OWASP
Open Web Application
Security Project

# Top 10 Privacy Risks in Web Applications

**OWASP BeNeLux Day 2016**

18 March 2016, Luxemburg

Burgmair Stefan (Project member, msg systems, Germany)

# About me

**Burgmair Stefan**

- Master's degree in Information Systems and Management (Munich University of Applied Sciences, Germany)
- Consultant for Information Security at msg systems
- Founded the Top 10 Privacy Risks Project as part of my Master's Thesis together with Florian Stahl
- Stefan.Burgmair@msg-systems.com

.msg

OWASP
Open Web Application
Security Project

# Agenda

1. Situation
2. Project
3. Countermeasures
4. Summary

# What privacy is about

Privacy risks are related to personal data.

It is not only about Security, but also: *

- A Limitation of Collection
- Data Quality
- Specification of the Purpose
- Use Limitation
- Transparency
- Individual Participation

A privacy risk is a violation of these OECD Guidelines.

OWASP Open Web Application Security Project

* According to the OECD Guidelines on the Protection of Privacy

# Recent developments

- EU-General Data Protection Regulation aims for formal adoption in early 2016
- Privacy by Design will be legally required
  - "Privacy by Design is an approach to systems engineering which takes privacy into account throughout the whole engineering process"
- But what should be done e.g. in a Web-Application?

OWASP
Open Web Application Security Project

* Source of picture:
https://en.wikipedia.org/wiki/Software_development_process

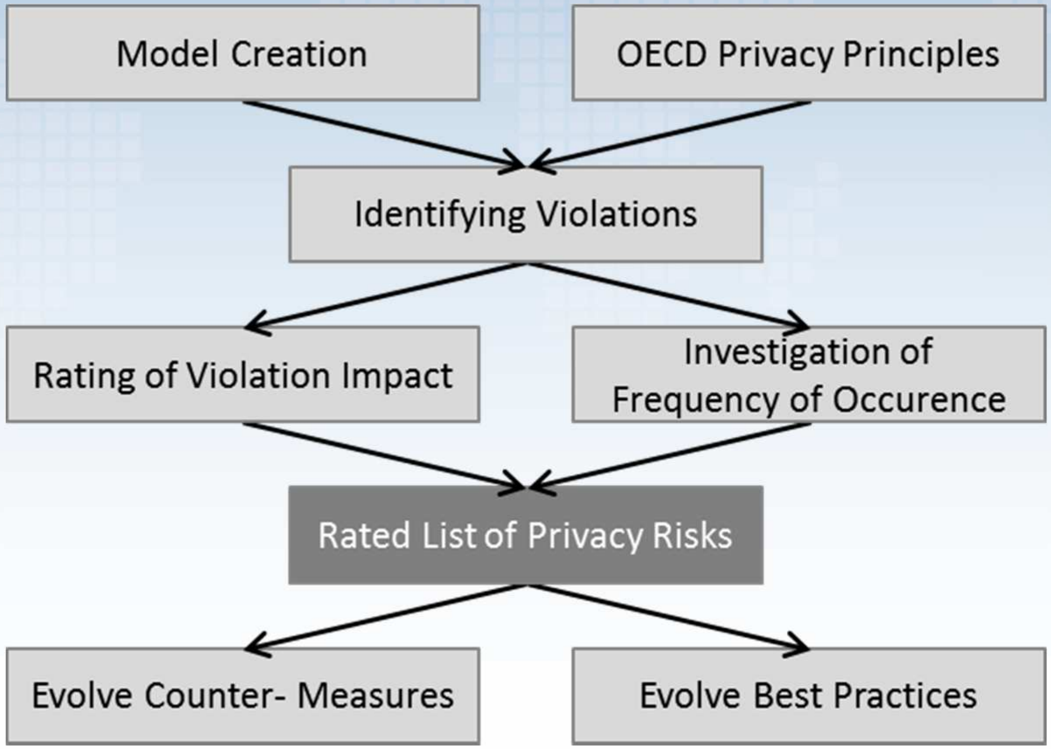
# Project Goal

- Identify the most important technical and organizational privacy risks for web applications
- Independent from local laws based on OECD Privacy Principles
- Focus on real-life risks for
  - User (data subject)
  - Provider (data owner)
- Help developers, business architects and legal to reach a common understanding of web application privacy
- Provide transparency about privacy risks
- Not in scope: Self-protection for users

OWASP
Open Web Application Security Project

# Project Method

Approach of the project:



