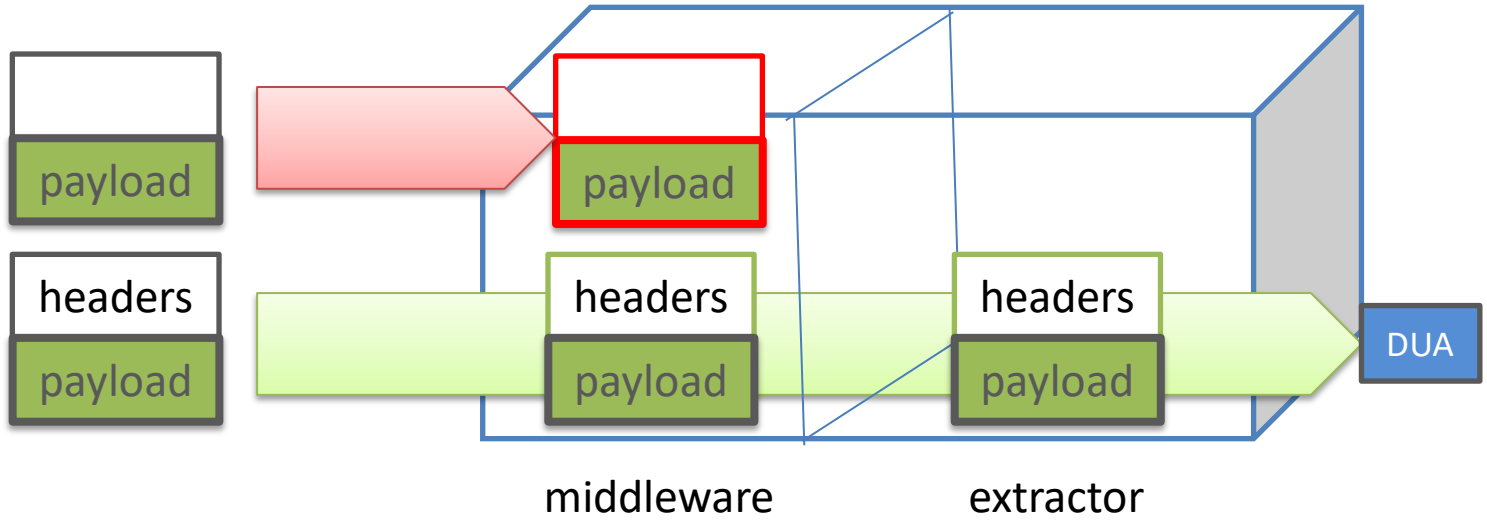
Data Usage Agreement

Attribute	Description	Example
name	A descriptive label that quickly allows the reader to understand the scope of the agreement	billing
location	A URl that identifies where the signed agreement document is stored	www.dua.org/billing-000232143432.pdf
agreed date time	The timestamp when the agreement was signed by the data owner	1553988607

Data Usage Agreement



Implementing DUA



1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

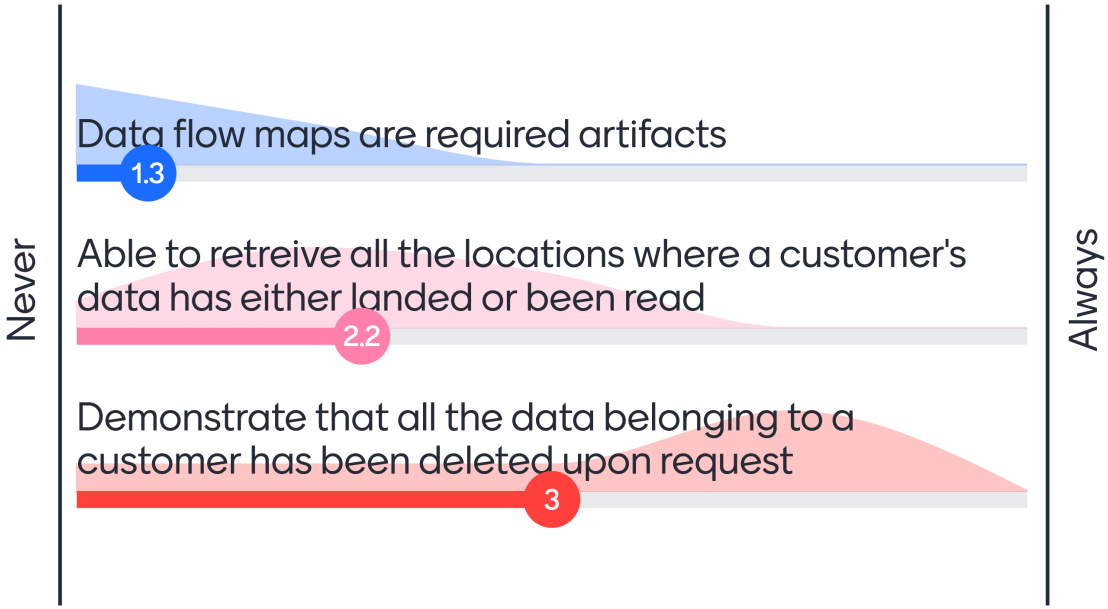
Name all of the touch points in your system when processing data.

