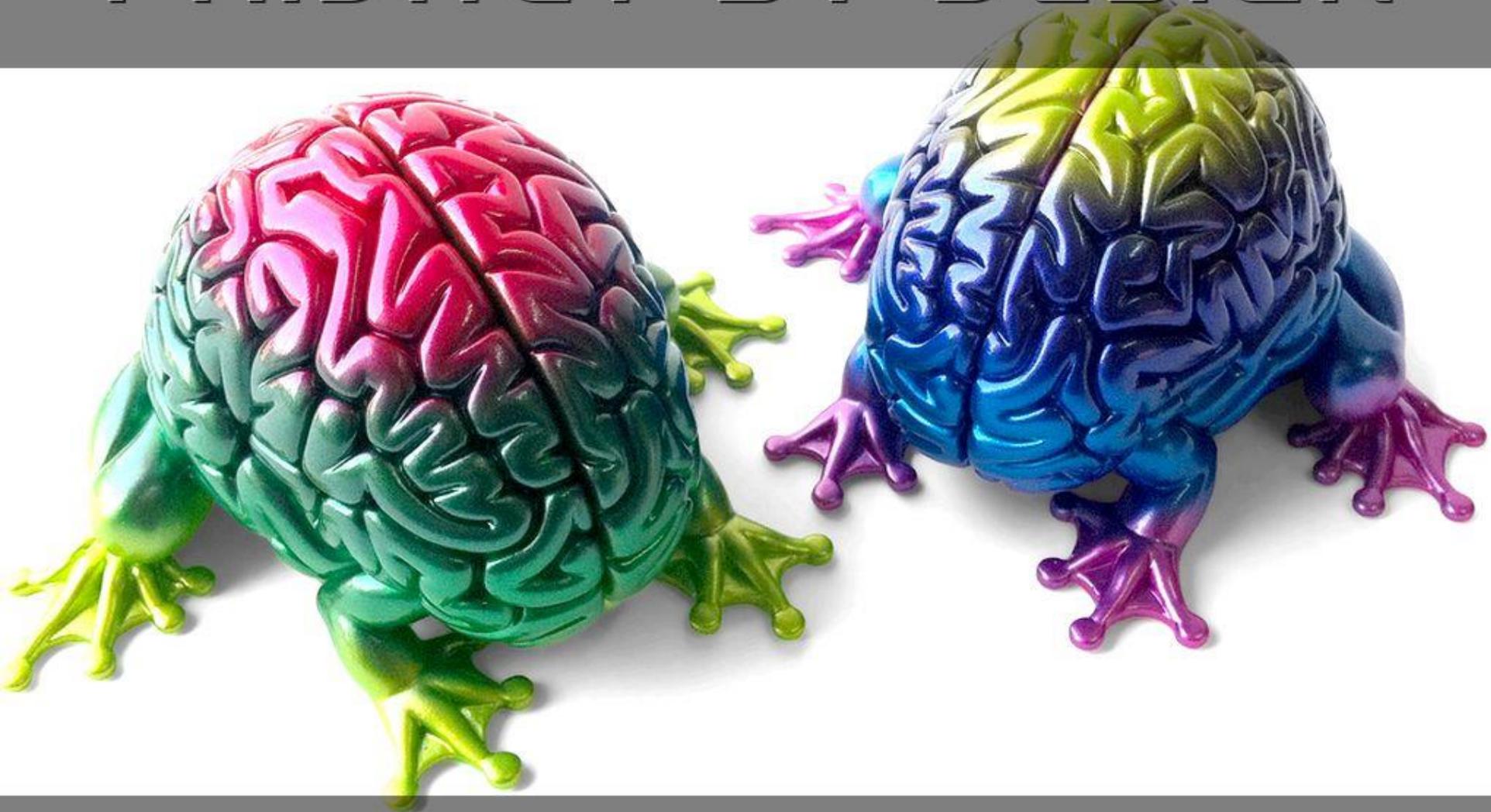


PRIVACY BY DESIGN



FROM A CODERS PERSPECTIVE



A GUIDE FOR START-UPS

ENGINE
START





PRIVACY

keep em
off

Privacy partially overlaps
with security
(confidentiality) but may also
take the form of bodily
integrity (inviolability of the
physical body).

A close-up, high-angle shot of a man's face. He is wearing a dark cowboy hat. He has a serious, intense expression. He has a dark lip piercing in his lower lip. The background is a blurred, outdoor setting with a blueish-grey sky.

THE GOOD

THE BAD

THE UGLY



THE BAD



AIL statistics 2015

160K

global warnings

1600

TOR hidden
services

7500

related to
Luxembourg

THE GOOD



GENERAL DATA PROTECTION REGULATION

- Europe wide harmonisation
- stronger responsibility & DPIA
- administrative sanctions
- right to be forgotten
- data portability
- privacy by design/default

A photograph of two LEGO Star Wars minifigures. On the left is Darth Vader, wearing his iconic black hooded cloak and having a white mask with yellow eyes. On the right is a Clone Trooper in a red suit with a black visor. The minifigures are positioned as if in a confrontation. A semi-transparent grey horizontal band runs across the middle of the image, containing the text 'THE UGLY' in white, bold, sans-serif capital letters.