Model Creation

OECD Privacy Principles

Identifying Violations

Rating of Violation Impact

Investigation of Frequency of Occurence

Rated List of Privacy Risks

Evolve Counter- Measures

Evolve Best Practices

OWASP Open Web Application Security Project

# Results: Top 10 Privacy Risks

P1 Web Application Vulnerabilities

P2 Operator-sided Data Leakage

P3 Insufficient Data Breach Response

P4 Insufficient Deletion of personal data

P5 Non-transparent Policies, Terms and Conditions

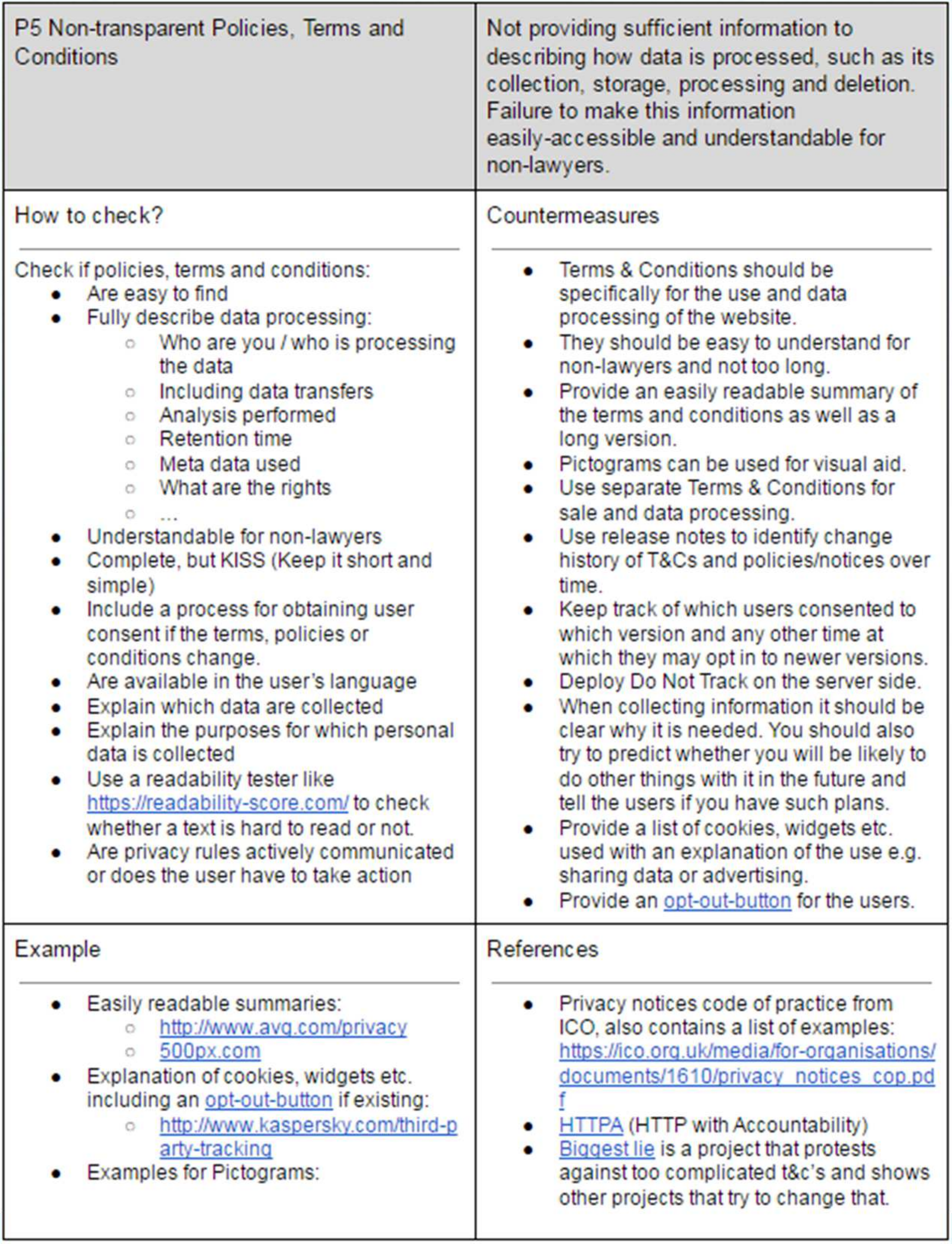
P6 Collection of data not required for the primary purpose

