GDPR
How to prepare your business

shopware

Preface

The eCommerce industry is facing a constant stream of new challenges. Companies, consumers and now politicians are continually placing new demands on the industry. In recent years, particularly in the field of data protection, there have been growing calls for improvements. The EU finally decided to act and has created new cross-border standards.

On 25 May 2018, the European General Data Protection Regulation (GDPR) will come into force and replace national regulations. It standardises how personal data is processed through-out the EU. Even though the UK is leaving the EU, the country will also observe the GDPR as it has already passed a data protection law complying with the GDPR. In addition, it will apply to all companies and institutions operating within the EU that work with personal data including names, addresses, bank details, dates of birth, photos, etc.

Personal data will be better protected by the GDPR and consumers will be able to get a better understanding of how data is handled through greater transparency in processing. The GDPR is also designed to facilitate a smoother data exchange between companies.

Such changes sound good to consumers, but of course they do not implement themselves overnight – it takes time and hard work. Companies should therefore deal with the amendment in good time. Especially in eCommerce, you should be prepared and adapt your shop to the new data protection regulation.

In this whitepaper, we aim to give you an overview of everything you need to know about the GDPR: What has changed and what impact will it have on your online shop? Get insight into the views of experts from Trusted Shops and C3 Media and a range of practical tips.

Stefan Heyne

CEO and co-founder,
Shopware

Content

1. GDPR in a nutshell

The General Data Protection Regulation (GDPR) will come into force on 25th May 2018; it is intended to strengthen and unify data protection for all individuals within the European Union (EU). It will apply to the UK (even though we are negotiating to leave the EU), and will replace the current UK Data Protection Act 1998.

The GDPR will give people much more say over what companies can do with personal data, and there are tough new fines for non-compliance and breaches that can be levied. Indeed, some commentators have suggested that this could spawn "no win no fee" legal representations where companies have not taken notice of the new regulation. Once the legislation comes into effect, companies must ensure personal data is processed lawfully, transparently, and for a specific purpose. In many instances, the basis of personal data being captured lawfully will be to enable a contract between the individual and the company. In other cases, it will be a requirement to obtain consent from the individual to capture and process their personal data.

How does GDPR impact your website and marketing?
The key is transparency. All companies capturing personal data (whatever the lawful basis) must ensure that a privacy notice, written in plain English, is accessible to individuals before they provide that data. One means is for companies to add a clear link (not hidden in small print) to the privacy notice on their website.

If consent is being used for the lawful basis on which to capture personal data then this must be given freely and affirmatively, so no prefilled check boxes, or only an option to elect to opt-out. Equally, where consent is given, it must be easy to withdraw consent e.g. if consent is given by simply ticking a box on a website, then it should be possible to withdraw consent by similarly unticking a box. You may well need granular consent options for giving and withdrawing content for each separate piece of processing e.g. for internal marketing, as distinct from third party marketing.

Personal data must only be kept for a reasonable period of time and for the process it was captured for (this should be defined in your privacy notice); if data is being captured and stored, you need the means to easily remove old data. Additionally, individuals have the right to be forgotten, i.e. ask for the personal data to be removed, so you need means to do that too.

In the UK, it is the Information Commissioner's Office (ICO) that will have the power to enforce the GDPR. Their website is also a useful reference point for finding out more about the GDPR.

***Timothy Willis** is the Cofounder & Managing Director of C3.*
C3 run a straight talking eCommerce agency based in the South and North West of the UK, helping to deliver multi-channel solutions to B2B and B2C customers.

2. What is the General Data Protection Regulation?

1. Why was the GDPR drawn up?
The main objective of the General Data Protection Regulation (GDPR) is to harmonise European data protection. A further objective is to keep up with the rapid technological developments made by the digital society with up-to-date data protection legislation – something the outdated 1995 directive was no longer capable of doing. Data protection legislation will also be significantly strengthened, particularly through new and effective sanctioning mechanisms.

