

# Privacy by Design

*clusterfuck*

Your Data is a ~~Train Wreck~~ Without It



# Privacy by Design

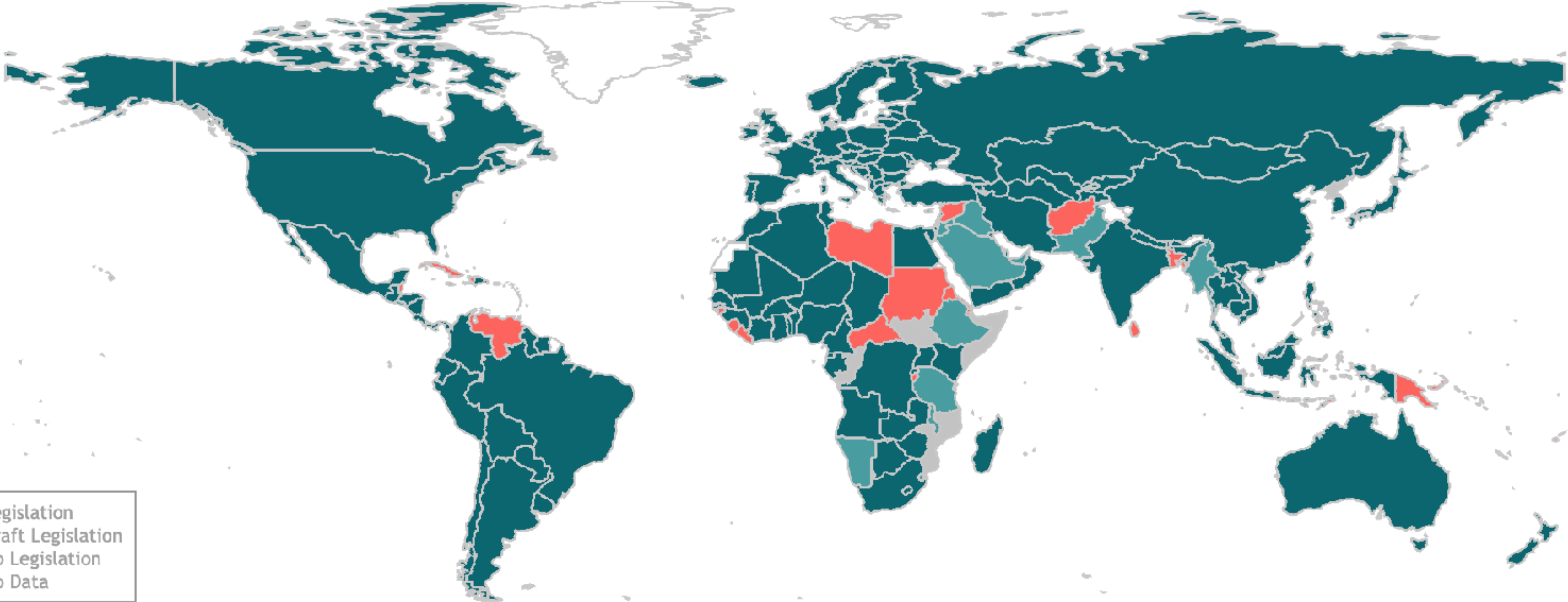
**“... privacy assurance must ideally become an organisation’s default mode of operation.”**

Dr. Ann Cavoukian



# Data protection through technology design

# Data Protection and Privacy Legislation Worldwide



- Legislation
- Draft Legislation
- No Legislation
- No Data

Source: UNCTAD, 14/12/2021

**Proactive, not Reactive.  
Preventative not Remedial.**

# Privacy as the Default Setting



# Privacy Embedded into Design

# Full Functionality. Positive-Sum, not Zero-Sum

**End-to-End Security.  
Full Lifecycle Protection.**

# Visibility and Transparency

**Respect for User Privacy.  
Keep it User-Centric.**

# What Privacy by Design is not

---

- Hiring a Chief Privacy Officer

# What Privacy by Design is not

---

- Hiring a Chief Privacy Officer
- Watching privacy training

# What Privacy by Design is not

---

- Hiring a Chief Privacy Officer
- Watching privacy training
- **Completing a checklist**



# What Privacy by Design is not

---

- Hiring a Chief Privacy Officer
- Watching privacy training
- Completing a checklist
- **Add a privacy notice to your site**

# What Privacy by Design is not

---

- Hiring a Chief Privacy Officer
- Watching privacy training
- Completing a checklist
- Add a privacy notice to your site
- **Getting a certificate**

Privacy by design aims to create a **privacy conscious** and **user-friendly** environment.

You are responsible to know on  
what **regulates the data** you work  
with

**Less framework.  
More guidelines.**

Let PbD **guide your strategy**, not be your strategy.