P7 Sharing of data with third party

P8 Outdated personal data

P9 Missing or Insufficient Session Expiration

P10 Insecure Data Transfer



| P5 Non-transparent Policies, Terms and Conditions | Not providing sufficient information to describing how data is processed, such as its collection, storage, processing and deletion. Failure to make this information easily-accessible and understandable for non-lawyers. |
|---|---|
| How to check?<br>Check if policies, terms and conditions:<br>• Are easy to find<br>• Fully describe data processing:<br>○ Who are you / who is processing the data<br>○ Including data transfers<br>○ Analysis performed<br>○ Retention time<br>○ Meta data used<br>○ What are the rights<br>○ ...<br>• Understandable for non-lawyers<br>• Complete, but KISS (Keep it short and simple)<br>• Include a process for obtaining user consent if the terms, policies or conditions change.<br>• Are available in the user's language<br>• Explain which data are collected<br>• Explain the purposes for which personal data is collected<br>• Use a readability tester like https://readability-score.com/ to check whether a text is hard to read or not.<br>• Are privacy rules actively communicated or does the user have to take action | Countermeasures<br>• Terms & Conditions should be specifically for the use and data processing of the website.<br>• They should be easy to understand for non-lawyers and not too long.<br>• Provide an easily readable summary of the terms and conditions as well as a long version.<br>• Pictograms can be used for visual aid.<br>• Use separate Terms & Conditions for sale and data processing.<br>• Use release notes to identify change history of T&Cs and policies/notices over time.<br>• Keep track of which users consented to which version and any other time at which they may opt in to newer versions.<br>• Deploy Do Not Track on the server side.<br>• When collecting information it should be clear why it is needed. You should also try to predict whether you will be likely to do other things with it in the future and tell the users if you have such plans.<br>• Provide a list of cookies, widgets etc. used with an explanation of the use e.g. sharing data or advertising.<br>• Provide an opt-out-button for the users. |
| Example<br>• Easily readable summaries:<br>○ http://www.avg.com/privacy<br>○ 500px.com<br>• Explanation of cookies, widgets etc. including an opt-out-button if existing:<br>○ http://www.kaspersky.com/third-party-tracking<br>• Examples for Pictograms: | References<br>• Privacy notices code of practice from ICO, also contains a list of examples: https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf<br>• HTTPA (HTTP with Accountability)<br>• Biggest lie is a project that protests against too complicated t&c's and shows other projects that try to change that. |

OWASP
Open Web Application Security Project

# Results: Top 10 Privacy Risks

P1 Web Application Vulnerabilities

**P2 Operator-sided Data Leakage**

P3 Insufficient Data Breach Response

P4 Insufficient Deletion of personal data

**P5 Non-transparent Policies, Terms and Conditions**

P6 Collection of data not required for the primary purpose

**P7 Sharing of data with third party**

P8 Outdated personal data

**P9 Missing or Insufficient Session Expiration**

P10 Insecure Data Transfer

# P2: Operator-sided Data Leakage

How to check:

- Is the provider certified according to ISO 27001 or ISO 27018?
- Have there been former breaches to the operator?
- Do an Audit of the Operator
  - Are privacy best practices in place?
  - Is awareness training mandatory for all employees?
  - How is personal data anonymized?
  - Is personal data encrypted?
  - Who has access to the data (Needtoknowprinciple)?

# P2: Operator-sided Data Leakage

Internal procedures or staff are often a reason for data leakage

- Identity and Access management (physical and logical)
- Lack of awareness and procedures
  - Awareness campaigns
  - Establishing security protocols, policies and procedures for handling sensitive information
- Unnecessary Copies of Personal Data
  - Implement a restrictive data access management for staff and externals
  - Implement a data retention and deletion management
  - Data Leakage Prevention (DLP) solutions

# P2: Operator-sided Data Leakage

Another Issue: Anonymization of personal data

- Used for publication, research or usage inside and outside the operators organization
  - e.g. “We are using anonymized data for marketing purposes”
- Various types of data can be used to identify people
  - Through background knowledge and comparison tables
  - An unique identifier based on e.g. location data or device configuration
  - 87 % of the US-citizens (216 million of 248 million) are uniquely identifiable according to their {5-digit ZIP-code, gender, date of birth} *
- Anonymization is <u>not trivial</u> and can be breached under specific circumstances
  - e.g. AOL search data leak

- Example: Social Networks
  - Do you know this person?
  - Have you studied here?
  - Do you life here?

