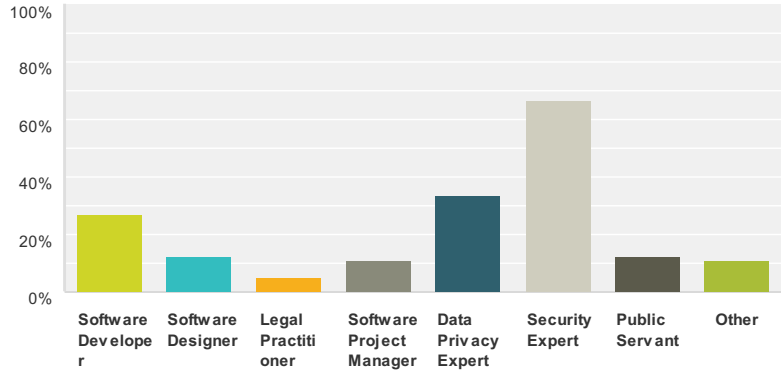
OWASP Top 10 Privacy Risks Survey

Q1 Do or did you work as a:

Answered: 63 Skipped: 0



Answer Choices	Responses	
Software Developer	26.98%	17
Software Designer	12.70%	8
Legal Practitioner	4.76%	3
Software Project Manager	11.11%	7
Data Privacy Expert	33.33%	21
Security Expert	66.67%	42
Public Servant	12.70%	8
Other	11.11%	7
Total Respondents: 63		

Q2 In total, how many years of professional experience do you have related to privacy?

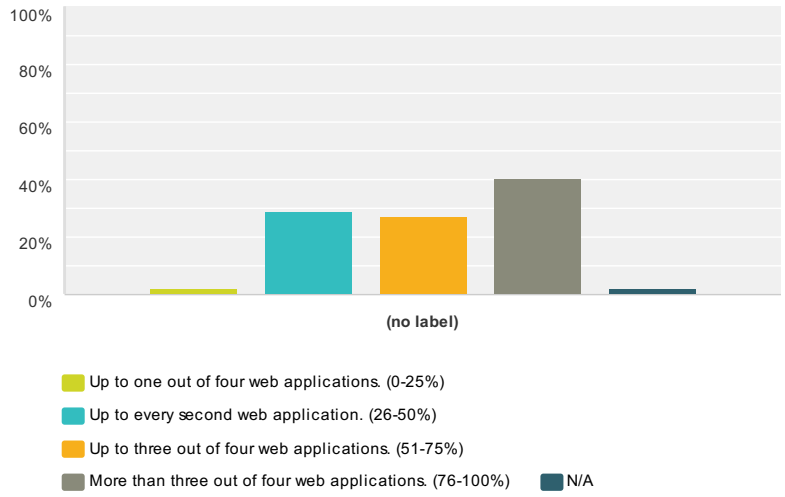
Answered: 63 Skipped: 0

Q3 In total, how many years of professional experience do you have related to web applications?

Answered: 63 Skipped: 0

Q4 Collection of data not required for main purposeWeb applications collect data not required for the main (user-consented) purpose of the application. Example: A user signs up at a web shop and enters his name, address and bank data for the payment and shipping of goods as the main purpose. Collecting further data like browsing behavior for advertising is not covered by the main purpose.In your experience, how many web applications collect data from users that are not necessary for the main purpose?

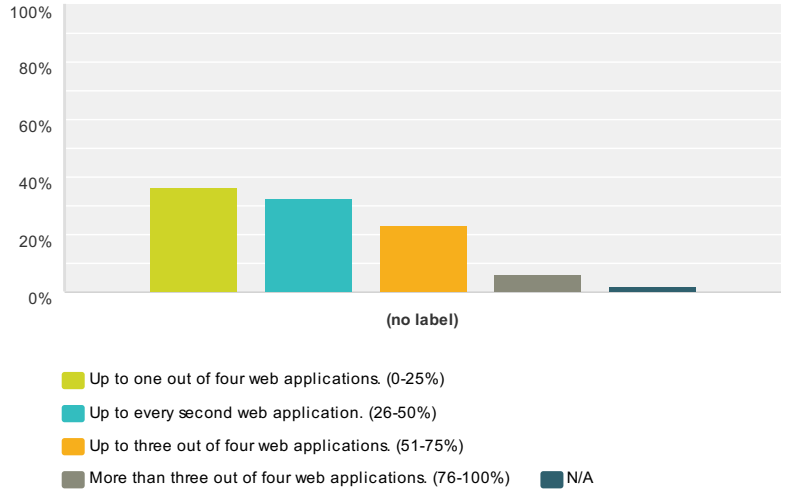
Answered: 52 Skipped: 11



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**1.92%** 1	**28.85%** 15	**26.92%** 14	**40.38%** 21	**1.92%** 1	52	3.08

Q5 Collection of Incorrect Data The collected data is incorrect or imprecise for the purposes used. This can be caused by • an ambiguous description what to enter in a form field,• an error during the saving process, • an error during the inclusion of a contact list or social network account,• unreliable, invalidated data sources, • Or misinterpretation of the collected data.E.g. the credit card security code can be abbreviated with CVV2 what can lead to confusion of users.In your experience, how many web applications collect incorrect or imprecise data?

