FAQ about the General Data Protection Regulation (GDPR)

TRUSTED SHOPS

1. When does the GDPR come into force?

The GDPR was promulgated 25 May 2016 and comes into effect 25 May 2018.

2. Is there a transition period?

We are currently in the transition period. Therefore online retailers should have already started working on procedures for complying with the GDPR in order to be prepared for when it comes into effect on 25 May.

3. Will there be a fundamental change in data protection law compared to today?

No. The basic principles as set out in European data protection law by Directive 95/46/EC remain in place under the GDPR. These are for example the principle of data minimisation or the principle of purpose limitation. There are also new principles, such as privacy by default and privacy by design.

4. What is changing for online retailers in practice?

One fundamental change is the introduction of the accountability principle: According to this, companies must prove their compliance with the GDPR. This results in increased obligations in terms of documentation and proof: Managing a directory of processing activities, carrying out data protection impact assessments as well as documenting data protection incidents.

The risk of not complying with the data protection regulations has also increased significantly: Infringements can be punished with fines of up to 20 million euros or up to 4% of the total worldwide annual sales.

Other changes include:

- Information obligations vis-à-vis people concerned (e.g. data protection statement) are more extensive;
- The right to data portability as well as the deadlines for processing requests for exercising the rights of people concerned are to be observed;
- The use of cookies and advertising tools can generally be justified in the future by a balancing test - subject to a different rule in the coming ePrivacy regulation;
- Contracts with service providers for data processing must fulfil stricter requirements.

5. What changes do online retailers have to implement and where?

The following changes must be implemented:

- The procedures in which personal data is processed must be documented in a directory of processing activities
- The data protection statement must be updated
- Declarations of consent permissible until now under French law are still effective so long as they fulfil the stricter requirements of voluntariness. If not, they must be re-worked.
- Contracts for data processing must be checked and re-worked if necessary;
- Data protection impact assessments must be carried out if the person responsible carries out data procedures which carry a high risk for the rights and freedoms of the people concerned.
- Internal processes must be adjusted to guarantee the rights to information, authorisation, deletion, objection and the new right to data portability. Requests from the people concerned must in general be processed within one month;
- A reaction plan for data breaches in order to make the authorities aware of the breach within 72 hours needs to be introduced.

6. An online shop bears the Trusted Shops Trustmark - does this mean it already fulfils the criteria of the GDPR?

No, as not all requirements of the GDPR are checked when awarding the quality mark. Auditing for the Trustmark does not, for example, include testing the internal documentation, like the directory of procedures.

7. Is the Trustmark denied if the online shop doesn't make the changes on the due date?

The Trustmark isn't automatically denied. We recommend, however, preparing the appropriate changes beforehand in such a way that they can be incorporated in the shop immediately on the due date.

Please note that even after successful certification by Trusted Shops, your shop should constantly adjust to the current legal framework conditions as well as the TS quality criteria.

8. Does the online shop now need a data protection officer?

Service providers must offer sufficient guarantees that ensure that the requirements of the GDPR are complied with through suitable technical and organisational measures.

If you find a suitable service provider, you must conclude a data processing contract with them which must fulfil the content-related requirements of article 28, para. 3 GDPR.

9. What must an online retailer pay attention to when it comes to their services (sending newsletters, shop software, payment providers, tracking tools...)?

Service providers must offer sufficient guarantees that ensure that the requirements of the GDPR are complied with through suitable technical and organisational measures.

If you find a suitable service provider, you must conclude a data processing contract with them which must fulfil the content-related requirements of article 28, para. 3 GDPR.

10. What questions should an online retailer ask their service provider?

You have to find out whether the service provider offers sufficient guarantees for complying with the requirements of the GDPR. The awarding of a data protection certificate is an important indicator of the fact that the provider fulfils the requirements of the GDPR.

In addition, you have to ensure that you conclude a data processing contract with the service provider which contains the necessary information obligations according to article 28, para. 3 GDPR. For example, the data processing contract must stipulate whether and under what conditions the commissioning of sub-contractors is possible.

A further point is the transfer of personal data to states outside the EU: Is the data staying in the EU, or is it being transferred to one or several third-party states? When it comes to international data transfers, you need to check whether there are guarantees for ensuring appropriate levels of data protection.