OWASP
Open Web Application Security Project

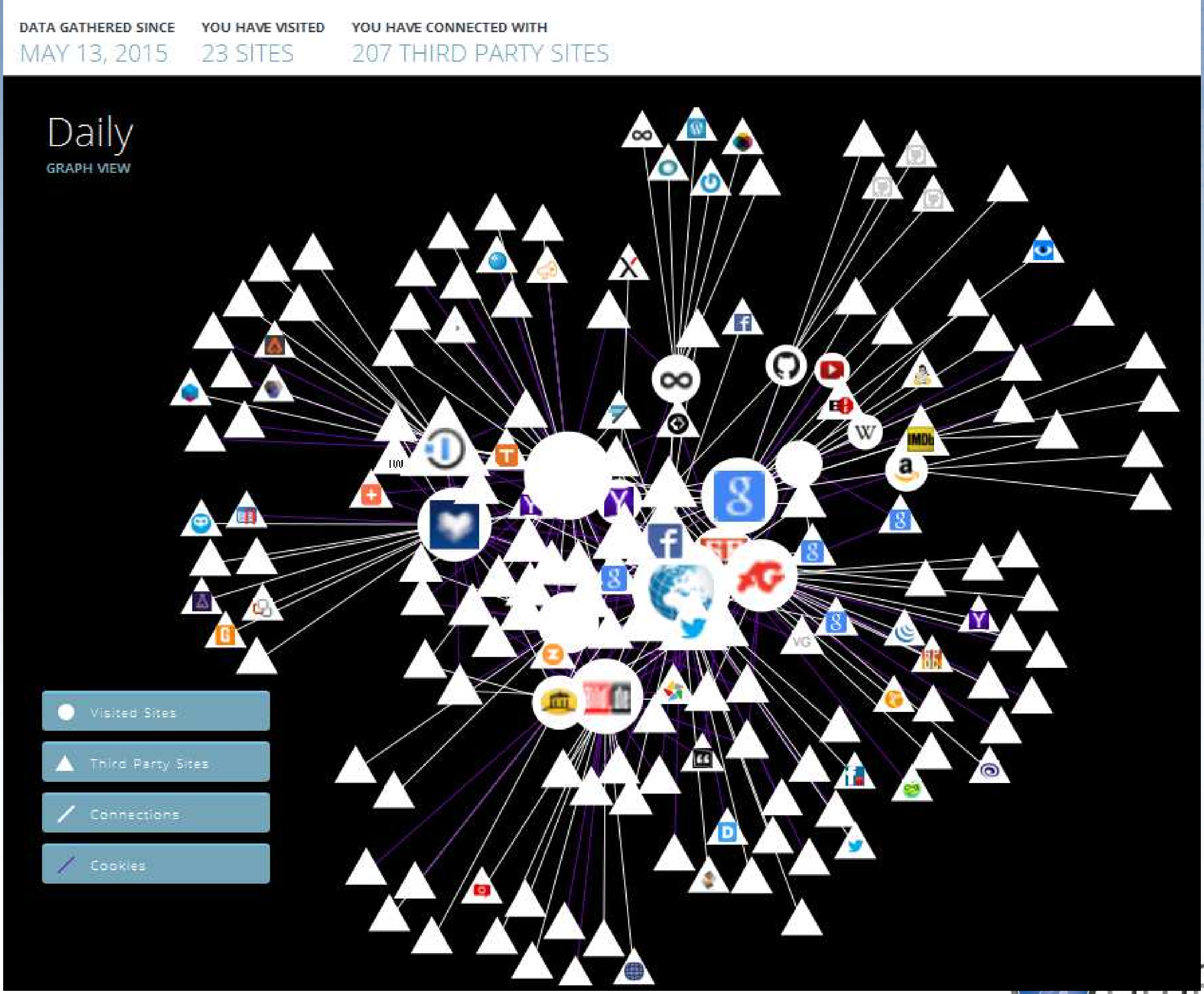
# P7: Sharing of Data with 3rd Party

Third Parties:

- Advertisers, Subcontractors, Social networks, etc.
- Used for Analytics, Video integration, Maps, Recommendation Button, etc.

Problems:

- Data is transferred or sold to third parties without user's knowledge and consent
- Complete loss of control



DATA GATHERED SINCE
MAY 13, 2015

YOU HAVE VISITED
23 SITES

YOU HAVE CONNECTED WITH
207 THIRD PARTY SITES

* Picture source: LightBeam (Addon for Firefox)

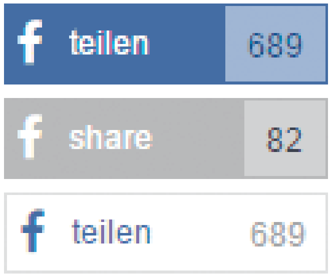
# P7: Sharing of Data with 3rd Party

## How can I identify whether I need to take action:

- Can you provide a list of all third parties in use?
- Is there a contract with those third parties ?
- Is privacy and handling of personal data part of it?