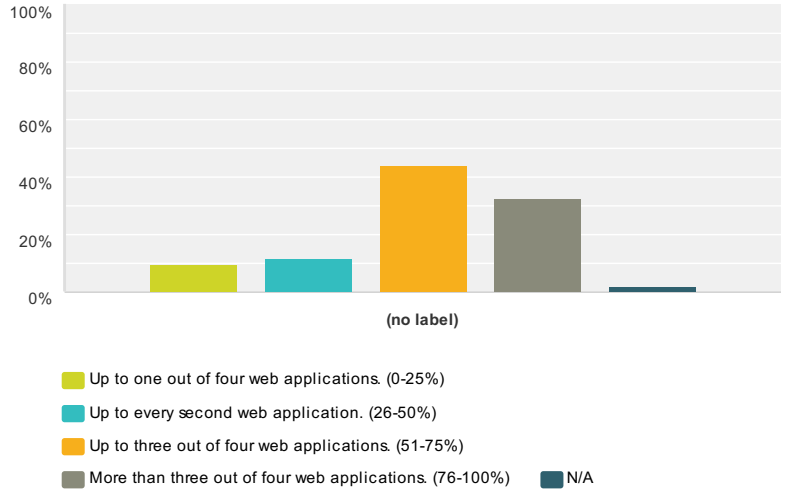
Answered: 52 Skipped: 11



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**36.54%** 19	**32.69%** 17	**23.08%** 12	**5.77%** 3	**1.92%** 1	52	1.98

Q6 Collection without consent Web applications gather information about users without consent.• From the user itself by tracking user behavior, e.g. through cookies, evercookies, web-based device fingerprinting, canvas fingerprinting, mouse tracking or location data.• From other sources: e.g. by buying information from third parties or using webcrawlers or similar technology to obtain more information about a user.In your experience, how many web applications collect personal data without consent?

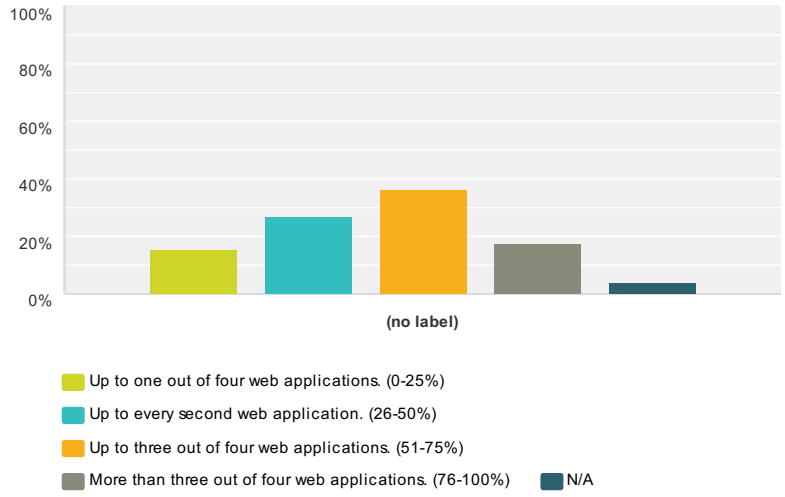
Answered: 52 Skipped: 11



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**9.62%** 5	**11.54%** 6	**44.23%** 23	**32.69%** 17	**1.92%** 1	52	3.02

Q7 Problems with getting Consent The data subject has to give consent to the collection and the purpose(s) for which the data will be used. Issues during that process like the following can lead to a false assumption of consent: • Assuming implicit consent where explicit consent is required• Using given consent for one application/function for another application/function• Assuming consent to changed conditions without properly informing the user and giving him the opportunity to opt-out.Example: A user agrees with the conditions of Google Docs and the Google Corporation. Also the YouTube account is affected by those conditions that the user is not aware of or willing to consent.In your experience, how many web applications have not sufficiently implemented the process of getting consent?

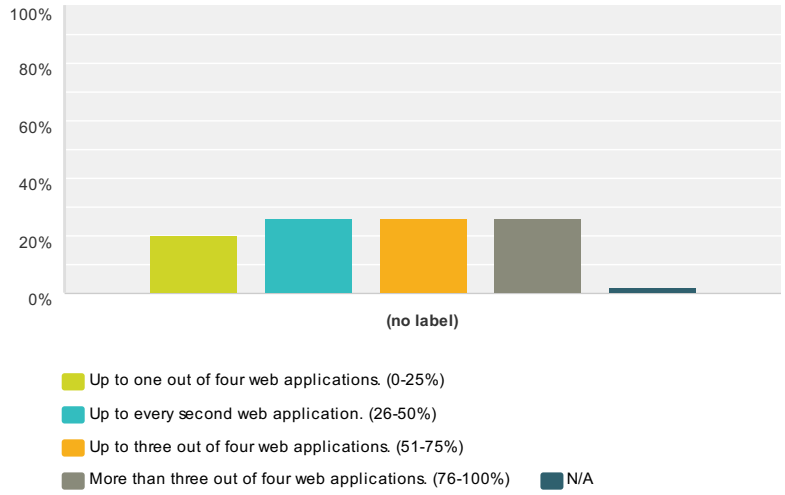
Answered: 52 Skipped: 11



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**15.38%** 8	**26.92%** 14	**36.54%** 19	**17.31%** 9	**3.85%** 2	52	2.58