2. Who is affected by the new General Data Protection Regulation?
All companies that process personal data are affected by the General Data Protection Regulation. Even small and medium-sized online retailers must comply with the requirements of the General Data Protection Regulation.
Companies with fewer than 250 employees are normally exempt from the particularly burdensome requirement to keep a record of processing activities (formerly the "record of procedures"), except when personal data is only processed occasionally. This condition, however, does not apply to eCommerce because customer data is processed regularly. As a result, even small and medium-sized online retailers are required to keep a record of processing activities.

3. What do you see as the biggest challenges facing the affected companies?
The biggest challenge for companies is to design and document the procedures through which they process personal data in compliance with the GDPR.
How much time and effort a company actually needs to invest greatly depends on the extent to which it already complies with the previous regulation. The effort required is much lower for companies that are already in a good position in terms of data protection than for those almost starting from scratch.

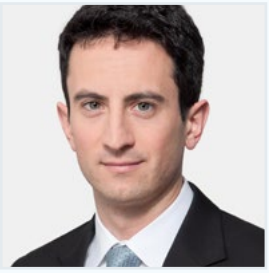
4. What opportunities do you see in the new General Data Protection Regulation?
Data protection will gain a new standing in companies, not least due to the high sanctions. In the past, people often thought that data protection regulations had no teeth. As a result, some companies – especially very large ones – chose to risk sanctions rather than adjust their business practices. This could change in the future, ensuring that data protection compliance is perceived as an important prerequisite for business activities.

5. Who benefits most from the GDPR?
Customers and users of internet services benefit as their personal data is better protected. Companies that offer efficient solutions for compliance with the GDPR will also reap the rewards. Providers that have already engaged with the issue of data protection will find themselves in a favourable position.

6. When will penalties be applied and what are the sanctions for companies?
The conditions for imposing fines are described in Article 83 of the GDPR. If companies do not comply with the requirements of the GDPR, i.e. with regard to data processing principles or what are known as the "rights of data subjects", they risk sanctions. Very serious violations could result in fines of up to €20 million, or 4% of the company's entire global annual turnover. Companies with appropriate legal counsel are therefore likely to adopt a risk-based approach: the higher the risks associated with data processing, the greater the degree of diligence required by the company.

7. What measures should companies take to prepare for the GDPR?
There are various concrete measures that companies will have to take. The first step will be to get an overview of the current procedures through which personal data is processed within the company. In an online shop, these may include tracking tools, newsletter services and credit checks. These procedures must be documented in a record of processing activities that may be requested and examined by data protection authorities at any time within the context of audits.
The online shop's privacy policy and declarations of consent must be adapted to the requirements of the GDPR. The new rules on the "rights of data subjects" must be observed, i.e. the rights of individuals vis-à-vis those responsible for processing data. A response plan for reporting data breaches must also be introduced and, last but not least, all existing contracts for order processing with service providers such as web hosts or providers of tracking tools must be checked and, in most cases, renewed.

8. When should companies start to implement these measures?
The GDPR enters into force on 25 May 2018. Providers such as Trusted Shops are offering practical solutions for online retailers to help them design their online shop in compliance with the GDPR.

