GDPR – Websites: technical requirements

Use the following table as the minimum requirements to be observed in developing and / or hosting websites. See the notes below (including links) to understand the rationale for this table.

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 ativo (only tcp/443 port)	https://mywebsite.pt (ex.)	https://mywebsite.pt (ex.)
security	latest upgrades / patches applied	√	√
security	antivirus	√	√
W3C standards	HTML 5.2	√	√
W3C standards	CSS level 3	√	√
W3C standards	Responsive Design	√	√
GDPR	digital certificate (encryption)	https active by default	purpose: safety
GDPR	forms (contact)	unchecked by default eazy confirmation 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	encryptation	purpose: safety
GDPR	database / data classification	sort columns with personal information	purpose: privacy
GDPR	database / vulnerability assessement	to perform vulnerability testing	purpose: security, availability

GDPR – Websites: technical requirements

Grades:

- for the platform the minimum versions for the products used are indicated, and the most recent versions should preferably be used
- the hosting provider must be certified by ISO 27001 (information security)
- products must be GDPR "compliance"
- all products must be updated frequently (patches and upgrades) according to the manufacturer's instructions
- only utilities (jquery, bootstrap, etc.) or CMS Wordpress (*) should be used if there are no practical alternatives, always taking into account that their use implies an increased risk of vulnerability
- platform and development security should be tested with professional tools or using the "GDPR-IsMyWebsiteInSecure?" which is part of the guide "GDPR -Websites: security, privacy, performance and quality"
- security is a necessary, but not sufficient, requirement to ensure that the Website is GDPR "compliance"

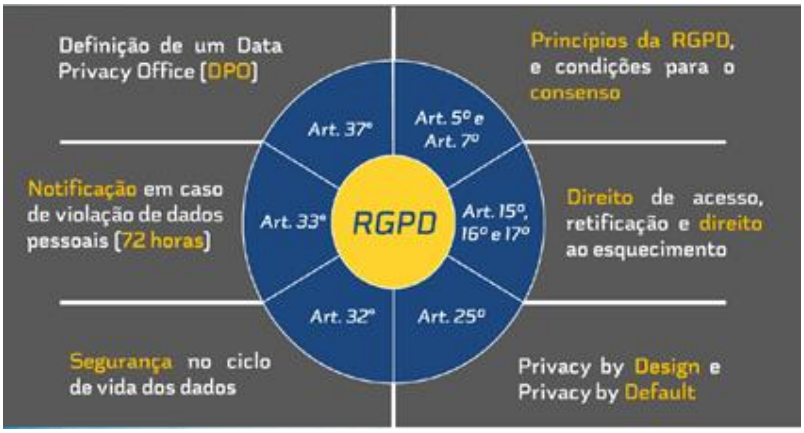
Wordpress (*)

…the most often exploited, dangerous, and damaging packages employed on websites are content management systems, and WordPress (WP) seems to appear most often in discussions of content management systems that are putting your data and users at risk. Using a web site developer who relies on WP and does not have documented, tested controls in place to protect your data and users against the WP flaws is likely to be considered the definition of negligence at some point in the near future.

Specific Mitigation Actions, ENISA - European Union Agency For Network and Information Security

The mitigation vector for this threat type includes: https://www.enisa.europa.eu/
· Use web-traffic filtering to detect and block malicious payloads and destinations (IP's, URL's).
· Use web-traffic encryption technologies such as SSL/TLS.
· Update/patch web-browsers and web-server technologies and products regularly.
· Update/patch CMS based websites regularly (i.e. WordPress, Joomla or Drupal) and avoid the utilisation of third-party plugins (usually responsible for most of the attacks against CMS's).
· Protect all endpoint systems from unpatched software containing known vulnerabilities.
· Avoid the installation of malicious programs through potentially unwanted programs (PUPs).
· Monitor the behaviour of software to detect malicious object, such as web browser plug-ins.
· Use web address, web content, files and applications reputation solutions, blacklisting and filtering to establish risk-oriented categorization of web resources.
· Check the application and web-browser settings to avoid unwanted behaviour based on default settings (esp. for mobile devices) to provide a more secure environment (i.e. disabling unused features, extensions and plugins – particularly from untrusted/unverified sources).