Q8 Outdated Personal Data Personal data can get outdated over time and should be kept up-to-date to the extent necessary for their purposes. Example: A web shop has to update his records if a customer has changed his address so that goods and bills are delivered to the correct location.In your experience, how many web applications use outdated personal data?

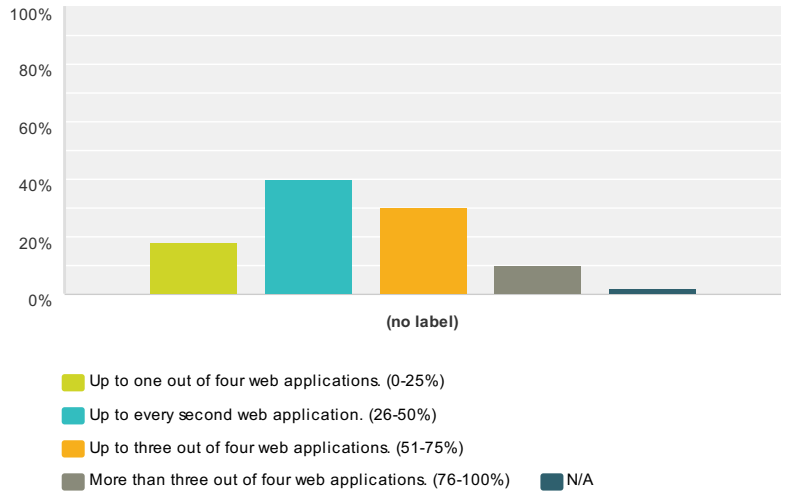
Answered: 50 Skipped: 13



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**20.00%** 10	**26.00%** 13	**26.00%** 13	**26.00%** 13	**2.00%** 1	50	2.59

Q9 Inability of users to modify stored data To improve data quality, users need the possibility to check personal data related to them and to change or delete this data if it is incorrect. To comply with these requirements procedures have to be implemented that allow the data subject to ascertain• whether and what kind of data the application has related to him/her, • that the data is communicated, • if there is an error to correct those data and • to be given reasons if a request is denied.These procedures can be implemented online or offline. The offline solution additionally requires a contact address.In your experience, how many web applications do not have a sufficient process for data modification?

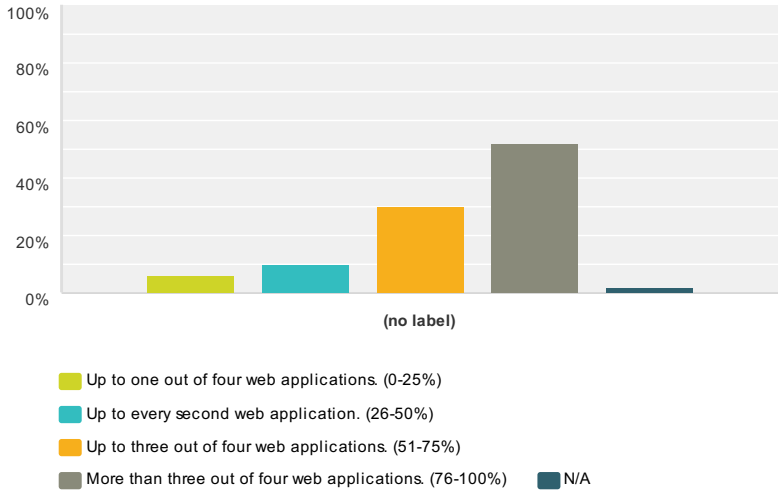
Answered: 50 Skipped: 13



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**18.00%** 9	**40.00%** 20	**30.00%** 15	**10.00%** 5	**2.00%** 1	50	2.33

Q10 Insufficient deletion of personal data Deletion of personal data is insufficient if it is incomplete or inappropriate late. Personal data should be deleted from all internal and external storage locations (e.g. database, backups, third parties, etc.) when it is not needed anymore. The operator has to ensure that he is capable to delete all personal data about a data subject in an appropriate period of time.In your experience, how many web applications fail to delete personal data sufficiently?