THE UGLY

BEE SECURE **AGENDA VIDEO CONTACT PUBLICATIONS**
NEWS THÈMES OUTILS A PROPOS

Jouets connectés au Luxembourg : 5014 profils d'enfants résidents dans la nature

2013

Jouets connectés au Luxembourg : 5014 profils d'enfants dans la nature

ACTUALITÉS AGENDA NEWSLETTERS EMPLOI GALA GOLDEN-I CIONET LUXEMBOURG CONTACT

IT nation LU
 TECHNOLOGY - BUSINESS - STRATEGIES

POST transforme la relation client

LES BOU TECH DIGITAL PARTNER

ap agilepartner

Jouets connectés au Luxembourg : 5014 profils d'enfants dans la nature

La Commission nationale pour la protection des données et Securitymadein.lu, dans

Géhackte Lern-App: 9.000 Luxemburger betroffen | Tageblatt

Le Quotidien

Géhackte Lern-App: 9.000 Luxemburger betroffen | Tageblatt

Tageblatt
 LITZBURG

BACHMAYER MÜNCHEN DIGITAL SPORT WIRTSCHAFT KULTUR LIFESTYLE WISSEN CAMPUS SERVICE

Plus de 9.000 profils informatiques volés | Paperjam News

PAPERJAM Business zu Lëtzebuerg
 NEWS DOSSIER GUIDE CLUB SERVICES

ODER KEYPLAN, DAS SPAREN MIT INVESTMENTFONDS

0€ GEBÜHREN 40 VERSCHIEDENE FONDS 3 MÖGLICHKEITEN GELD ANZULEGEN

JOUETS CONNECTÉS VTECH

Plus de 9.000 profils informatiques volés

Thierry Raizer

La CNPD prévient d'une fuite

Luxemburger Wort
 English Edition | Contact

Lokales

LOKALES POLITIK INTERNATIONAL WIRTSCHAFT KULTUR SPORT LIFESTYLE PANORAMA WISSEN MYWORT DOSSIERS BLOGS FOTOS VIDEOS

VTECH-Konten im großen Stil gestohlen

veröffentlicht am Donnerstag, 3. Dezember 2015 um 14:55



L'essentiel Online - 9.200 comptes clients piratés au Grand-Duché - Luxembourg

L'essentiel

Actualités Économie Sports People Hi-tech Lifestyle Cinéma Musique Concours Vidéo Diagrammes Plus

Luxembourg Grande Région France Europe Monde Fats divers Inscrites Dossiers

Taux spécial Autofestival Pas de frais de dossier Conditions préférentielles pour les membres Raiffeisen

Raiffeisen

9 200 comptes clients

RTL.lu - Lëtzebuerg - Iwwer 9.000 Lëtzebuerg Spill-Konte gehackt

LUXE hacker Dont

RTL RTL.lu Radio Télé 5 minutes.lu Editus

Lëtzebuerg International Meinung Sport Trafic Meteo Kultur Life&Style Fotoen Auto Service POST

Lëtzebuerg Lokales Panorama Police Statec News Medien Bourse Bonneleieër Archiv

Technologie intuitive, expérience unique

RENAULT
 Passion for life

Fuite bei Vtech

Iwwer 9.000 Lëtzebuerg Spill-Konte gehackt

Vum groussen Hackergrëff op de Produzent vu Léiercomputere Vtech sinn zu Lëtzebuerg iwwer 5.000 Kanner, an iwwer 4.000 Eltereprofilen betraff.