# Privacy Impact Assessments

Proactive, not Reactive

- Perform a DPIA or PIA

## Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

# Privacy Impact Assessments

---

Proactive, not Reactive

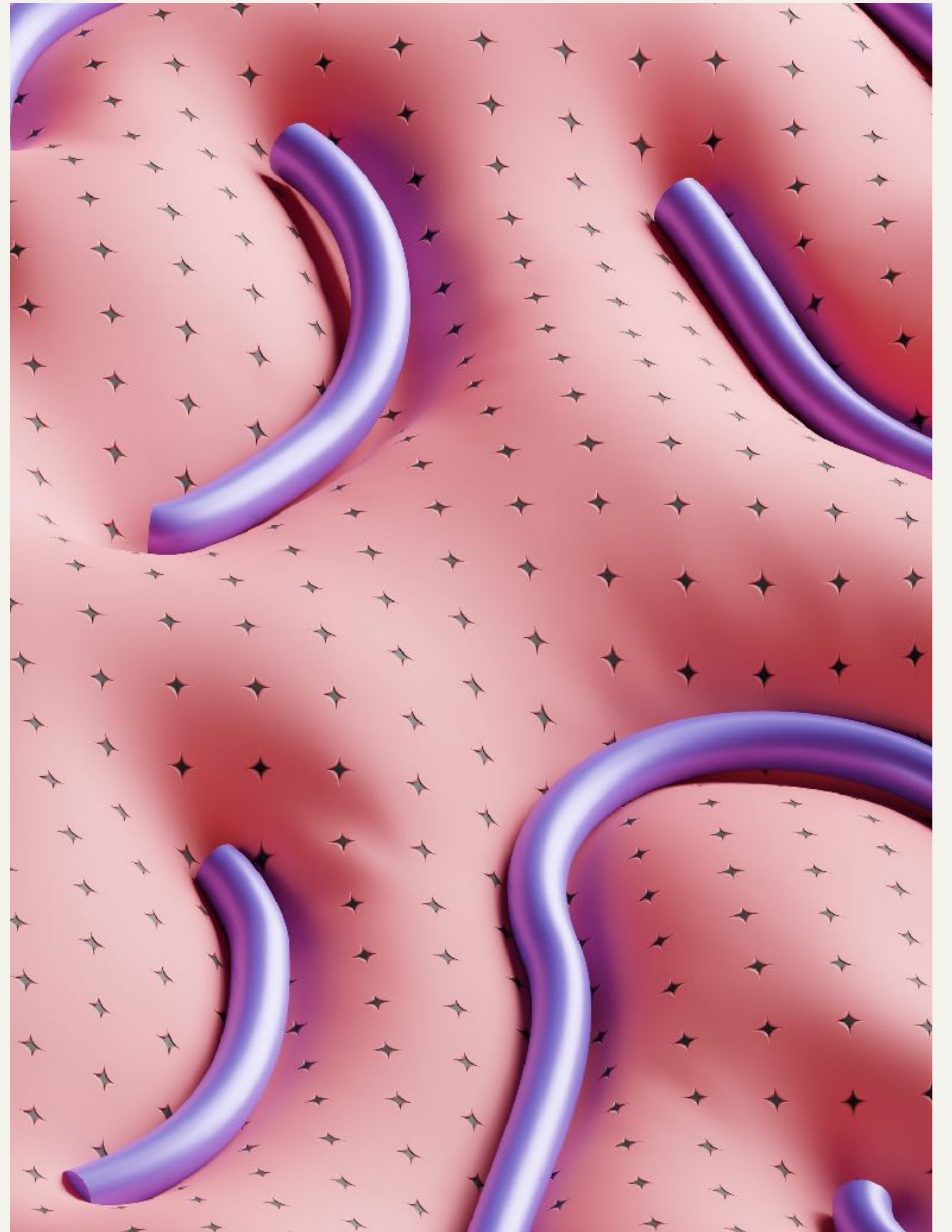
- Perform a DPIA or PIA
- **Mitigate risks before they arise**