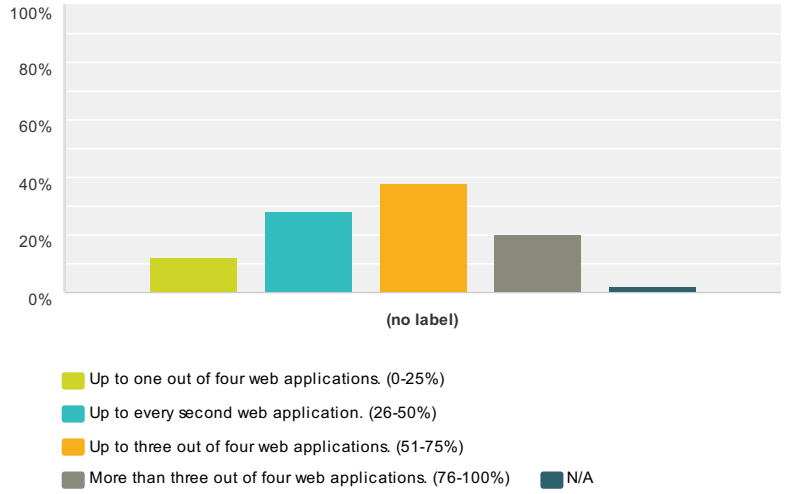
Answered: 50 Skipped: 13



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**6.00%** 3	**10.00%** 5	**30.00%** 15	**52.00%** 26	**2.00%** 1	50	3.31

Q11 Unrelated use Operators use personal data in ways unrelated to the original purpose of the collection, without informing affected people of the change. Example: A web shop operator analyzes collected data for personalized advertisement without knowledge or consent of the concerned data subjects.In your experience, how many web applications use personal data in ways unrelated to the main purpose?

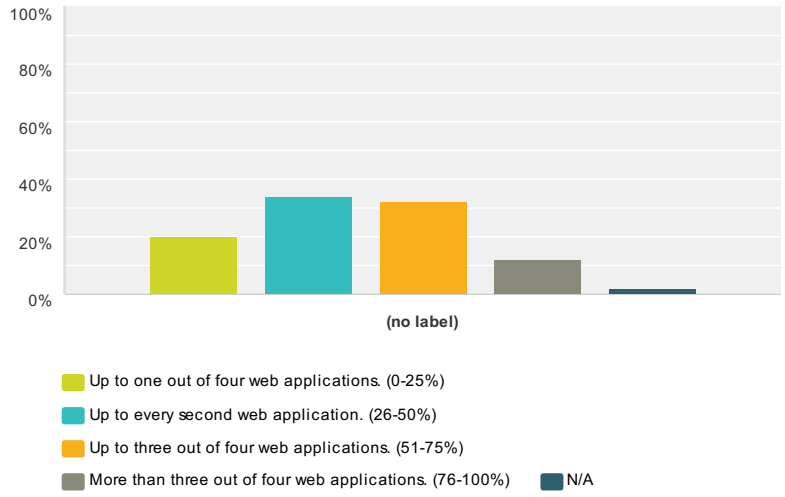
Answered: 50 Skipped: 13



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**12.00%** 6	**28.00%** 14	**38.00%** 19	**20.00%** 10	**2.00%** 1	50	2.67

Q12 Data Aggregation and ProfilingIn some cases data collected by a web application is accumulated with personal data from other sources. Sources for this data can be applications of the operator or third party sources.Example: An organization operates a web shop and a video platform. Merging personal data from both applications allows generating more complete user profiles. Those may contain more information than the user is willing to grant a single application.In your experience, how many web applications merge data from multiple sources to create more comprehensive profiles without consent?

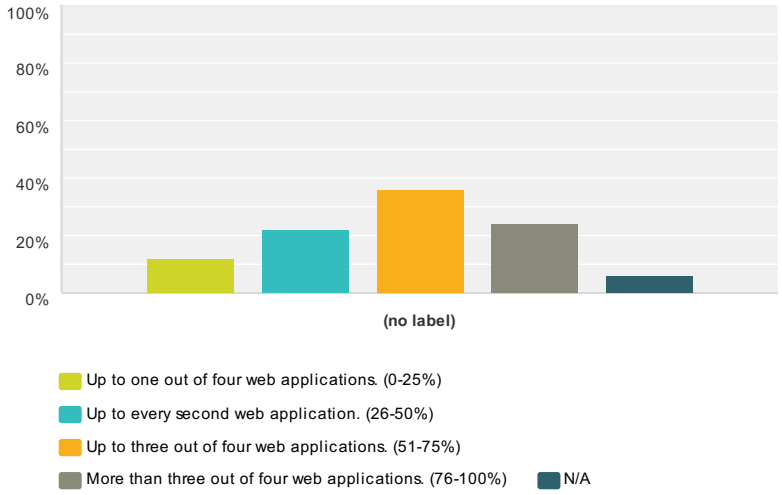
Answered: 50 Skipped: 13



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**20.00%** 10	**34.00%** 17	**32.00%** 16	**12.00%** 6	**2.00%** 1	50	2.37

Q13 Sharing of data with third party There are several ways how a web application or its operator can share personal data with a third party. The data can be sold (e.g. for advertisement purposes) or shared without consent e.g. by embedding third party scripts like widgets (e.g.: maps or social network buttons) or web bugs/trackers (e.g.: beacons or conversion pixels).In your experience, how many web applications share personal data with third parties without the user's consent?

