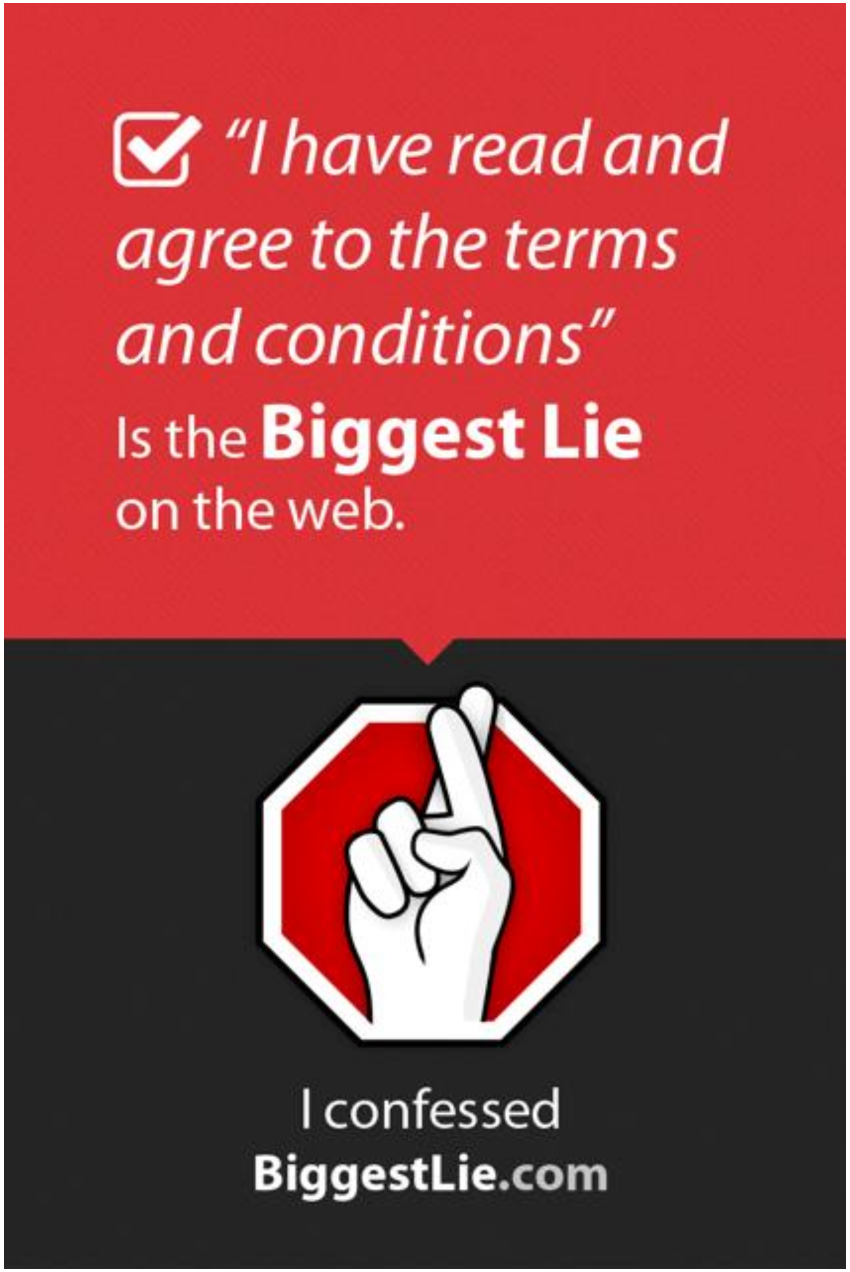
Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative

SUPSI

# Privacy by Design

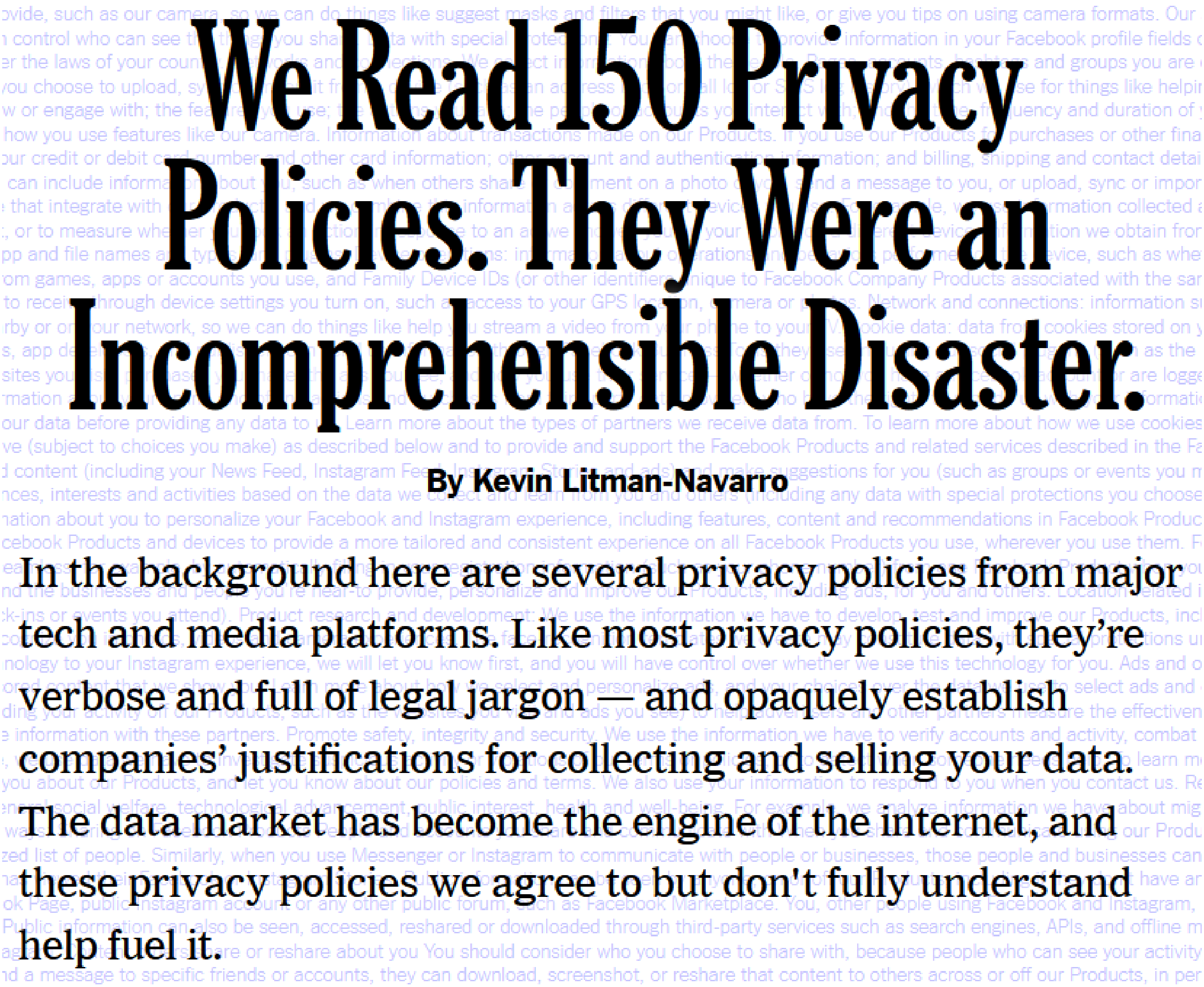
## Risks & Principles

**SUPSI DTI**
**Angelo Consoli**
**November 2024**


☑ "I have read and agree to the terms and conditions"
Is the Biggest Lie on the web.
I confessed
BiggestLie.com