6

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

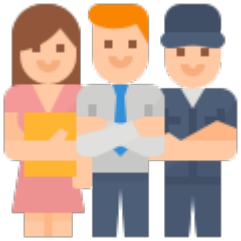


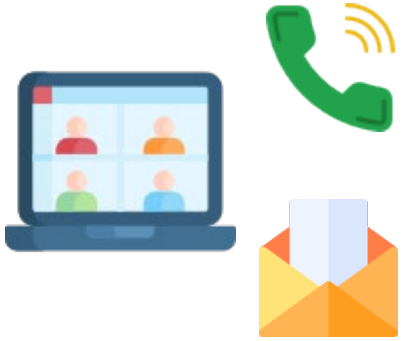
6

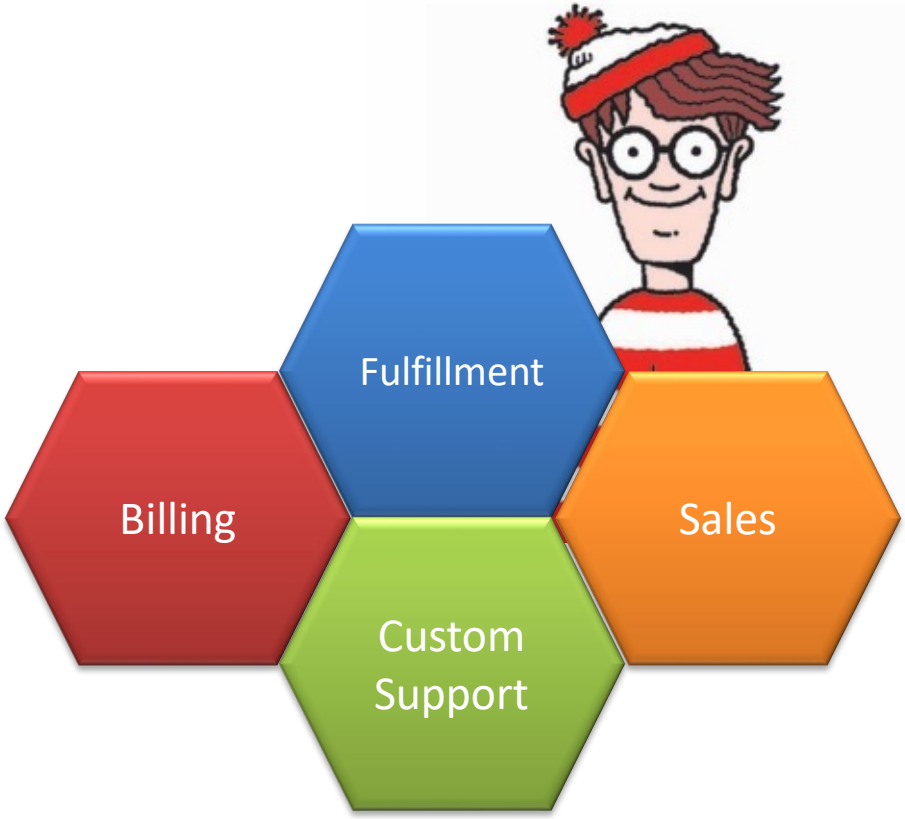
Data Tracker Chain

It only took 2 minutes for them to process my order and billing information, but they said I have to wait 2 weeks if I want all my personal information deleted.

Data Domains







Data Residue

- **Backups** – database recovery, manual copies, automated replications
- **Logs** – info or debug settings
- **Test Data** – nonproduction environment
- **Cache** – system memory and caching
- **Temporary** – landings and temp tables
- **Monitoring & Reporting** – reverse engineered identifyable data

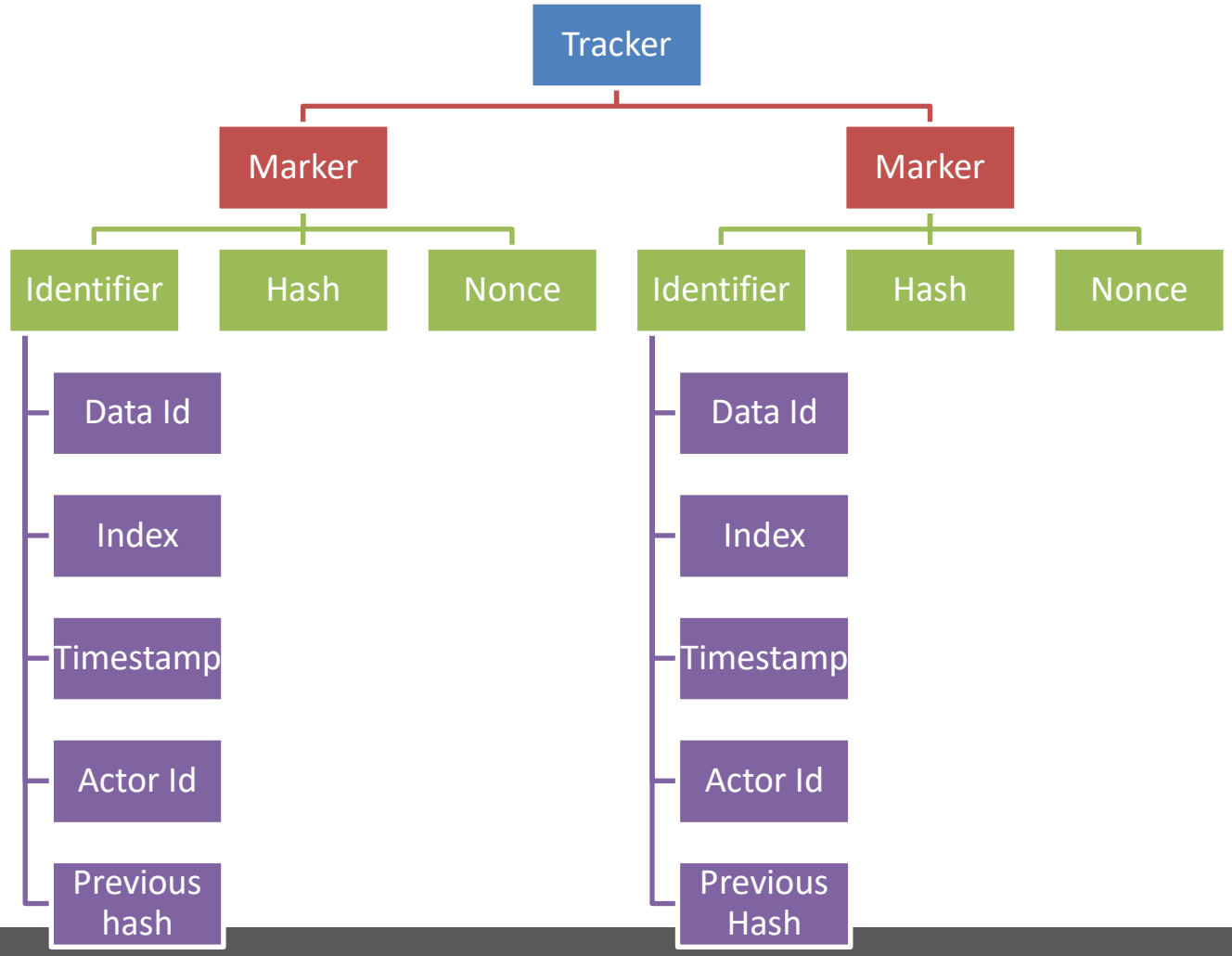
Data Tracker Chain

Inform : Inform data subjects about the processing of their personal data in a timely and adequate manner.