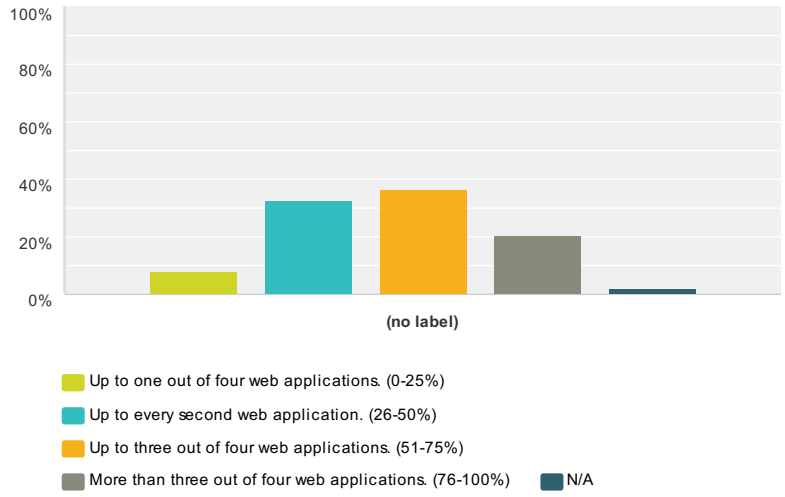
Answered: 50 Skipped: 13



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**12.00%** 6	**22.00%** 11	**36.00%** 18	**24.00%** 12	**6.00%** 3	50	2.77

Q14 Operator-sided Data Leakage Personal data can leak from the operator to employees, social engineers or third parties through:• Bad access management (e.g. excessive administrator access)• Shared storage of data• Unintended revealing of personal data e.g. through weak anonymisation • Inappropriate duplicate handling: Copies of personal data are not treated with the same standards as the original data from the web application• Data remaining on discarded storageThis does NOT include attacks on web applications from outside like SQL injection etc.In your experience, how many web application operators fail to protect personal data from data leakage appropriately?

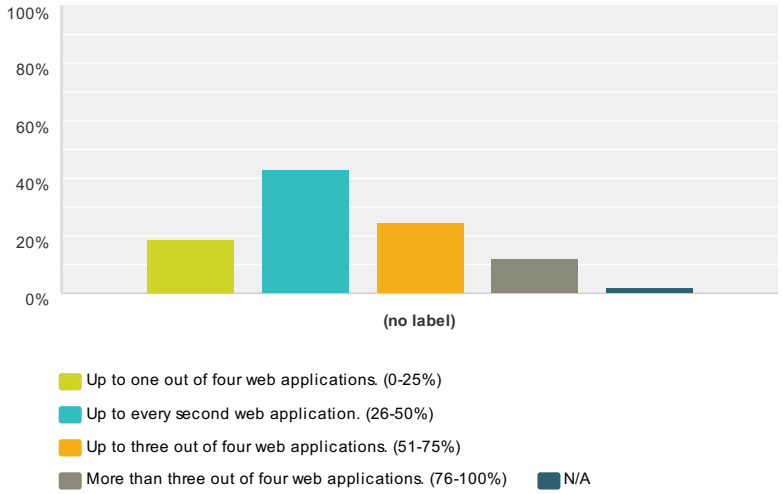
Answered: 49 Skipped: 14



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**8.16%** 4	**32.65%** 16	**36.73%** 18	**20.41%** 10	**2.04%** 1	49	2.71

Q15 Insecure data transfer Sending unencrypted data e.g. by http can violate user's privacy (e.g. personal data like contact data or even passwords in http requests or the cleartext URL). In your experience, how many web applications fail to transfer personal data securely?

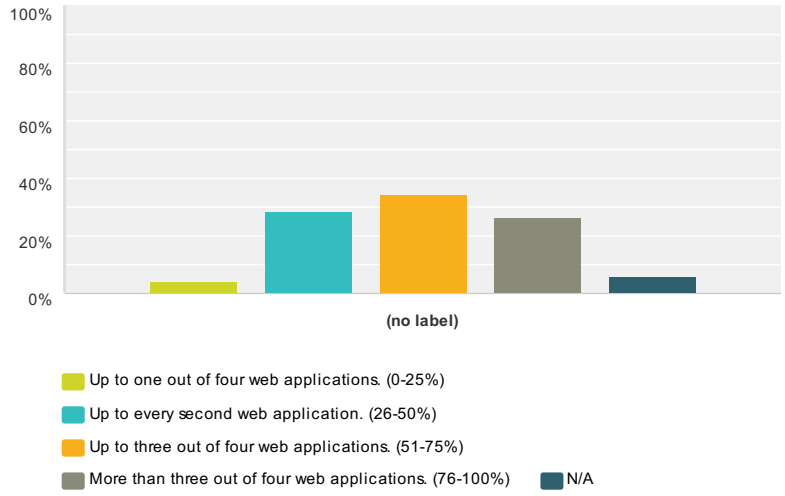
Answered: 49 Skipped: 14



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**18.37%** 9	**42.86%** 21	**24.49%** 12	**12.24%** 6	**2.04%** 1	49	2.31