## New York Times Article

## December 2019



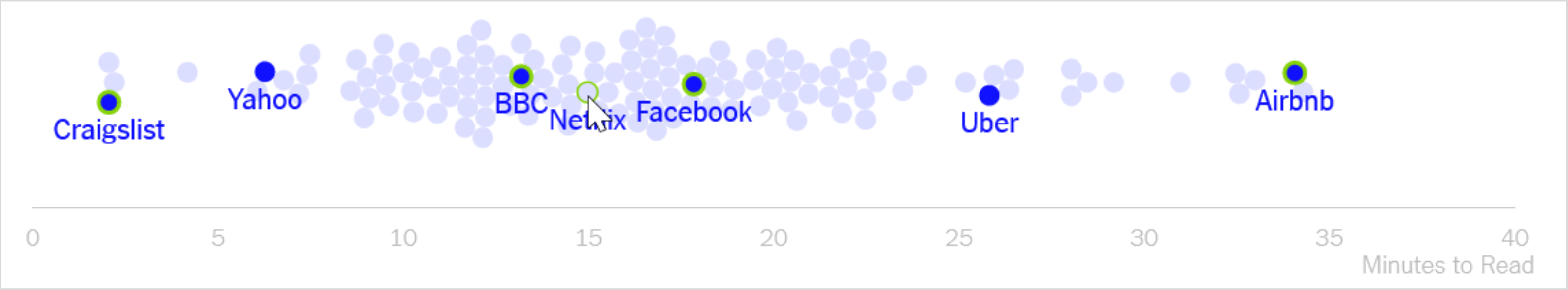
# We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.

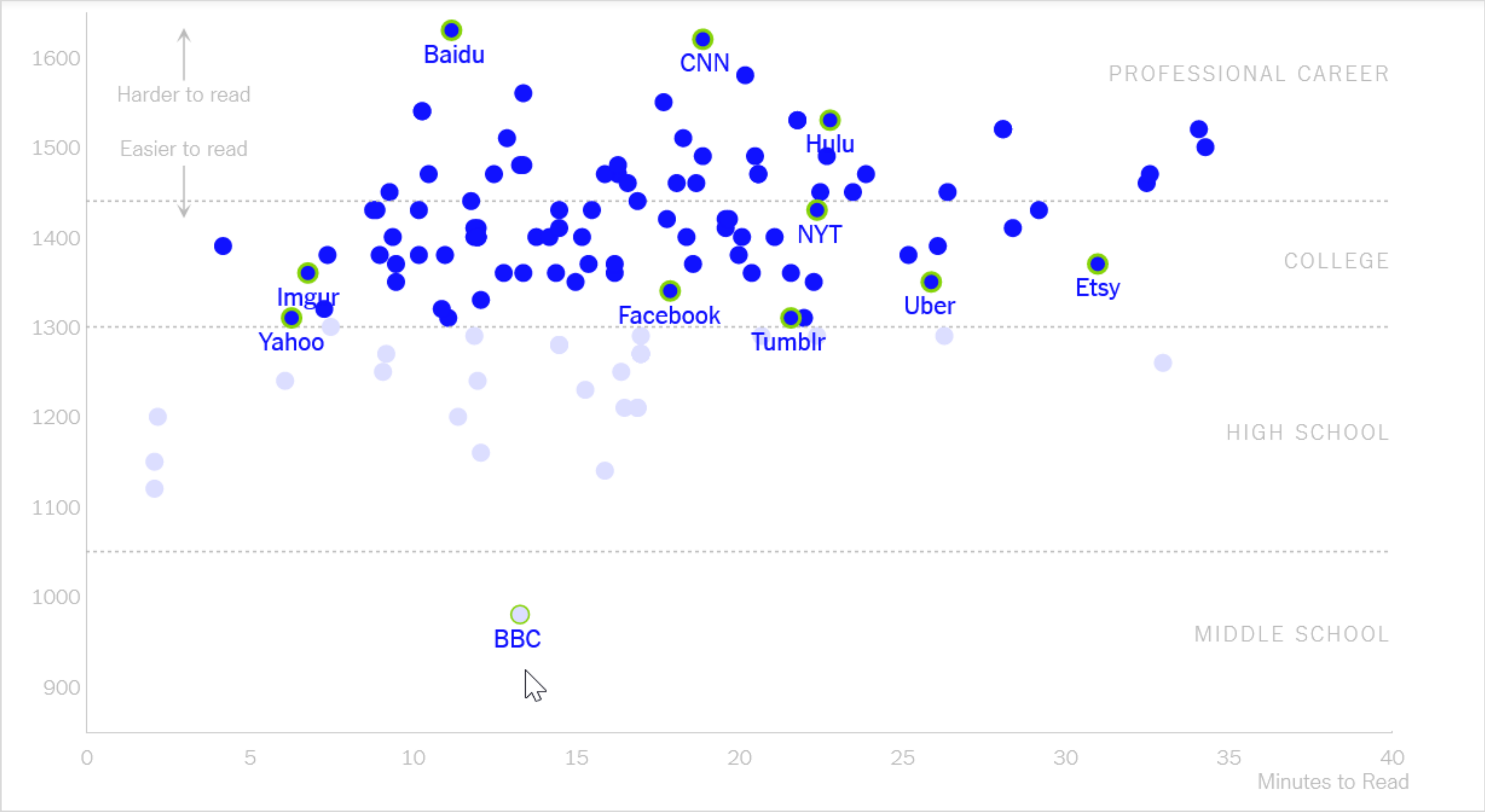
By Kevin Litman-Navarro

In the background here are several privacy policies from major tech and media platforms. Like most privacy policies, they're verbose and full of legal jargon — and opaquely establish companies' justifications for collecting and selling your data. The data market has become the engine of the internet, and these privacy policies we agree to but don't fully understand help fuel it.

