

GDPR

Websites compliance?

GDPR – Websites compliance?

- GDPR - Exact security controls are not specified in the GDPR
 - WHAT to achieve
 - BUT Not HOW to do it
- “Web applications are becoming more interesting targets for adversaries as more businesses and firms are becoming dependent on web services, both in revenue and reputation”
- “Web based attacks continued to be observed as one of the most important threats due to their wide spread surface across the threat landscape...”
source “ENISA – Threat Landscape Report 2018”

GDPR – Websites compliance?

- What can we do?
 - “GDPR Websites - technical requirements”, guide
 - “GDPR Websites - security, privacy, performance and quality”, guide
 - “GDPR-IsMyWebsiteInSecure.exe”, tool

“Security is a necessary but not sufficient requirement for website compliance with the GDPR.”

GDPR

Technical requirements

GDPR – technical requirements

platform	Operating System	Windows Server 2016	Linux Ubuntu server 18.04.x LTS
platform	Database	SQL Server 2016	MySQL 8.x
platform	Web Server	IIS 10.x	Apache 2.4
platform	Development	.net Core 2.2	PHP 7.3
platform	Content Mangement System	-----	WordPress 5.2
security	firewall (only tcp/443 port)	https://mywebsite.pt (ex.)	https://mywebsite.pt (ex.)
security	latest upgrades / patches applied	√	√
security	antivirus	√	√

minimum versions for which manufacturers indicate some degree of GDPR “compliance”.

hosting must have ISO 27001 certification - information security

not shared hosting, not shared server

GDPR – technical requirements

GDPR	digital certificate (encryption)	https active by default	purpose: safety
GDPR	forms (contact)	unchecked by default minimal information	purpose: minimization and consent
GDPR	cookies (necessary, preferences, statistics, marketing)	no cookies before user agrees privacy policy users can withdraw consent any time for any page allows strictly necessary cookies	purpose: privacy and consent
GDPR	privacy policy	url's for each term / policy	purpose: consent and explicit action
GDPR	opt-in	email marketing (ex.) channel (sms, email, ivr,...)	purpose: consent, privacy
GDPR	database / backup's	encrypted. In physical location other than source server. With reserved access.	purpose: safety
GDPR	database / migration	encryption	purpose: safety
GDPR	database / data classification	sort columns with personal information	purpose: privacy
GDPR	database / vulnerability assesement	to perform vulnerability testing	purpose: security, availability

GDPR – technical requirements

- Content Security Policy

- no JavaScript inline, use external file (event handler's)
- no CSS style inline, use external file (class)
- only as exception:
 - `<script nonce="$random"> //inline code </script>`
 - `content-security-policy: script-src 'nonce-$random'`

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src>

- Security Vulnerabilities

- WordPress Plugins (<https://developer.wordpress.org/plugins/security/>)
- No code not used (Google Chrome dev. tools, coverage)
- No third party tools (Google Chrome dev. tools, audit, best practices)
 - jQuery, moment.js, Bootstrap, etc.

GDPR – technical requirements

THIS WEBSITE USES COOKIES

You can find out more about which cookies we are using or switch them off in settings.

☒ Necessary ☒ Preferences ☒ Statistics ☐ Marketing [Hide details ^](#) [OK](#)

Cookie declaration

About cookies

Necessary (2)

Preferences (0)

Statistics (4)

Marketing (18)

Unclassified (0)

