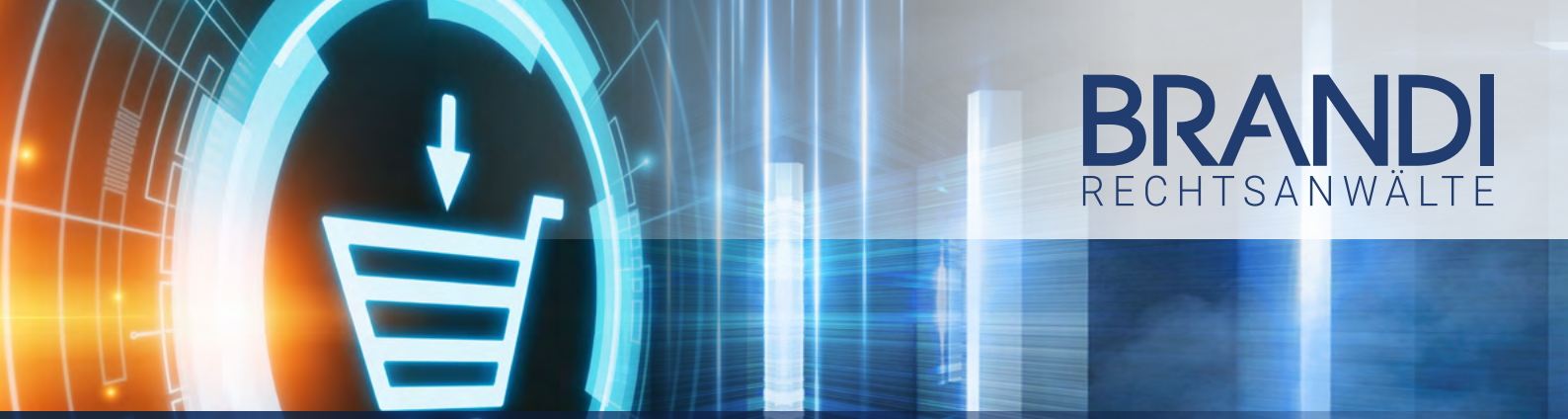

BRANDI
RECHTSANWÄLTE

DATA PROTECTION IN ONLINE TRADE

Information on data protection I August 2022

Introduction

Online trade offers companies the opportunity to present their products and services to a large number of (potential) customers and to expand their geographical reach. When visiting online stores and placing online orders, personal data is processed by the companies. In this respect, the controllers must comply with the requirements of data protection law, in particular the General Data Protection Regulation (GDPR). This article contains information on data protection in online trade and practical implementation tips.

On March 24, 2022, the Data Protection Conference (Datenschutzkonferenz, DSK), the body of independent German federal and state data protection supervisory authorities, also published information on data protection-compliant online trade by means of guest access, which can be used as guidance on this topic.

Legal basis for data processing in connection with orders

Order forms and portals in online stores enable customers to conclude contracts online with the provider of the online store. The processing of personal data in this context requires the existence of a legal basis.

Legal basis for individual orders and guest accesses

The legal basis for data processing in the context of guest access and individual orders is the fulfillment of a contract pursuant to Article 6(1)(1)(b) of the GDPR. According to this, the processing of personal data is lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

According to the provision, only the processing of personal data that is necessary for the performance of an individual contract is permissible. This also applies in particular with regard to the principle of data minimisation pursuant to Article 5(1)(c) of the GDPR, according to which data processing must be limited to the extent necessary for the purposes of the processing. In the case of a first-time order, the controller cannot per se assume that the customer will place further orders in the future and that the customer data should be stored for possible but uncertain future transactions. Accordingly, the legal basis is only applicable to the data required for the processing of the individual order, but not to the processing of further data, for example in the context of a continuous customer account.

In order to set up such a continuous customer account, it would be necessary to process further data in addition to the data required for fulfillment of the contract, for example registration data for repeated use of the online store. To ensure that customers are not forced to provide more data than is required for the one-time performance of the contract and to establish a long-term business relationship, it should regularly be possible to place orders via a guest access, via which only the personal data of the customers required for the performance of the contract and for the fulfillment of legal obligations is recorded. With the aid of such a guest access, customers can carry out an online transaction without having to create a continuous customer account.

Controllers who offer goods or services in online commerce must therefore always give their customers the option of placing an order independently of registering for a customer account. However, this is not a statement about whether the controller combines all orders of a customer in an internal customer account for internal purposes.