*https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html*

# Some interesting statistics ...

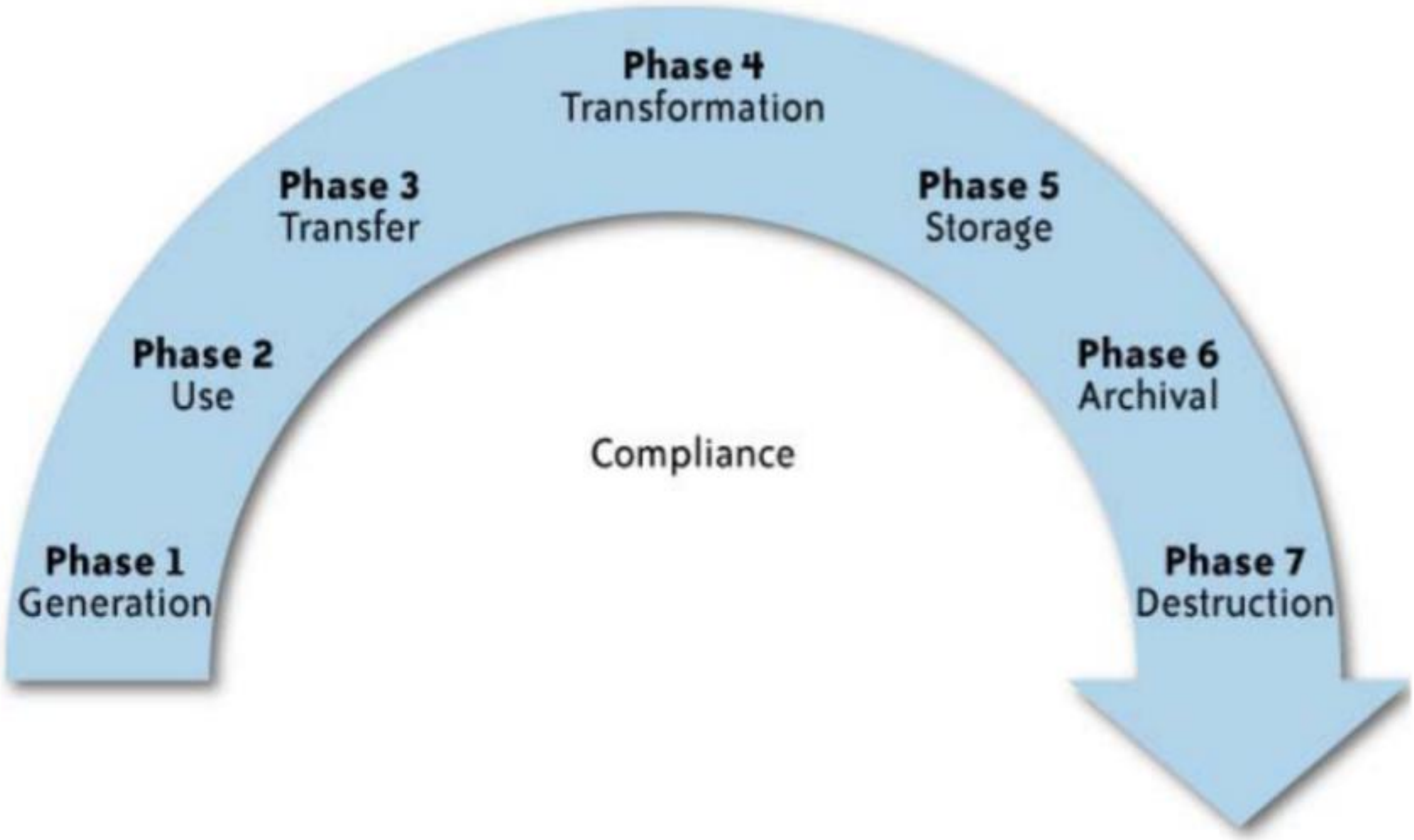




# Personally Identifiable Information (PII)

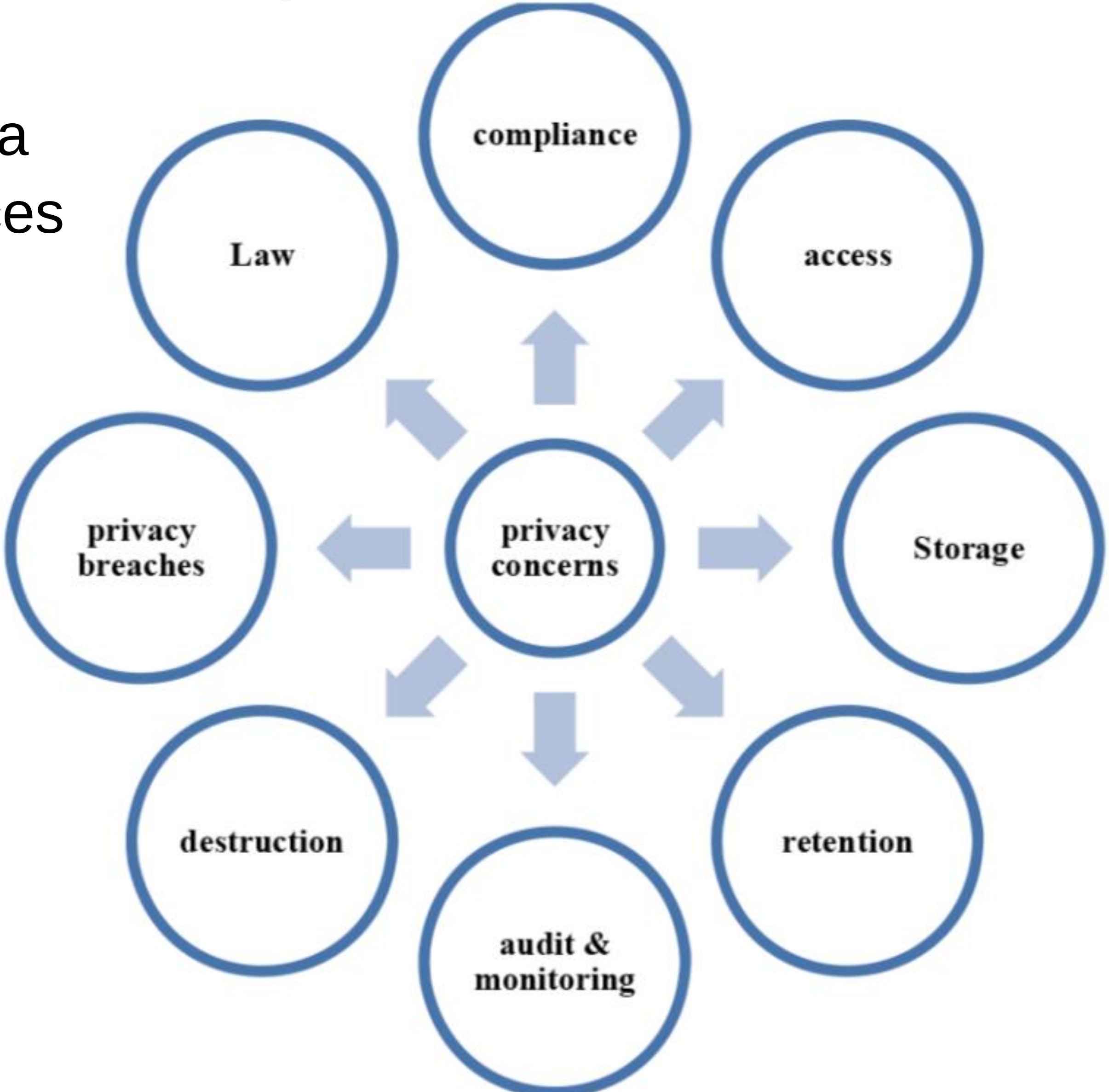
- All geographic subdivisions smaller than state
- Birth date
- Telephone/Fax numbers
- E-mail addresses
- Social Security Number
- Medical Record Number
- Health Plan Number
- Account Number
- Certificate / license number
- Vehicle identifier/serial number
- Device identifier/serial number
- Uniform Resource Locators (URLs)
- IP addresses
- Biometric identifiers
- Photos
- Other unique characteristics
- Full face photograph
- Criminal record