Leschten Update: 04.12.2015, 07:34:27

4 Commentaire(n)

E-Mail schécken

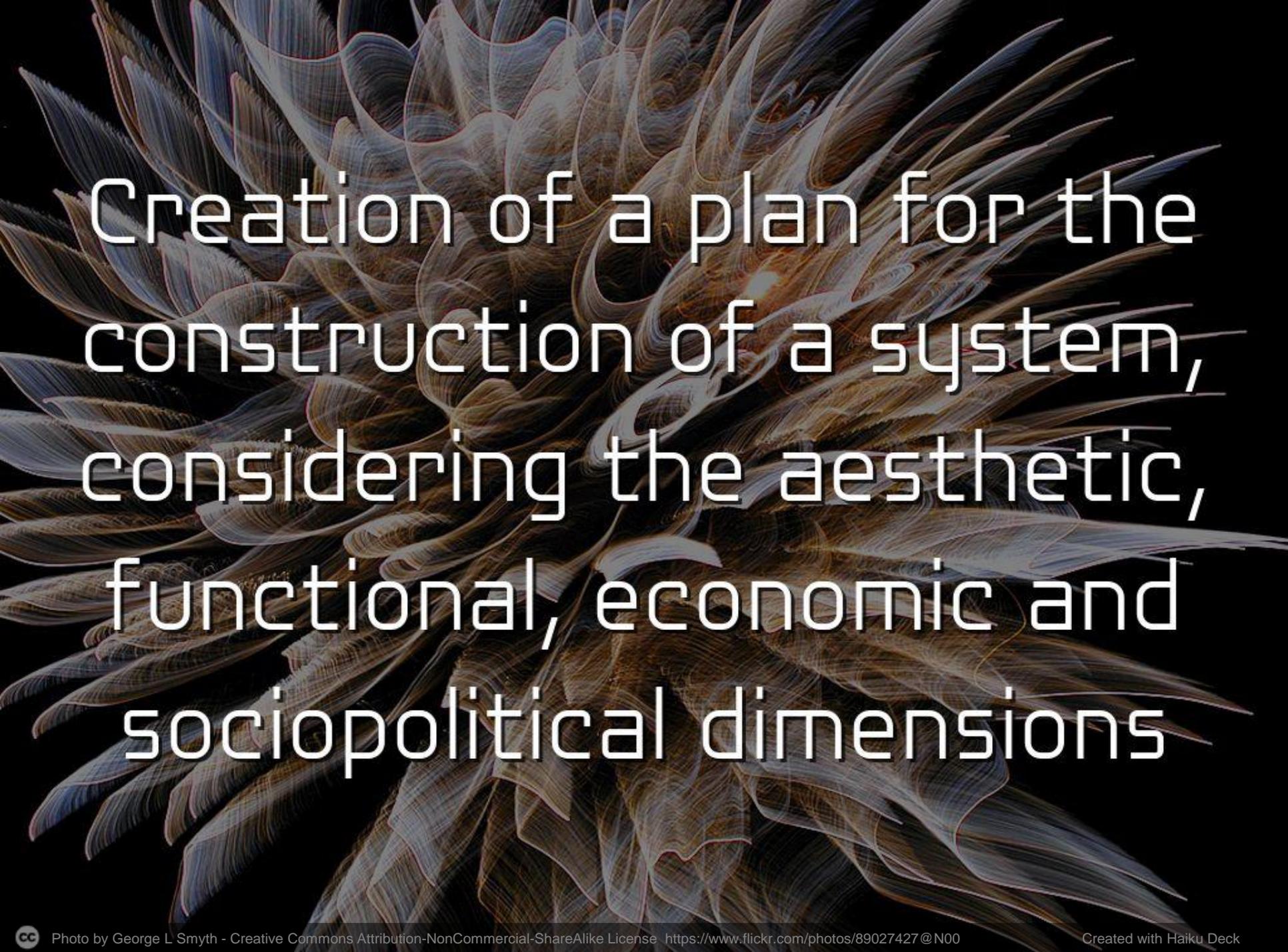
Printen

Recommander





DESIGN



Creation of a plan for the
construction of a system,
considering the aesthetic,
functional, economic and
sociopolitical dimensions

