GDPR – Websites: technical requirements

Utilize a seguinte tabela como os requisitos mínimos a observar no desenvolvimento e/ou alojamento de Websites.
Veja as notas infra (incluindo links) para perceber a fundamentação desta tabela.

plataforma	Operating System	Windows Server 2016	Linux Ubuntu server 18.04.x LTS
plataforma	Database	SQL Server 2016	MySQL 8.x
plataforma	Web Server	IIS 10.x	Apache 2.4
plataforma	Development	.net Core 2.2	PHP 7.3
plataforma	Content Mangement System	--------	WordPress 5.2
segurança	firewall ativo (only tcp/443 port)	https://mywebsite.pt (ex.)	https://mywebsite.pt (ex.)
segurança	últimos upgrades/patches aplicados	√	√
segurança	antivírus	√	√
W3C standards	HTML 5.2	√	√
W3C standards	CSS level 3	√	√
W3C standards	Responsive Design	√	√
GDPR	certificado digital (encriptação)	https active by default	objectivo: segurança
GDPR	forms (contact)	unchecked by default eazy confirmation minimal information	objectivo: minimização e consentimento
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	objectivo: privacidade e consentimento
GDPR	privacy policy	url's distintos para cada termo / política	objectivo: consentimento e explícita ação
GDPR	opt-in	email marketing (ex.) | canal (sms, email, ivr,…)	objectivo: consentimento, privacidade
GDPR	database / backup's	Encriptado em local físico distinto do servidor origem com acesso reservado	objectivo: segurança
GDPR	database / migration	Encriptation	objectivo: segurança
GDPR	database / data classification	classificar colunas com informação pessoal	objectivo: privacidade
GDPR	database / vulnerability assessement	efetuar teste de vulnerabilidade	objectivo: segurança, disponibilidade

Notas:

GDPR – Websites: technical requirements

- para a plataforma são indicadas as versões mínimas para os produtos utilizados, sendo que preferencialmente devem ser utilizadas as versões mais recentes
- quem aloja deve estar certificado pela ISO 27001 (segurança da informação)
- os produtos devem ser GDPR "compliance"
- todos os produtos devem ser atualizados frequentemente (patches e upgrades) de acordo com as instruções do fabricante
- só devem ser utilizados utilitários (jquery, bootstrap, etc.) ou o CMS Wordpress (*) se não existirem alternativas práticas, tendo sempre em atenção que a sua utilização implica um acréscimo de risco de vulnerabilidade
- a segurança da plataforma e do desenvolvimento devem ser testadas com ferramentas profissionais ou utilizando a ferrramenta "GDPR - Is my Website inSecure?" que faz parte do guia "GDPR -Websites: security, privacy, performance and quality)
- a segurança é um requisito necessário, mas não suficiente para garantir que o Website é GDPR "compliance"

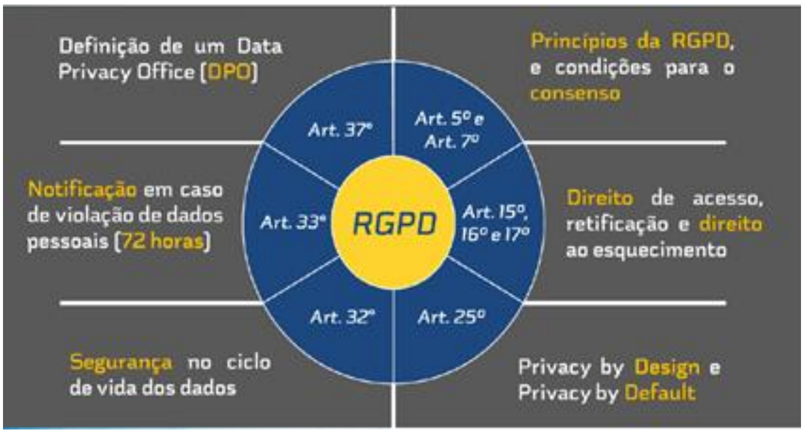
### Wordpress (*)

…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


Definição de um Data Privacy Office (DPO)
Princípios da RGPD, e condições para o consenso
Art. 37º
Art. 5º e Art. 7º
Notificação em caso de violação de dados pessoais (72 horas)
Art. 33º
RGPD
Art. 15º, 16º e 17º
Direito de acesso, retificação e direito ao esquecimento
Art. 32º
Art. 25º
Segurança no ciclo de vida dos dados
Privacy by Design e Privacy by Default