## What can be done:

- Third party services should not be used per default if it is not required (e.g.: shariff for social network buttons[1])
- Masking of data before transfer if possible
- Development of a Third Party Monitoring Strategy:
  - Gateway release for third party content (whitelist or blacklist)
  - Contractual arrangements regarding Policies, Data usage, …
  - Monitoring of user complaints



[1] https://github.com/heiseonline/shariff

* Picture source: heise.de

# P5: Non-transparent Policies, Terms & Conditions

Problems:

- Privacy Policies, Terms & Conditions are not up-to-date, inaccurate, incomplete or hard to find
- Data processing is not explained sufficiently
- They do not support rational decision making
- Conditions are too long and users do not read them
- A study asserts that it would require 244 hours / year to read the online privacy policies of every visited website[1]

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

[1] from The Cost of Reading Privacy Policies A. McDonald, L. Cranor

* Picture source: BiggestLie.com

# P5: Non-transparent Policies, Terms & Conditions

## How to check

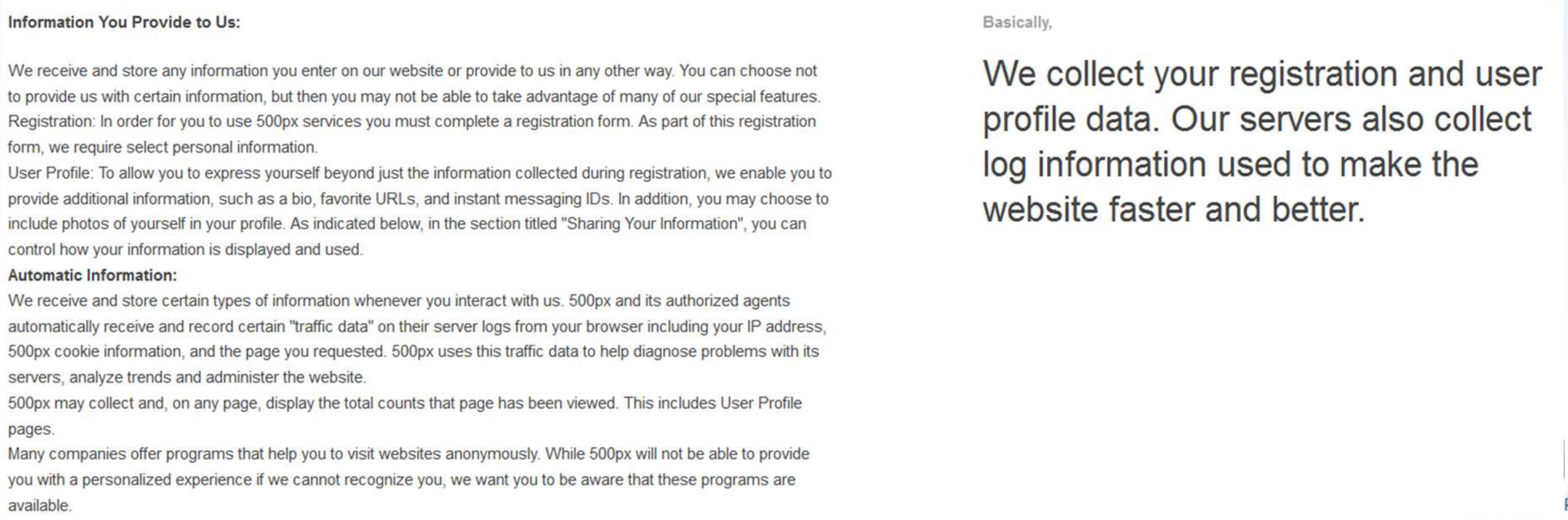
- Is the purposes for which personal data is collected explained so a non-lawyer can understand them
- Use a readability tester
- Are privacy rules actively communicated or does the user have to take action
- Is Do Not Track deployed on the server side

* Picture source: https://500px.com/privacy

# P5: Non-transparent Policies, Terms & Conditions

## Countermeasures

- Point out where to find the privacy related policies
- Add succinct and understandable summaries of legal paragraphs
- Use pictograms for visual aid



**Information You Provide to Us:**

We receive and store any information you enter on our website or provide to us in any other way. You can choose not to provide us with certain information, but then you may not be able to take advantage of many of our special features.
Registration: In order for you to use 500px services you must complete a registration form. As part of this registration form, we require select personal information.
User Profile: To allow you to express yourself beyond just the information collected during registration, we enable you to provide additional information, such as a bio, favorite URLs, and instant messaging IDs. In addition, you may choose to include photos of yourself in your profile. As indicated below, in the section titled "Sharing Your Information", you can control how your information is displayed and used.

**Automatic Information:**

We receive and store certain types of information whenever you interact with us. 500px and its authorized agents automatically receive and record certain "traffic data" on their server logs from your browser including your IP address, 500px cookie information, and the page you requested. 500px uses this traffic data to help diagnose problems with its servers, analyze trends and administer the website.
500px may collect and, on any page, display the total counts that page has been viewed. This includes User Profile pages.
Many companies offer programs that help you to visit websites anonymously. While 500px will not be able to provide you with a personalized experience if we cannot recognize you, we want you to be aware that these programs are available.