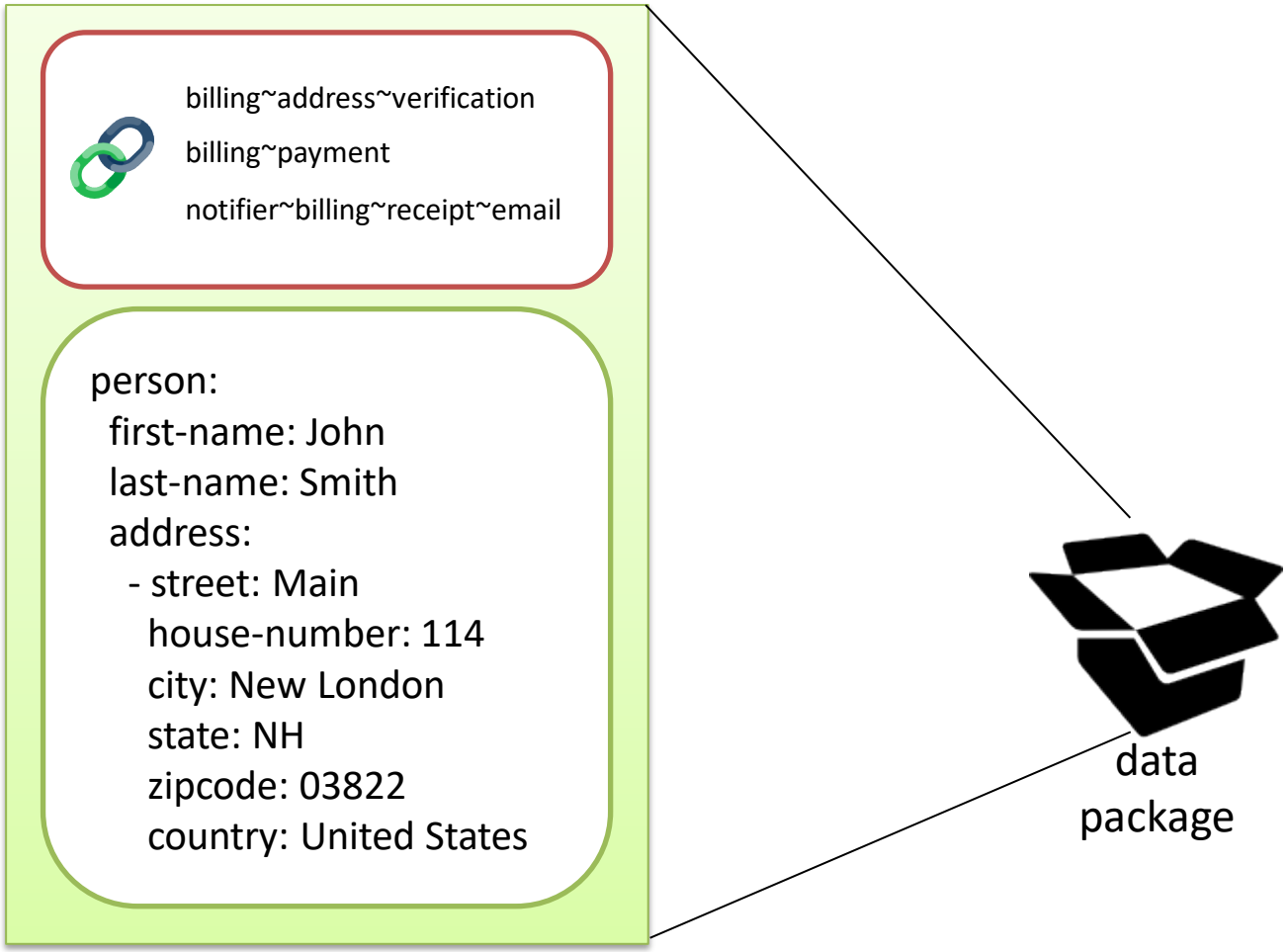
Control : Provide data subjects adequate control over the processing of their personal data.

Demonstrate : Demonstrate you are processing personal data in a privacy-friendly way.

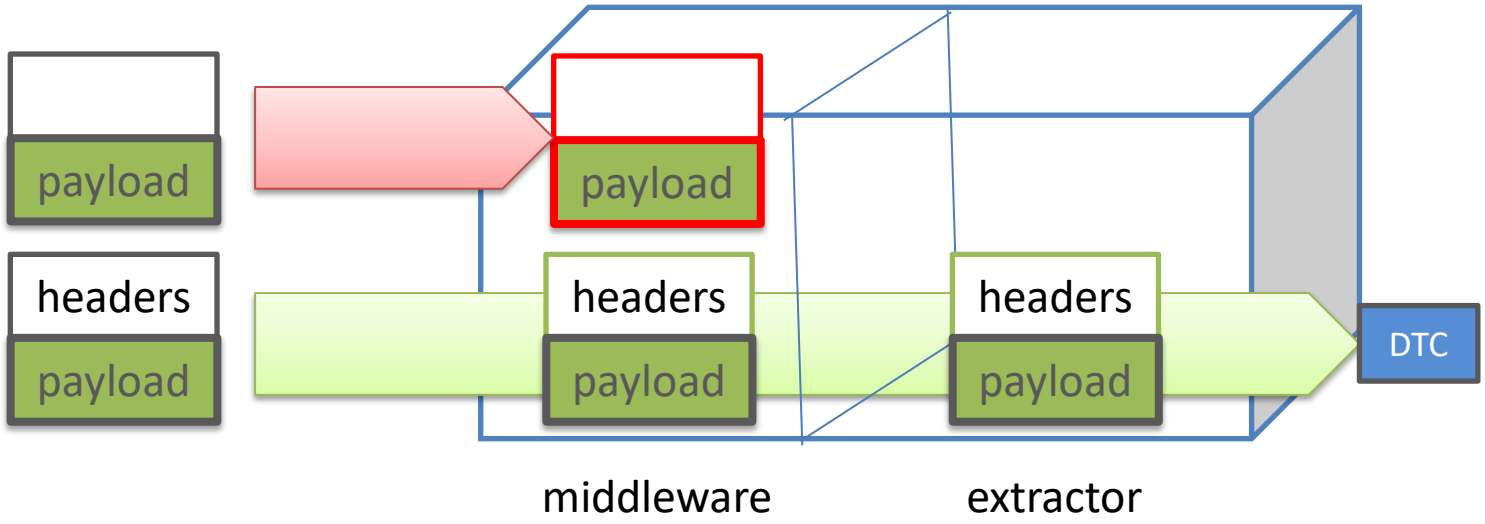
Data Tracker Chain



Data Tracker Chain



Implementing DTC



1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

Data Privacy Inspector

Inspector Regex at your service.

Traditional Approach

Batching

Scheduling

Rigid logic

Unidirectional

Current Approach

Individual

Real time

Learn & adapt

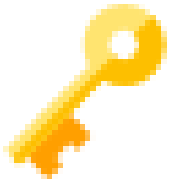
Bidirectional

Data Privacy Inspector

Control : Provide data subjects adequate control over the processing of their personal data.