# Incorporate Privacy

Privacy as a Default

- Data Minimisation





# Incorporate Privacy

Privacy as a Default

- Data Minimisation
- **Purpose**



# Incorporate Privacy

Privacy as a Default

- Data Minimisation
- Purpose
- Retention

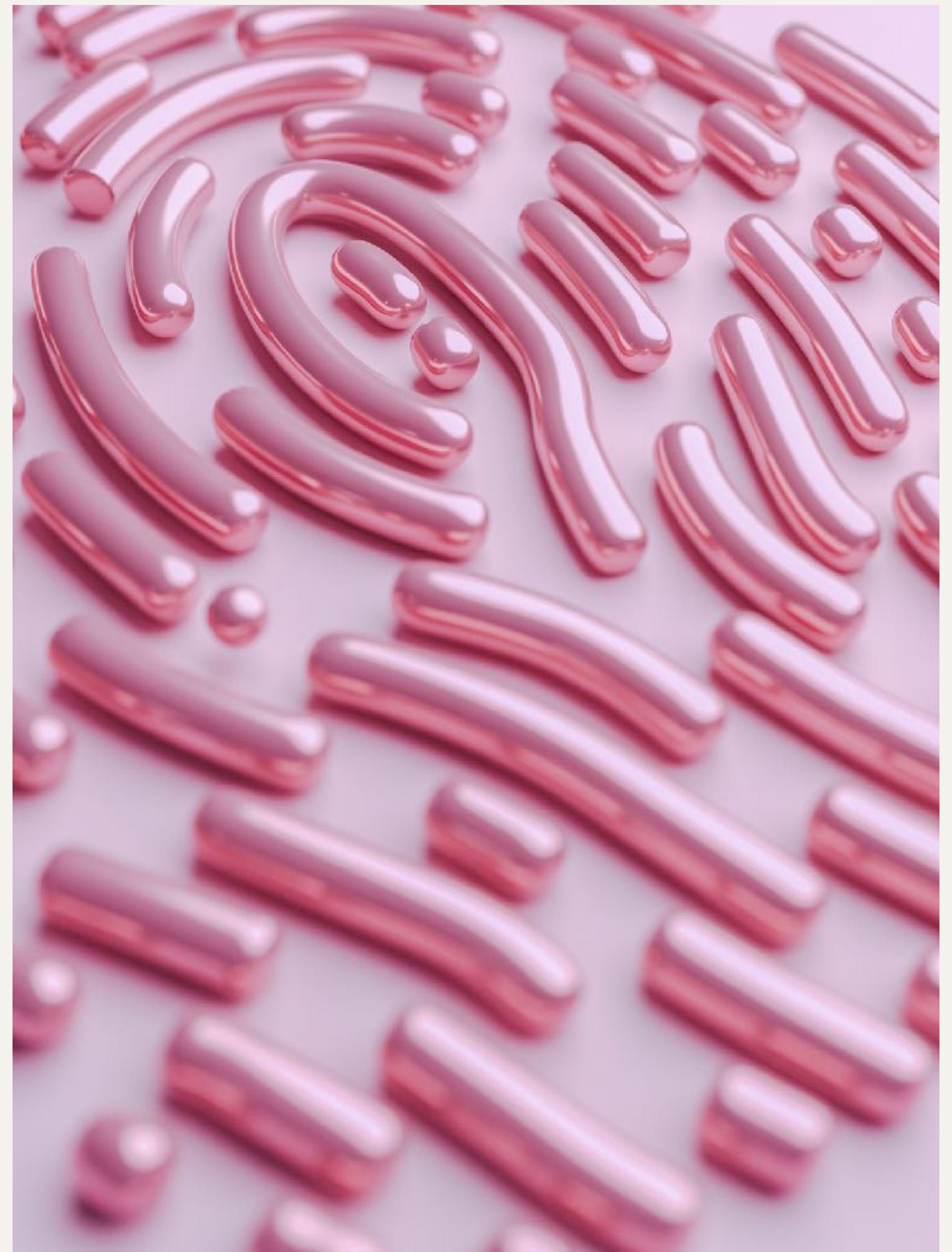


# Privacy Enhancing Technologies

---

Privacy embedded by Design

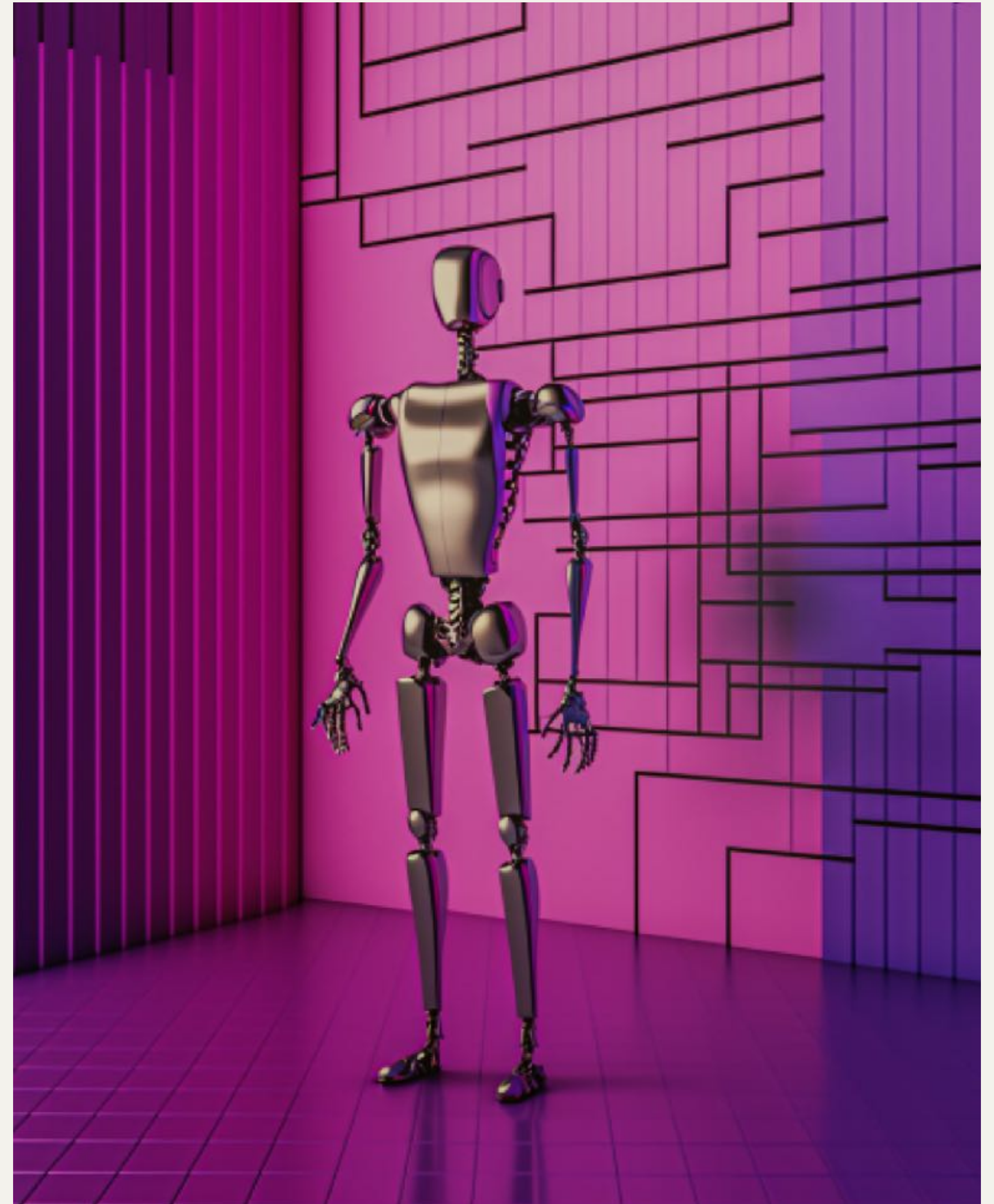