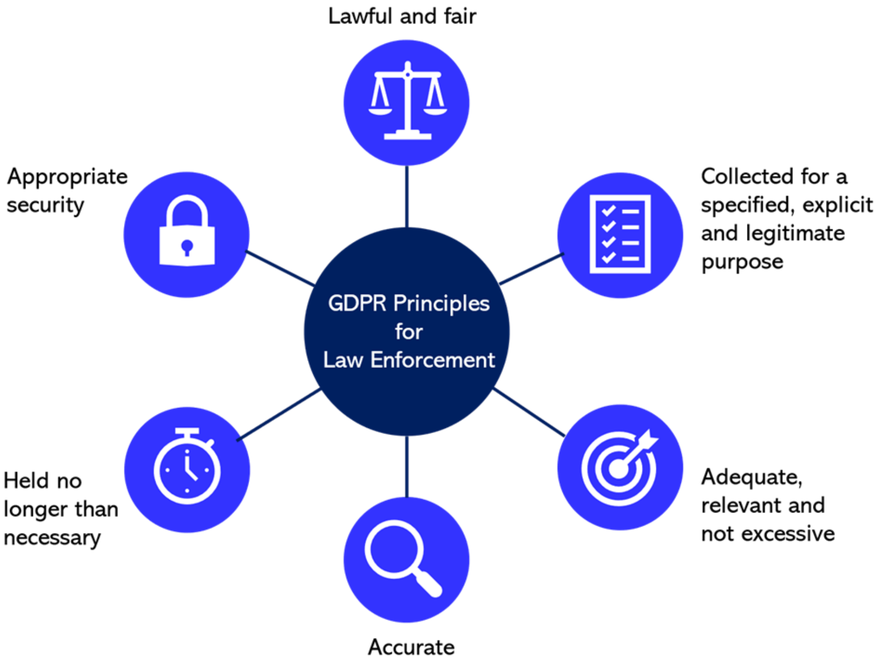
# Data lifecycle



# Privacy concerns

- For inhouse data
- For cloud services




Lawful and fair
Appropriate security
Collected for a specified, explicit and legitimate purpose
GDPR Principles for Law Enforcement
Held no longer than necessary
Adequate, relevant and not excessive
Accurate

# INTERNATIONAL PRIVACY PRINCIPLES & FRAMEWORKS

# International Privacy Principles

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

# Privacy Principles Framework

- NIST (New Framework from 2020)
- OECD privacy principles
- NSTIC FIPPs
- U.S.-EU Safe Harbor & U.S.-Swiss Safe Harbor
- ISO/ IEC 29100
- APEC privacy framework
- Madrid Resolution on International Privacy Standards

# International Privacy Principles

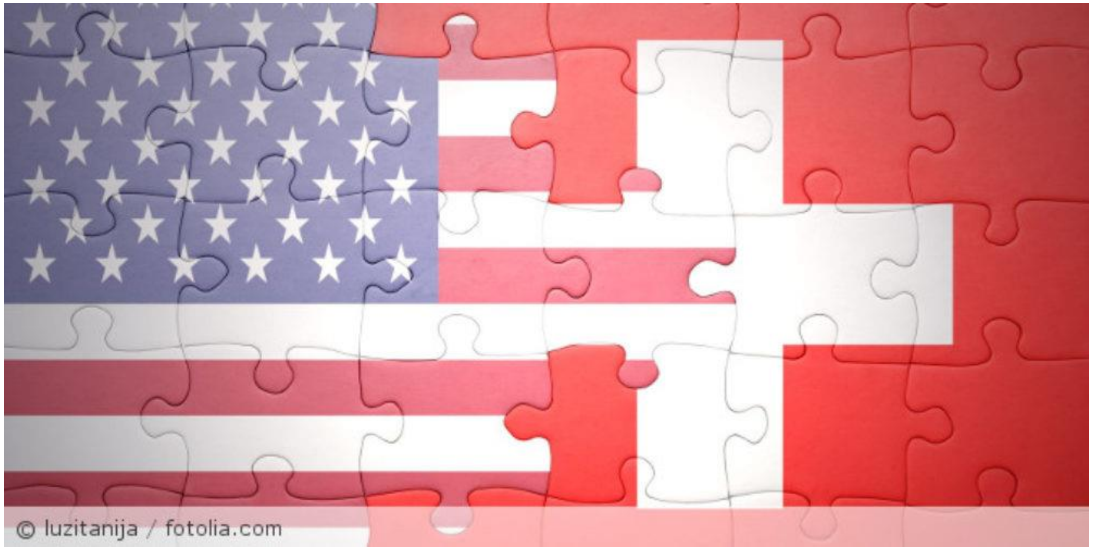
**Table 1: privacy principles in international privacy frameworks**

| Principle | NSTIC FIPPs | OECD privacy principles | U.S.-EU Safe Harbor & U.S-Swiss Safe Harbor | APEC privacy framework | Madrid Resolution on International Privacy Standards | ISO/ IEC 29100 |
|---|---|---|---|---|---|---|
| Collection limitation | √ | √ |  | √ |  | √ |
| Consent and choice | √ | √ | √ | √ | √ | √ |
| Collection methods |  | √ |  | √ |  |  |
| Data integrity | √ | √ | √ | √ | √ | √ |
| Data minimization |  |  |  |  | √ | √ |
| Use and retention limitation | √ | √ |  | √ |  | √ |
| Disclosure and transfer data | √ |  | √ |  | √ | √ |
| Notice, transparency and openness | √ | √ | √ | √ | √ | √ |
| Rights and access | √ | √ | √ | √ | √ | √ |
| Security safeguards and encryption | √ | √ | √ | √ | √ | √ |
| Sensitive data |  |  | √ |  | √ | √ |
| Accountability and auditing | √ | √ | √ | √ | √ | √ |
| Purpose legitimacy and specification | √ | √ |  |  | √ | √ |
| Proactive measures |  |  |  | √ | √ |  |

*A Framework for Enhancing Privacy Provision in Cloud Computing*

# U.S.-EU Safe Harbor & U.S-Swiss Safe Harbor

Johann Schneider-Ammann announced the approval of the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States.