GDPR - https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1



GDPR – Websites: technical requirements

GDPR - Exact security controls are not specified in the GDPR

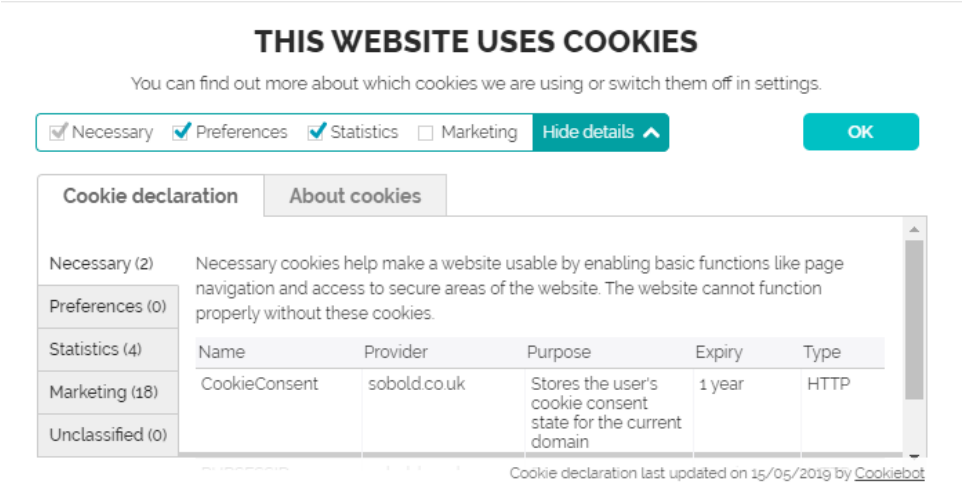
– WHAT to achieve
– BUT Not HOW to do it

GDPR - Opt-in

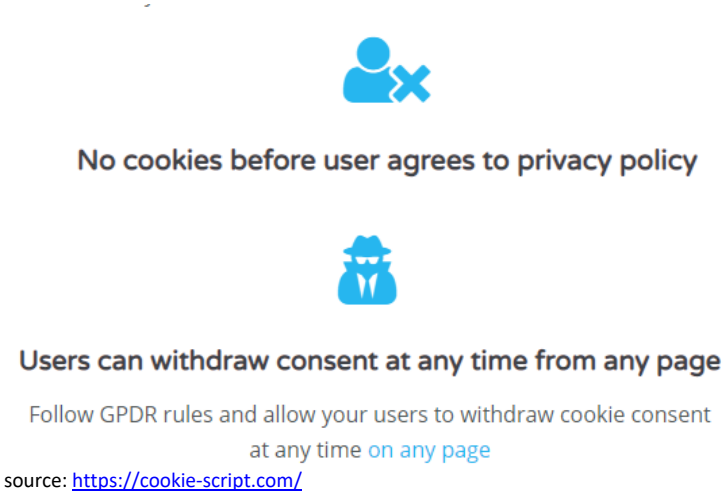
"…In other words, individuals need a mechanism that requires a deliberate action to opt in, as opposed to pre-ticked boxes. Although the GDPR doesn't specifically ban opt-out consent, the Information Commissioner's Office (ICO) says that opt-out options "are essentially the same as pre-ticked boxes, which are banned""

GDPR - Cookies http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

"The ePrivacy directive – more specifically Article 5(3) – requires prior informed consent for storage or for access to information stored on a user's terminal equipment. In other words, you must ask users if they agree to most cookies and similar technologies (e.g. web beacons, Flash cookies, etc.) before the site starts to use them"