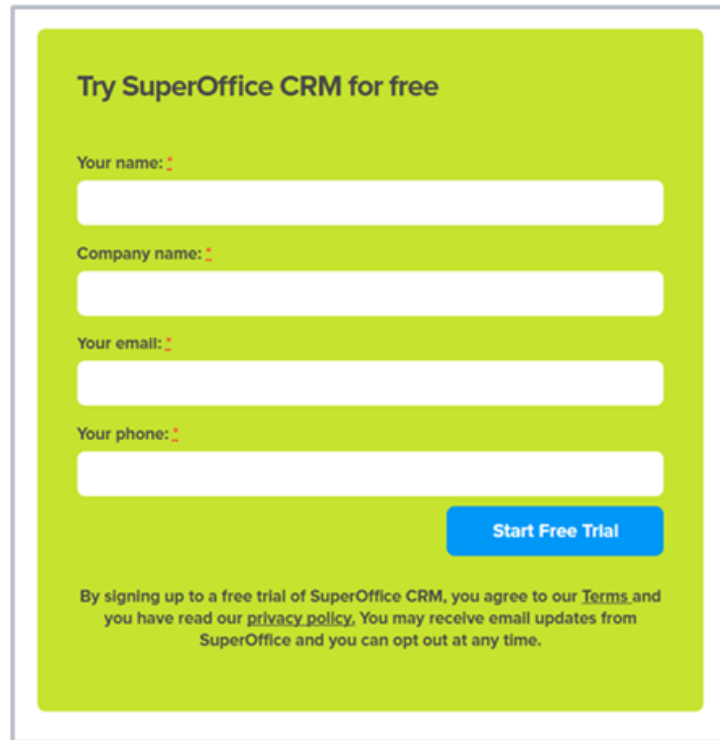
Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Name	Provider	Purpose	Expiry	Type
CookieConsent	sobold.co.uk	Stores the user's cookie consent state for the current domain	1 year	HTTP

Cookie declaration last updated on 15/05/2019 by [Cookiebot](#)

No cookies before user agrees to privacy policy. Users can withdraw consent at any time from any page
source: <https://sobold.co.uk/is-my-website-gdpr-compliant-what-is-the-general-data-protection-regulation/>

GDPR – technical requirements



Try SuperOffice CRM for free

Your name: *

Company name: *

Your email: *

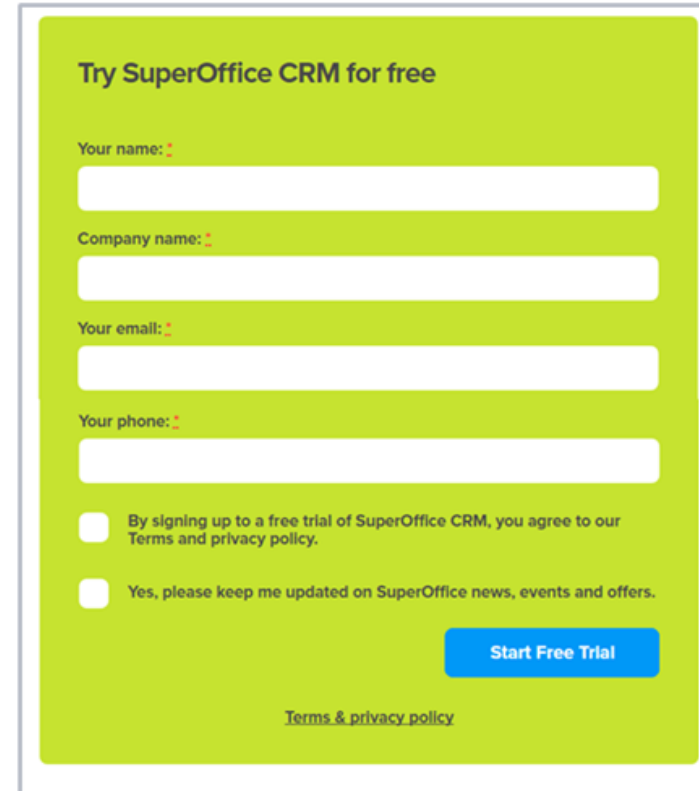
Your phone: *

[Start Free Trial](#)

By signing up to a free trial of SuperOffice CRM, you agree to our [Terms](#) and you have read our [privacy policy](#). You may receive email updates from SuperOffice and you can opt out at any time.

This form is not compliant with GDPR because it does not include explicit consent checkboxes for the trial terms and marketing updates.

