

# **RSA**Conference2022

San Francisco & Digital | June 6 – 9

SESSION ID: DSO-R01

## **Top 10 Privacy Risks in Web Applications**

**Florian Stahl**

Senior Manager / Project Leader  
msg security advisors / OWASP

<https://owasp.org/www-project-top-10-privacy-risks/>

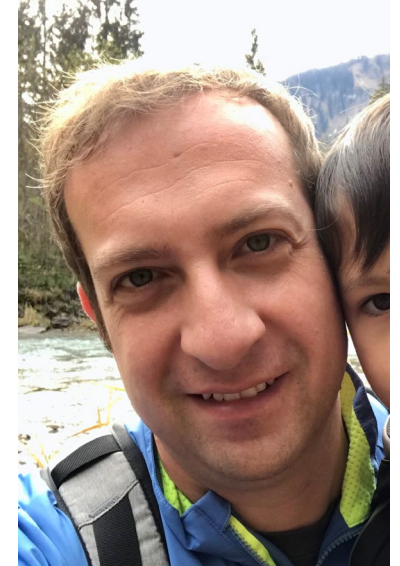
***TRANSFORM***



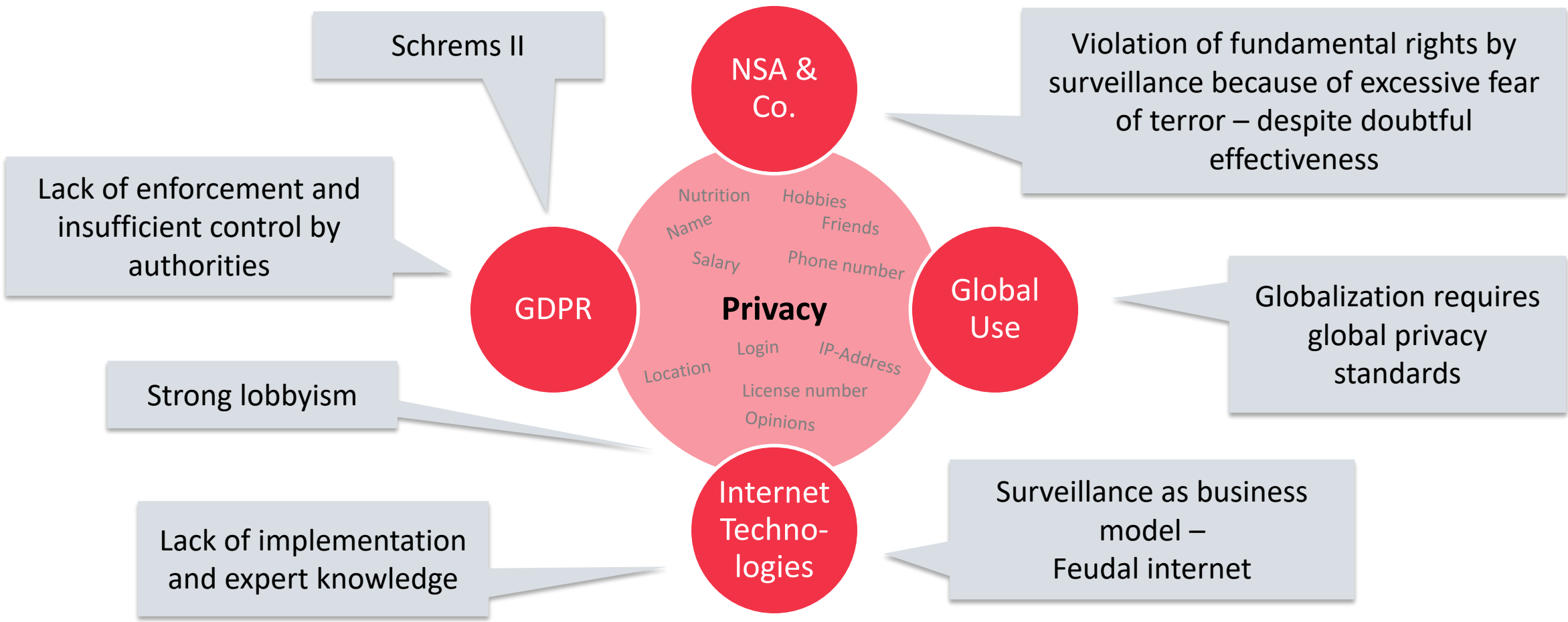
# About me

## Florian Stahl

- Principal Consultant / Senior Manager @ msg Security Advisors (Munich, Germany)
- MSc, CISSP, CISM, CIPT
- 15 years of experience in information security & privacy (from pentester to team manager)
- Founder and Leader of the OWASP Top 10 Privacy Risks Project
- Hobbies: Family, tennis, snowboarding, travelling
- [florian.stahl@owasp.org](mailto:florian.stahl@owasp.org)



# Situation



# OWASP Top 10 Privacy Risks Project – Facts & Figures

- 2014 Foundation & Publication of version 1.0
- 2015 Member of IPEN (Internet Privacy Engineering Network)
- 2016 Publication of countermeasures
- 2021 Publication of version 2.0
- 2022 Updated countermeasures v2.0
- Available in 5 languages (soon in 7)
- OWASP Lab Project