Enforce: Commit to processing personal data in a privacy-friendly way, and adequately enforce this.

Identifying Building Blocks



Keywords

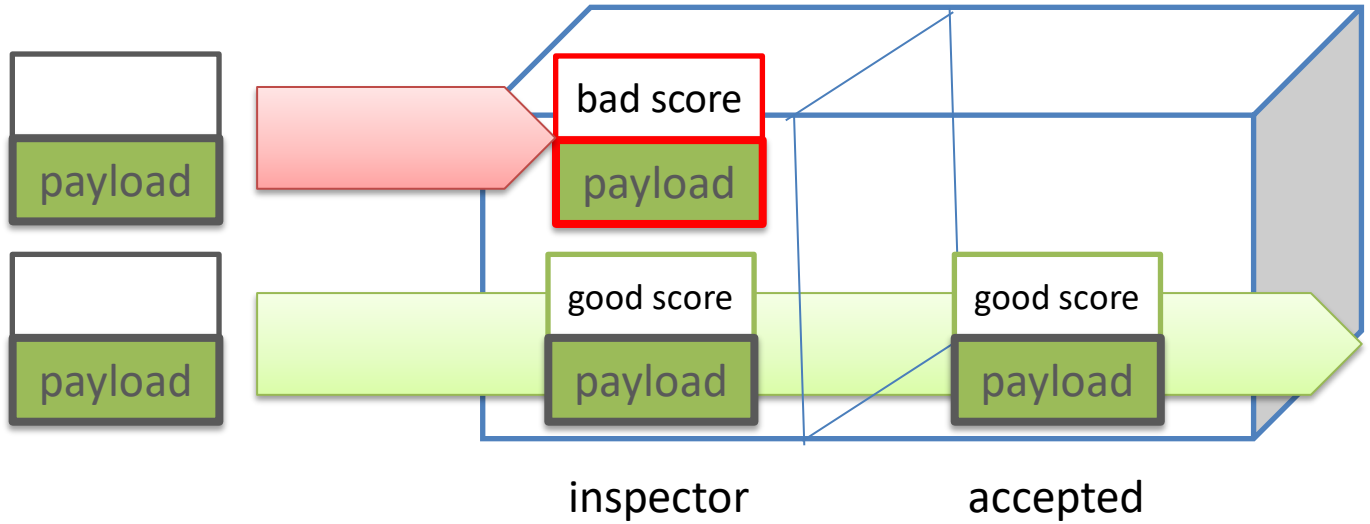
Regex

Patterns

Implementing DPI

<table>
<tr><th>Initiate</th><th>Train</th><th colspan="2">Adjust</th><th>Inspect</th></tr>
<tr><td>Default</td><td rowspan="2">autotrain</td><td rowspan="3">suggestions</td><td rowspan="2">Include</td><td rowspan="3">Score</td></tr>
<tr><td>Categories</td><td rowspan="2">train</td></tr>
<tr><td>Custom</td><td>Ignore</td></tr>
</table>

Implementing DPI



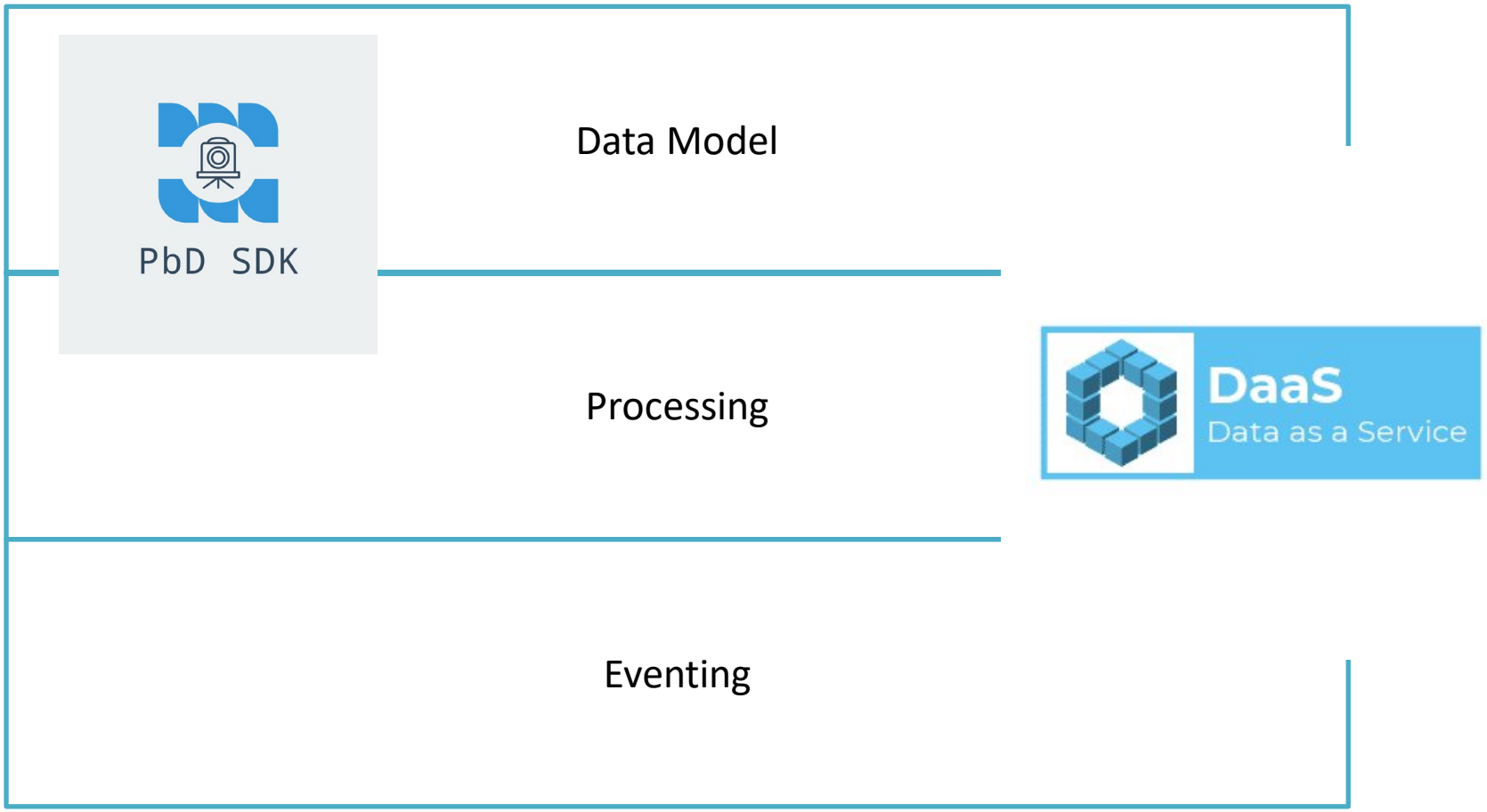
1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