Not compliant



Try SuperOffice CRM for free

Your name: *

Company name: *

Your email: *

Your phone: *

☐ By signing up to a free trial of SuperOffice CRM, you agree to our Terms and privacy policy.

☐ Yes, please keep me updated on SuperOffice news, events and offers.

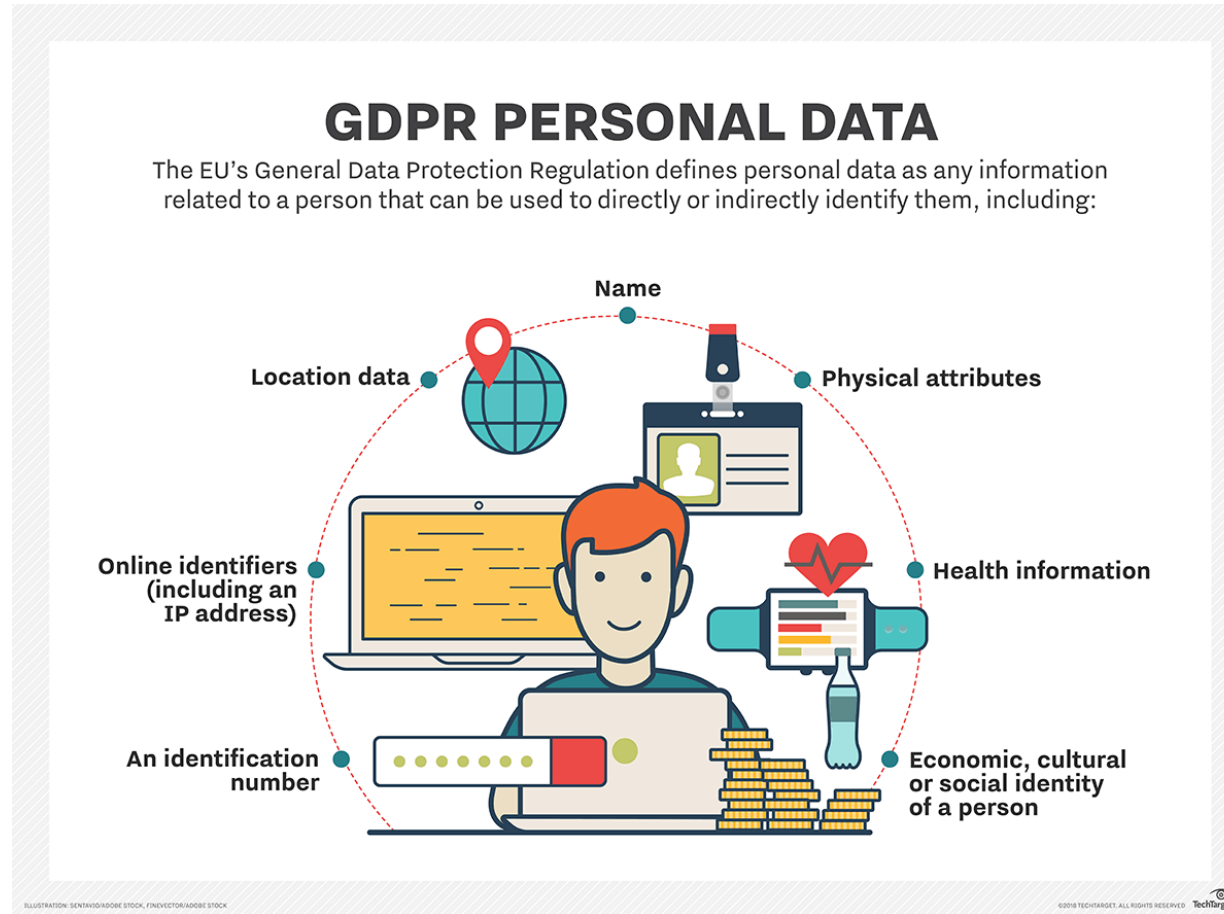
[Start Free Trial](#)

[Terms & privacy policy](#)

This form is GDPR compliant because it includes explicit consent checkboxes for the trial terms and marketing updates.