GDPR – Websites: technical requirements

### GDPR - Exact security controls are not specified in the GDPR

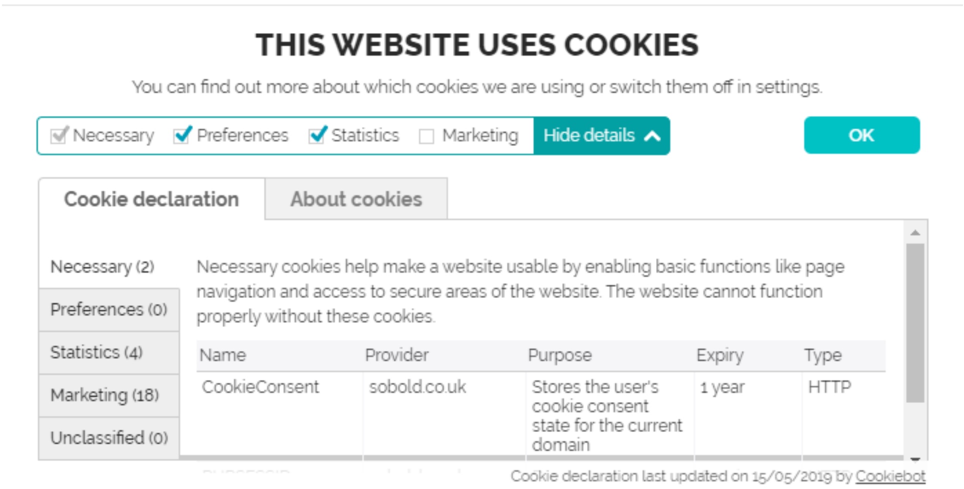
– WHAT to achieve
– BUT Not HOW to do it

### 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"



THIS WEBSITE USES COOKIES

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

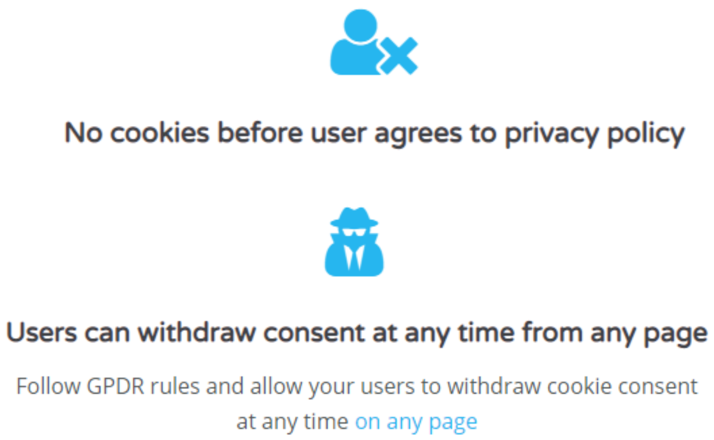
☑ Necessary ☑ Preferences ☑ Statistics □ Marketing

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

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



No cookies before user agrees to privacy policy

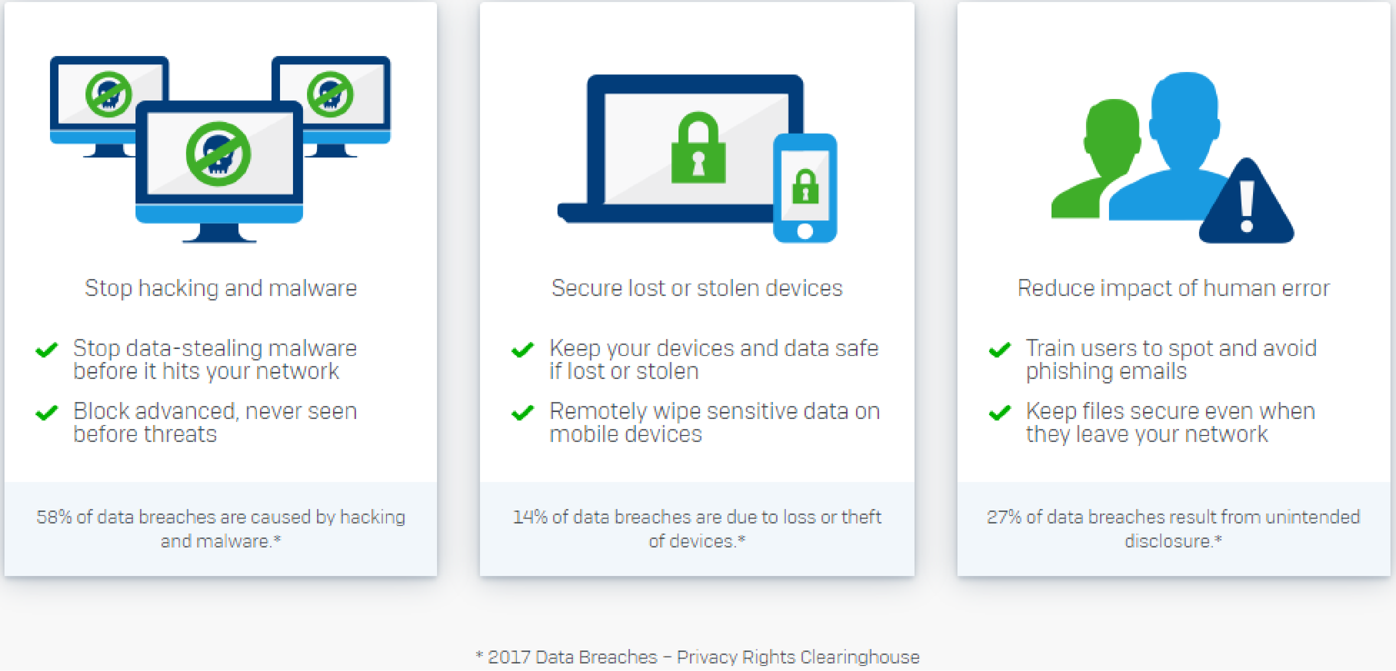
Users can withdraw consent at any time from any page