REAL-LIFE PRIVACY

GOES BEYOND



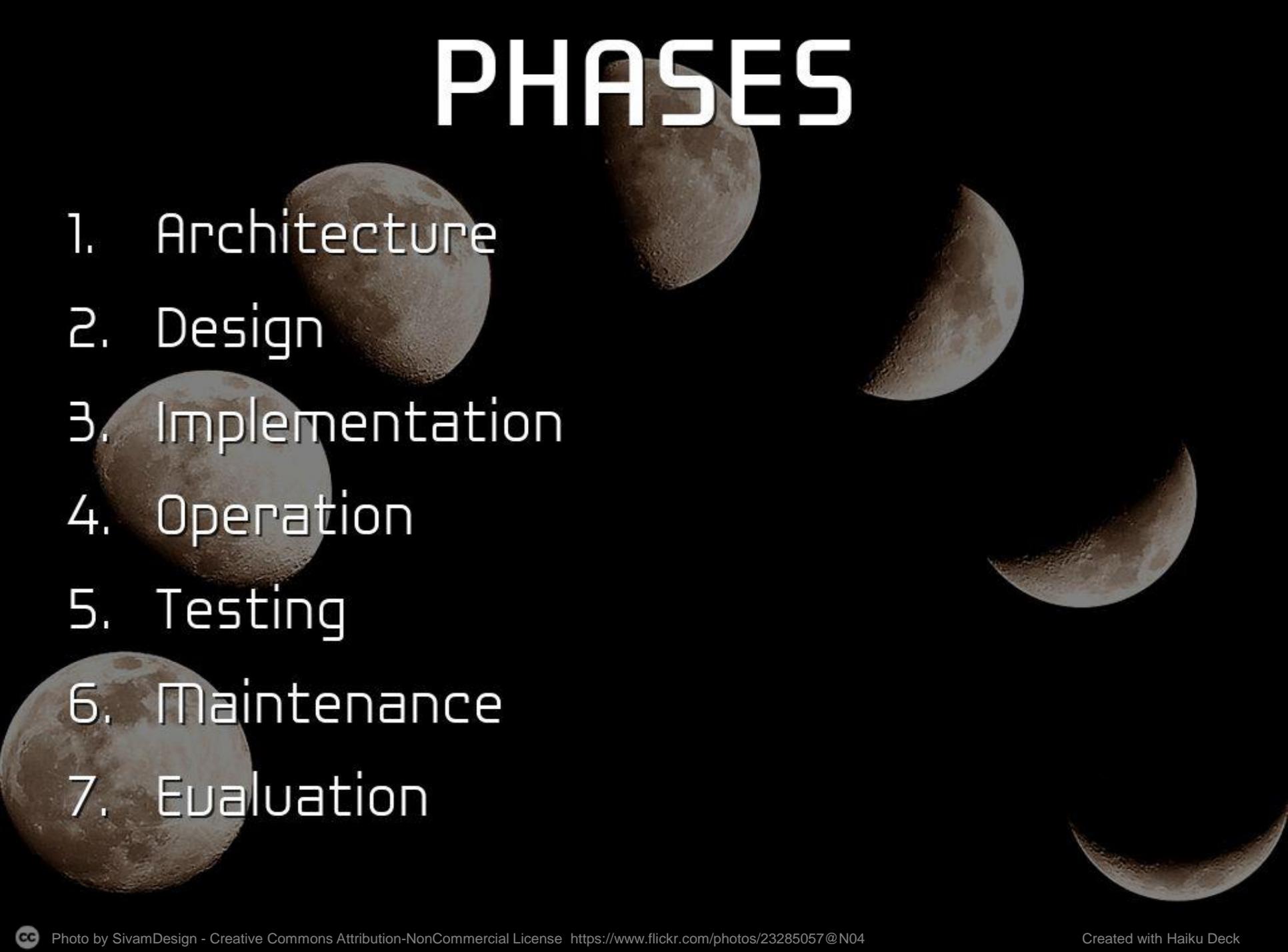


Forget about law
privacy is too
important to keep it to
lawyers ;)