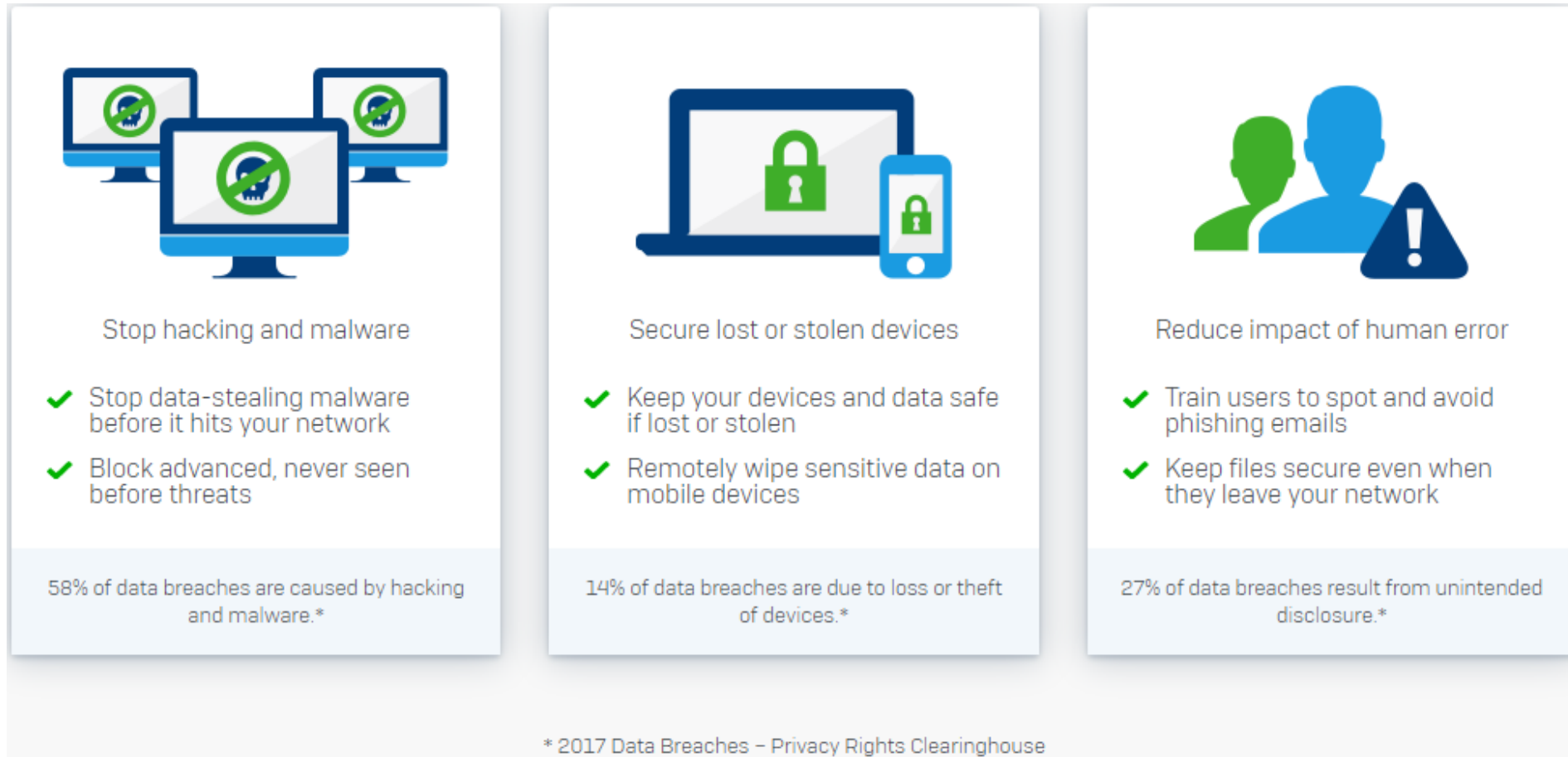
GDPR Compliant

GDPR – technical requirements



source: Techtargget

GDPR – technical requirements



source: <https://www.sophos.com/en-us/solutions/compliance/gdpr.aspx>

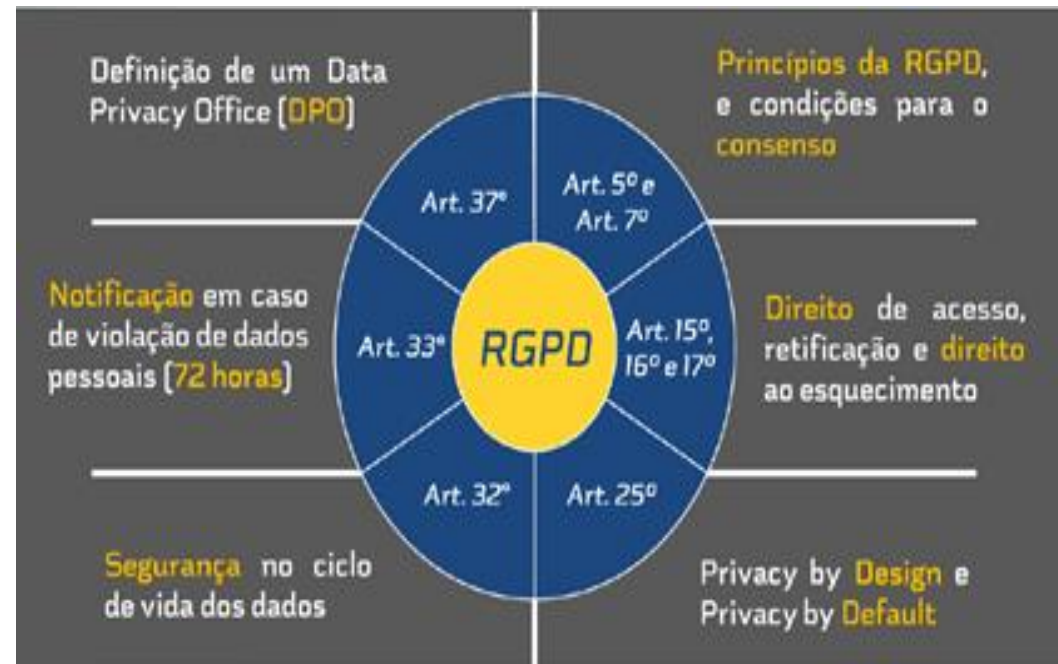
GDPR – technical requirements

- <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1>
- <https://www.enisa.europa.eu> (European Union Agency For Network & Information Security)
- <https://www.nist.gov/cyberframework> (NIST - National Institute of Standards and Tecnology)
- <https://www.iso.org/isoiec-27001-information-security.html> (ISO 27001)
- <https://www.iso.org/news/2012/10/Ref1667.html> (ISO 27032 - Guidelines for cybersecurity)
- http://ec.europa.eu/ipg/index_en.htm (European Commission - Information Providers Guide)
- <https://www.w3.org/> (W3C - The World Wide Web Consortium)
- <https://www.microsoft.com/en-us/trustcenter/cloudservices/sql/gdpr>
- <https://docs.microsoft.com/en-us/windows-server/security/gdpr/gdpr-winserver-whitepaper>
- <https://www.mysql.com/why-mysql/white-papers/mysql-enterprise-edition-gdpr/>
- <https://mysqlserverteam.com/exporting-masked-and-de-identified-data-from-mysql/>