Legal basis for continuous customer accounts

Data processing in the context of setting up and using a continuous customer account cannot generally be justified on the basis of contract fulfillment for the aforementioned reasons. This requires a different legal basis, namely the consent of the data subject pursuant to Article 6(1)(1)(a) of the GDPR. With his consent, the customer makes a corresponding conscious declaration of intent, according to which he would like to enter into a permanent business relationship and also permits the processing of data not required for the execution of the business. Such consent can be obtained during the registration process for the customer account or directly during the online order process.

The continuous customer account is then set up with the assignment of access data so that customers can clearly identify themselves to the controller. This gives customers the opportunity to access their account at any time, change their data themselves and view orders. The permanent storage of data enables customers to place future orders without having to enter all their personal data again.

The granting of the corresponding consent to data processing in the establishment and use of the continuous customer account must be voluntary (Article 4 No. 11 and Article 7(4) of the GDPR). It is therefore not possible to make the performance of a contract dependent on consent to the processing of personal data that is not necessary for the performance of the contract. In principle, an online order may therefore not be made dependent on the customer declaring his consent to the creation of a customer account at the

same time. Customers in the online store must therefore also be able to order the same offers from the same responsible party by equivalent means other than a continuous customer account (cf. para. 37 f. of the Guidelines 05/2020 on consent pursuant to Regulation 2016/679 of the European Data Protection Board (EDSA) of May 4, 2020). In the DSK's view, an ordering option is equivalent if no disadvantages arise, i.e., ordering effort and access to these options correspond to those of a continuous customer account - such as with guest access - and technical and organizational measures are taken to ensure an appropriate level of data protection. Thus, without an alternative guest access or an equivalent ordering option, the voluntary nature of consent to data processing in the context of a continuous customer account cannot be guaranteed. If interpreted correctly, it is not contrary to equivalence if the offers can also be ordered as a guest, but special benefits (discounts) may then not be available.

In individual cases, there may be special circumstances under which a continuous customer account may exceptionally be considered necessary for the performance of the contract. In these exceptional cases, consent to data processing is not required, but rather the fulfillment of the contract pursuant to Article 6(1)(1)(b) of the GDPR can be used as the legal basis. In the DSK's view, the principle of data minimisation should then be taken into account, for example by automatically deleting the customer account after a short period of inactivity.

A customer club may differ from a continuous customer account insofar as it does not or not only serves the purpose of facilitating future orders, but also enables customers to access certain information and functions as well as special offers and promotions. Insofar as the establishment of a membership in a customer club is the subject of a contract, the fulfillment of the contract can also be considered as the legal basis for the related data processing.

Legal bases for further data processing in online trade

Personal data is subject to the principle of purpose limitation pursuant to Article 5(1)(b) of the GDPR. Accordingly, they may only be collected for specified, clear and legitimate purposes and may not be processed in a manner incompatible with these purposes.

Personal data collected for the defined purpose of order processing may therefore not be processed for other purposes, for example for advertising purposes. Rather, a separate legal basis may be required for this.

Data processing for advertising purposes

In principle, both the consent of the data subject pursuant to Article 6(1)(1)(a) of the GDPR and a weighing of interests pursuant to Article 6(1)(1)(f) of the GDPR can be considered as legal bases for data processing for the purpose of direct marketing. Whether a company can rely on its legitimate interests for data processing for the purpose of direct marketing or whether it must obtain the consent of the data subject for this purpose generally depends on a case-by-case assessment. When assessing the conditions under which direct advertising in its various forms is permissible, the values set out in the German Unfair Competition Act (UWG) must also be taken into account. Under competition law, Section 7 of the UWG regulates the conditions under which an unacceptable, unreasonable nuisance can be assumed to be caused by advertising.

If in a continuous customer account the personal data are processed for advertising purposes, it is a processing that goes beyond the mere establishment and management of the customer account. The data processing is therefore not already covered by the consent to set up and maintain the continuous customer account. In this respect, the required consent of the data subjects must be obtained separately. This can also be done during the registration or ordering process or via the settings in the customer account. It is important for practical implementation that the data subjects must actively consent to the data processing, for example by ticking a checkbox themselves. Consent is also revocable with effect for the future, so that customers must have the option of withdrawing their consent at any time - again, for example, via the account settings. It should be noted, however, that in accordance with Section 7(3) of the UWG, consent is not required for all advertising measures for existing customers; in some cases, the option to object may be sufficient.