Q16 Web Application Vulnerabilities Web applications can contain vulnerabilities that an attacker can exploit from the internet to get access to the data base or to abuse accounts or sessions. The data controller should protect personal data by keeping the application secure. A collection of widespread and dangerous vulnerabilities is the OWASP Top 10 list:• Injection• Broken Authentication and Session Management• Cross-Site Scripting (XSS)• Insecure Direct Object References• Security Misconfiguration• Sensitive Data Exposure• Missing Function Level Access Control• Cross-Site Request Forgery (CSRF)• Using Components with Known Vulnerabilities• Invalidated Redirects and ForwardsIn your experience, how many web applications fail to protect personal data because of vulnerabilities?

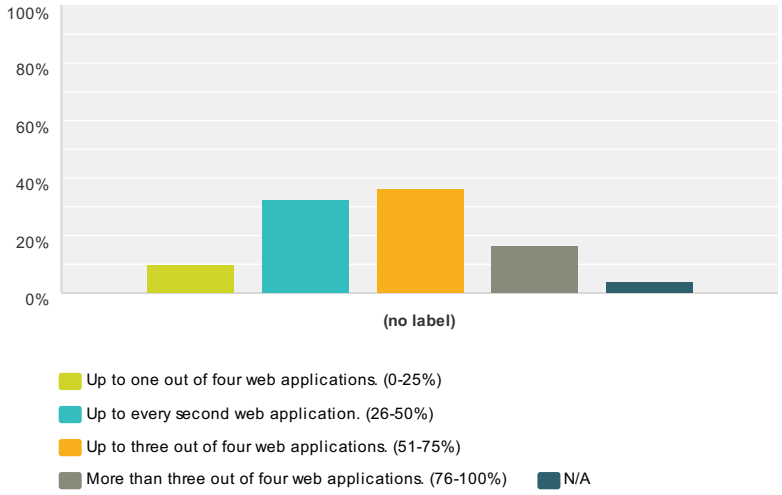
Answered: 49 Skipped: 14



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**4.08%** 2	**28.57%** 14	**34.69%** 17	**26.53%** 13	**6.12%** 3	49	2.89

Q17 Insufficient Data Breach Response In case of a data breach the operator has to take appropriate countermeasures like patching. Furthermore affected data subjects should be informed enabling them to reduce harm by reactive countermeasures like password changes or credit card locking. In your experience, how many web applications (or related operators) fail to protect personal data because they do not react properly on a data breach?

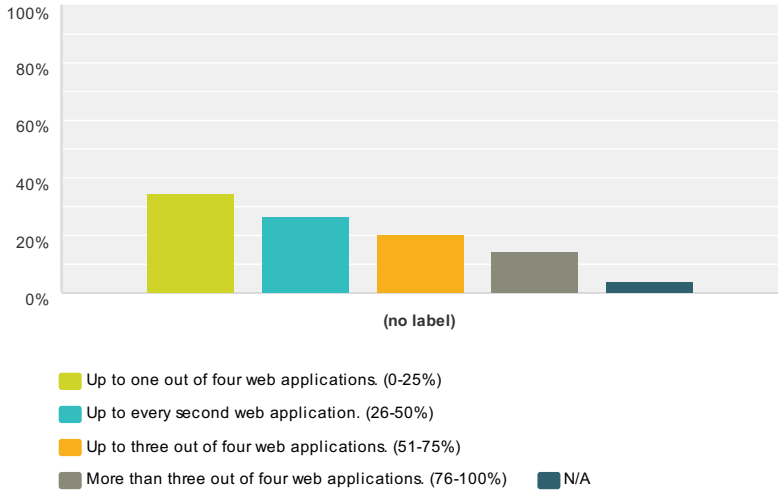
Answered: 49 Skipped: 14



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**10.20%** 5	**32.65%** 16	**36.73%** 18	**16.33%** 8	**4.08%** 2	49	2.62

Q18 Form field design issues Form fields collecting personal data should be configured in a way that protects privacy:• Autocomplete function in form fields for personal data should be disabled (default value in HTML5 is “on”)• Critical data like passwords, account numbers etc. should be masked: “***”In your experience, how many web applications fail to design their form fields privacy friendly?