Basically,

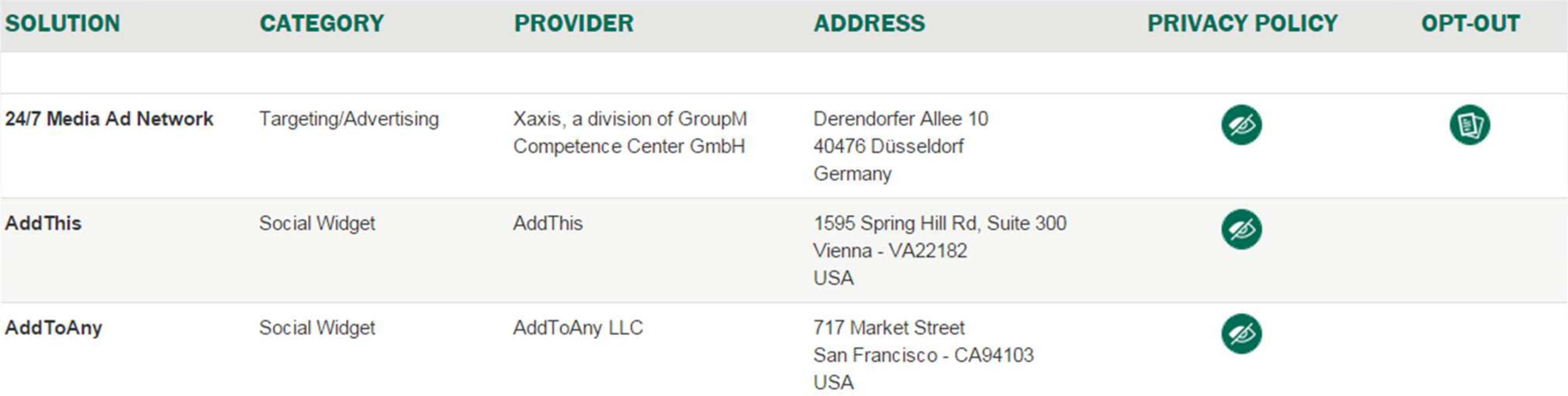
We collect your registration and user profile data. Our servers also collect log information used to make the website faster and better.

* Picture source: https://500px.com/privacy

# P5: Non-transparent Policies, Terms & Conditions

## Countermeasures

- Update of the conditions together with changes of functions
  - Keep track of which user gave consent to which version
- Make the conditions available in every relevant language
- Provide transparency about third parties:



| SOLUTION | CATEGORY | PROVIDER | ADDRESS | PRIVACY POLICY | OPT-OUT |
|---|---|---|---|---|---|
| **24/7 Media Ad Network** | Targeting/Advertising | Xaxis, a division of GroupM Competence Center GmbH | Derendorfer Allee 10<br>40476 Düsseldorf<br>Germany | ● | ● |
| **AddThis** | Social Widget | AddThis | 1595 Spring Hill Rd, Suite 300<br>Vienna - VA22182<br>USA | ● | |
| **AddToAny** | Social Widget | AddToAny LLC | 717 Market Street<br>San Francisco - CA94103<br>USA | ● | |

* Picture source: http://www.kaspersky.com/third-party-tracking

# P9: Missing or Insufficient Session Expiration

Session Expiration is not only a security topic but influences privacy and user experience

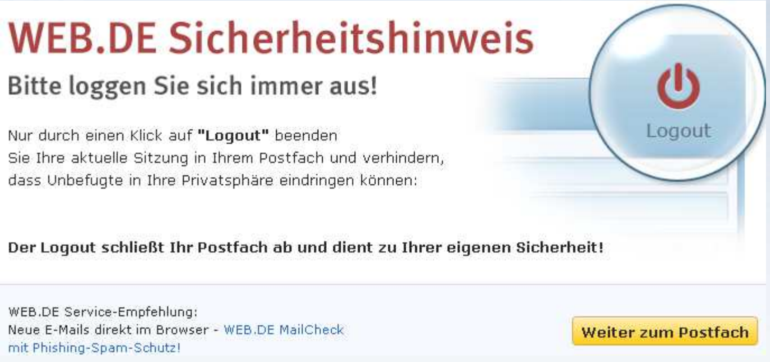
- Users are not aware about the collection of their data
- Missing logout might raise security issues

Some companies try to track the user behavior as long as possible

# P9: Missing or Insufficient Session Expiration

## How to check:

- Is it obvious whether the user is currently logged in?
- Is the logout button highly visible?



WEB.DE Sicherheitshinweis

Bitte loggen Sie sich immer aus!