Privacy Design Strategies

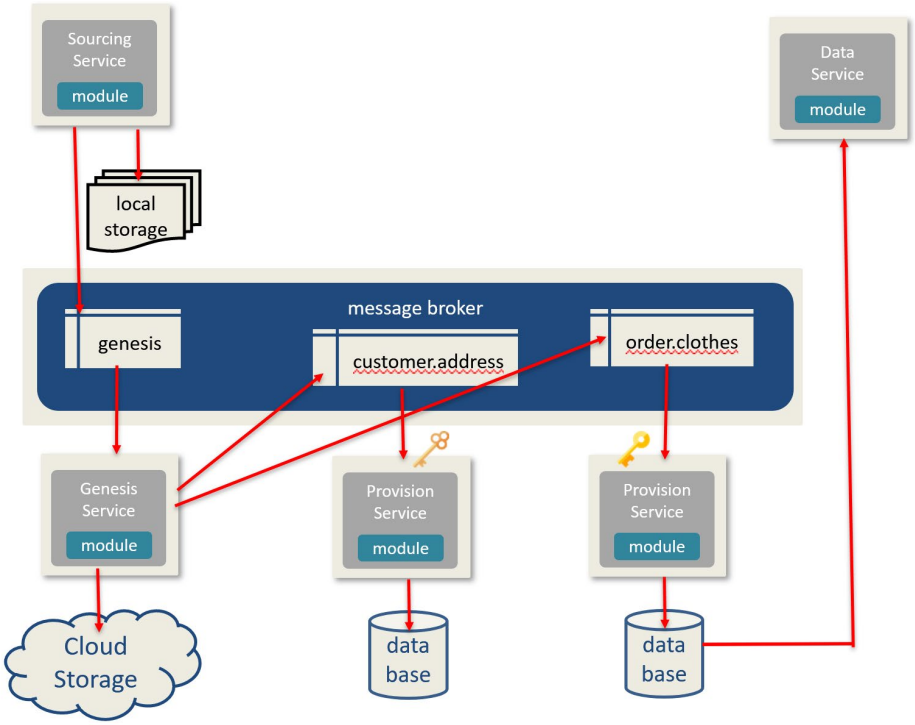
Strategy	Description
Minimize	Limit as much as possible the processing of personal data.
Separate	Separate the processing of personal data as much as possible.
Abstract	Limit as much as possible the detail in which personal data is processed.
Hide	Protect personal data, or make it unlinkable or unobservable. Make sure it does not become public or known.
Inform	Inform data subjects about the processing of their personal data in a timely and adequate manner.
Control	Provide data subjects adequate control over the processing of their personal data.
Enforce	Commit to processing personal data in a privacy-friendly way, and adequately enforce this.
Demonstrate	Demonstrate you are processing personal data in a privacy-friendly way.

Privacy Design Strategies (The Little Blue Book)
Jaap-Henk Hoepman
Agusut 23, 2019

Implementing Strategies



DaaS Pattern



- Minimize
- Separate
- Control

DaaS Document


```
{
  "_id": "customer~address~iStore~5000",
  "_rev": null,
  "source_name": "iStore",
  "source_uid": 5000,
  "category": "customer",
  "subcategory": "address",
  "author": "istore_app",
  "process_ind": false,
  "last_updated": 1605904974,
  "data_usage_agreements": [⟺],
  "data_tracker": {⟺},
  "meta_data": {⟺},
  "tags": [⟺],
  "data_obj": [⟺]
}
```


- Abstract
- Separate
- Minimize

1. overview
2. data usage agreements
3. data tracker chain
4. data privacy inspector
5. forward thinking

Appendix

picture by - 1314:Freepik.com
icons by www.flaticon.com
Image by pixabay.com

2

data usage agreements

Implementing DUA

VALIDATION_DEFAULT	Default validation level is VALIDATION_LOW
VALIDATION_HIGH	Check to see if the Data-Usage-Agreement header is set, has a valid format, and that the location of the agreements are valid.
VALIDATION_LOW	Check to see if the Data-Usage-Agreement header is set and has a valid format, but doesn't check to see if the location of the agreements are valid.
VALIDATION_NONE	Turns off validation so that only the Data-Usage-Agreement header doesn't need to be set

Demo DUA


```
GET / HTTP/1.1
Host: localhost:8088
Content-Type: application/json
Data-Usage-Agreement:
[{"agreement_name":"billing","location":"https://github.com/dsietz/pbd/blob/master/tests/duas/Patient%20Data%20Use%20Agreement.pdf","agreed_dtm": 1553988607}]
```

```
    Finished dev [unoptimized + debuginfo] target(s) in 0.51s
     Running `target\debug\examples\data-usage-agreement.exe`
Starting service on localhost:8088 ...
DUA { agreement_name: "billing", location: "https://github.com/dsietz/pbd/blob/master/tests/duas/Patient%20Data%20Use%20Agreement.pdf", agreed_dtm: 1553988607 }
```

3

data tracker chain

Implementing DTC

VALIDATION_DEFAULT	Default validation level is VALIDATION_LOW
VALIDATION_HIGH	Check to see if the Data-Tracker-Chain header is set and that the chain is valid.
VALIDATION_LOW	Check to see if the Data-Tracker-Chain header is set, but doesn't check if the chain is valid.
VALIDATION_NONE	Turns off validation so that only the the Data-Tracker-Chain header doesn't need to be set