11. How should an online shop check whether its data protection statement is sufficient?

Above all, you need to review the current data procedures undertaken in your online shop (tracking tools, newsletters, credit assessment, transferring data to third parties). The data protection statement has to provide information regarding these data procedures. The following mandatory information on the procedures must be specified:

- Name and contact details of the person responsible and, if necessary, of the data protection officer
- Intended legal basis
- Legitimate interest of the person responsible
- Data recipient or categories of data recipients
- Information on transferring to third-party countries
- Deletion periods or the criteria for stipulating these periods
- Information about the rights to disclosure, authorisation, blocking, deletion, objection and data transferability
- The right to complain to regulatory authorities
- Reference to the right to object at any time to consent granted
- The existence of a right to complain to a regulatory authority
- The logic involved for automated decision-making (including profiling) as well as the range and the desired outcomes of the process
- The source of data if data is not collected from the person concerned (e.g. from an official source).

12. Is scoring still allowed?

Scoring is still allowed under certain conditions. These conditions remain the same for online retailers: Scoring may take place with the express permission of the person concerned or if scoring is necessary for the fulfilment of a contract. The latter is the case if the customer selects the 'purchase on account' or 'pay by instalments' payment methods. A new condition is that the person affected must be informed of the logic involved as well as the range and the desired outcomes of the process.

13. In practice, what exactly will the payment of fines look like in future?

Art. 83 GDPR stipulates significantly higher fines than before. For certain statutory violations, a fine of up to 20 million euros, or 4% of the company's annual sales are envisaged. It's difficult to determine to what extent the regulatory authorities will actually make use of these powers. A clear increase in the fines for data protection infringements should be expected, however.

14. Are there particular data protection laws for children?

Children require particular protection, therefore there are special regulations for children in the GDPR. According to these special regulations, the processing of personal data of children under the age of 16 is only lawful if consent is given or authorised by the holder of parental responsibility for the child.

FAQ about the General Data Protection Regulation (GDPR) and Trusted Shops products

TRUSTED SHOPS

1. Should Trusted Shops adapt their data protection? And if so, how exactly?

Like all European companies, Trusted Shops is already working on implementing the requirements of the GDPR in our activities. In addition to re-working the directory of processing activities and other documentation, this also includes adjusting the data protection statements on websites and updating training for employees regarding the GDPR.

2. Does Trusted Shops offer the option to conclude a contract on data processing?

With the start of the GDPR and in conjunction with the corresponding changes in the statutory requirements, Trusted Shops will offer online shops which use Trusted Shops products the option to conclude a contract on data processing.

Currently, we're working on creating a standard draft which we will give to interested customers before the GDPR comes into effect. Please understand that due to the number of Trusted Shops customers and the transition phase, Trusted Shops cannot offer individual contract drafts to all customers to check and agree to.

Of course, the draft offered by Trusted Shops will comply with legal provisions and will consider the interests of our customers to an appropriate degree.

3. Should an online retailer declare their use of Trusted Shops products in their data protection statement?

As the change in the law means that the information obligations of website operators increase, an online shop must, in the future, declare in their data protection statement when - as a result of consent from the buyer or as part of a data processing agreement with Trusted Shops - they are transferring personal data to Trusted Shops or allow Trusted Shops to collect such data on the online shop's website.

The information in the data protection statement should describe the collection and processing of data and name the categories of data collected. Trusted Shops GmbH should be expressly named as the online shop's data processor. In addition, the data protection statement should explain the purpose of the processing as well as the legal basis for the processing. If consent for the transfer of personal data to Trusted Shops is given, then the right of withdrawal or, if necessary, the right of objection must be stated.

4. What data is collected when Trusted Shops products are used?

A. An online shop which uses Trusted Shops products via the API offered:

If an online shop uses Trusted Shops products using the Trusted Shops API, the buyer's personal data that is transferred to Trusted Shops and the time it will be transferred depend on the individual settings of the API.

Therefore, it is not possible to make any conclusive statement on what data is transferred between the online shop and Trusted Shops when a Trusted Shops API is used. Details on the APIs offered by Trusted Shops are available at api.trustedshops.com.

Please note that transferring personal data of buyers to Trusted Shops via the API needs prior consent from the person concerned as this is a case of transferring personal data for marketing purposes. The online shop is therefore obliged to obtain the appropriate consent in advance.

B. An online shop which has integrated the Trustbadge:

a) Data transfer when visiting an online shop with an integrated Trustbadge

Same as to opening a website retrieving a Trustbadge that is integrated into an online shop via a browser client (that means simultaneously with opening the website) produces automatically a webserver log entry. As it is a standard format, this includes information on the browser client (date, time, referrer, IP address of the client, user agent...). This data is usage data which accumulates in any data transfer on the internet. In particular, the inclusion of any third-party content involves transfer of this data.

Trusted Shops does not use this usage data to create a usage profile and no conclusion on the website visitor is made. This data is used only to guarantee operation without disruption.

