Demonstration Use Case for the W3C’s Data Privacy Vocabulary

# Contributors (so far)

* Eva Schlehahn (ULD)
* Harald Zwingelberg (ULD)
* Bud P. Bruegger (ULD)

# Purpose

The W3C *Data Privacy Vocabularies and Controls* Community Group (DPVCG)[[1]](#footnote-1) has created two vocabularies[[2]](#footnote-2), namely the *Data Privacy Vocabulary[[3]](#footnote-3)* and the *GDPR Legal Basis Vocabulary[[4]](#footnote-4)*. This document describes a simple use case that serves to illustrate how these vocabularies can be used. For this purpose, it starts with an informal description of the use case, and then expresses its various aspects using the formal vocabularies.

The use case serves for demonstrating the use of the vocabularies and is not meant to be completely realistic or comprehensive.

# Current Status

This document so far concentrates on the informal part, while the formal parts are yet to be created.

# Informal Description of the Use Case

The use case is concerned with a realistic example of **online shopping**. It consists of multi-faceted processing activities that pursue different purposes, have different life times, and require different sets of data. These data sets may intersect. The following describes the different facets of the use case:

## Involved Entities

The example of online shopping has a number of participating entities. In particular these are:

* The online shop who acts as controller.
* One or several shipping services which for the purpose of this use case illustration are assumed to act as processors of the online shop.
* Customers who act as data subjects.

## Purposes

The processing activities of the example online shop pursue the following purposes:

* Order Processing
* Payment
* Order Delivery
* Status Notification
* Customer Convenience
* Accounting
* Customer Support
* Warranty
* Continuing Customer Relationship

While these purposes are treated separately for analytical purposes, in actual processing there may be a strong interdependency of purposes and a processing step may involve multiple purposes.

The above purposes described in further detail in the sequel:

### Order Processing

Order Processing is concerned with which items are contained in an order, how these items can be obtained internally in the shop, what their cost is, and what is necessary to package them.

### Payment

This purpose is concerned with obtaining the payment for the merchandize and the shipping of the merchandize.

### Order Delivery

This purpose is concerned with how the ordered merchandize can be delivered or shipped to the customer.

### Status Notification

This purpose is concerned with keeping the customer informed about the current status of the order. Such notifications typically include tracking information for the shipment.

### Customer Convenience

This purpose is concerned with rendering it easier to customers to interact with the online store. It focuses particularly on avoiding that customers repeated have to type in the same data. For this purpose, it is for example common to store addresses and payment instrument data across individual orders.

### Accounting

Accounting is concerned with the operations of the online shop as a commercial enterprise, as well as the legal requirements of accounting and taxation.

### Customer Support

Customer support, while potentially more general in character, is here only concerned with a single order. In particular, it has to handle cases where shipments are delayed or lost, or where the merchandize is faulty or unsuited. The according processing supports, among others, the return of merchandize and possible reimbursements.

### Warranty

The example assumes that the online shop manages the warranty of certain products. For this purpose, it needs to be possible to determine that a possibly warranty claim indeed refers to merchandize sold by the store and that the warranty period has not yet expired.

### Continuing Customer Relationship

In this example, continuing customer relationship is concerned with informing customers of special offers and new items. It is assumed that there is no customization of offers for specific customers and that the activities are therefore restricted to the delivery of information to customers.

## Legal Bases

The different parts of the processing that make up online shopping are typically sustained by different legal bases. The following discusses possible legal bases for each purpose:

### Order Processing

The purchase of merchandize from an online shop can be considered a contract. Order processing can thus be based on Article 6(1)(b) GDPR “processing is necessary for the performance of a contract”.

### Payment

Payment is also necessary for the fulfillment of the same contract and is thus also covered by Article 6(1)(b) GDPR.

### Order Delivery

The same goes for order delivery that again is covered by Article 6(1)(b) GDPR.

### Status Notification

Status notifications are today considered an integral part of the operations of an online shop. Notifications can thus be considered part of the core activities pursued to fulfill a the contract of the purchase and the legal basis is thus represented by Article 6(1)(b) GDPR.

### Customer Convenience

Customer convenience is not required for the core activity to fulfill the contract that regulates a purchase. It must therefore be an option that is offered to customers who need to grant their consent according to Article 6(1)(a) GDPR.

### Accounting

Accounting constitutes one of the core activities of any commercial enterprise. It is further governed by laws on commerce (in Germany, for example, the Handelsgesetzbuch) and taxation (in Germany, for example, the Abgabeordnung). Accordingly, the matching legal basis for the required processing in the GDPR is either Article 6(1)(f) “legitimate interests pursued by the controller” or, more fittingly, Article 6(1)(c) “compliance with a legal obligation”.

### Customer Support

Customer support is necessary for the fulfillment of the contract of a purchase. It is thus also covered by Article 6(1)(b) GDPR.

### Warranty

Warranty is also an integral part of a commercial operation. It may also be mandated by law. The suitable legal basis is thus either represented by Article 6(1)(b) or 6(1)(c) GDPR, respectively.

### Continuing Customer Relationship

An online shop informing its customer base about offers and news can under certain circumstances be based on the legitimate interest of the online shop, or alternatively it may be possible based on request (i.e., consent) by the customer. Accordingly, the legal basis is either Article 6(1)(f) or 6(1)(a).