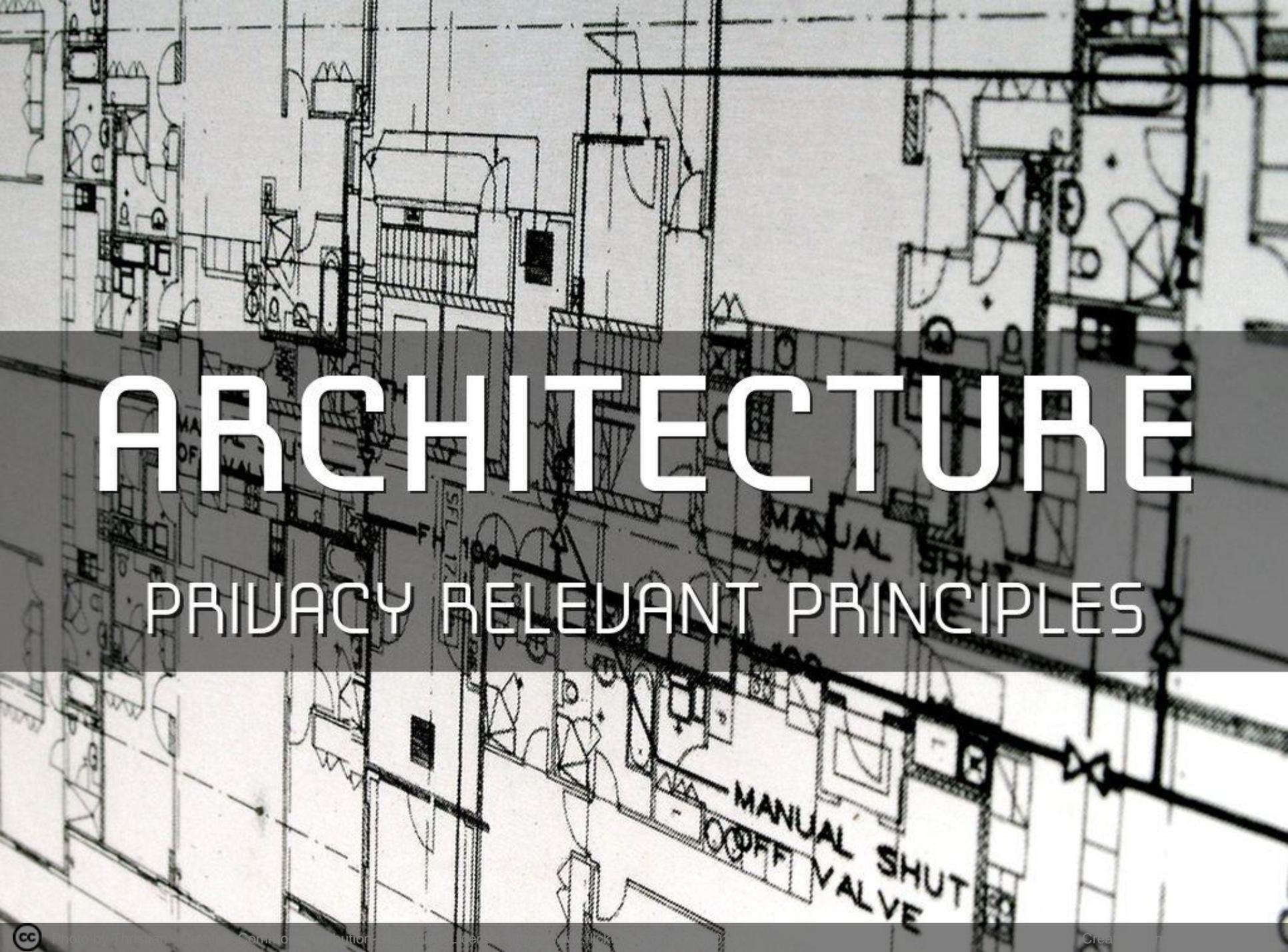
SECURE CODING

APPLIED TO PRIVACY CONCERNS

PHASES



1. Architecture
2. Design
3. Implementation
4. Operation
5. Testing
6. Maintenance
7. Evaluation

A detailed architectural floor plan of a building, showing various rooms, corridors, and structural elements. The drawing is in black ink on a light background, with a semi-transparent dark grey horizontal band across the middle. The text is overlaid on this band.

ARCHITECTURE

PRIVACY RELEVANT PRINCIPLES

KEY DECISIONS

- Program organisation (modules)
- Major data structures
- Key algorithms
- Error processing
- Active or passive privacy
- Fault tolerance

PRINCIPLES

⚡ NO SURPRISES

- "working backwards"

Use and share information that is transparent and benefits the user.



USER CONTROL

Develop products and advocate for best practices that put users in control of their data and online experiences.

- know your enemy

Maintain multi-layered security controls and practices, many of which are publicly available.

- chain of trust

VISIBLE SETTINGS

Strike a thoughtful balance of safety and user experience.

● LIMITED DATA COLLECTION

Collect what we need, de-identify when possible, and delete when no longer necessary.

- Auth/Aut/Acc/Aud

- Res/Recog/Recou

- Fail/degrade safely