Storage of information about means of payment

The storage of information about means of payment as part of a continuous online customer account also requires informed consent in the opinion of the DSK. The EDSA states in this regard in its recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions of May 19, 2021 that the storage of credit card data after payment for goods or services is not in itself necessary for the performance of a contract, but is merely useful to facilitate a potential next transaction and sale.

According to the EDSA, financial data should be classified as confidential personal data, the breach of which has serious consequences for the daily life of the data subject and the processing of which in order to facilitate further purchases therefore entails an increasing risk of breaches of credit card data security, as it implies processing in other systems. For this reason, in the EDSA's view, in this specific context, the fundamental rights and freedoms of the data subject would regularly take precedence over the interest of the controller when weighing the interests. In the EDSA's view, consent pursuant to Article 6(1)(1)(a) of the GDPR is thus the only suitable legal basis for the lawfulness of this data processing. In order to counter the security risks, to give the data subject the opportunity to retain control over his or her data and to actively decide on the use of his or her credit card data, the data subject's express consent should therefore be obtained before his or her credit card data is stored after a purchase. For this purpose, it is sufficient, for example, to ask directly when the payment data is entered whether the data should be stored for the next order.

Information obligations

According to the principle of transparency, personal data must be processed in a manner that is comprehensible to the data subject (Article 5(1)(a) of the GDPR). The data subjects must therefore be informed about the data processing that takes place in the context of online trade in accordance with the information obligations from Articles 13 and 14 of the GDPR. The duty to inform covers not only data processing in the context of processing orders, but also, for example, information regarding data processing when setting up and using a guest account or a continuous customer account, regarding the tracking of users, for example with the help of cookies and similar technologies, regarding data processing for advertising purposes and the storage of information about means of payment.

In practical terms, the information can be provided, for example, via the data protection declaration on the respective website. When designing the data protection declaration, care should be taken to use understandable language and to ensure clarity. The information requirements of Article 13 of the GDPR should be fulfilled when data is collected for the first time. In this respect, it makes sense to

refer to the data protection declaration in the ordering and registration processes before the data subjects complete the respective process.

Technical and organisational measures

Personal data processed in the context of online trading must be adequately protected. Controllers and processors must therefore take appropriate technical and organisational measures to ensure a level of protection for the data that is commensurate with the risk. In doing so, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons must be taken into account (Article 32(1) of the GDPR).

In this regard, the GDPR does not specify which measures must be taken specifically for which online functions. Possible measures include, for example, pseudonymization and encryption of personal data.

Data deletion

According to the principle of storage limitation pursuant to Article 5(1)(e) of the GDPR, personal data must be stored in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were processed. Accordingly, the storage period for personal data should be limited to the absolute minimum necessary.

In order to implement this in practice, the controller should provide for time limits for data deletion. In particular with regard to orders placed, there may be statutory retention periods which oblige the controller to retain the corresponding order data for a certain period of time. Insofar as the storage of data is necessary for the fulfillment of a legal obligation, an immediate deletion of order data is therefore not possible. Corresponding obligations to retain data may arise above all from commercial and tax law requirements, in particular from Section 257 of the German Commercial Code (Handelsgesetzbuch, HGB) and Section 147 of the German Fiscal Code (Abgabenordnung, AO).

For example, in the case of guest access, data that is no longer required after fulfillment of the contract must be deleted immediately in accordance with Article 17(1)(a) of the GDPR. If the data is only processed for the fulfillment of legal storage obligations, the DSK recommends that technical and organisational data blocking measures be taken to separate this data from the data in operational access.

Conclusion

The principle of data minimisation, according to which data processing must be limited to what is necessary for the purposes of processing, also applies in online trading. Without the corresponding consent of the data subject, only the personal data required to fulfill the contract may therefore be processed for online orders as a rule. This means that customers must be able to decide freely whether they wish to conclude a contract only once as part of a guest order and enter their data again each time they place an order, or whether they wish to enter into a long-term business relationship and have a continuous customer account set up. Controllers who offer goods or services in online commerce must therefore provide their customers with guest access, irrespective of whether they also provide them with a continuous customer account.

The general requirements of data protection law must also be taken into account, including data protection information obligations, data security and the principle of storage limitation.

Johanna Schmale

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net