GDPR

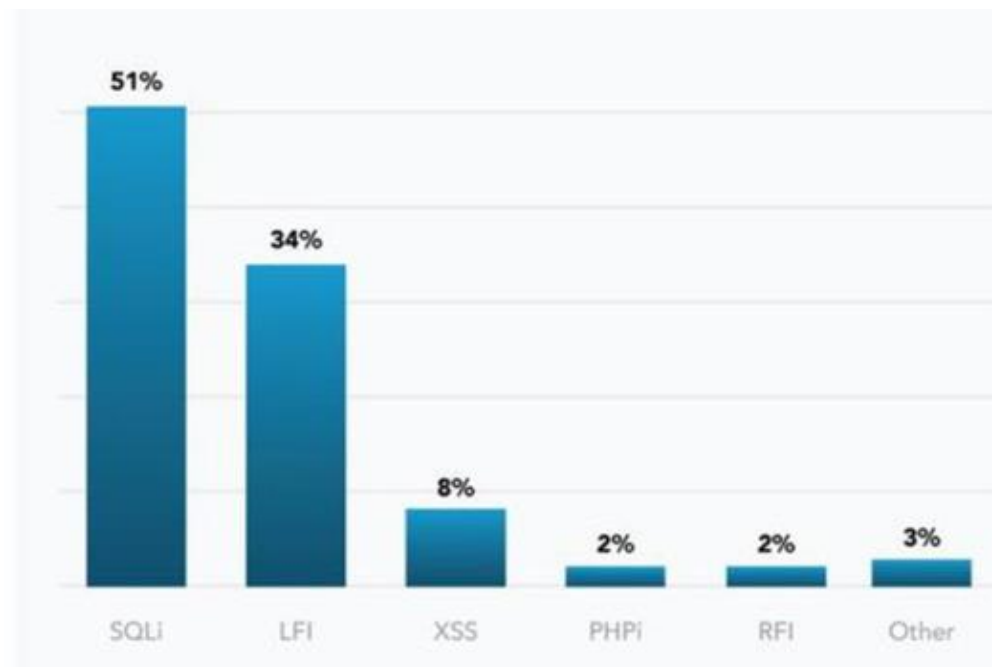
Websites - security, privacy, performance and quality

GDPR - Websites: security, privacy, performance and quality



<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e4224-1-1>
(GDPR, art.º 32 treatment safety)

GDPR - Websites: security, privacy, performance and quality



source: ENISA Threat Landscape Report 2018 January 2019, 15 Top Cyberthreats and Trends

GDPR - Websites: security, privacy, performance and quality

Category	Test	Tool	Metric
security	yes	https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap https://nmap.org/ (-sV -v -A url)	tcp/443
security	yes	https://www.wpsec.com/	no vulnerabilities
security	yes	https://www.ssllabs.com/ssltest/index.html	A
security	yes	https://observatory.allizom.org/	A
security	yes	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	no vulnerabilities
security	(*)	https://pentest-tools.com/website-vulnerability-scanning/sql-injection-scanner-online http://sqlmap.org/	zero
privacy/cookies	yes	https://www.ezigdpr.com/products/gdpr-website-compliance-checker	no action
privacy/cookies	(*)	https://www.cookiebot.com/en/	no action

(*) further test if you have not obtained the indicated "score"

GDPR - Websites: security, privacy, performance and quality

- https://infosec.mozilla.org/guidelines/web_security
- https://infosec.mozilla.org/fundamentals/security_principles.html
- <https://developers.google.com/web/fundamentals/security/csp/>
- <https://content-security-policy.com/>
- <https://www.hacker101.com/videos>
- <https://kali.training/>
- <https://www.owasp.org/index.php/>
- <https://scotthelme.co.uk/hardening-your-http-response-headers/>
- <https://developers.google.com/web/fundamentals/performance/why-performance-matters/>

GDPR - Is my Website inSecure?

- Script tool that allows you to easily and quickly indicate if a website is insecure (there are no 100% safe websites!)
- Uses tools from the public domain specialized in a security area
- The result should always be complemented by a vulnerability analysis, ex. [https://www.owasp.org/index.php/OWASP Zed Attack Proxy Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project))
- “GDPR-IsMyWebsiteInsecure.exe” is free to use and is available on <https://github.com/oazevedo/GDPR-is-my-Website-Insecure>

GDPR - Is my Website inSecure?

Thank you