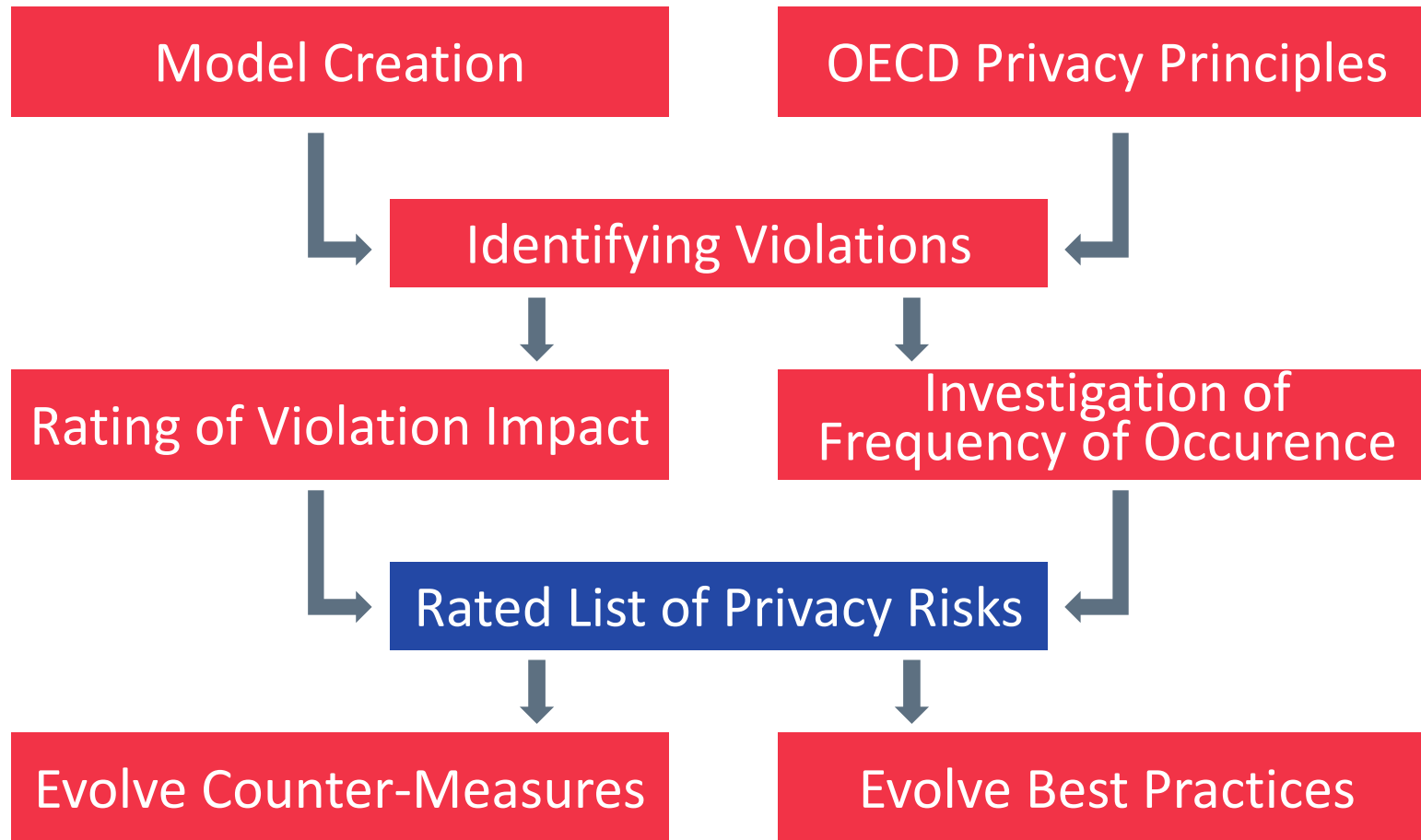


# Project Goal

- Identify the 10 most important **technical and organizational** privacy risks for web applications
- Provide transparency about privacy risks (legal, reputational, financial, but also risks for freedom)
- Independent from “local” laws based on OECD Privacy Principles
- Show countermeasures
- Educate developers, business architects and legal
- Not in scope: Self-protection for users

1. Limitation of Collection
2. Data Quality
3. Specification of the Purpose
4. Use Limitation
5. Security
6. Transparency
7. Individual Participation
8. Accountability

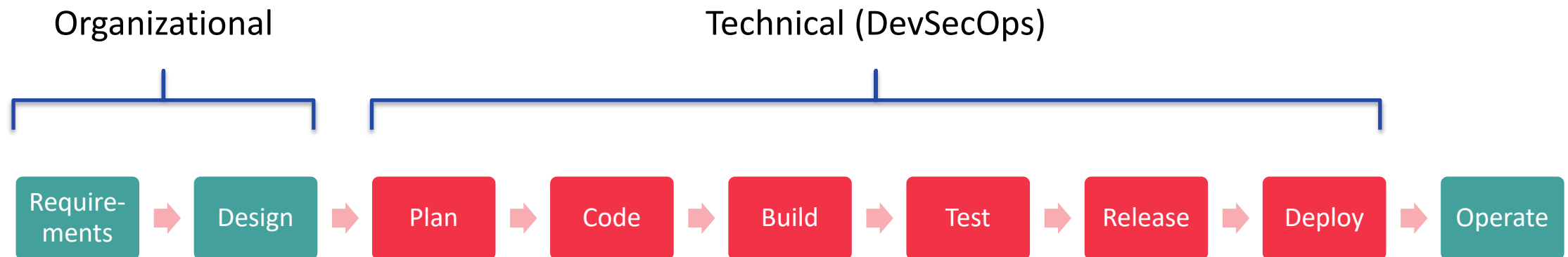
# Project Method





# Privacy in DevSecOps

- Privacy is everyone's problem and split into organizational and technical topics
- Some decisions must be taken before DevSecOps – or maybe DevPrivOps?
- Split responsibilities make privacy challenging (legal, architects, developers)
- Establish a process to consider privacy from the product idea to its deployment



# Results Overview



## 2021 OWASP Top 10 Privacy Risks

2021	2014	Privacy Risks	Frequency	Impact	Type
1	1	⇒ Web application vulnerabilities	High	Very high	T
2	2	⇒ Operator-sided data leakage	High	Very high	O+T
3	3	⇒ Insufficient data breach response	High	Very high	O+T
4	New	☒ Consent on everything	Very high	High	O+T
5	5	⇒ Non-transparent Policies, Terms and Conditions	Very high	High	O
6	4	⚡ Insufficient deletion of personal data	High	High	O+T
7	New	☒ Insufficient data quality	Medium	High	O+T
8	9	↗ Missing or insufficient session expiration	Medium	Very high	T
9	13	↗ Inability of users to access and modify data	High	Very high	O+T
10	6	⚡ Collection of data not required for the user-consented purpose	High	High	O