THE PRINCIPLES BY MOZILLA DATA PRIVACY



PRINCIPLES (2)

⚡ NO SURPRISES

- event repeatability

Use push notifications in a way that is transparent and benefits the user.



USER CONTROL

Develop products and advocate for best practices that put users in control of their data and online experiences.

- multi-layer defense

DEPTH

Maintain multi-layered security controls and practices, many of which are publicly available.

- KISS (modularise)

VISIBLE SETTINGS

Strike a thoughtful balance of safety and user experience.

● LIMITED DATA

Collect what we need, de-identify where possible, and delete when no longer necessary.

- Seek statelessness

- Reuse code

- Address "weak links"

THE PRINCIPLES BY MOZILLA DATA PRIVACY



DESIGN

PRIVACY RELEVANT PRINCIPLES



PRINCIPLES

⚡ NO SURPRISES

- **DPIA**
User data is not processed in a way that is transparent and left to the user.

👤 USER CONTROL

Develop products and advocate for best practices that put users in control of their data and online experiences.

- **DEFENSE IN DEPTH**
Compartmentalization

🔒 VISIBLE SETTINGS

A thoughtful balance of safety and user experience.

● LIMITED DATA

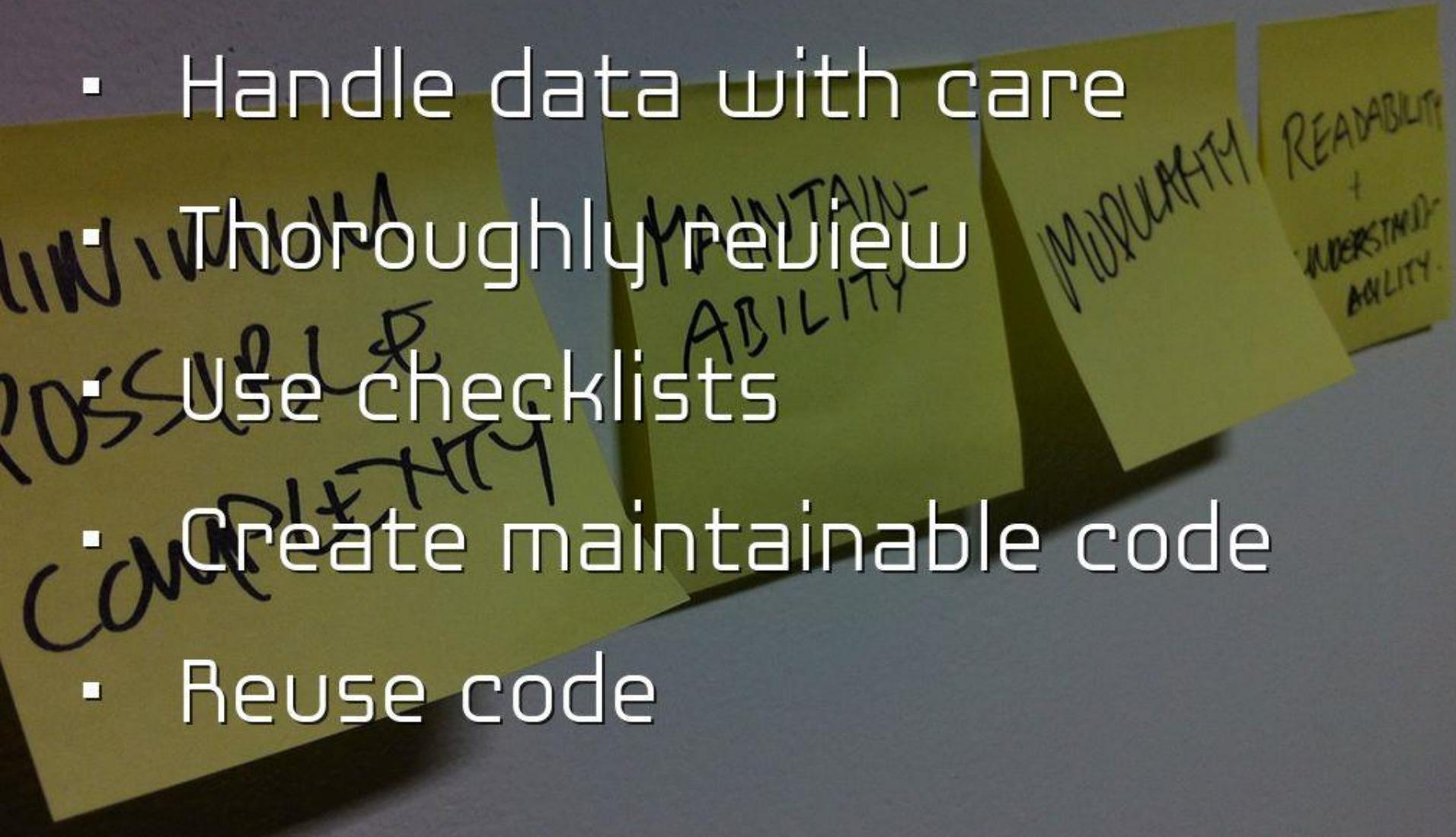
Collect what we need, de-identify where possible, and delete when no longer necessary.