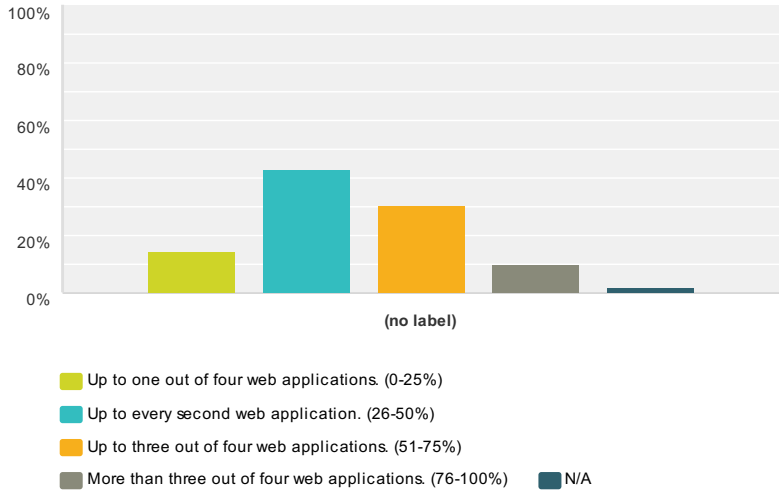
Answered: 49 Skipped: 14



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**34.69%** 17	**26.53%** 13	**20.41%** 10	**14.29%** 7	**4.08%** 2	49	2.15

Q19 Missing or Insufficient Session Expiration Some web applications try to collect user behavior as long as possible. Inappropriate long or missing automatic session timeouts extend the opportunity to collect data like browsing behavior via web bugs or location data. Manual session expiration is hindered by a not easily accessible logout button.In your experience, how many web applications intendedly lack an appropriate session expiration to collect personal data?

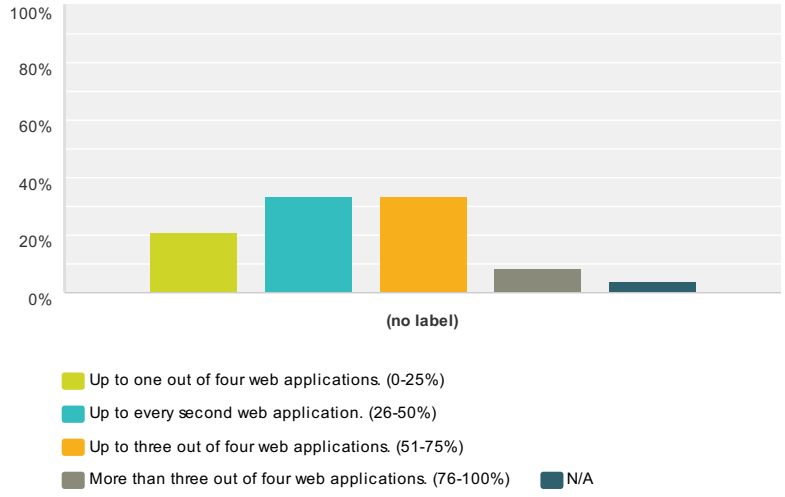
Answered: 49 Skipped: 14



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**14.29%** 7	**42.86%** 21	**30.61%** 15	**10.20%** 5	**2.04%** 1	49	2.38

Q20 Misleading ContentApplications can mislead people through their content about privacy standards. Misguiding content can be caused by:• the webpage itself, e.g. a social network does not make the user aware about who will have access to data he is entering • contextual cues on the webpage itself (e.g. a German language webpage with a German top-level domain (.de) might imply adherence to strict German privacy laws, but the application truly lower standards because it runs in a country with more lenient privacy laws), • other applications e.g. through native ads (advertising banners that look like they are content of the webpage) which lure users to sites looking similar to the original site People are probably not aware that their information will be used in ways the content of the webpage does not indicate and by unrelated agents. Even if the terms and conditions describe this behavior, the content should make that obvious, too.In your experience, how many web applications provide content to mislead users regarding privacy standards?

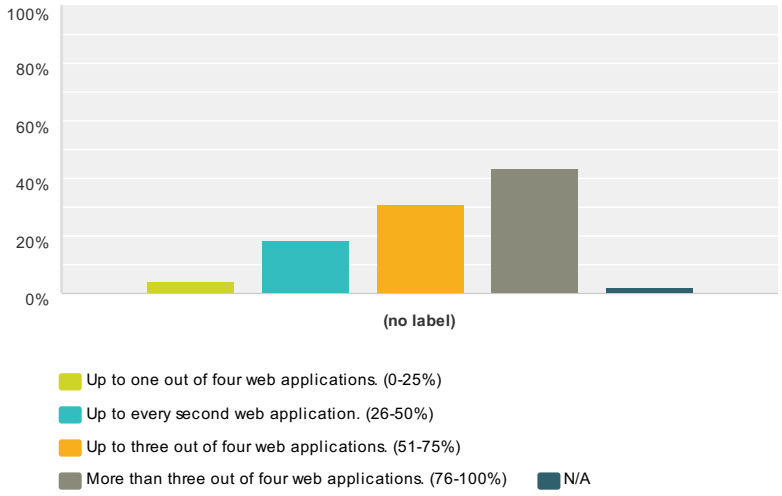
Answered: 48 Skipped: 15



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**20.83%** 10	**33.33%** 16	**33.33%** 16	**8.33%** 4	**4.17%** 2	48	2.30

Q21 Non-transparent Policies, Terms and Conditions The policies, terms and conditions inform users about the collection, the main purposes and the use of personal data. Issues can be:• The conditions are hard to find, outdated, incorrect, hard to understand, incomplete or published in an unreasonable form, e.g. in another language than the content is• Missing information about the identity and residence of the data controller • Non-transparency about effective privacy laws: Depending on the countries in which the operator is based in and where he is storing or processing the data, there are different privacy laws applicable. In your experience, how many web applications fail to provide transparent policies, agreements, terms and conditions about their privacy standards?