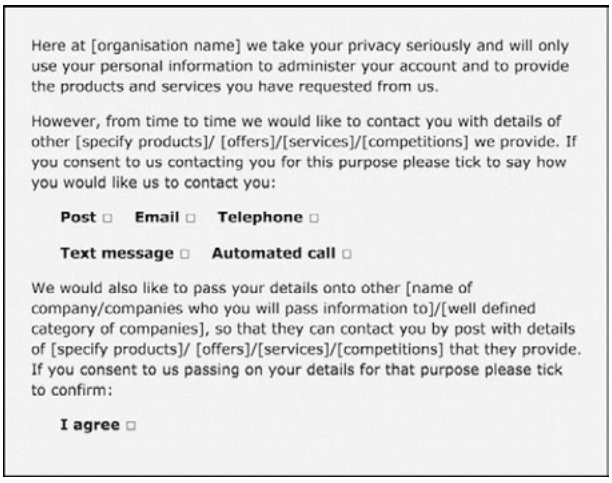


Rafael Gomez-Lus *is a legal expert for Spain and the EU for Trusted Shops GmbH and a licensed Spanish lawyer. He holds a law degree from Zaragoza University, Spain, and a Master's in International Business from Grenoble Ecole de Management, France. He is also the author of a Spanish handbook for online retailers and whitepapers on consumer law in Spain.*

3. Important changes for companies

1. Consent

Companies wishing to collect personal data must obtain prior consent from the data subject, in which they expressly agree to the processing of their personal data when there is no prior legal permission to do so (e.g. because the data is not required for the fulfilment of a contract with a customer). In addition, each declaration of consent must be accompanied by a note informing the data subject of their rights to revoke their consent at any time. The consent and the information about the revocation must be present in an easily accessible and understandable text that is in accordance with the principle of simplicity. Companies must be able to prove that the subjects have consented to the processing of their data.



Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

Post □ **Email** □ **Telephone** □

Text message □ **Automated call** □

We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

I agree □

2. Accountability (Article 5 (2), 24 (1))

All companies that process personal data must comply with the GDPR. This concerns the lawfulness of data processing, the processing of data in good faith, the transparent processing of data, the usefulness of data processing, the consideration of data minimisation in data collection, the collection of the correct data, the consideration of the storage limit, and compliance with integrity and confidentiality in data processing. Companies must be able to demonstrate compliance with the above legal principles ("accountability"). This requires the introduction and application of data protection management, which clearly defines the roles and persons responsible for data protection and identifies the work processes for processing personal data.

3. Data transmission

Everyone has the right to receive their personal data generated by a company in an electronic format and to transmit that information to another entity, provided that:

- The processing is based on consent of the data subject
- The processing takes place by means of an automated procedure

The data subjects may also require companies to forward the data directly to another recipient, if this is technically possible for the company issuing the data.

4. Right to be forgotten

Data subjects have the right to demand deletion of the data collected by companies. Companies are obliged to immediately delete the data collected on this person, in particular if:

- The purpose of collecting the personal data is no longer necessary and all retention periods have expired, e.g. from commercial or tax law.
- The data subject files an objection against the data processing and there are no grounds for the processing.
- The processing of personal data is not lawful.
- The personal data is to be deleted because EU law or the law of the Member States specifies this.

5. Penalties (Article 83 GDPR)

Penalties for violating the General Data Protection Regulation have been significantly increased. For example, fines of up to €20 million or up to 4% of the global annual turnover can be incurred. Minor violations of the General Data Protection Regulation may incur penalties of up to €10 million or 2% of the global annual turnover. The amount owed will be the higher of the two figures for the company.

6. Easier for data subjects to file complaints

By standardising data protection regulations at EU level, it will be easier for data subjects who find that their data protection rights have been infringed to file complaints. This is mainly due to the fact that complaints can be submitted to the data protection authorities of their own country in future. Data subjects no longer have to file their complaints in the country where the responsible company is headquartered.

7. Law of the place of performance → scope of application

The law of the place of performance states that not only companies based in the European Union are covered by the General Data Protection Regulation, but also those companies whose offer is addressed to a particular national market in the European Union, or the data subjects whose personal data is collected are resident in the European Union. The aim is to create a level playing field for all companies operating in the European Union market.