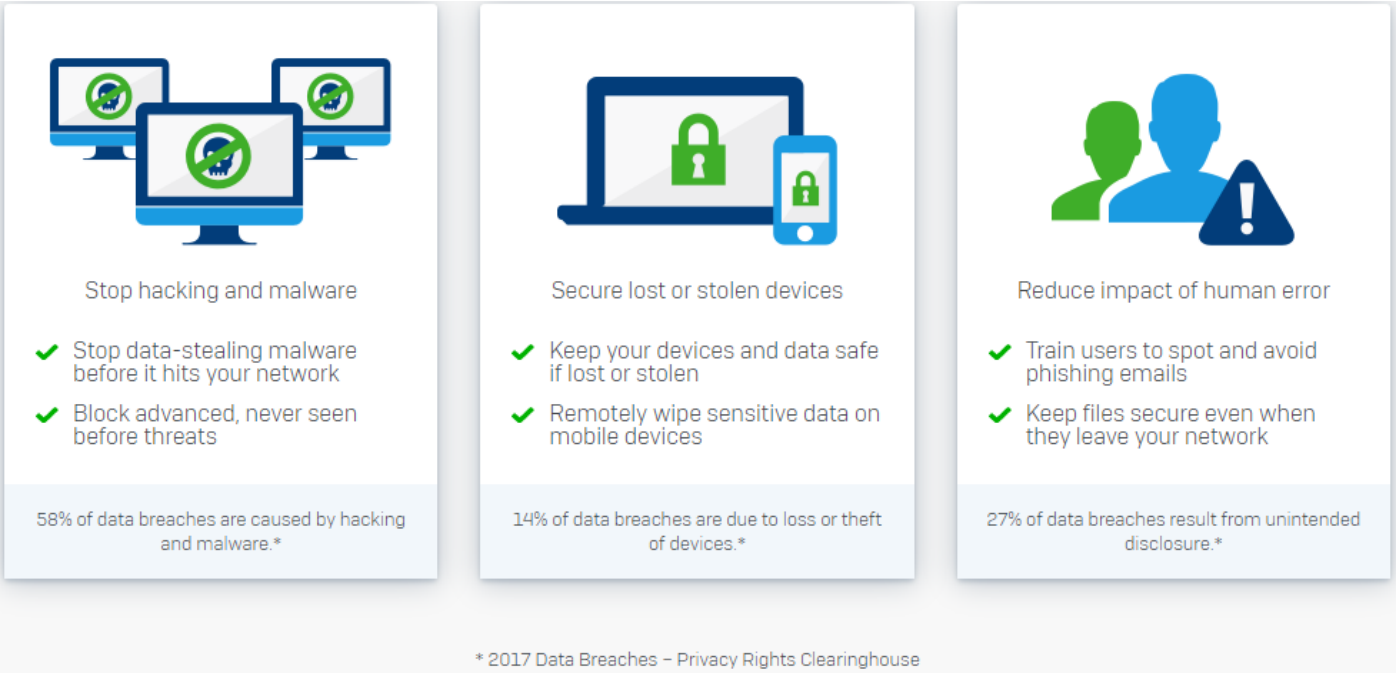
source: https://sobold.co.uk/is-my-website-gdpr-compliant-what-is-the-general-data-protection-regulation/