- **Differential Privacy**



# Privacy Enhancing Technologies

Privacy embedded by Design

- Differential Privacy
- Synthetic data



# Privacy Enhancing Technologies

Privacy embedded by Design

- Differential Privacy
- Synthetic data
- Pseudonymisation/  
Obfuscation/Data Masking

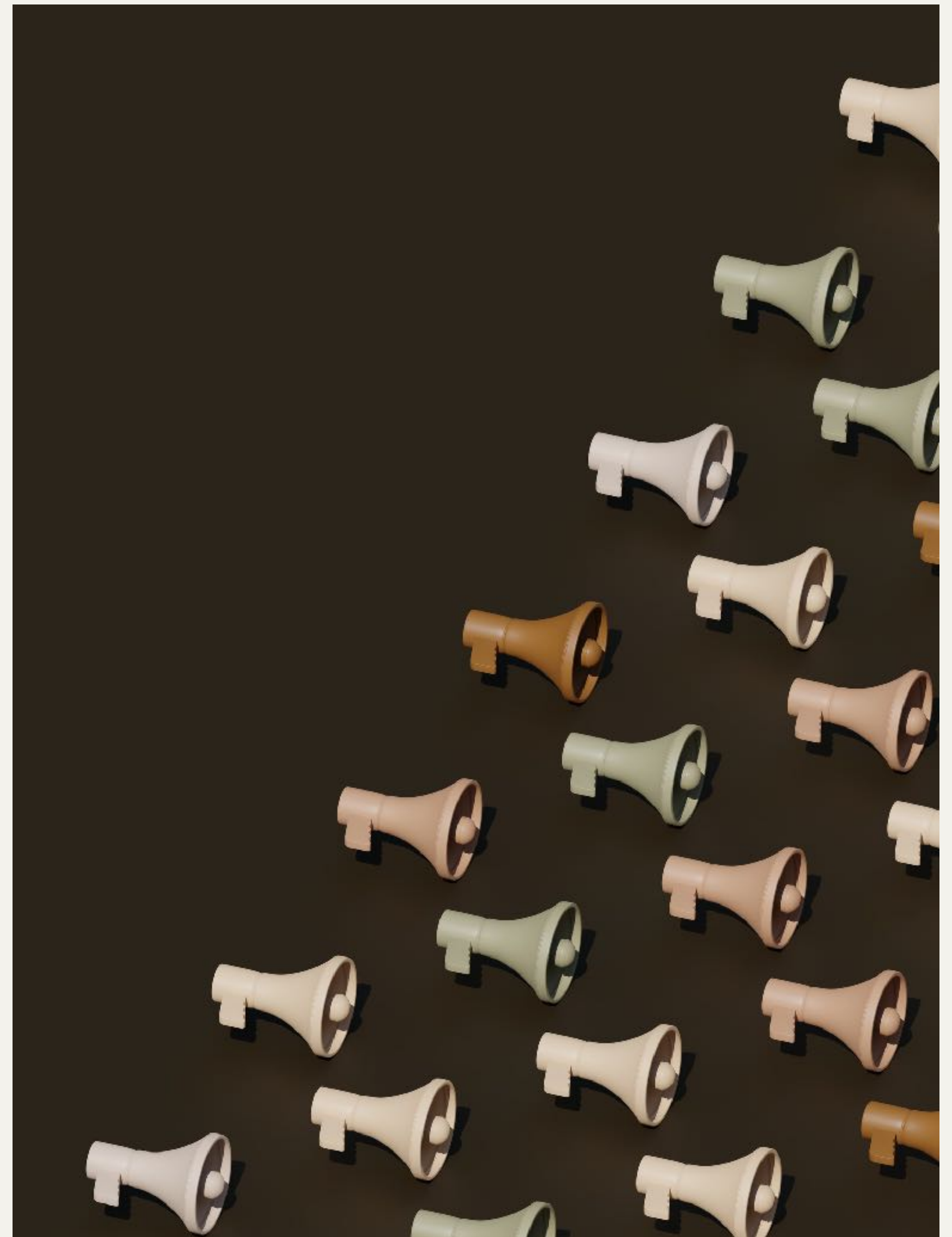


# Work towards business goals

---

Full functionality. Positive-sum, not zero-sum.