Demo DTC


```
GET / HTTP/1.1
Host: localhost:8088
Content-Type: application/json
Data-Tracker-Chain:
W3siaWRlbnRpZmllciI6eyJkYXRhX2lkIjoib3JkZXJ+Y2xvdGhpbmd+aVN0b3JlfjE1MTUwIiwiaW5kZXgiOjAsIn
RpbWVzdGFtcCI6MCwiYWN0b3JfaWQiOiIiLCJwcmV2aW91c19oYXNoIjoiMCJ9LCJoYXNoIjoiMjcyMDgxNjk2NjEx
NDY0NzczNzI4MDI0OTI2NzkzNzAzMTY3NzgyIiwibm9uY2UiOjV9LHsiaWRlbnRpZmllciI6eyJkYXRhX2lkIjoib3
JkZXJ+Y2xvdGhpbmd+aVN0b3JlfjE1MTUwIiwiaW5kZXgiOjEsInRpbWVzdGFtcCI6MTU3ODA3MTIzOSwiYWN0b3Jf
aWQiOiJub3RpZmllcn5iaWxsaW5nfnJlY2VpcHR+ZW1haWwiLCJwcmV2aW91c19oYXNoIjoiMjcyMDgxNjk2NjExND
Y0NzczNzI4MDI0OTI2NzkzNzAzMTY3NzgyIn0sImhhc2giOiI1MDEwNDE0OTcwMTA5ODcwMDYzMjUxMTE0NDEyNTg2
NzczNjE5MyIsIm5vbmNlIjo1fV0=
```

```
    Finished dev [unoptimized + debuginfo] target(s) in 8.94s
     Running `target\debug\examples\data-tracker-chain.exe`
Starting service on localhost:8088 ...
[{"identifier":{"data_id":"order~clothing~iStore~15150","index":0,"timestamp":0,"actor_id":"","previous_hash":"0"},"hash":"272081696611464773728024926793703167782","nonce":5},{"identifier":{"data_id":"order~clothing~iStore~15150","index":1,"timestamp":1578071239,"actor_id":"notifier~billing~receipt~email","previous_hash":"272081696611464773728024926793703167782"},"hash":"501041497010987006325111441258677361 93","nonce":5}]
```

4

data privacy inspector

Demo DPI

Dear Aunt Bertha,

I can't believe it has already been 10 years since we moved to back to the Colorado.

I love Boulder and haven't thought of leaving since. So please don't worry when I tell you that we are moving in less than a week.
We will be upgrading to a larger home on the other side of the city on Peak Crest Lane.
It have a great view of the mountains and we will have a two car garage.

We will have the same phone number, so you can still reach us. But our new address with be 1345 Peak Crest Lane Boulder, Colorado 125468.

Let us know if you ever want to vist us.

Sincerely,
Robert

```
    Running `target\debug\examples\data-privacy-inspector.exe`
Starting service on localhost:8088 ...
DPI Score: 15
```

6

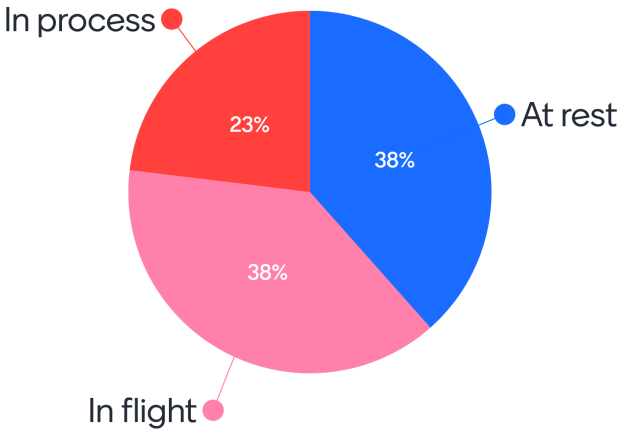
data security gaurd

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

When is data encryption important?



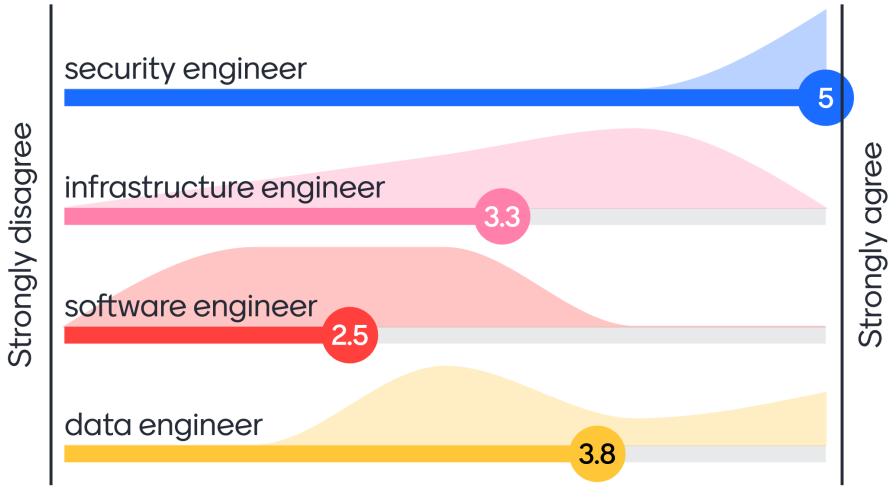
5

Audience Participation

Go to **www.menti.com** and use the code **4090 1266**

Mentimeter

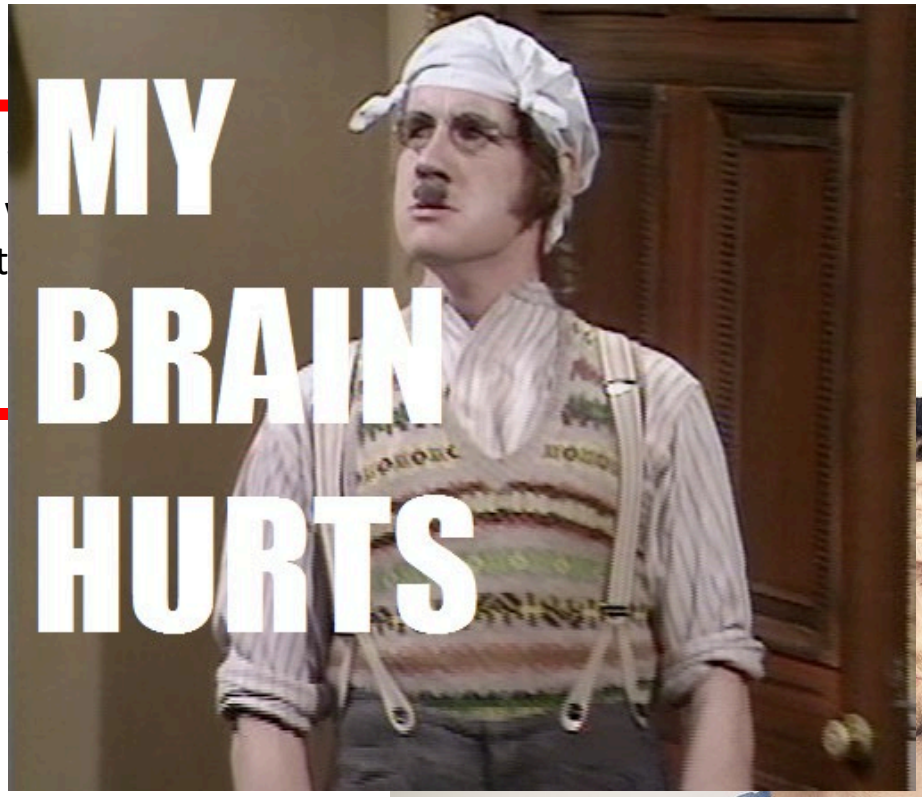
How expereinced are the following technical roles in implement security practices, (e.g.: encryption)



6

Data Security Guard

So I should send
what encryption
the padding is set



Data Security Guard

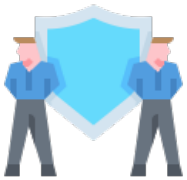
Hide : Protect personal data, or make it unlinkable or unobservable. Make sure it does not become public or known.