8.Record of all processing activities (Article 30 GDPR)

The persons responsible for the processing of personal data in a company must create a record listing all the processing activities carried out. In this way, companies create transparency and protect themselves legally. The record of the competent authority for data protection must be disclosed upon request. The record should contain the following information:

- Name and contact details of the responsible person
- The purpose of data processing
- A category description of the data subjects and the personal data
- Categories of recipients who have received personal data for processing
- Where possible, intended deadlines for the deletion of different data categories
- A general description of the technical and organisational measures

9. Extension of information requirements (Articles 13, 14 GDPR)

Companies that collect personal data or receive it from third parties (e.g. scores from an credit agency) must provide the data subjects with extensive information about the data collection. The information must be communicated to the data subject at the time of data collection.
Among other things, the data subject must be informed of the following information:

- Name and contact details of the responsible person
- Contact details of the data protection officer
- The purpose and legal basis for the processing
- The legitimate interests that are being pursued with the data processing

10. Data protection impact assessment (Article 35 GDPR)

If it is suspected that the processing of personal data could pose a high level of risk to the data subject, companies must carry out a data protection impact assessment in advance, which identifies the potential impact of data collection on the subject and assesses whether data processing should be carried out or not, or whether additional protective measures should be taken to reduce risks.

11. Data protection impact assessment (Article 33 GDPR)

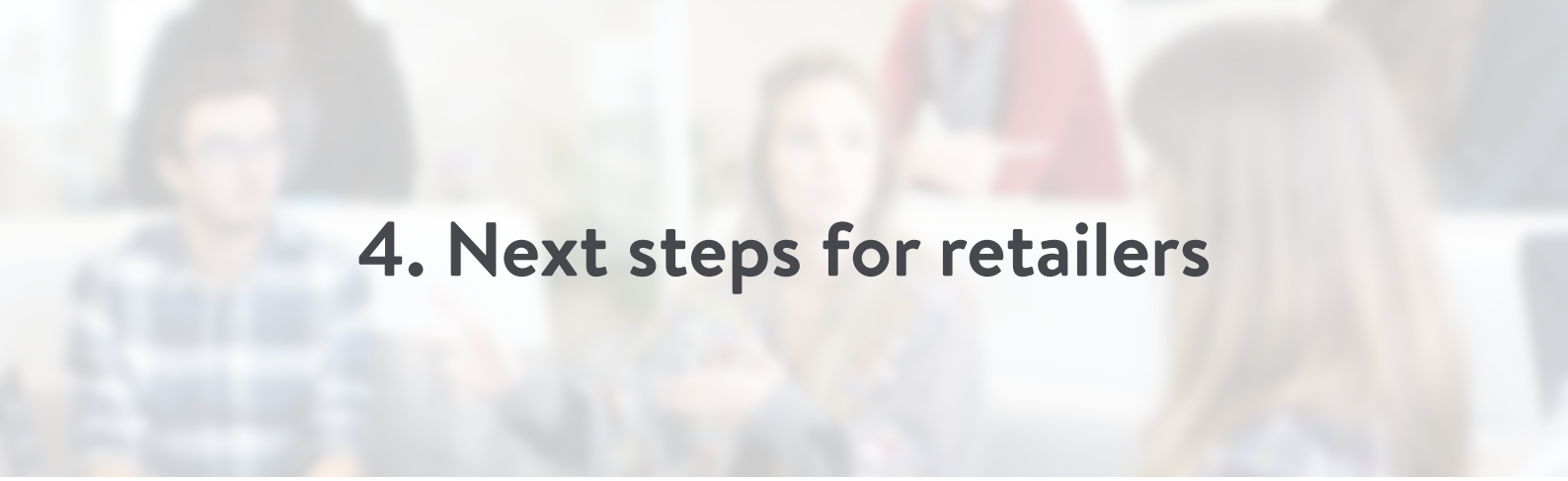
In the event of a breach of data protection obligations, companies must notify the competent authority immediately and no later than 72 hours after notification of the breach. The notification shall specify the nature of the data protection breach, the name and contact details of the Data Protection Officer, a description of the alleged consequences of the data breach and a description of the actions planned to remedy the breach. If the breach of data protection represents a high risk for the data subjects, they must also be informed, e.g. by email or a message on the website of the company itself.