Follow GPDR rules and allow your users to withdraw cookie consent at any time on any page

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

GDPR – Websites: technical requirements

### GDPR – Data Breaches



Stop hacking and malware

- ✓ Stop data-stealing malware before it hits your network
- ✓ Block advanced, never seen before threats

58% of data breaches are caused by hacking and malware.*

Secure lost or stolen devices

- ✓ Keep your devices and data safe if lost or stolen
- ✓ Remotely wipe sensitive data on mobile devices

14% of data breaches are due to loss or theft of devices.*

Reduce impact of human error

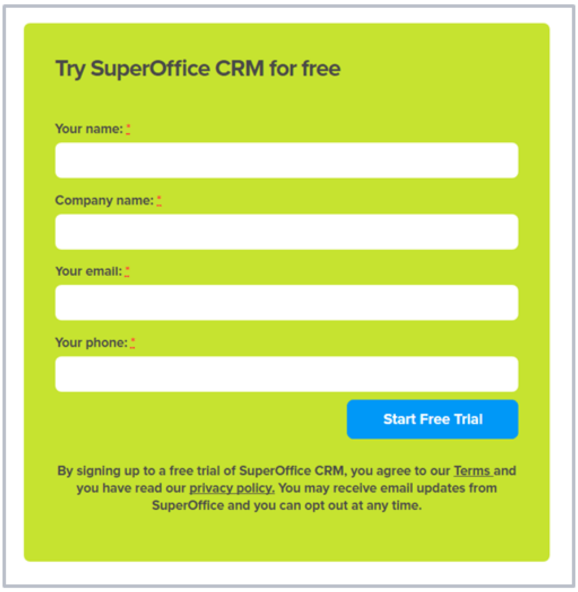
- ✓ Train users to spot and avoid phishing emails
- ✓ Keep files secure even when they leave your network