© luzitanija / fotolia.com

# GDPR ? Small Introduction

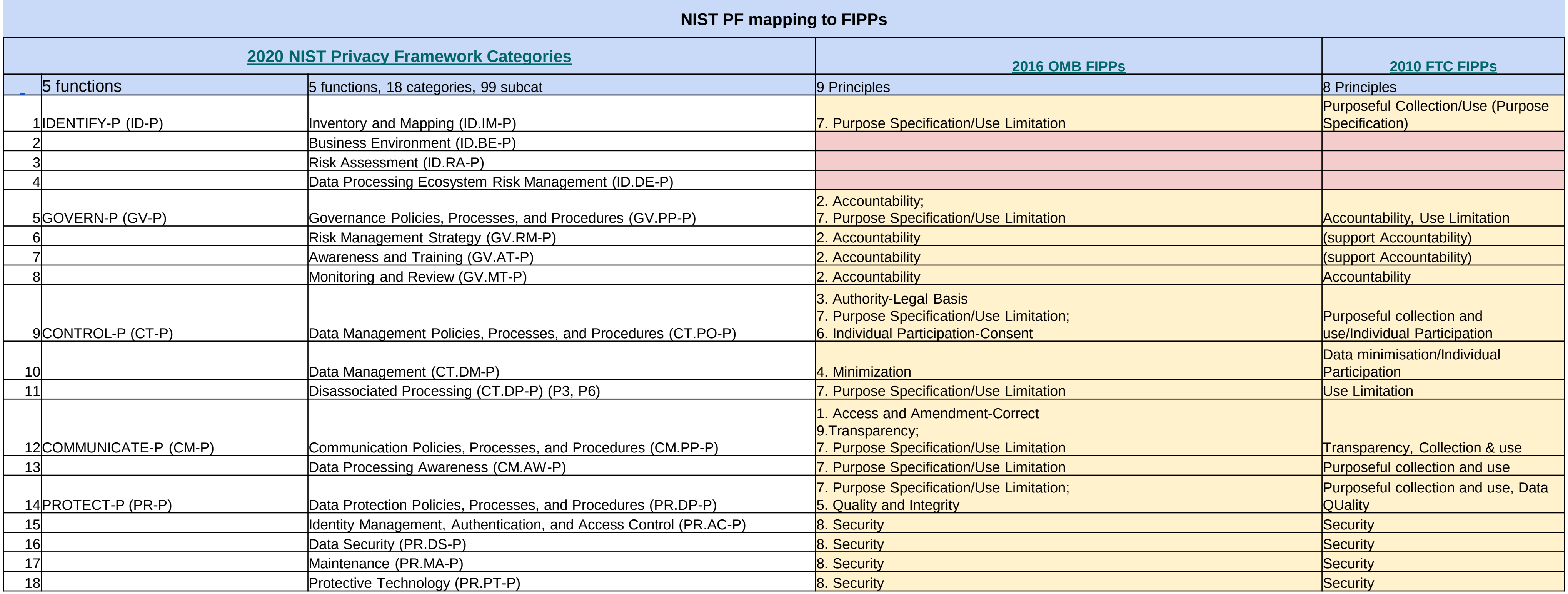
- GDPR = General Data Protection Regulation; entry into force: 25.05.2018
- Problems with GDPR application (U.S. Prespective):

1. The GDPR strengthens the largest players.
2. The GDPR weakens small- and medium-sized firms.
3. The GDPR is cost prohibitive for many firms.
4. The GDPR silences free speech and expression.
5. The GDPR threatens innovation and research.
6. The GDPR increases cybersecurity risk.
7. The GDPR and the CCPA create risks for identity theft and online fraud.
8. The GDPR has not created greater trust online.
9. The GDPR and the CCPA use the pretense of customer control to increase the power of government.
10. The GDPR and the CCPA fail to meaningfully incorporate the role of privacy enhancing innovation and consumer education in data protection.

# ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

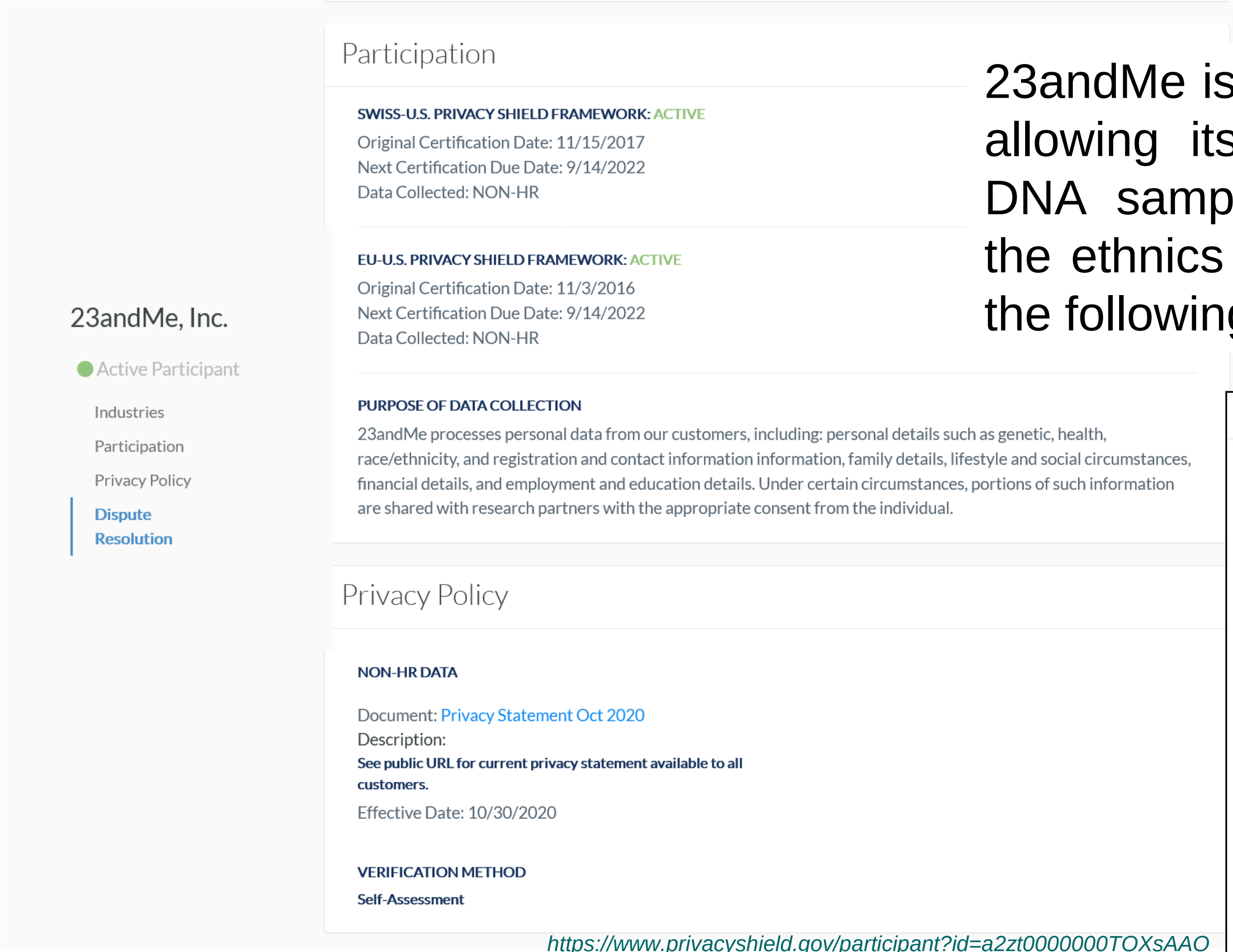
# NIST Privacy Framework (2020) mapping to FIPPs (2016 and 2010)