THE PRINCIPLES BY MOZILLA DATA PRIVACY



PRINCIPLES

- Handle data with care
- Thoroughly review
- Use checklists
- Create maintainable code
- Reuse code



OPERATIONS



PRIVACY RELEVANT PRINCIPLES



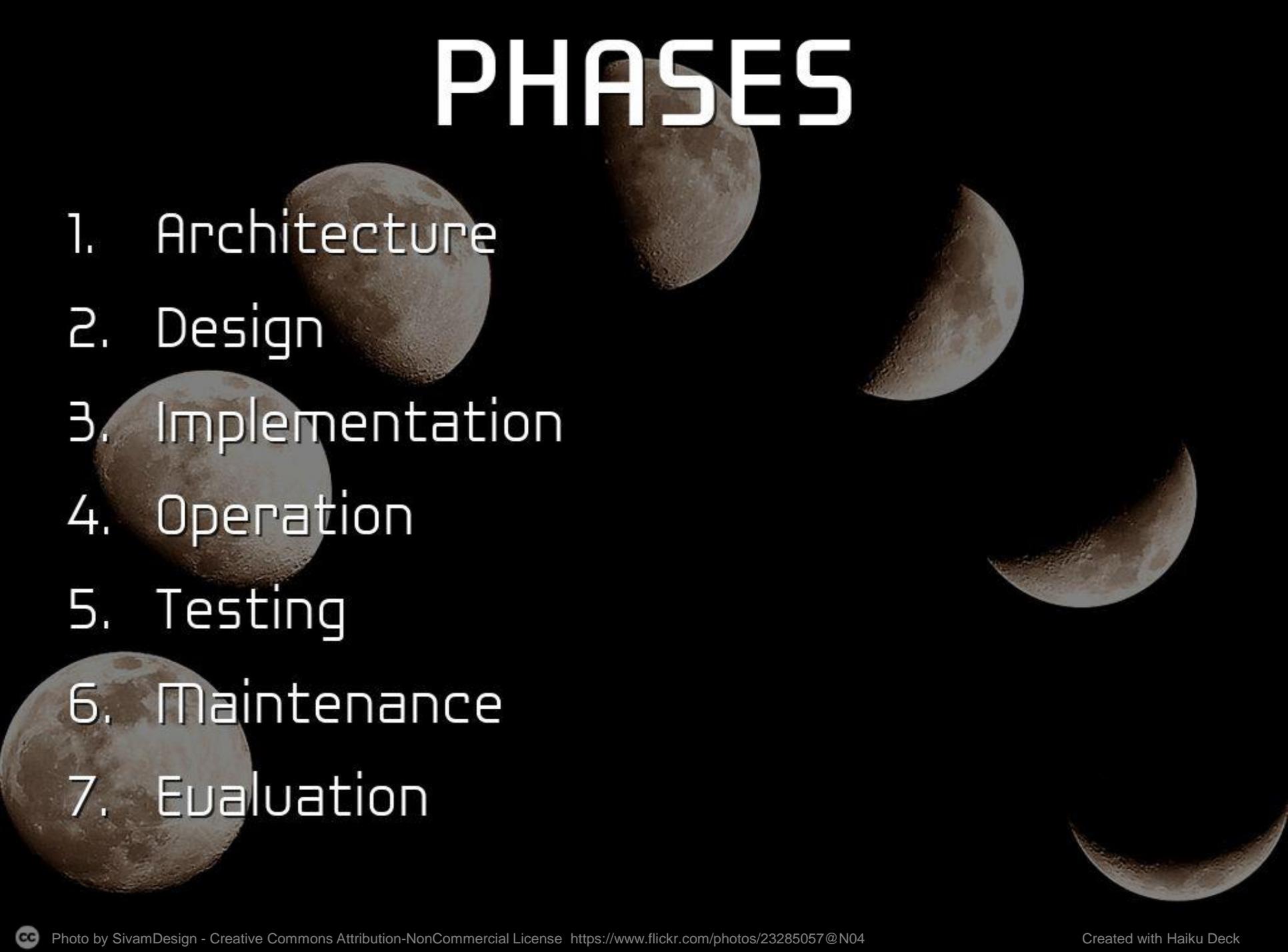
PRINCIPLES

- Harden network / connections
- Secure OS
- Deploy carefully
- Sound operation practices

③
NET MTP
METHODS
AS ~~ROY~~ INTENDED

④
REPRESENTATIONS

PHASES

The background of the slide features a series of seven moon phases arranged in a descending arc from the top center towards the bottom right. The phases include a full moon, a gibbous moon, a half moon, a waning gibbous moon, a crescent moon, a thin crescent moon, and a very thin crescent moon. The moon's surface is detailed with craters and darker patches.

1. Architecture
2. Design
3. Implementation
4. Operation
5. Testing
6. Maintenance
7. Evaluation



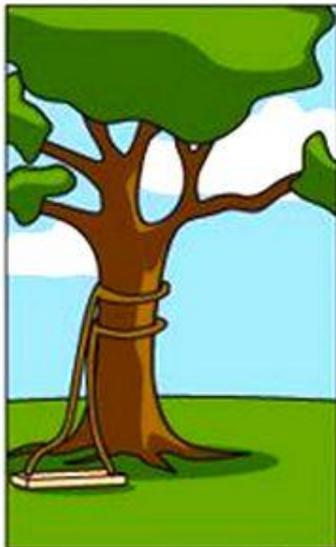
How the customer explained it



How the Project Leader understood it



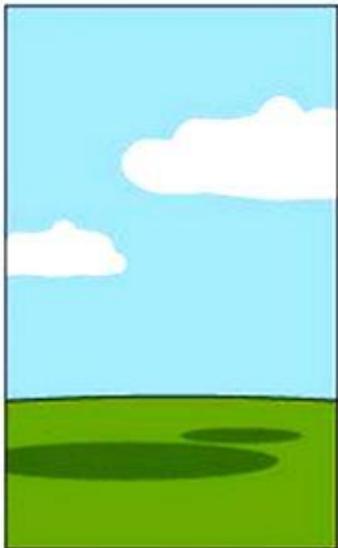
How the Analyst designed it



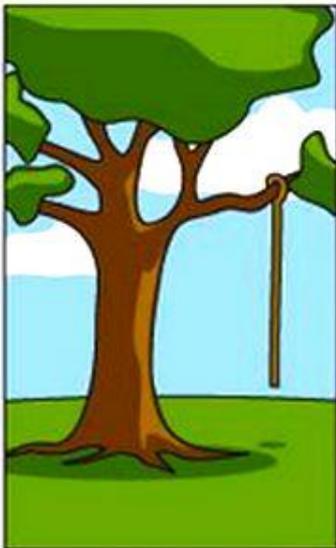
How the Programmer wrote it



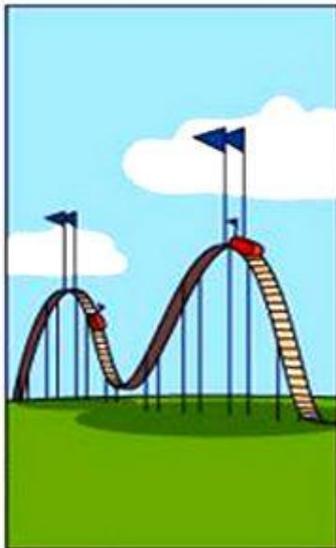
How the Business Consultant described it