Control : Provide data subjects adequate control over the processing of their personal data.

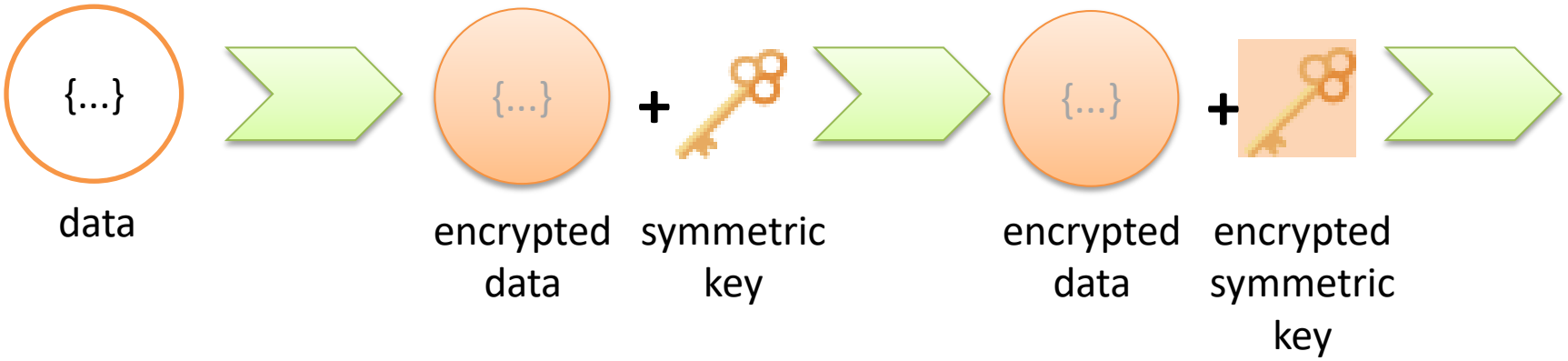
Enforce: Commit to processing personal data in a privacy-friendly way, and adequately enforce this.

Separate: Separate the processing of personal data as much as possible.

Data Security Guard

PrivacyGuard	TransferSet
	
Functionality	Attributes
key generation	encrypted symmetric key
encrypt / decrypt	nonce
secure for transfer	padding
	encrypted data

Data Security Guard



data

encrypted data

symmetric key

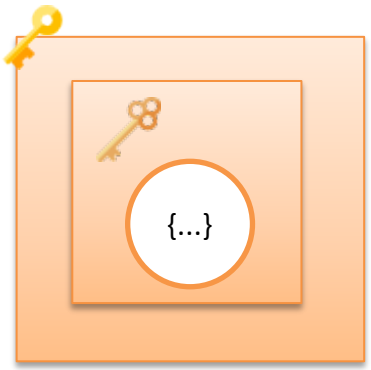
encrypted data

encrypted symmetric key

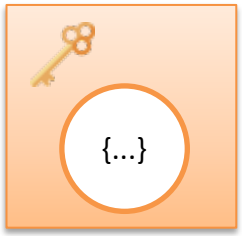
individually generated key

public key

Data Security Guard



Delegator
Entrypoint for data feed. Uses private key to decrypt symmetric key in TransferSet



Data Processor
Processes the data. Uses symmetric key to decrypt data

Data Security Guard

asymmetric key

enforces that data is **hidden** and **controls** who can see it

generated symmetric key

Supports **separation** of common data records to deter mass processing of data records.

Demo DSG

GET / HTTP/1.1
Host: localhost:8088
Content-Type: application/json
Content-Length: 1097

{"encrypted_data":[130,37,248,85,153,227,79,249,207,97,173,90,24,95,190,46],"encrypted_symmetric_key":[50,133,49,31,191,107,92,185,73,215,226,59,30,241,210,149,177,158,166,200,98,86,22,245,251,224,49,239,177,245,236,43,255,190,251,162,47,218,206,2,72,253,181,24,143,32,41,233,13,35,195,225,155,110,95,59,223,209,126,134,218,58,45,97,40,184,148,184,188,141,143,235,131,154,76,1,246,8,19,107,226,71,148,231,196,209,197,85,151,36,203,107,125,168,145,93,57,217,188,71,211,239,3,25,230,27,165,65,191,250,178,21,248,49,70,199,34,91,62,22,5,50,50,180,134,31,137,30,155,215,253,109,46,220,209,218,50,98,194,151,63,8,4,164,100,225,94,122,81,93,130,170,255,168,186,76,251,163,179,250,169,167,52,158,223,187,170,101,66,108,22,153,195,140,203,149,243,129,137,161,246,115,156,87,140,96,163,209,169,244,175,34,150,216,43,234,24,7,220,197,87,65,196,43,230,223,61,7,47,171,193,239,121,46,208,245,161,188,113,49,216,205,147,122,233,136,24,58,157,99,54,188,100,14,19,55,11,218,199,148,3,2,74,148,5,174,155,118,136,64,210,182,101,50,168,74],"nonce":[100,109,70,86,87,48,111,104,67,71,78,54,66,74,114,48],"padding":1}

```
    Finished dev [unoptimized + debuginfo] target(s) in 7.77s
     Running `target\debug\examples\data-security-guard.exe`
Starting service on localhost:8088 ...
Message Received: _test123!#
```

5

forward thinking

DaaS Document

```
"data_usage_agreements": [
  {
    "agreement_name": "billing",
    "location": "https://dua.org/agreements/v1/billing.pdf",
    "agreed_dtm": 1553988607
  },
  {
    "agreement_name": "shipping",
    "location": "https://dua.org/agreements/v1/shipping.pdf",
    "agreed_dtm": 1553988607
  }
],
```