- Communicate across teams

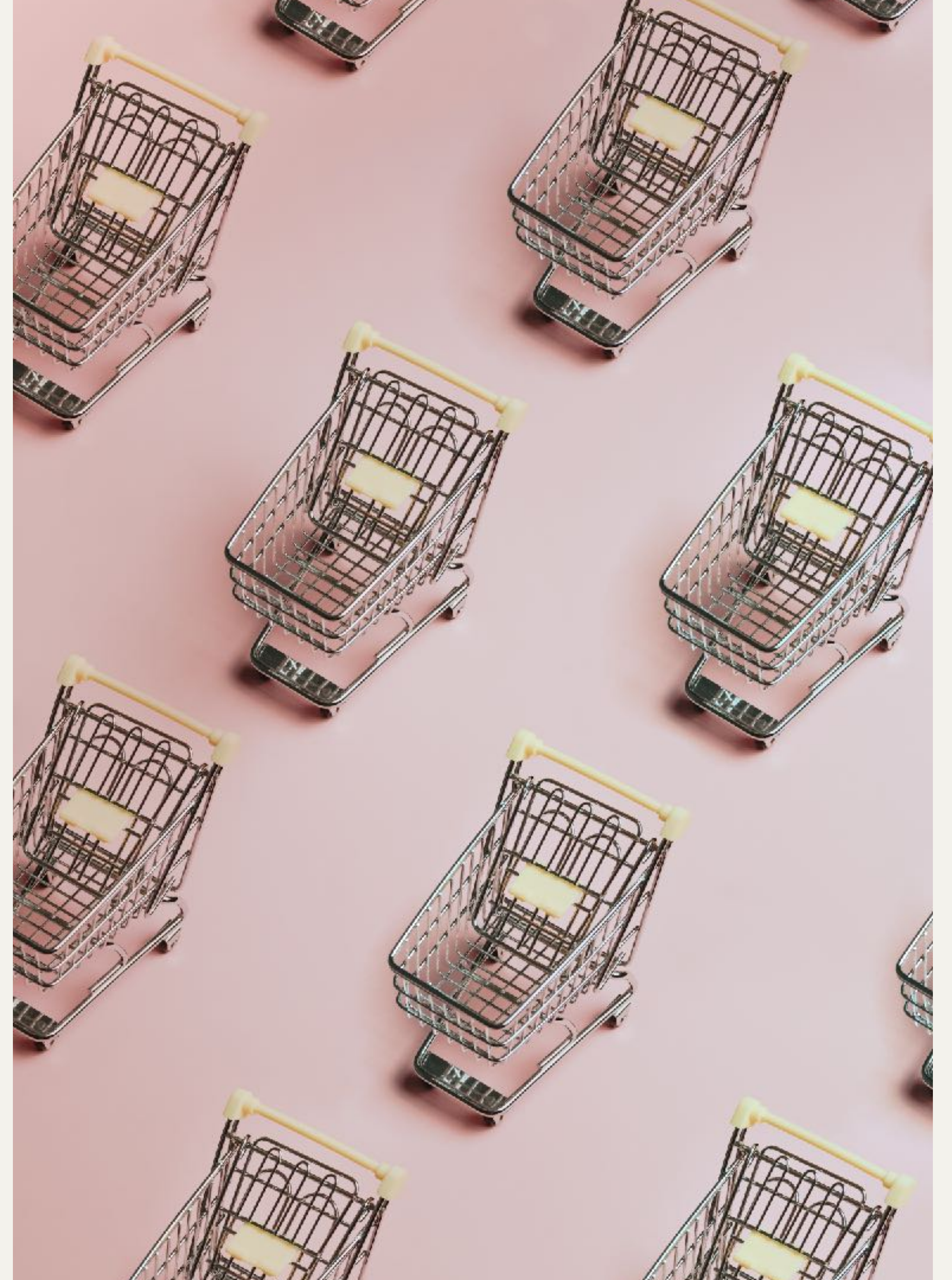


# Work towards business goals

---

Full functionality. Positive-sum, not zero-sum.