27% of data breaches result from unintended disclosure.*

* 2017 Data Breaches – Privacy Rights Clearinghouse

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

### GDPR - Forms Compliant



Try SuperOffice CRM for free

Your name: *

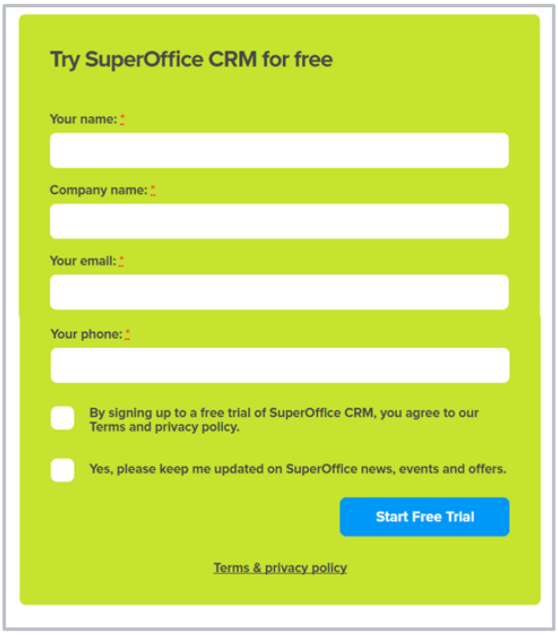
Company name: *

Your email: *

Your phone: *

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

Not compliant



Try SuperOffice CRM for free

Your name: *

Company name: *

Your email: *

Your phone: *

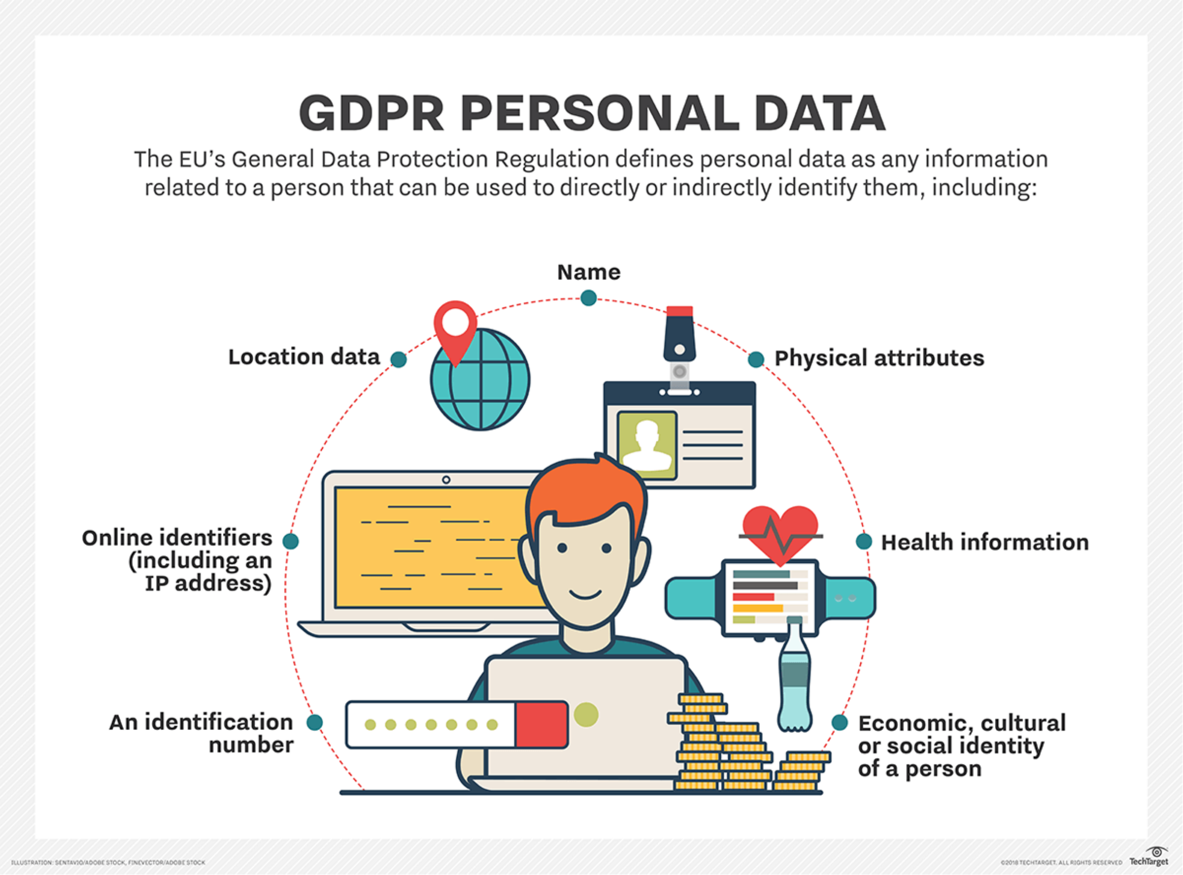
□ By signing up to a free trial of SuperOffice CRM, you agree to our Terms and privacy policy.

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

GDPR Compliant

GDPR – Websites: technical requirements

### GDRP - Personal Data



GDPR PERSONAL DATA

The EU's General Data Protection Regulation defines personal data as any information related to a person that can be used to directly or indirectly identify them, including:

Name
Location data
Physical attributes
Online identifiers (including an IP address)
Health information
An identification number
Economic, cultural or social identity of a person
ILLUSTRATION: SENTAVIO/ADOBE STOCK, FINEVECTOR/ADOBE STOCK
©2018 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

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

### Informação adicional

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 - segurança da informação)
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/