Type O: Organizational, T: Technical



# P1: Web Application Vulnerabilities

**Explanation:** 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.

## Risk Mitigation:

- Train developers regarding web application security
- Apply secure coding guidelines
- Perform security source code scans (SAST, DAST) and penetration tests (e.g. based on OWASP Top 10)
- Use up-to-date software libraries (server, DB, libs)?
- Install updates, patches and hotfixes on a regular basis (application, server, DB, etc)
- Don't forget to secure test data if it contains (real) personal data



## P2: Operator-sided Data Leakage

**Explanation:** Failure to prevent the leakage of any information containing or related to user data, or the data itself, to any unauthorized party resulting in loss of data confidentiality. Introduced either due to intentional malicious breach or unintentional mistake.

### Risk Mitigation:

- Request appropriate security controls from your operator like Awareness campaigns, Encryption of personal data, Identity & Access Management, strong Anonymization or Pseudonymization, etc.
- Assess and/or audit the operator (before signing the contract or using it):
  - Research the reputation and reliability of the operator
  - Request self-assessment or perform on-site audit
  - Request certification like ISO 27001, SOC2 Report, Cloud Provider Security Assessment



# P3: Insufficient Data Breach Response

**Explanation:** Not informing the affected persons (users) about a possible breach or data leak, resulting either from intentional or unintentional events; failure to remedy the situation by fixing the cause; not attempting to limit the leaks.

## Risk Mitigation:

- Create an Incident Response Plan including procedures to inform persons affected by a data breach
- Regularly test incident response procedures and establish a CERT (Computer Emergency Response Team)
- Maintain a Software BOM (Bill of Material) that includes release versions of all libraries in use
- Prepare for software updates and patching (e.g. document code, retain developer knowledge)
- Monitor for incidents / data leakage by connecting a SIEM (Security Information & Event Management) tool