- Communicate across teams
- Understand requirements



# Keep it Secure

---

End to End Security

- Ensure that your data is secure for the whole life cycle



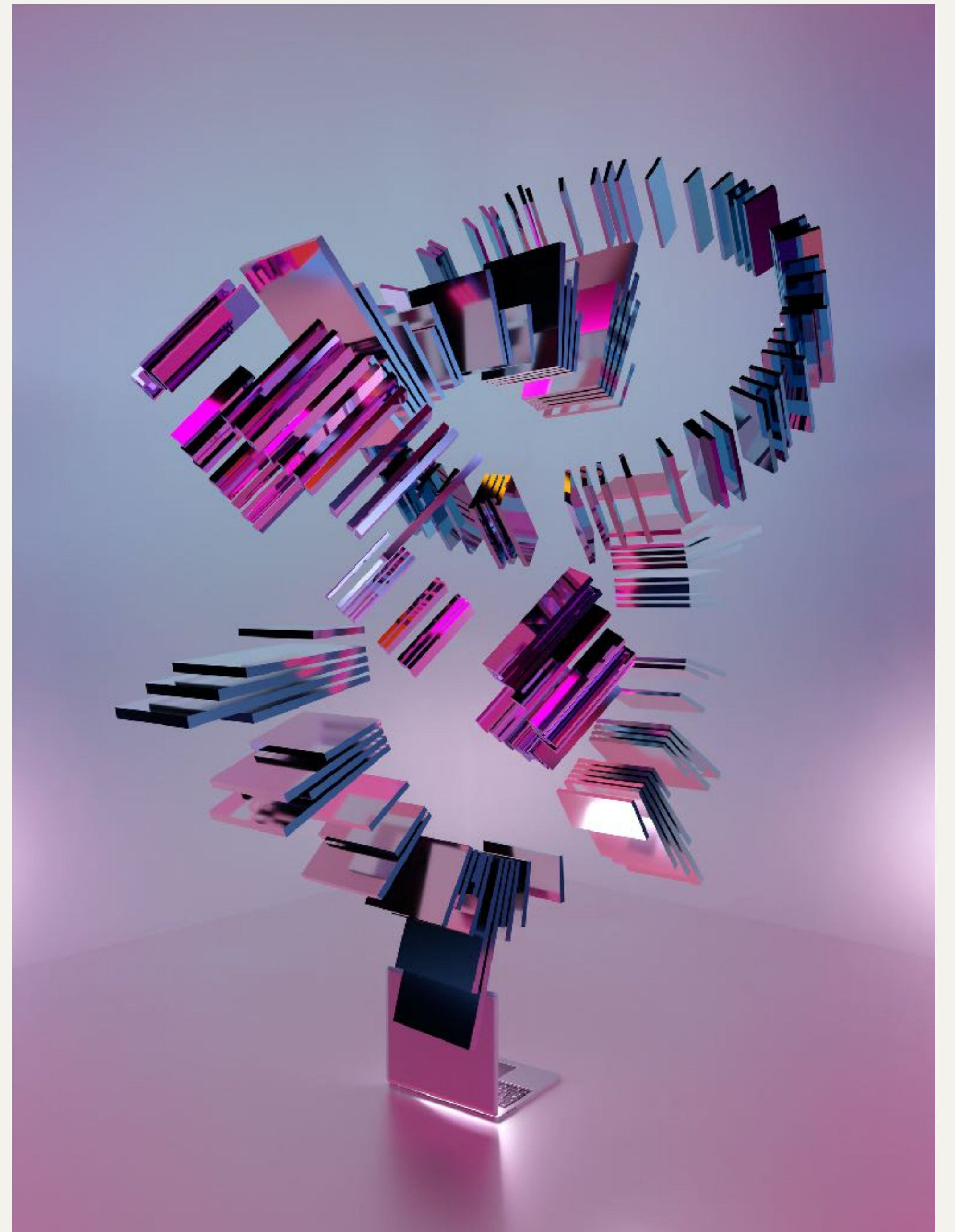


# Keep it Secure

---

End to End Security

- Ensure that your data is secure for the whole life cycle
- **Storage**



# Keep it Secure

---

End to End Security

- Ensure that your data is secure for the whole life cycle
- **Storage**
- **Deletion**



# Keep it Secure

---

End to End Security

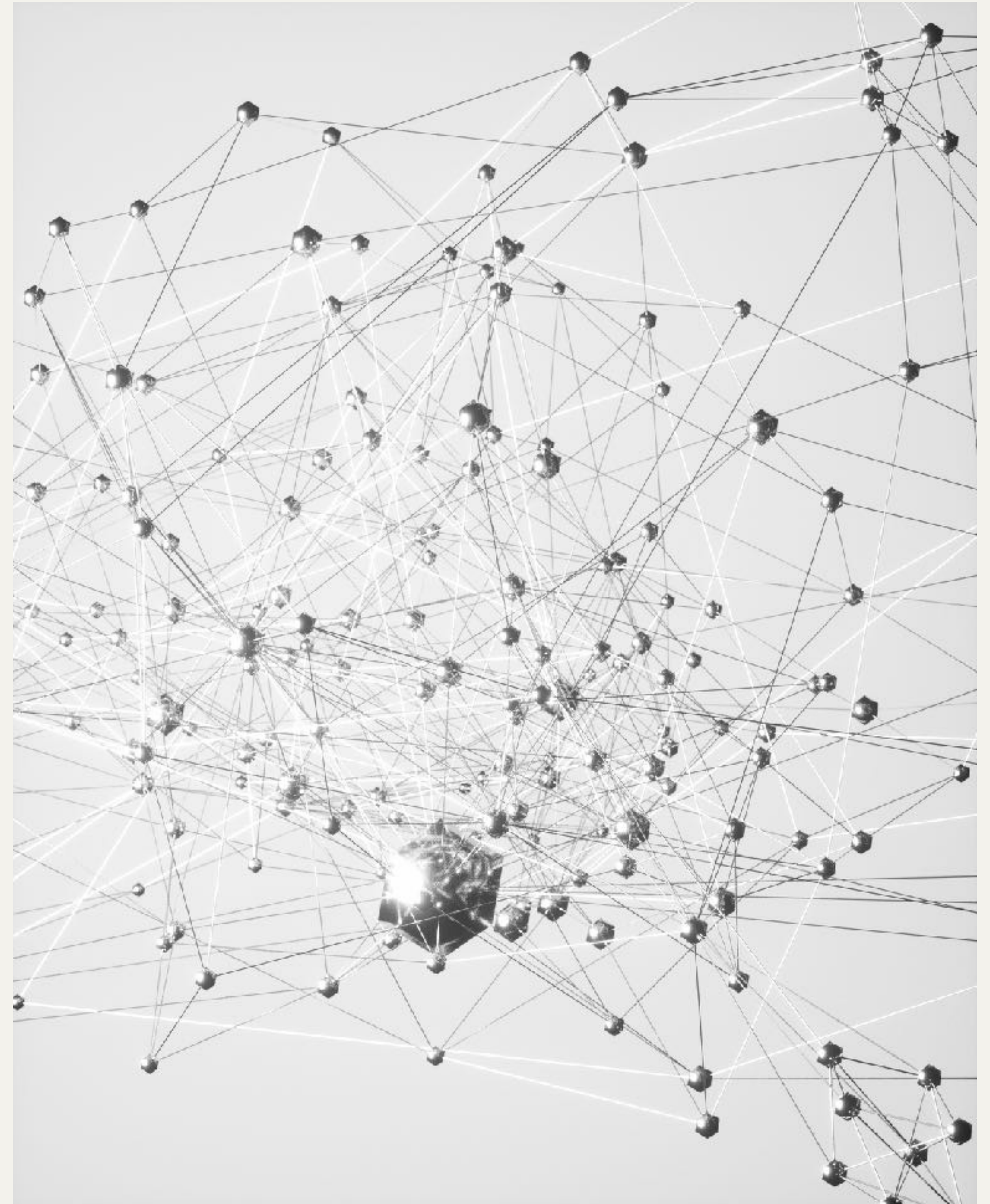
- Ensure that your data is secure for the whole life cycle
- Storage
- Deletion
- **Access controls**