| NIST PF mapping to FIPPs | | | | |
|---|---|---|---|---|
| 2020 NIST Privacy Framework Categories | | | 2016 OMB FIPPs | 2010 FTC FIPPs |
| _ | 5 functions | 5 functions, 18 categories, 99 subcat | 9 Principles | 8 Principles |
| 1 | IDENTIFY-P (ID-P) | Inventory and Mapping (ID.IM-P) | 7. Purpose Specification/Use Limitation | Purposeful Collection/Use (Purpose Specification) |
| 2 | | Business Environment (ID.BE-P) | | |
| 3 | | Risk Assessment (ID.RA-P) | | |
| 4 | | Data Processing Ecosystem Risk Management (ID.DE-P) | | |
| 5 | GOVERN-P (GV-P) | Governance Policies, Processes, and Procedures (GV.PP-P) | 2. Accountability;<br>7. Purpose Specification/Use Limitation | Accountability, Use Limitation |
| 6 | | Risk Management Strategy (GV.RM-P) | 2. Accountability | (support Accountability) |
| 7 | | Awareness and Training (GV.AT-P) | 2. Accountability | (support Accountability) |
| 8 | | Monitoring and Review (GV.MT-P) | 2. Accountability | Accountability |
| 9 | CONTROL-P (CT-P) | Data Management Policies, Processes, and Procedures (CT.PO-P) | 3. Authority-Legal Basis<br>7. Purpose Specification/Use Limitation;<br>6. Individual Participation-Consent | Purposeful collection and use/Individual Participation |
| 10 | | Data Management (CT.DM-P) | 4. Minimization | Data minimisation/Individual Participation |
| 11 | | Disassociated Processing (CT.DP-P) (P3, P6) | 7. Purpose Specification/Use Limitation | Use Limitation |
| 12 | COMMUNICATE-P (CM-P) | Communication Policies, Processes, and Procedures (CM.PP-P) | 1. Access and Amendment-Correct<br>9.Transparency;<br>7. Purpose Specification/Use Limitation | Transparency, Collection & use |
| 13 | | Data Processing Awareness (CM.AW-P) | 7. Purpose Specification/Use Limitation | Purposeful collection and use |
| 14 | PROTECT-P (PR-P) | Data Protection Policies, Processes, and Procedures (PR.DP-P) | 7. Purpose Specification/Use Limitation;<br>5. Quality and Integrity | Purposeful collection and use, Data QUality |
| 15 | | Identity Management, Authentication, and Access Control (PR.AC-P) | 8. Security | Security |
| 16 | | Data Security (PR.DS-P) | 8. Security | Security |
| 17 | | Maintenance (PR.MA-P) | 8. Security | Security |
| 18 | | Protective Technology (PR.PT-P) | 8. Security | Security |

*https://www.nist.gov/privacy-framework/fair-information-practice-principles-fipps-crosswalk*

# An example, company 23andMe



23andMe, Inc.

● Active Participant

## Participation

**SWISS-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE**

Original Certification Date: 11/15/2017
Next Certification Due Date: 9/14/2022
Data Collected: NON-HR

**EU-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE**

Original Certification Date: 11/3/2016
Next Certification Due Date: 9/14/2022
Data Collected: NON-HR

**PURPOSE OF DATA COLLECTION**

23andMe processes personal data from our customers, including: personal details such as genetic, health, race/ethnicity, and registration and contact information information, family details, lifestyle and social circumstances, financial details, and employment and education details. Under certain circumstances, portions of such information are shared with research partners with the appropriate consent from the individual.

## Privacy Policy

**NON-HR DATA**

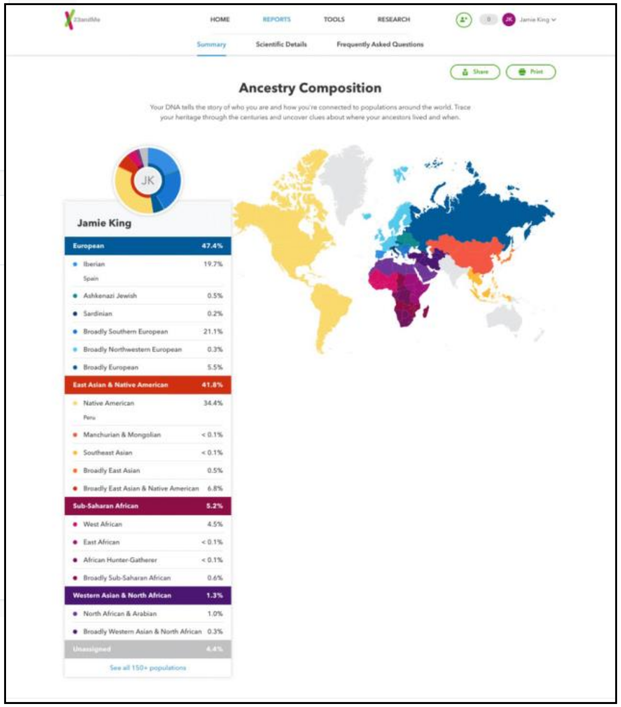
Document: Privacy Statement Oct 2020
Description:
**See public URL for current privacy statement available to all customers.**
Effective Date: 10/30/2020

**VERIFICATION METHOD**

**Self-Assessment**

https://www.privacyshield.gov/participant?id=a2zt0000000TOXsAAO

23andMe is an American company allowing its customers via saliva DNA sample a reconstruction of the ethnics Ancestry tree, such as the following report



**Ancestry Composition**

Your DNA tells the story of who you are and how you're connected to populations around the world. Trace your heritage through the centuries and uncover clues about where your ancestors lived and when.