- Inform
- Control
- Demonstrate
- Enforce

DaaS Document


```
"data_tracker": {
  "chain": [
    {
      "identifier": {
        "data_id": "customer~address~iStore~5000",
        "index": 0,
        "timestamp": 0,
        "actor_id": "",
        "previous_hash": "0"
      },
      "hash": "32935007786589101041074141906394507444O",
      "nonce": 5
    },
    {
      "identifier": {
        "data_id": "customer~address~iStore~5000",
        "index": 1,
        "timestamp": 1578071239,
        "actor_id": "address-validator",
        "previous_hash": "32935007786589101041074141906394507444O"
      },
      "hash": "152046408419549889806141140555584827365",
      "nonce": 5
    },
    {
      "identifier": {
        "data_id": "customer~address~iStore~5000",
        "index": 2,
        "timestamp": 1578071245,
        "actor_id": "customer-profile-manager",
        "previous_hash": "152046408419549889806141140555584827365"
      },
      "hash": "68667386159702151632691701486238515851",
      "nonce": 5
    }
  ]
},
```

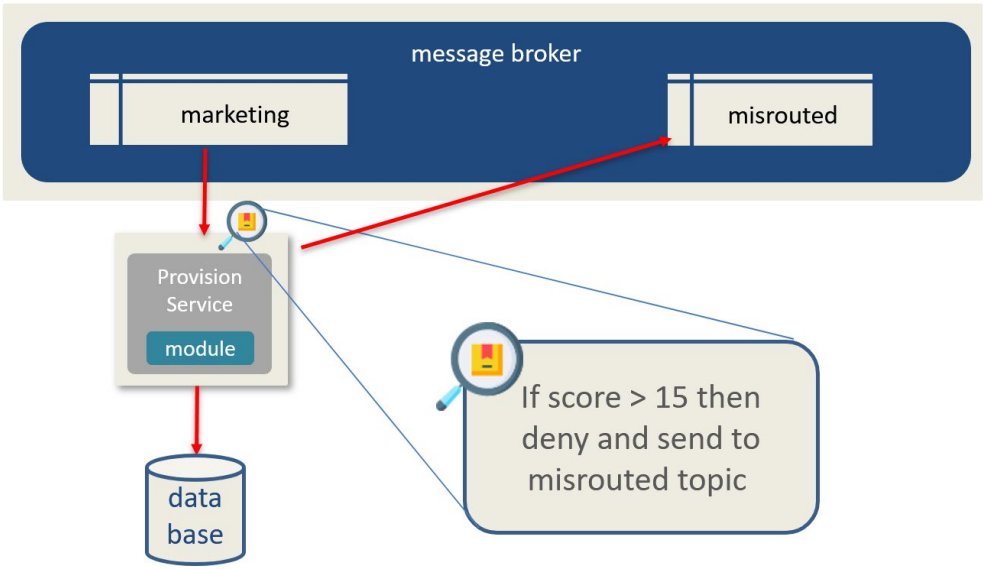

- Control
- Demonstrate
- Enforce
- Inform

DaaS Document

```
"meta_data": {
  "country": "Unitied States",
  "state": "NH"
},
"tags": [
  "billing",
  "shipping"
],
```

- Minimize
- Separate
- Abstract

DaaS Document



- Control
- Enforce

DaaS Document

```
"data_obj": [
  123,
  34,
  101,
  110,
  99,
  114,
  121,
  112,
  116,
  101,
  100,
  95,
  100,
  97,
  116.
```

TransferSet {

encrypted_data: [241, 29, 103, 1, 48, 118, 149, 12, 5, 66, 157, 183, 141, 108, 67, 129, 24, 233, 241, 14, 59, 252, 156, 196, 95, 239, 153, 237, 102, 164, 195, 5, 45, 9, 212, 47, 182, 130, 160, 50, 142, 83, 71, 225, 159, 188, 239, 2, 108, 132, 203, 54, 39, 124, 215, 133, 71, 3, 204, 36, 128, 110, 139, 25, 94, 87, 142, 171, 56, 80, 126, 177, 235, 109, 78, 225, 174, 11, 21, 128, 162, 158, 93, 99, 237, 212, 91, 217, 188, 151, 35, 30, 103, 251, 216, 105, 252, 59, 221, 86, 184, 98, 131, 210, 181, 81, 4, 137, 6, 208, 97, 238, 78, 99, 31, 237, 207, 241, 59, 71, 205, 148, 240, 239, 24, 124, 2, 146, 67, 45, 157, 163, 42, 164, 62, 160, 39, 9, 152, 16, 106, 172, 137, 68, 35, 32, 73, 61, 108, 91, 192, 136, 251, 186, 197, 42, 199, 227, 250, 164, 142, 37, 114, 73, 159, 143, 67, 134, 60, 165, 19, 98, 183, 176, 150, 99, 202, 117, 247, 65, 128, 42, 41, 131, 99, 28, 219, 61, 140, 124, 106, 235],

encrypted_symmetric_key: [8, 50, 17, 181, 144, 91, 66, 61, 206, 165, 79, 133, 248, 188, 229, 25, 49, 110, 54, 58, 219, 159, 152, 216, 167, 93, 225, 2, 118, 52, 127, 194, 230, 107, 253, 32, 134, 174, 172, 159, 11, 4, 44, 119, 36, 196, 44, 201, 185, 183, 193, 181, 101, 105, 204, 149, 101, 216, 185, 246, 155, 30, 115, 221, 63, 162, 109, 117, 105, 92, 51, 210, 188, 77, 173, 62, 114, 176, 57, 109, 91, 78, 232, 111, 177, 174, 15, 20, 131, 158, 64, 149, 159, 74, 115, 127, 248, 233, 241, 52, 232, 26, 63, 115, 167, 114, 234, 216, 4, 232, 69, 251, 234, 108, 149, 65, 96, 3, 106, 123, 15, 33, 34, 118, 21, 205, 147, 57, 207, 134, 110, 179, 245, 15, 98, 207, 230, 130, 128, 110, 147, 233, 108, 184, 193, 16, 108, 218, 160, 227, 241, 148, 82, 154, 63, 15, 178, 101, 150, 248, 142, 85, 126, 66, 171, 20, 120, 182, 45, 127, 150, 184, 23, 143, 80, 208, 114, 205, 110, 65, 2, 55, 187, 143, 232, 147, 64, 211, 51, 113, 167, 94, 236, 236, 118, 21, 15, 226, 215, 194, 239, 46, 31, 161, 38, 60, 39, 140, 235, 59, 156, 164, 253, 227, 145, 223, 41, 41, 212, 65, 72, 77, 235, 90, 142, 76, 21, 8, 36, 105, 27, 207, 45, 171, 54, 32, 41, 224, 70, 197, 7, 21, 23, 157, 209, 159, 150, 55, 218, 151, 241, 158, 231, 254, 157, 72],

nonce: [88, 119, 111, 113, 88, 83, 70, 74, 111, 83, 103, 52, 120, 107, 105, 53],

padding: 1

}

- Enforce
- Hide
- Control