# Ensure Transparency

Visibility and Transparency

- Data maps



# Ensure Transparency

Visibility and Transparency

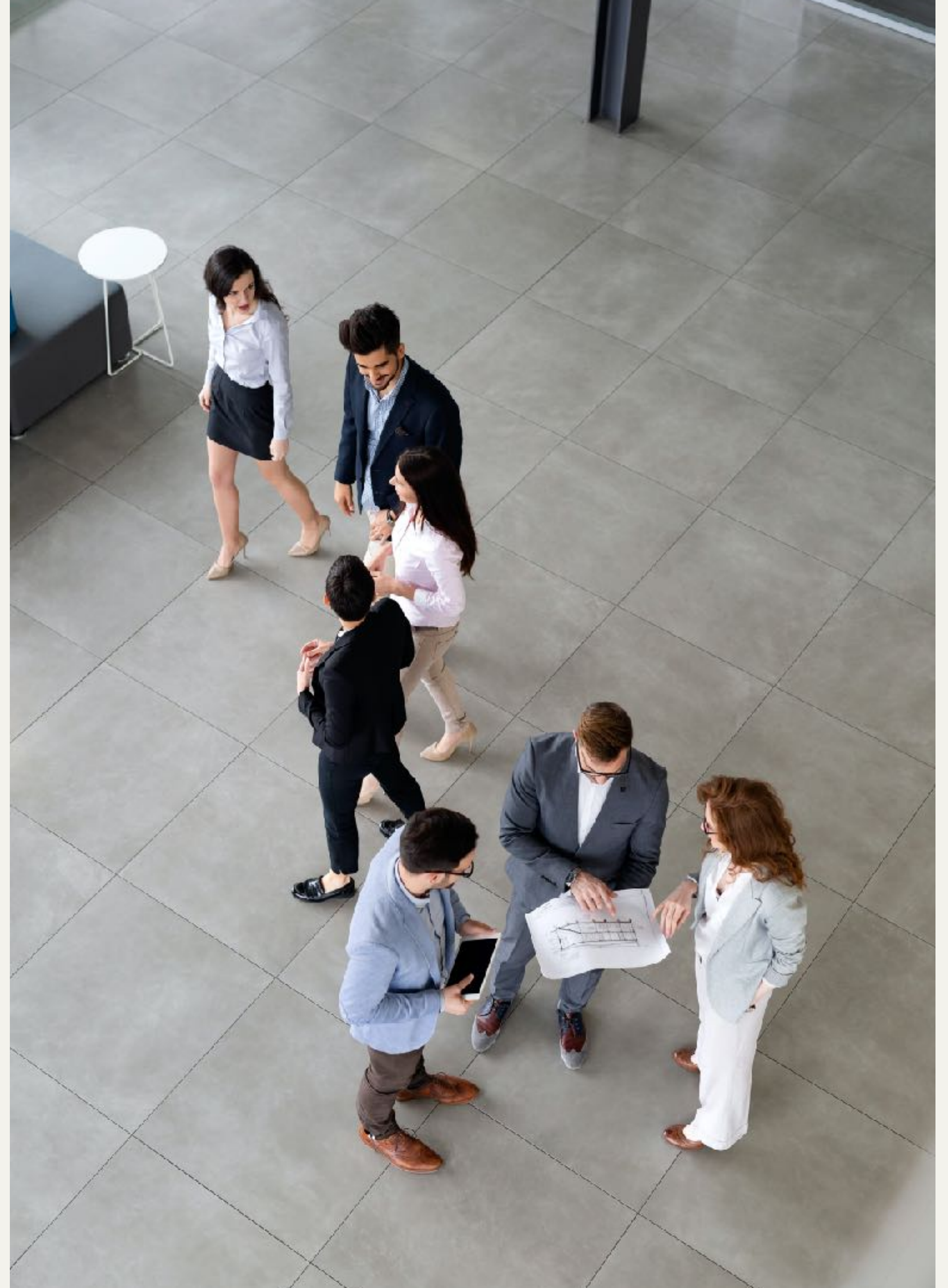
- Data maps
- Clarity about what is being processed