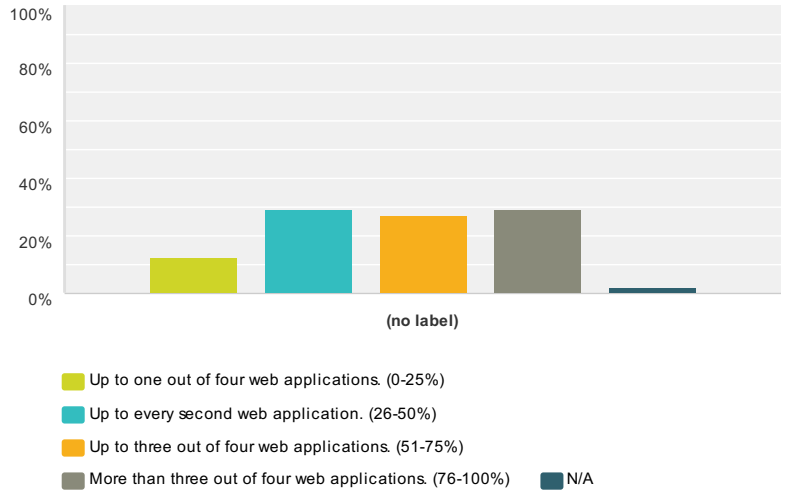
Answered: 48 Skipped: 15



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**4.17%** 2	**18.75%** 9	**31.25%** 15	**43.75%** 21	**2.08%** 1	48	3.17

Q22 Inappropriate Policies, Terms and Conditions Organizations use their privacy policies, terms and conditions to override privacy rights of the users. The OECD Privacy Guidelines are a minimum standard that should not be undermined:• Collect data only with consent,• The purpose of collection needs to be specified and is binding• Reasonable security safeguards need to be implemented• Users need to know which data is collected and processed, how and by whom.Example: A web shop reserves the right to collect further data about a user from sources of their choice without any further information about the collection and the usage of those data.In your experience, how many web applications override basic privacy rights in their terms and conditions?

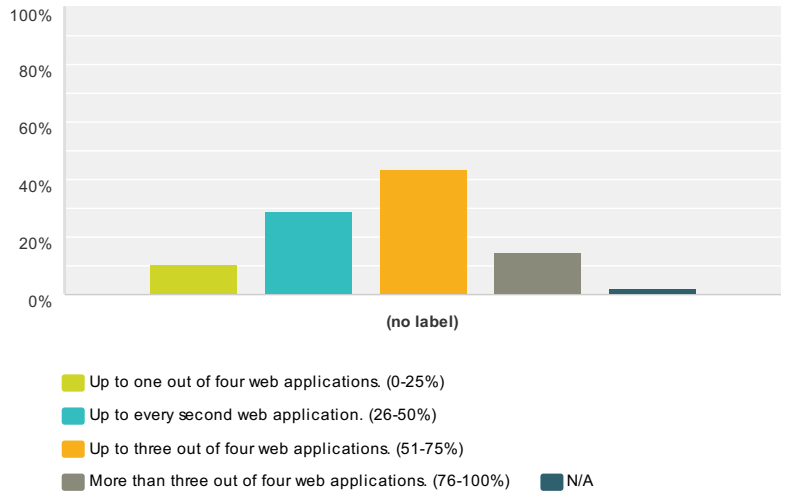
Answered: 48 Skipped: 15



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**12.50%** 6	**29.17%** 14	**27.08%** 13	**29.17%** 14	**2.08%** 1	48	2.74

Q23 Transfer or processing through third party Web applications use third parties to store or process data (also known as cloud computing). The policies or protocols of the third party provider might lack of clarity about the user's relationship with the web application provider. There can be issues with:• the security level, • information processes, or• illegitimate data usage by the third party.In your experience, how many web applications fail to use third party services for data processing in a privacy friendly way?

Answered: 48 Skipped: 15



	Up to one out of four web applications. (0-25%)	Up to every second web application. (26-50%)	Up to three out of four web applications. (51-75%)	More than three out of four web applications. (76-100%)	N/A	Total	Average Rating
(no label)	**10.42%** 5	**29.17%** 14	**43.75%** 21	**14.58%** 7	**2.08%** 1	48	2.64

Q24 Type in or paste your brief comments:

Answered: 11 Skipped: 52