In addition, visiting a shop page which has the Trustbadge incorporated does not result in any personal data (e.g. name, e-mail address etc.) being transferred to us automatically or being stored.

b) Data transfer when placing an order in an online shop

If the buyer does not themself use Trusted Shops products, only the order number is transmitted to Trusted Shops when the Trustbadge is integrated. This is for verifying later guarantees or reviews.

Other data - in particular personal data - is only transmitted if Trusted Shops products for the buyer are actively used by the shop customer and they agree to the data transfer and/or have done so in the past for future purchases.

Only data which is necessary for using our products is collected. When using the Trusted Shops's buyer protection with shop reviews, this data generally comprises the order date, order number, a customer number (if one exists), the order total, the currency, the expected delivery date (if needed), the payment method and the buyer's e-mail address. When product reviews are integrated by the shop, the URL of the product and the product image, the product name, the product SKU, GTIN and MPN as well as the manufacturer are collected. If a review request is sent without the Trusted Shops' buyer protection, only the order number and the e-mail address are needed. Trusted Shops does not collect further personal data of users in this way.

Whether the buyer is already registered for a particular product usage is checked automatically using a neutral parameter of the e-mail address hashed by a cryptographic one-way hash function (MD 5 procedure). Before being transferred, the e-mail address is converted into a hash value which cannot be decrypted by Trusted Shops. If there is no match, the parameter is discarded. The e-mail address is then only collected if the buyer has decided to use Trusted Shops products. The buyer's e-mail address in plain writing or other data are not transferred as part of the automatic transfer.

The data received is only used for executing the contracts concluded and is stored internally for the duration of the mutual contract fulfilment. Afterwards, the data is then blocked from further use and is deleted for good after all commercial and tax law-related retention periods have passed.

If the buyer decides to not use Trusted Shops products for buyers and leaves the site, data is neither transmitted to Trusted Shops nor stored or processed by Trusted Shops.

5. What needs to be considered when sending review requests?

A review request constitutes an advertisement

When sending an e-mail review request, conditions relating to data protection and competition law must be considered as sending such an e-mail is a way of using personal data for advertising purposes.
The review request constitutes an advertisement.

Obtaining consent

As a result, sending a review request always requires getting express consent. Simply having the e-mail address is not sufficient. This is also the case if the e-mail address is passed on to a third party for them to send a review request. This is the case, for example, when using the Review Collector or the Automatic Collection by Trusted Shops. In the General Membership Conditions, Trusted Shops contractually obliges the online retailer to obtain effective consent. If data is transferred without obtaining consent beforehand, this is not just a contractual infringement by the online retailer; Trusted Shops can, in the event of any damages, obtain compensation from the online retailer.

Therefore, when activating the functionality, this pre-condition is expressly referred to.

An action by the customer is needed: This can a checkbox or a separate button for consent to receiving review request or it can be another action, e.g. filling in a field which is only needed for registering for a review request. Daher wird bei Aktivierung der Funktion ausdrücklich auf diese Voraussetzung hingewiesen.

Scope

The scope of the consent and its consequences must be explicit: what data is passed on to whom, who uses it, for what purpose and do they use it regularly or just once etc. Should a third party send the review requests, the consent declaration must also include consent to pass on the e-mail address to third parties for the purposes of sending a review request. If the review request is sent by Trusted Shops, the online shop must obtain consent for the e-mail address to be given to Trusted Shops for the purposes of sending a review request.

In addition, it must also be made clear that the consent can be withdrawn at any time. The retailer must be able to prove that consent was obtained.

Consent can be given, for example, via a checkbox in the customer account:

Consent with checkbox:

[ ] After every purchase that I make, I would like to be sent an e-mail reminding me to submit a review and I agree that my e-mail address will be given to Trusted Shops GmbH for this purpose.

or (if the review request is sent by the online shop itself)

[ ] I would like to review my purchases. Please send me an e-mail for this after every purchase I make.

Obtaining consent in the log-in area or through a link in the order confirmation e-mail has the advantages that, in the first case, the e-mail address is confirmed and in the second case, only the owner of the e-mail address gets the link. In both cases, a so-called double opt-in as verification would be superfluous.

Review postcards

Enclosing a review postcard is fine. It could, for example, be a flyer with a quick link to the review profile. The stricter rules for e-mail advertising do not apply to this sending method.

In the case of personal contact, the customer can be asked to give feedback immediately. As no e-mail address is used for this, prior consent is not necessary.

Trusted Shops is Europe's trustmark in e-commerce.

Do you have further questions about the Trusted Shops trust solutions?
The Trusted Shops team would be pleased to help you.

+44 (0)203 364 5906

members@trustedshops.com