# Ensure Transparency

Visibility and Transparency

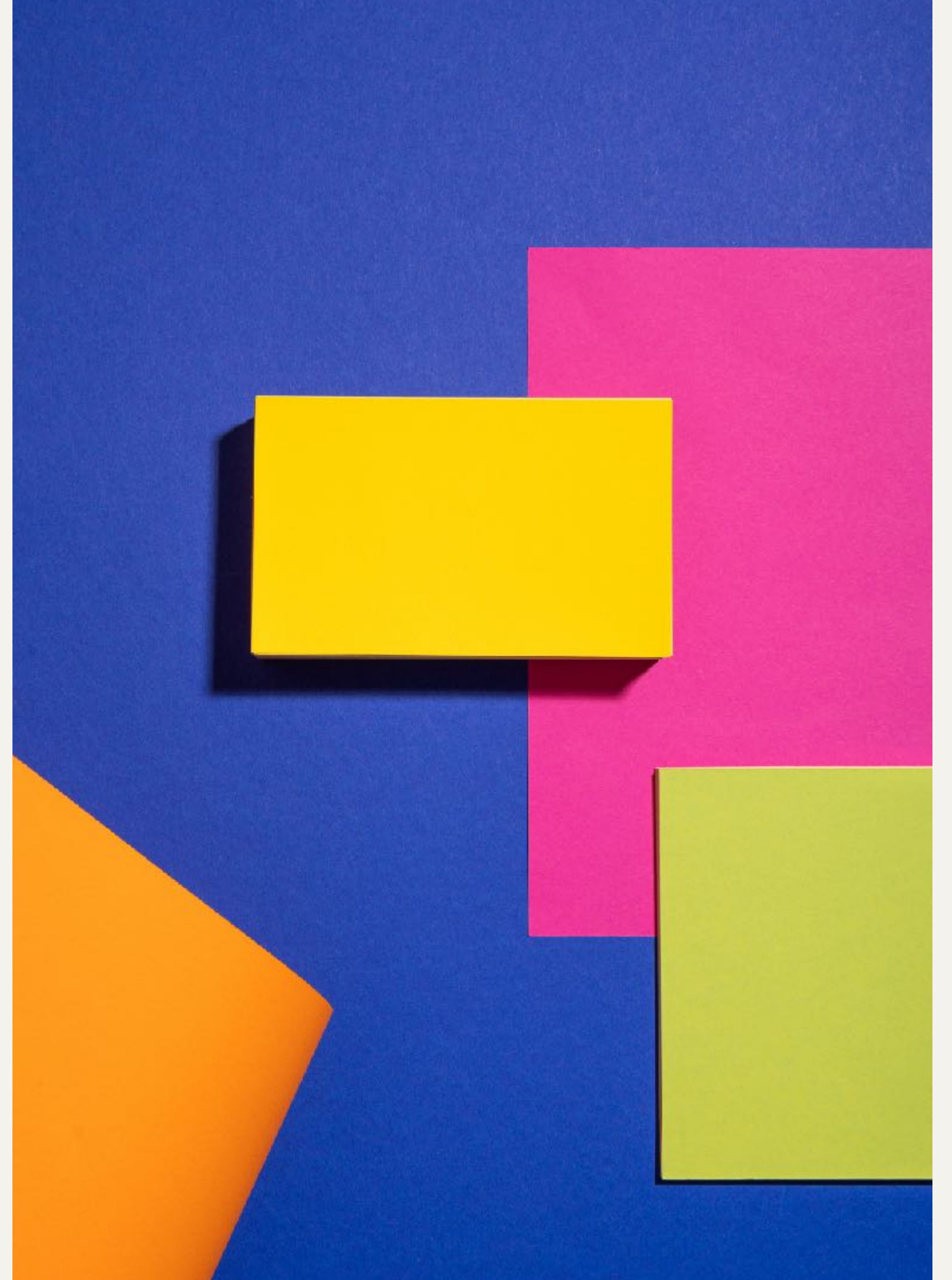
- Data flow maps
- Clarity about what is being processed
- **Policies**



# Ensure Transparency

Visibility and Transparency

- Data flow maps
- Clarity about what is being processed
- Policies
- **Notices**



# Empower the User

Respect for user privacy. Keep it user-centric.

- How can users access and control their data?





# Empower the User

Respect for user privacy. Keep it user-centric.

- How can users access and control their data?
- Allow for data portability



# Why?

Why..Why..Why..Why..Why



What if...

How do we un-*clusterfuck*  
your data?

Privacy must be considered **integral** to  
the ~~innovation~~ process.

PbD is a set of beliefs that serve as  
a **foundation** for decision-making

Intended to **guide** organisations in making ethical, moral, or logical choices.



Provide an **understanding** in how to approach various situations and help ensure consistency, fairness, and integrity in the processes.

An integral foundation that guides your understanding when making a decision.

Thank You 🧐

Link to additional resources: [ssolberg.com/pbd-resources](https://ssolberg.com/pbd-resources)