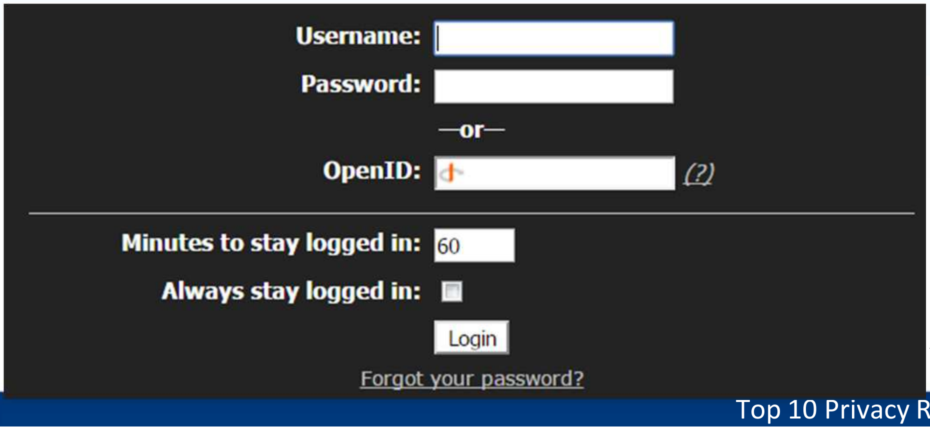
Nur durch einen Klick auf **"Logout"** beenden Sie Ihre aktuelle Sitzung in Ihrem Postfach und verhindern, dass Unbefugte in Ihre Privatsphäre eindringen können:

**Der Logout schließt Ihr Postfach ab und dient zu Ihrer eigenen Sicherheit!**

WEB.DE Service-Empfehlung:
Neue E-Mails direkt im Browser - WEB.DE MailCheck mit Phishing-Spam-Schutz!

## Countermeasures:

- Usage of reasonable session timeouts
- Generate a reminding message in case a user did not log out



| | |
|---|---|
| **Username:** | |
| **Password:** | |
| | —or— |
| **OpenID:** | (?) |
| **Minutes to stay logged in:** | 60 |
| **Always stay logged in:** | □ |

sources: enigmagroup.org, web.de

# Summary

- Privacy in many web applications should be improved
- Lack of awareness regarding privacy risks
- No practical guidance on how to avoid privacy risks so far
- OWASP Top 10 Privacy Risks project created to address those issues and educate developers and lawyers
- The project identifies technical and organizational risks independent from local laws
- Try to consider these risks when implementing or auditing web applications and apply countermeasures!

OWASP
Open Web Application Security Project

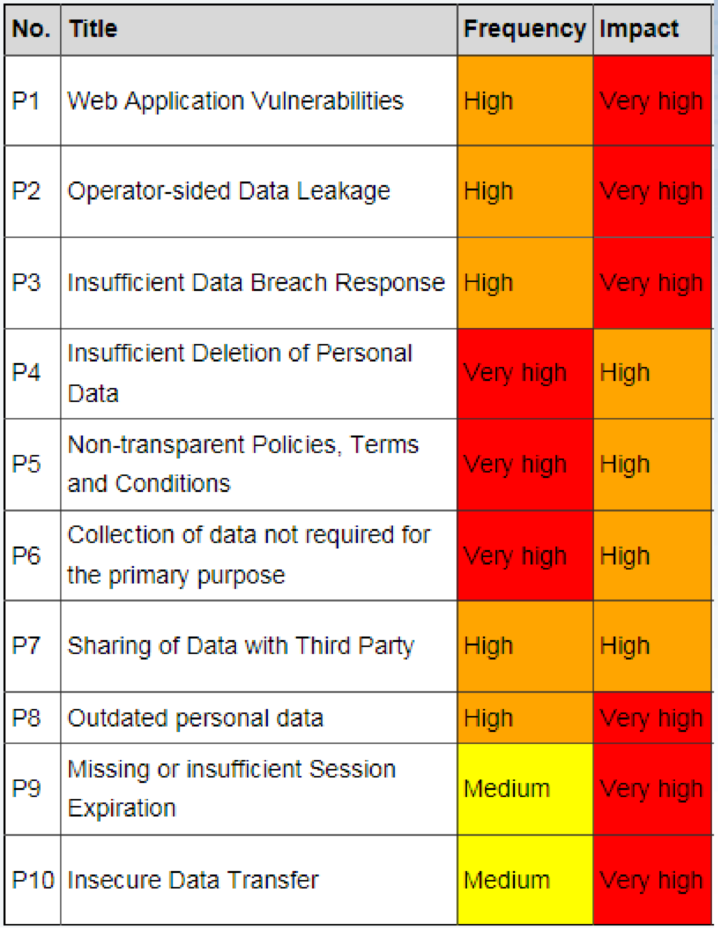
# Further information

- OWASP Top 10 Privacy Risks Project: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