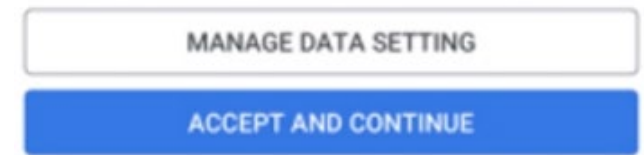
# P4: Consent on Everything \*New\*

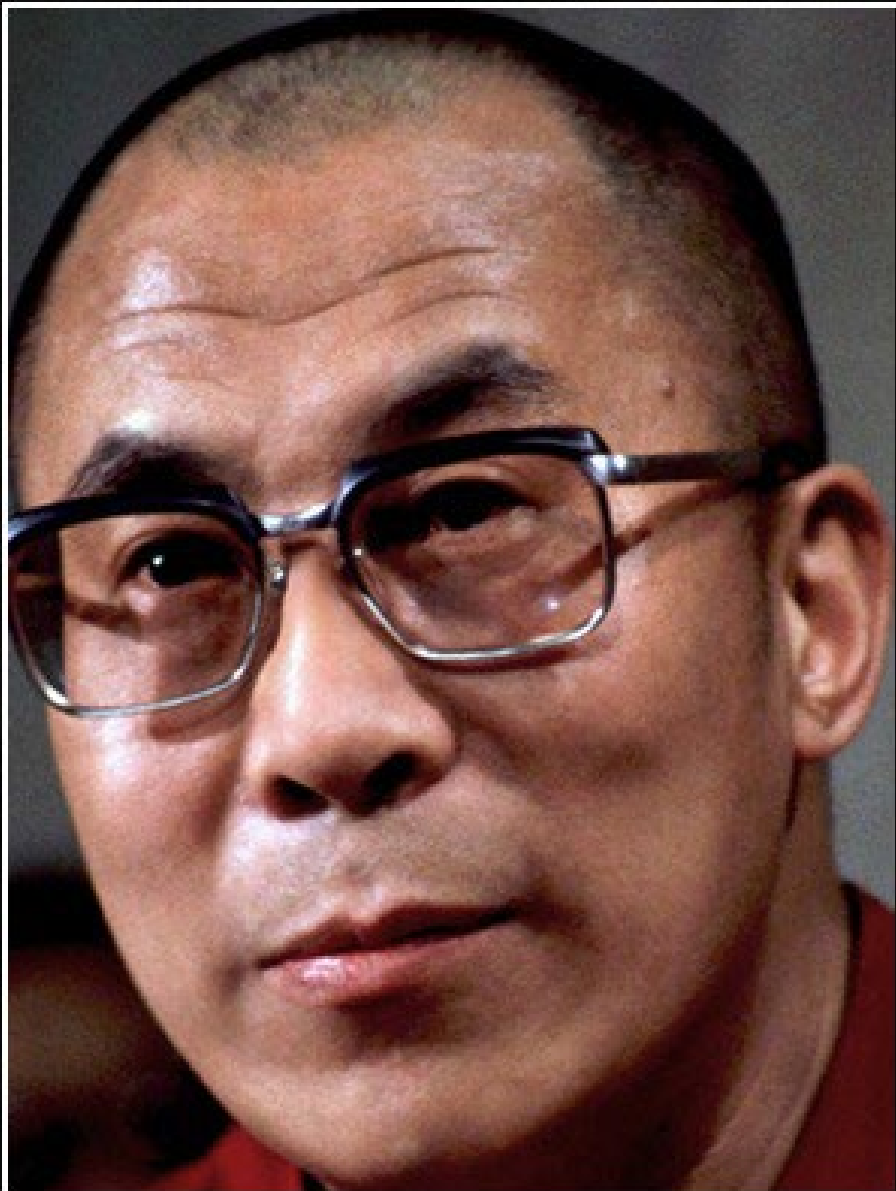
**Explanation:** Aggregation or inappropriate use of consent to legitimate processing of personal data. Consent is "on everything" and not collected separately for each purpose (e.g. use of website and profiling for advertising).

## Risk Mitigation:

- Collect consent separately for each purpose (e.g. different checkboxes for use of website and profiling for advertising).
- Consent must be traceable and audit-proof
- Consent should be voluntarily
- [Helen Nissenbaum on Post-Consent Privacy - YouTube](#)

**“Stop Thinking About Consent: It Isn’t Possible and It Isn’t Right”**





A lack of transparency results in  
distrust and a deep sense of  
insecurity.

— Dalai Lama —

AZ QUOTES

# P5: Non-transparent Policies, Terms & Conditions

**Explanation:** Not providing sufficient information to describing how user data is processed, such as its collection, storage, and processing. Failure to make this information easily-accessible and understandable for non-lawyers.

## Risk Mitigation:

- Policies, terms and conditions should be:
  - Easy to find and understandable for non-lawyers
  - Fully describe data processing (which data is collected, for what purpose, ...)
  - In the user's language
  - Complete, but KISS (Keep it short and simple)
- A short version of the T&Cs and pictograms can be used for easier understanding
- Use release notes to identify change history of T&Cs and policies/notices over time
- Deploy Do Not Track (W3C standard) and provide Opt-out





# P6: Insufficient Deletion of Personal Data

**Explanation:** Failure to effectively and/or timely delete personal data after termination of the specified purpose or upon request.