12. One-stop-shop principle

With the one-stop-shop principle, the GDPR allows companies operating throughout Europe to set up a single point of contact for crossborder data processing. The "leading" supervisory authority shall be established at the central administrative headquarters of the company in the European Union. The one-stop-shop principle may be of major significance, especially for larger companies.

13. Sending newsletters

The regulations that apply to the sending of newsletters essentially remain in effect after the introduction of the General Data Protection Regulation. It is required that the email recipient expressly agrees to receive emails. A double optin procedure is recommended for gaining consent, since this procedure must also be classified as legally compliant under the GDPR. It is important that the recipient is informed in detail about what they are agreeing to when providing consent. The consent of the recipient must be voluntary and must be retained by the sender. Consent by silence shall not be obtained.



4. Next steps for retailers

Many online retailers think there is still plenty of time before the GDPR is implemented. But time is short, because implementing some of the measures is time-consuming. Therefore, online retailers should start making their adjustments promptly, as a GDPR infringement may result in severe fines of up to €20 million or 4% of their total annual turnover. In this article, we have summarised the key measures that online retailers need to implement in good time.

Update processing records

First, it's a good idea to conduct an inventory to get an overview of what data is being processed in the organisation (e.g. customer, employee and company data). As before, any process where personal data is collected and processed must be documented in records of processing activities. As of **25 May 2018**, the data protection supervisory authorities may ask companies to submit these at any time and impose fines if they fail to do so. The content of the "records of processing activities" – as they are called in the GDPR – is similar to that of the previous record of procedures. What is new is that it is no longer the data protection officer but the company management who are responsible for keeping the records.

Legal consent

For each processing of personal data on the basis of consent (e.g. in the case of sending out a newsletter), the data subject must be informed in advance of what they are agreeing to and of their revocation options. Consent must be given voluntarily and by a clear action (e.g. by ticking a box). Subjects must be able to revoke consent at any time after they have given it, with effect for the future. A new requirement is that it must be as easy to revoke consent as it is to give it. Caution: Consent already obtained retains its effectiveness only if it was obtained in accordance with the new legal situation.

Tightened reporting requirements

Shop operators will have to report to the competent supervisory authority any data breaches that could affect the rights and freedoms of data subjects, at the latest within 72 hours of them being identified. The notification includes a concrete description of the data breach (e.g. hacker attack or data theft), an estimation of potential consequences, naming of the data protection officer's contact details, and information about the measures that have already been taken. For online retailers, this involves considerably more time and

effort. Since any data breach must be documented and reported, it should be ensured that the short deadline can be met during operation.

Adapt the data protection policy

Online merchants are already required to provide a data protection policy on their website. This obligation will continue to apply, but the requirements for informing and instructing the data subjects will tighten as a result of the GDPR. Care must be taken to ensure that the technical explanations are precise yet understandable. In the future, not only will the purpose of data processing have to be mentioned, but also a clear legal basis for the processing of personal data. Existing data protection policies must therefore be adapted if they do not yet comply with the provisions of the GDPR.

Summary

The countdown is on, and sitting out is not an option. By 25 May 2018, shop operators will have to have implemented the requirements of the GDPR. Since some measures are time-consuming and there may be a need for action, depending on the current resources available in a company, implementation needs to start now. As of 25 May 2018, there will be a threat of heavy fines in the event of non-compliance or violation.

Retailers should start implementing these adaptations in good time, with these five steps:

1. Take an inventory of all data processing processes as a basis for the adaptation to the GDPR specifications.
2. Update the processing records and ensure that all data protection processes are properly recorded.
3. Check declarations of consent (e.g. for sending out newsletters) for transparency and effectiveness, and adapt the revocation notice in the declaration of consent, formulating it according to the new law.
4. Ensure that 72-hour deadlines (notification requirement) can be met in the event of data breaches.
5. Adapt the data protection policy – provide a legal basis for the processing of personal data.