Jamie King

| | |
|---|---|
| **European** | **47.4%** |
| ● Iberian<br>Spain | 19.7% |
| ● Ashkenazi Jewish | 0.5% |
| ● Sardinian | 0.2% |
| ● Broadly Southern European | 21.1% |
| ● Broadly Northwestern European | 0.3% |
| ● Broadly European | 5.5% |
| **East Asian & Native American** | **41.8%** |
| ● Native American<br>Peru | 34.4% |
| ● Manchurian & Mongolian | < 0.1% |
| ● Southeast Asian | < 0.1% |
| ● Broadly East Asian | 0.5% |
| ● Broadly East Asian & Native American | 6.8% |
| **Sub-Saharan African** | **5.2%** |
| ● West African | 4.5% |
| ● East African | < 0.1% |
| ● African Hunter-Gatherer | < 0.1% |
| ● Broadly Sub-Saharan African | 0.6% |
| **Western Asian & North African** | **1.3%** |
| ● North African & Arabian | 1.0% |
| ● Broadly Western Asian & North African | 0.3% |
| **Unassigned** | **4.4%** |

See all 150+ populations

# The challenge: Applying Law to Technology

- It must be part of the design and use of a technology.
- In most countries, legal privacy protection starts with just data security.
- Consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security.

# GDPR & Cybersecurity

The GDPR introduction a new era of ransomware:
**double extortion ransomware**

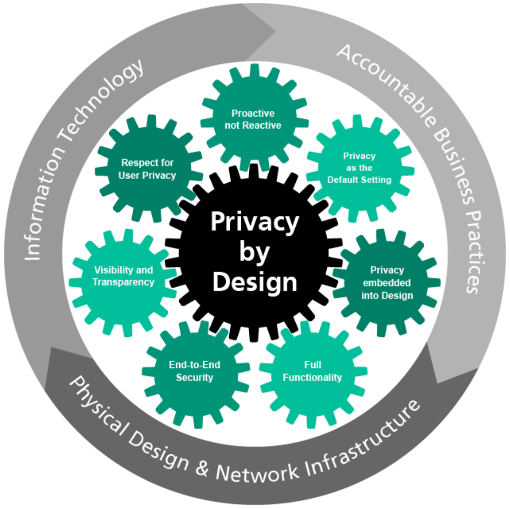
=

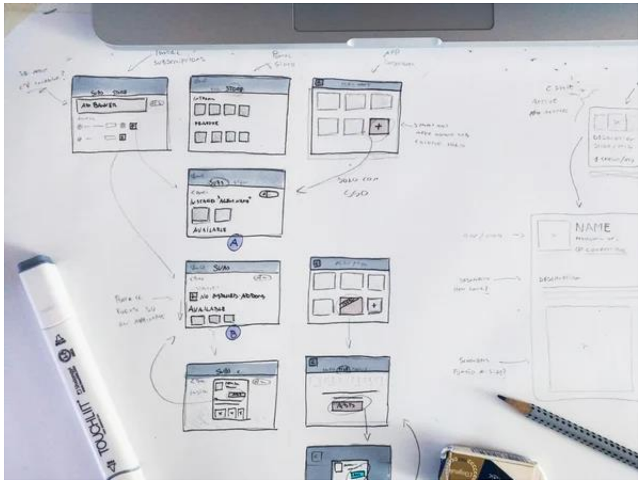
First threat = Data stolen

Second threat = Disclosure of confidential data

# GDPR & Cybersecurity

```
{"_id":{"$oid":"5e942345a37862b0f0ab5e40"},"content":"
All your data is a backed up. You must pay 0.015 BTC
to 1jAzyxPREckuUPwifEbiUKgDfE5racmph 48 hours for
recover it. After 48 hours expiration we will leaked
and exposed all your data. Also do not forget about
GDPR. You can buy bitcoin here, does not take much
time to buy https://localbitcoins.com with this guide
https://localbitcoins.com/guides/how-tobuy-bitcoins
After paying write to me in the mail with your DB IP :
g3t_base@protonmail.com"}
```


Information Technology
Accountable Business Practices
Physical Design & Network Infrastructure
Privacy by Design
Proactive not Reactive
Privacy as the Default Setting
Privacy embedded into Design
Full Functionality
End-to-End Security
Visibility and Transparency
Respect for User Privacy



# THE 7 FOUNDATIONAL PRINCIPLES

# Concept

- Privacy by Design concept was initially introduced by joint team of the Information and Privacy Commissioner of Ontario in Canada and Netherlands Organisation for Applied Scientific Research.

- The GDPR regulation active since 25 May 2018 integrates Privacy by Design concepts.

European Commission

GDPR
General Data
Protection Regulation

# Introduction - Privacy by Design

*Privacy By Design by Dr. Ann Cavoukian; Founder of the Privacy by Design concepts as we know it today*

# 1 - Proactive not Reactive; Preventative not Remedial

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to prevent them from occurring. In short, Privacy by Design comes *before-the-fact*, not after.

# 2 - Privacy as the Default Setting

We can all be certain of one thing - the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy - it is built into the system, by default.

# 3 - Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality

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

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

# 5 - End-to-End Security - Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved - strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

# 6 - Visibility and Transparency - Keep it Open

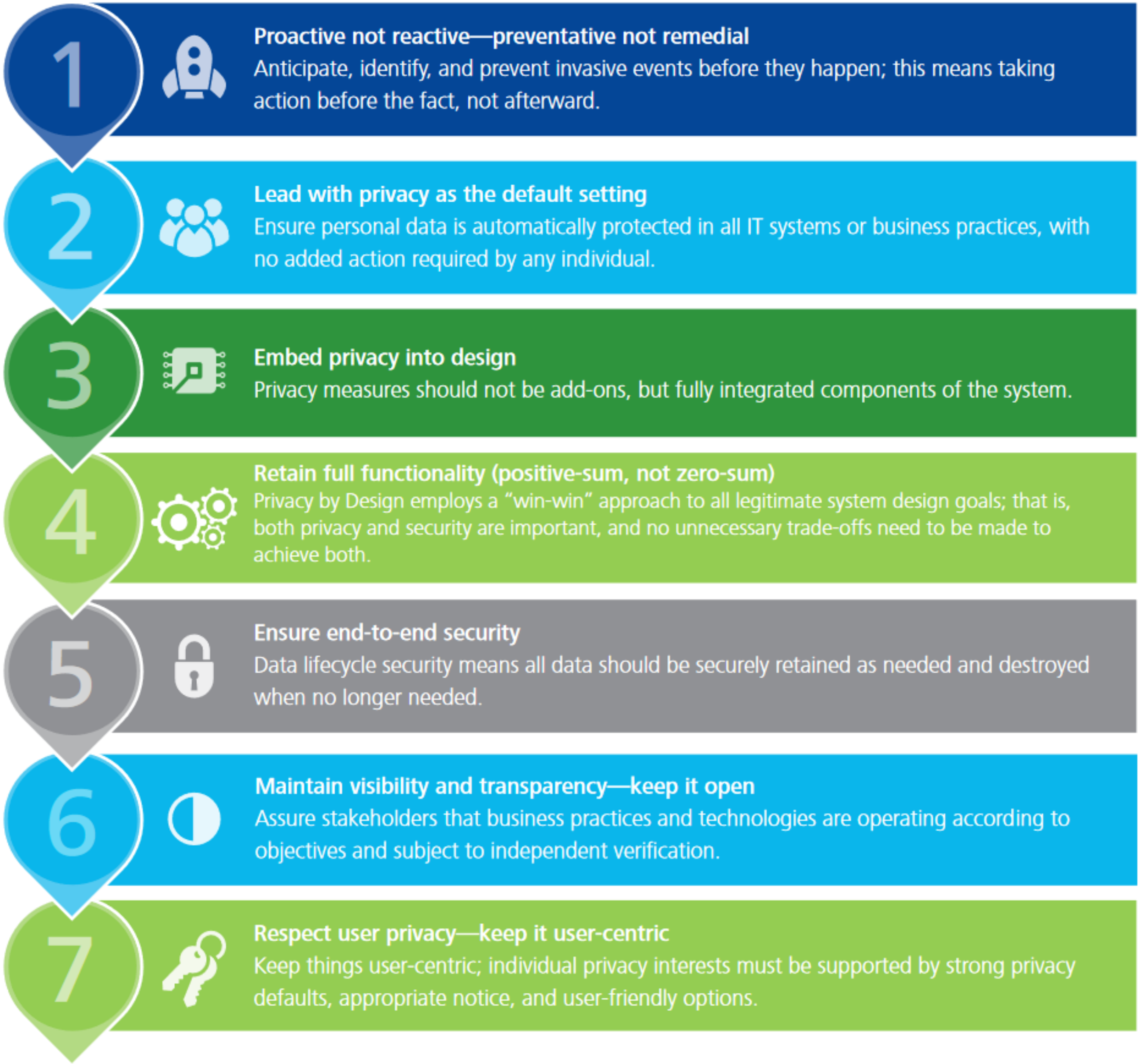
Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