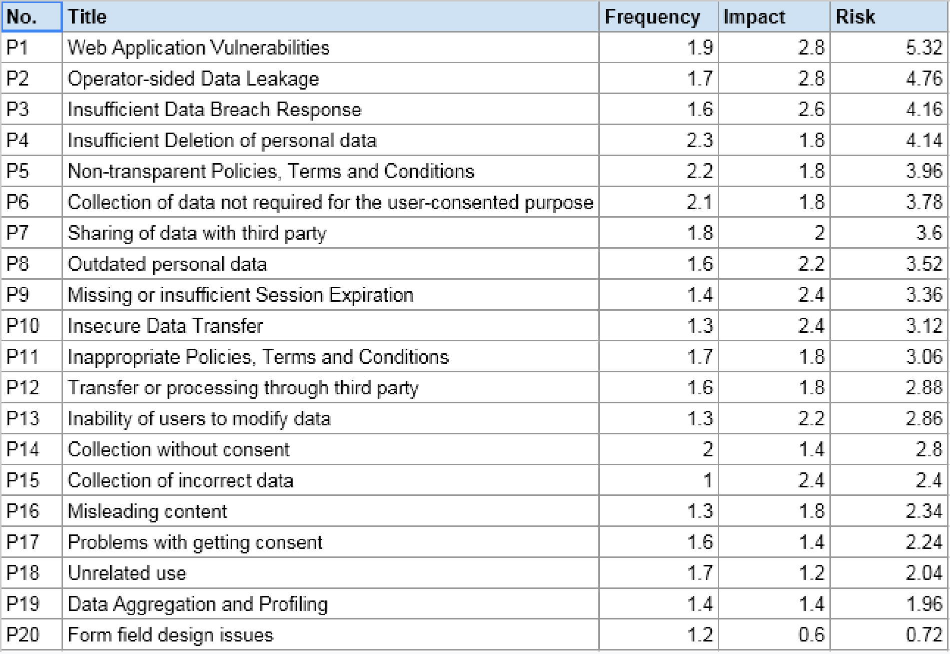
  → Feel free to contribute

- Internet Privacy Engineering Network (IPEN): https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN
- Project sponsor: http://www.msg-systems.com

# Results in detail



| 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 | Insufficient Deletion of Personal Data | Very high | High |
| P5 | Non-transparent Policies, Terms and Conditions | Very high | High |
| P6 | Collection of data not required for the primary purpose | Very high | High |
| P7 | Sharing of Data with Third Party | High | High |
| P8 | Outdated personal data | High | Very high |
| P9 | Missing or insufficient Session Expiration | Medium | Very high |
| P10 | Insecure Data Transfer | Medium | Very high |



| No. | Title | Frequency | Impact | Risk |
|---|---|---|---|---|
| P1 | Web Application Vulnerabilities | 1.9 | 2.8 | 5.32 |
| P2 | Operator-sided Data Leakage | 1.7 | 2.8 | 4.76 |
| P3 | Insufficient Data Breach Response | 1.6 | 2.6 | 4.16 |
| P4 | Insufficient Deletion of personal data | 2.3 | 1.8 | 4.14 |
| P5 | Non-transparent Policies, Terms and Conditions | 2.2 | 1.8 | 3.96 |
| P6 | Collection of data not required for the user-consented purpose | 2.1 | 1.8 | 3.78 |
| P7 | Sharing of data with third party | 1.8 | 2 | 3.6 |
| P8 | Outdated personal data | 1.6 | 2.2 | 3.52 |
| P9 | Missing or insufficient Session Expiration | 1.4 | 2.4 | 3.36 |
| P10 | Insecure Data Transfer | 1.3 | 2.4 | 3.12 |
| P11 | Inappropriate Policies, Terms and Conditions | 1.7 | 1.8 | 3.06 |
| P12 | Transfer or processing through third party | 1.6 | 1.8 | 2.88 |
| P13 | Inability of users to modify data | 1.3 | 2.2 | 2.86 |
| P14 | Collection without consent | 2 | 1.4 | 2.8 |
| P15 | Collection of incorrect data | 1 | 2.4 | 2.4 |
| P16 | Misleading content | 1.3 | 1.8 | 2.34 |
| P17 | Problems with getting consent | 1.6 | 1.4 | 2.24 |
| P18 | Unrelated use | 1.7 | 1.2 | 2.04 |
| P19 | Data Aggregation and Profiling | 1.4 | 1.4 | 1.96 |
| P20 | Form field design issues | 1.2 | 0.6 | 0.72 |