source: https://cookie-script.com/

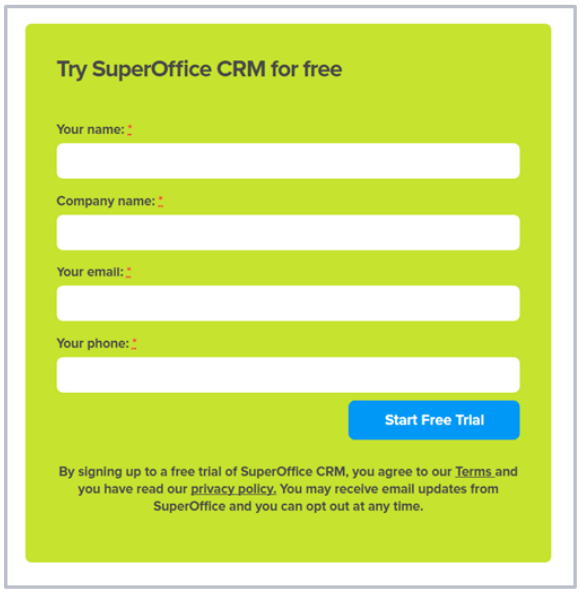
GDPR – Websites: technical requirements

GDPR – Data Breaches

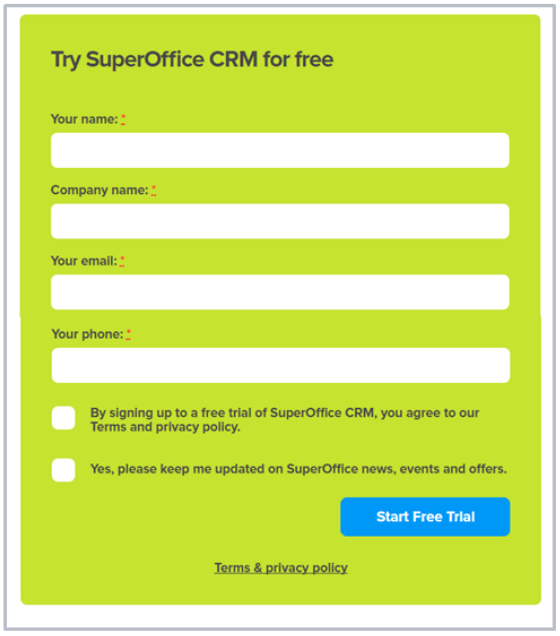


Source: https://www.sophos.com/en-us/solutions/compliance/gdpr.aspx

GDPR - Forms Compliant



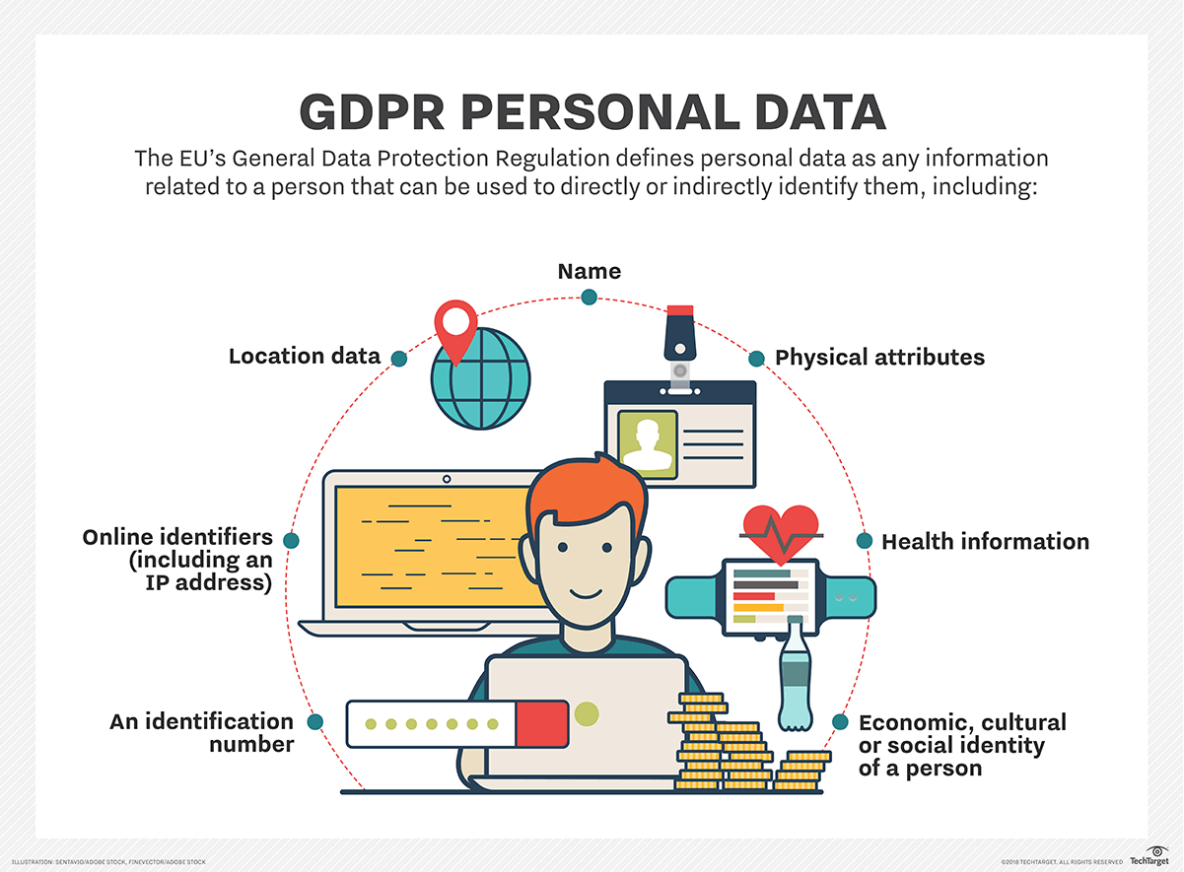
Not compliant



GDPR Compliant

GDPR – Websites: technical requirements

GDRP - Personal Data



source: techTarget

GDPR - ARCO rights

Customers now have a 'right to be forgotten' so that they can have their details removed from a website and the database if they request it. Webmasters should therefore have a process in place that caters for this and also facilitate a way that users can request this, whether it mentioning it clearly in their privacy policy or elsewhere on the website.

GDPR - Database Classification

https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-data-discovery-and-classification?view=sql-server-2017
https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-vulnerability-assessment?view=sql-server-2017
https://mysqlserverteam.com/exporting-masked-and-de-identified-data-from-mysql/
https://dev.mysql.com/doc/refman/8.0/en/security.html

Additional information

https://www.enisa.europa.eu (ENISA - European Union Agency For Network and Information Security)
https://www.nist.gov/cyberframework (NIST - National Institute of Standards and Tecnology, U.S. Department of Commerce)
https://www.iso.org/isoiec-27001-information-security.html (ISO 27001 – information security)
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/