## Risk Mitigation:

- Consider data retention or deletion policies / agreements and evaluate their appropriateness
- Delete personal data after termination of specified purpose (1-6 months is good practice, consider retention periods)
- Implement option to delete data on rightful user request
- Design your application to also consider deletion of copies, backups and interfaces to third parties
- Delete user profiles after longer period of inactivity



# P7: Insufficient Data Quality \*New\*

**Explanation:** The use of outdated, incorrect or bogus user data. Failure to update or correct the data.

## Risk Mitigation:

- Perform integrity checks where appropriate
- Provide an update form or other ways for the user to update his/her data
- Ask user if his/her data is still correct (e.g. “Please verify your shipping address”)
- Forward updated data to third parties / subsystems that received the user’s data before
- Question how long it is likely that data is up to date and how often it usually changes
- Important note: This risk shows that data integrity is part of data privacy

**“Data integrity is even more important than data privacy”**

Toomas Ilves, Former President of Estonia at Munich Cyber Security Conference Spring Forum 2022




# P8: Missing or Insufficient Session Expiration

**Explanation:** Failure to effectively enforce session termination. May result in collection of additional user-data without the user's consent or awareness.

## Risk Mitigation:


- User sessions must be terminated automatically depending on the criticality of the application (e.g. banking vs. search engine)
- Option: Provide user-defined logout period after X hours / days
- Provide an obvious logout button (easy to find)
- Educate users

### Where You're Logged In

 Windows PC · Frankfurt, Germany  
Edge (Chromium Based) · **Active now**

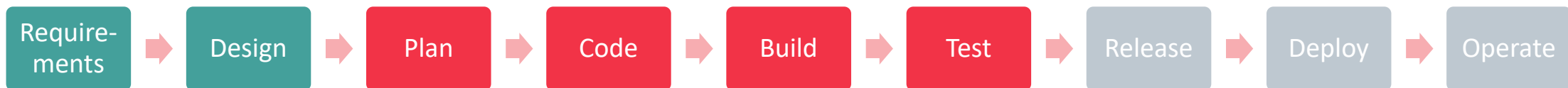
 iPhone · Landshut, Germany  
Mobile Safari · 19 hours ago

 iPhone · Regensburg, Germany  
Mobile Safari · August 2 at 8:54 PM

 iPhone · Bad Abbach, Germany  
Mobile Safari · July 31 at 8:22 PM

 iPhone · Munich, Germany  
Mobile Safari · July 29 at 8:28 PM

 iPhone · Weiden in der Oberpfalz, Germany  
Mobile Safari · July 26 at 5:45 AM



# P9: Inability of users to access and modify data

**Explanation:** Users do not have the ability to access, change or delete data related to them.

## Risk Mitigation:

- Provide easy-to-use ways to access, change or delete user data
- Design an appropriate data structure model to handle user rights
- This risk has some synergies / overlaps with P7 Insufficient Data Quality



# P10: Collection of data not required for the user-consented purpose

**Explanation:** Collecting descriptive, demographic or any other user-related data that are not needed for the purposes of the system. Applies also to data for which the user did not provide consent.

## Risk Mitigation:

- Define purpose of the collection
- Only collect personal data required to fulfill this purpose
- Notify and ask individuals if purpose or processing is changed
- Data minimization – only collect and store user data that is necessary
- Provide option to collect additional data voluntarily to improve service (e.g. product recommendation, personal advertisement)



# Apply What You Have Learned Today

- Next week you should:
  - Check the status of integration of privacy in your development processes
- In the first three months following this presentation you should:
  - Consult and integrate stakeholders (business, architects, legal) because privacy is not a technical-only topic
  - Identify gaps regarding privacy in your processes and products considering the OWASP Top 10 Privacy Risks
  - Check if the OWASP Top 10 Privacy Risks are mitigated by measures
- Within six months you should:
  - Address gaps and integrate privacy in your development process (Privacy by Design)
  - Train developers and apply privacy patterns and best practices to reduce risks



## Further information

- Project Website: <https://owasp.org/www-project-top-10-privacy-risks/>
- Countermeasures: <https://docs.google.com/document/d/1s6RLhyLi02-3LMOxC8IBQEGhVrqKT0QZYN1X4aBqSsM/>
- Privacy Design Pattern: <https://privacypatterns.eu/>
- [IPEN - Internet Privacy Engineering Network | European Data Protection Supervisor \(europa.eu\)](#)
- [GDPR developer's guide | CNIL](#)

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.