5. How Shopware has prepared for the GDPR

Shopware has been working regularly with well-known certification bodies to ensure that the system meets the requirements of the GDPR, which come into force in May.

It was found that Shopware already provides shop owners with the necessary functions they need to satisfy the requirements and rules set by the GDPR, as found in the regular end user documentation. These include, for instance, the ability to remove personal data from the system, which is a core requirement of the new data protection regulation.

Important: Shopware only provides the technical basis. The shop owner or website operator is responsible for the settings, content or text modules, and compliance with the GDPR.

For more information on how Shopware is prepared for the GDPR, please visit our Wiki.

*In his capacity as Director of Research & Development at Shopware, **Sebastian Klöpper** is responsible for the product roadmap and its implementation. The areas of support, quality assurance and documentation for all Shopware products also fall within his area of responsibility. Sebastian has been working for Shopware since 2007.*

6. Glossary

The following provides you with an overview of key terms used in relation to the GDPR

1. Supervisory authority
An independent government agency, established in each Member State in accordance with EU directives, able to advise and supervise companies, as well as impose fines and other measures in the event of data breaches.

2. Processor
Natural or legal persons, authorities, agencies or other bodies charged by controllers to process personal data.

3. Biometric data
Personal data on the physical, physiological or behavioural characteristics of a natural person with which they are uniquely identified (e.g. dactyloscopic data or facial images).

4. Filing system
Any structure in which personal information is collected in a structured manner and accessible based on specific criteria. It is irrelevant whether the data is centralised, decentralised or organised on a functional or geographic basis.

5. Third party
Natural or legal persons, authorities, agencies or other bodies, other than the data subject, the controller, the processor and persons who, under the direct responsibility of the controller or the processor, are authorised to process personal data.

6. Recipient
Natural or legal persons, authorities, agencies or other bodies to which personal data is disclosed.

7. Restriction of processing
The marking of stored personal data with the aim of limiting its processing in the future.

8. Consent
A voluntary and explicit expression of will by the data subject relating to a specific case, indicating that the data subject agrees to the processing of his or her personal data.

9. Genetic data
Any data that provides information about the inherited or acquired genetic characteristics of a natural person on the basis of which he or she is unequivocally identifiable.

10. Data concerning health
All data related to the physical or mental health of natural persons.

11. Profiling
Any form of automated processing of personal data collected with the aim of obtaining personal characteristics. In particular, this includes work performance,

economic situation, health, personal preferences, interests, reliability, behaviour, location or movements, which are used to analyse or make predictions about natural persons.

12. Pseudonymisation
A type of processing of personal data so that it cannot be attributed to individual persons.

13. Controller
Natural or legal persons, authorities, agencies or other bodies which, alone or jointly with others, determine the purpose for processing the personal data.

14. Processing
Any operation or series of operations designed to collect, record, organise, structure, store, adapt, alter, retrieve, consult, use, disclose, restrict, erase or destroy personal data.

15. Personal data breach
Any intentional or unintentional breach of data security that results in the loss, alteration, or unauthorised disclosure of the information to unauthorised third parties, who then use it.

7. Contacts/legal text

Shopware

Ebbinghoff 10

48624 Schöppingen, Germany

UK: +44 (0) 203 095 2445

World: 00 800 746 7626 0

info@shopware.com

C3 Media Ltd.

St Brandon's House

29 Great George St

Bristol

BS1 5QT

Tel: +44 (0)800 1488 234

hello@c3media.co.uk

Trusted Shops GmbH

Colonius Carré

Subbelrather Straße 15c

50823 Cologne, Germany

Tel: +49 (0) 221 – 77 53 66

Fax: +49 (0) 221 – 77 53 6 89

info@trustedshops.de

Detailed information

EU GDPR

UK Data Protection Act

Original legal text