# 7 - Respect for User Privacy - Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

# The 7 Foundational Principles

# Overview



1 **Proactive not reactive—preventative not remedial**
Anticipate, identify, and prevent invasive events before they happen; this means taking action before the fact, not afterward.

2 **Lead with privacy as the default setting**
Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.

3 **Embed privacy into design**
Privacy measures should not be add-ons, but fully integrated components of the system.

4 **Retain full functionality (positive-sum, not zero-sum)**
Privacy by Design employs a "win-win" approach to all legitimate system design goals; that is, both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.

5 **Ensure end-to-end security**
Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed.

6 **Maintain visibility and transparency—keep it open**
Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification.

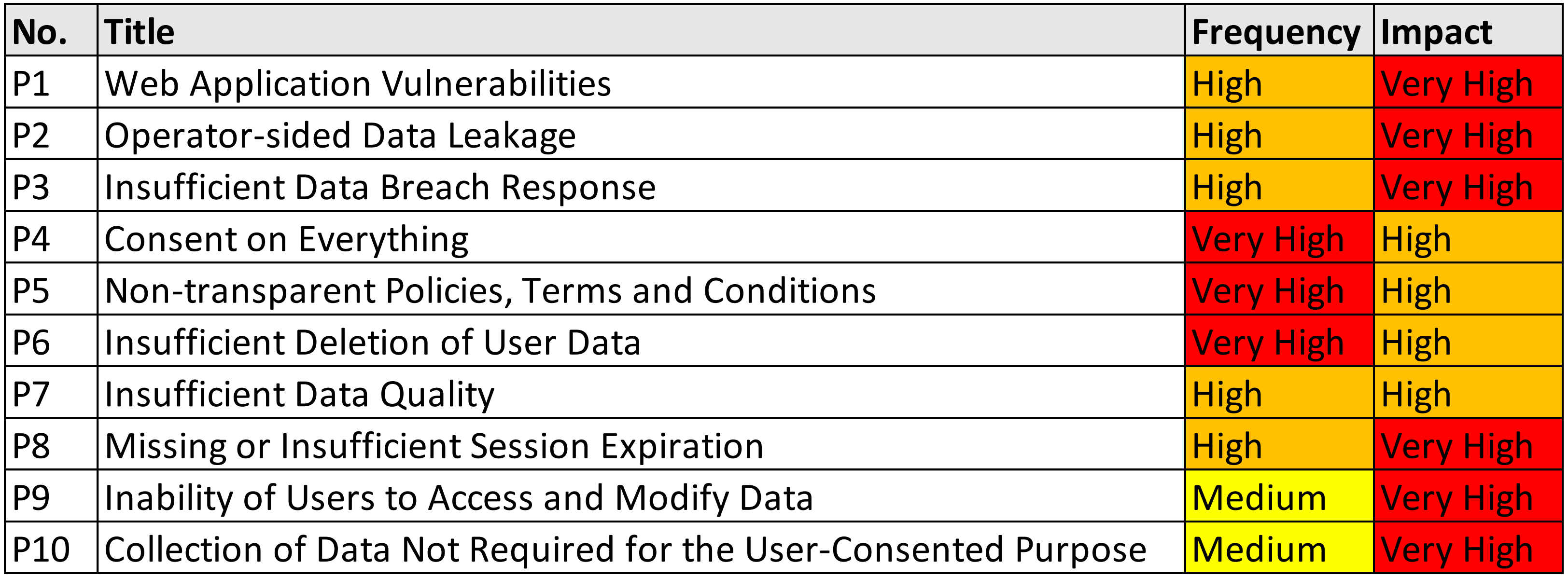
7 **Respect user privacy—keep it user-centric**
Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

*Privacy by Design Setting a new standard  for privacy certification, Deloitte*

# PRIVACY RISKS

# Top 10 Privacy Risks

- The OWASP foundation provides a Top 10 Privacy Risks list.



| No. | Title | Frequency | Impact |
|---|---|---|---|
| P1 | Web Application Vulnerabilities | High | Very High |
| P2 | Operator-sided Data Leakage | High | Very High |
| P3 | Insufficient Data Breach Response | High | Very High |
| P4 | Consent on Everything | Very High | High |
| P5 | Non-transparent Policies, Terms and Conditions | Very High | High |
| P6 | Insufficient Deletion of User Data | Very High | High |
| P7 | Insufficient Data Quality | High | High |
| P8 | Missing or Insufficient Session Expiration | High | Very High |
| P9 | Inability of Users to Access and Modify Data | Medium | Very High |
| P10 | Collection of Data Not Required for the User-Consented Purpose | Medium | Very High |

# Links

- https://www.ipc.on.ca/
- https://owasp.org/www-project-top-10-privacy-risks/
- https://docs.microsoft.com/en-us/previous-versions/windows/desktop/cc307403(v=msdn.10)?redirectedfrom=MSDN
- https://arxiv.org/ftp/arxiv/papers/1512/1512.06000.pdf
- https://sphn.ch/network/data-coordination-center/de-identification/
- https://www.nist.gov/privacy-framework/resource-repository/browse/guidelines-and-tools