Some EU Member states (such as Germany) have introduced further requirements compared to the GDPR in their national data protection laws. E.g. in Germany, there are differentiations made between marketing via email or via postal address. Moreover, it may be regulated nationally which customer data can be used specifically for marketing. One selected example: In Germany, \*email\* marketing for own products or products of partner enterprises needs to be based on explicit consent, thus excluding the possibility of legitimate interest.

## Necessary Data Elements

The following discusses which data elements are necessary for the different purposes.

### Order Processing

The data elements necessary to support order processing include **at least**:

* An identifier for the customer (customer number)
* An identifier and number of for each ordered item

### Payment

The data that are necessary here include the following:

* Total amount due
* Payment instrument, for example:
  + name of card holder
  + credit card number
  + expiration date
  + possibly the CVV Number ("Card Verification Value")
* Invoice data:
  + Name of person or company
  + Possibly VAT number of company
  + Billing address

### Order Delivery

To deliver an order, the following data is required:

* Shipping address
* Optionally contact information such as a telephone number that the shipping service can use to optimize delivery
* Selected shipping options (currier service, standard or express, etc.)

### Status Notification

To deliver status notifications, a suitable contact, such as an e-mail address of the customer is necessary.

While there are evidently alternative ways of delivering notifications, as for example as messages accessible from customer accounts, for simplicity it is assumed that the store pushes messages to the customer.

### Customer Convenience

Customer convenience, to avoid the need for repeated input of the same data by the customer, stores these data for later reuse. This is typically done in connection with an account that requires registration. It typically includes addresses for shipments and invoices, as well as payment instrument information.

### Accounting

XXX can someone provide input what exactly is needed here and whether this is dependent on national legislation?

### Customer Support

Customer support not only needs access to the data regarding the order, the payment, and the shipping, it also needs to manage the communications about the support case with the customer.

### Warranty

To process warranty claims, a record of which covered merchandize was sold on which date is necessary. Information about the amount paid for the merchandise may also be necessary in case of the possibility of reimbursement (in addition to repair and replacement). If the merchandise is identified by an individual serial number, storing serial number and date may be sufficient to determine whether the merchandise is still covered by warranty; in case that the individual pieces of merchandize are undistinguishable and could have been purchased elsewhere, data about the identity of the buyer maye also be necessary.

### Continuing Customer Relationship

Continuing customer relationship requires contact information, such as an e-mail address, in order to be able to send the relevant information.

## Necessary Storage Periods

Processing activities for different purposes usually have different life spans until they are completed. It is a principle of European data protection that personal data shall be deleted as soon as it is no longer needed for the purpose (data minimisation principle, see Article 5(1)(c) GDPR). The following therefore discusses how long data is needed for the different purposes.

### Order Processing

The processing of an order usually ends when the merchandize is packaged and sent off. However, when this happened, the information obtained for the order processing usually cannot be deleted yet. The reason being that the data it is still needed for other purposes such as payment, customer support, or accounting. The necessary storage period is therefore determined by these other purposes.

### Payment

Data on payment instruments is only necessary until the payment has been fully received. The data may however live on for other purposes such as customer convenience that stores this data for use in future orders.

### Order Delivery

Data needed for delivery of an order are usually no longer needed once the shipment has arrived at the shipping address. For other purposes, such as customer support, they may have to be stored longer, however.

### Status Notification

Contact information for the delivery of status notifications is no longer necessary once the merchandise has been delivered to the shipping address.

### Customer Convenience

Customer convenience data are only necessary as long as a customer has recurring contact with the online shop. In the case where a customer has not had any contact for a certain period of time (for example, a year), the data is unlikely to be further used and can be deleted. In case that the data also contains contact information of the customer, a notification in advance of the deletion may leave the choice of deletion to the customer.

### Accounting

In particular tax laws require a relatively long retention period of accounting data. For example, in Germany, certain data need to be stored for 10 years.

### Customer Support

Customer support typically requires the storage of data initially collected for other purposes (such as order, payment, or shipping) beyond the life time of those purposes. In particular, after delivery of the merchandize and thus the fulfillment of the purchasing contract, the customer must be given a certain time period (for example, 3 months), in which to initiate a customer support ticket. There may be national laws governing such time periods and the rules with which the enterprise must comply. Once this period has expired without opening a ticket, the data is no longer required. If a support ticket was opened, the communication data that was collected in order to process the ticket can be closed a certain period after the closure of the ticket.

### Warranty

Data kept to support warranty can be deleted after the expiry of the warranty period. Minimal warranty periods may be prescribed by law.

### Continuing Customer Relationship

Contact data to send informational material to customers should not be kept indefinitely, particularly if consent was used as a legal basis. Consent should always be given for a limited period of time (for example, a year) at the end of which customers can be asked to renew their consent or simply let it expire.

1. https://www.w3.org/community/dpvcg/ [↑](#footnote-ref-1)
2. https://www.w3.org/community/dpvcg/2019/10/01/two-vocabularies/ [↑](#footnote-ref-2)
3. https://www.w3.org/ns/dpv [↑](#footnote-ref-3)
4. https://www.w3.org/ns/dpv-gdpr [↑](#footnote-ref-4)