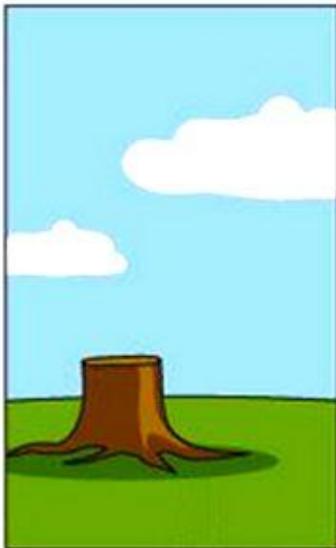
How the project was documented



What operations installed



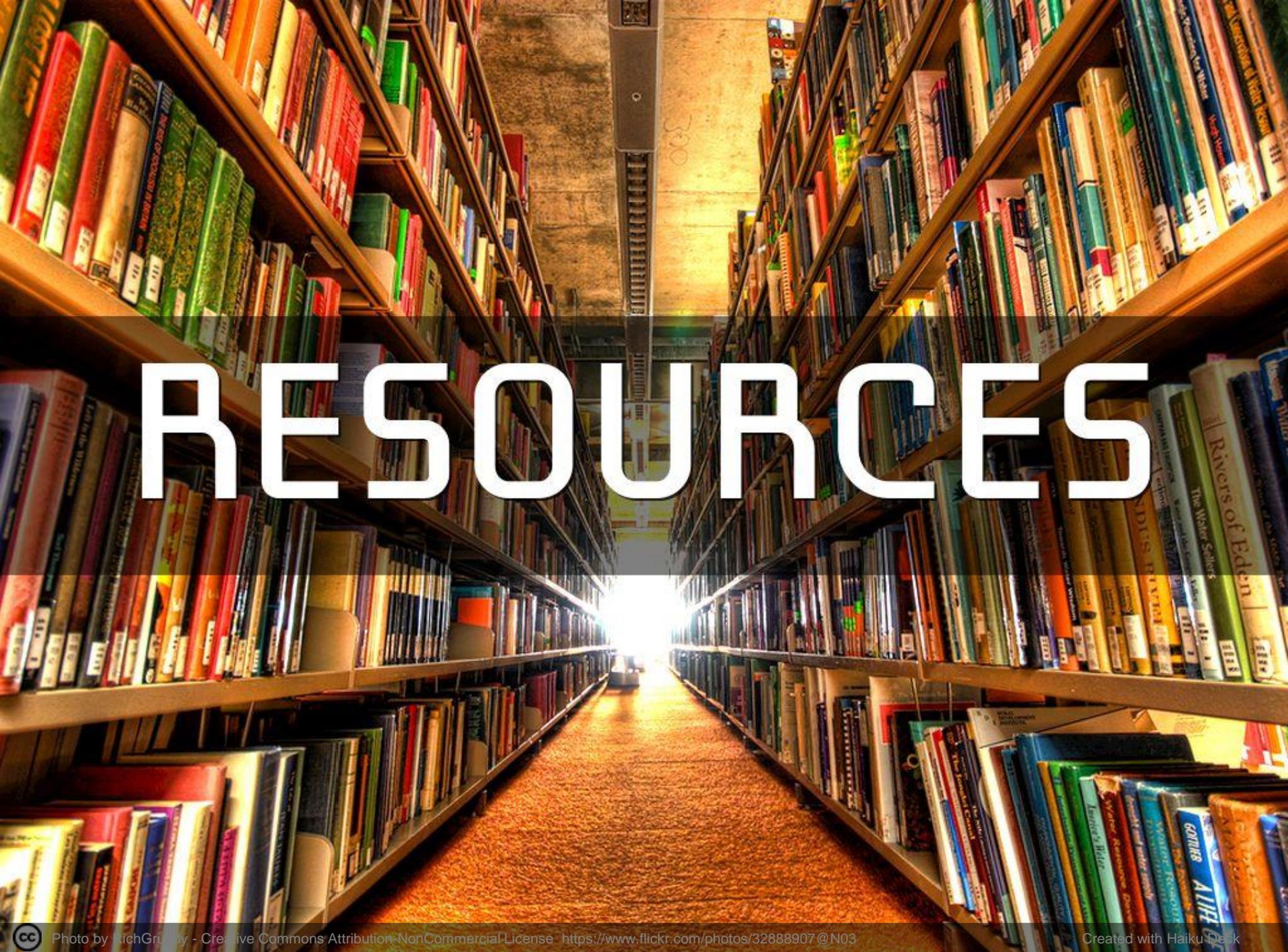
How the customer was billed



How it was supported



What the customer really needed



RESOURCES

OECD PRIVACY GUIDELINES

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle



OWASP

Top 10 Privacy Risks

Alpha Version 1.0

Website Application Vulnerabilities

Vulnerability is a key problem in any system that guards or operates on sensitive user data. Failure to suitably design and implement an application, detect a problem or promptly apply a fix (patch) is likely to result in a privacy breach. This risk also encompasses the OWASP Top 10 List



Frequency: High
Impact: Very High





Training developers in writing secure code

SKF is a fully open-source Python-Flask web-application that uses the OWASP Application Security Verification Standard to train you and your team in writing secure code, by design.



Fork on Github

View demo



2015 Open Source Rookies of the Year

We are honored to receive a honorable mention for the Black Duck Open Source Rookies of the Year awards.

14-03-2016 | [Article on blackducksoftware.com](http://blackducksoftware.com)



OWASP

Presentation about skf on the OWASP BeNeLux Days

18-02-2016

THANK YOU

PASCAL STEICHEN

Arigato

Dankscheen

Gracias

THANK YOU

Biyann

Shukuria

Komapsumnida

Paldies

Maake

gozaimashita

Fakaau

Ekhmet

Mehrbani

Yaqhanyelay
Efcharisto

Baiika Yuspagarátam
Minmonchar Atto

suk sama

Merci

Shukria

lah

Merastawhy

Lhanabaad

Chaltu

nuhun

Juspax

Snachalmuya