PrimeLife Checkout -

Ulrich König

PrimeLife Checkout -
a privacy-enabling e-shopping user interface

Ulrich König

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Germany
ULD61@datenschutzzentrum.de

Abstract. The PrimeLife Checkout user interface aims at supporting the user in enforcing her privacy preferences in an online purchase process. The user can choose how much privacy protection she wants, and the system visualises what shipping and payment methods are matching with her needs or why the selected methods are not suitable for the protection level of her choice. The interface displays which personal data will be transferred to whom for what purposes in a user friendly way. In most webshops, this information can only be retrieved by reading the shop's full privacy policy. In contrast, the proposed approach informs the user what happens with her data for which purpose while she is entering her data. Thereby it specifically addresses the challenge of a user friendly and more transparent policy display.

1 Introduction

The PrimeLife[1] Checkout user interface (PLC) is designed to give users control of their data in a checkout process. Usually the web-based checkout process works with many small steps. In each step today's checkout systems ask the user for specific data, like name, e-mail address, payment information etc. After each step, the data are transferred to the server of the webshop where the user has no control what the shop operator does with the data. Some shops employ scoring systems that use the data collected so far to decide which payment methods they offer to the user in a later step, as described in [LEP+01].

The PLC offers a different approach. The user-entered data will be checked on the local machine of the user to see whether they are valid. The rules for validating the data have to be provided by the shop at the beginning of the transaction. In this particular demonstrator, this is done with JavaScript entirely on the user's side. No data will be transferred to the service until the user finally confirms that she is willing to perform the purchase and all checks are done. Only when the user finally confirms, the data will be transferred to the webshop.

This text is organised as follows: Section 2 explains the "three steps design" chosen for the PLC. Section 3 outlines the different components of the PLC

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no 216483 for the project PrimeLife.

demonstrator and shows their functionality. The technical background is described in section 4, followed by evaluation results in section 5. Finally, section 6 summarises the findings.

2 Three steps design

In the online shopping process, users typically have to go through a number of steps to complete the checkout process. In every step, they have to enter and transfer personal data, like shipping address payment information etc. For example, seven steps are needed to buy something at amazon.com as visualised in Figure 1. However, usability tests of the multiple steps "Send Personal Data" dialogue performed in the PrimeLife project showed that users regarded six steps only for the data collection as too many [WP410]. The user has no knowledge if the data that she has entered will be accepted by the system, which is a problem.

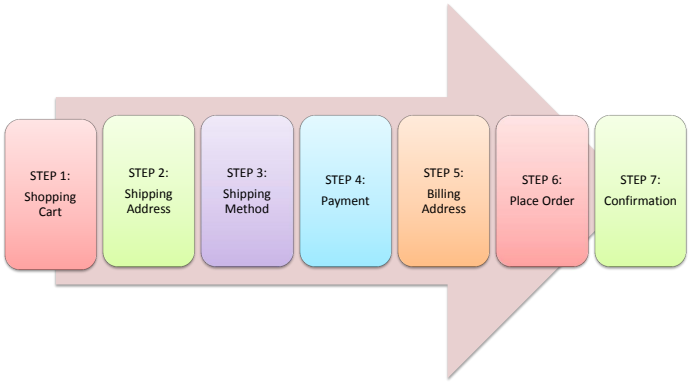

Fig. 1. Seven Steps solution by amazon.com.

A typical scenario is that the user has to enter data and click "next" for the next step where again she is asked for data. The whole set of data collected in one of the steps will immediately be sent to the server, where its validity is checked. If all data is correct, the user is taken to the next step. If not, the user will receive an error notice, has to fix the problem and try again. She has no control what the webshop does with these data until the transaction is finished or cancelled. In addition, the user will not know whether the privacy policy of the shop fulfils the user's requirements. For example at amazon.com, the user is told in step 6 after she has entered and transferred all her data to the amazon.com server: "Please review and submit your order", "By placing your order, you agree to amazon.com's privacy notice and conditions of use". Interested users may follow the link to the privacy policy displayed on all pages of the shop, but users are not actively notified on the parts of the privacy policy relevant to the transaction.

In general, another popular way of using data within the checkout process is to request a score value from credit agencies without the users' consent or at least without clearly informing the users. The offered payment methods are selected by the result of the score [LEP+01], instead of asking the user beforehand to whether such a credit rating is necessary at all. This is not the case when the user opts for cash on delivery or any form of prepayment.

The PLC solution chooses a different approach. The objective is to collect all necessary data in one single step. The moment the user enters the data, PLC will check their validity. This step is performed within the realm of the user's browser without transferring any data to the server. Therefore, the whole validity check is done before any data will be sent to the webshop's server[2]. The user gets instant feedback if the entered data are formally valid and fulfils all requirements from the service or if she has to correct something.

PLC can be used in two different ways. It can be integrated directly into the webshop interface, so that it is seamlessly usable by the user in her browser, or it can be installed on the user's computer as a stand-alone application. The details are described in section 4.

The resulting steps are shown in Figure 2 – the procedure just needs three steps for the purchase, the user gets instantaneous feedback, and she may correct her data if needed. This reduces the necessary amount of clicks required to finish the user's purchase. The individual steps are described in sections 2.1-2.3.

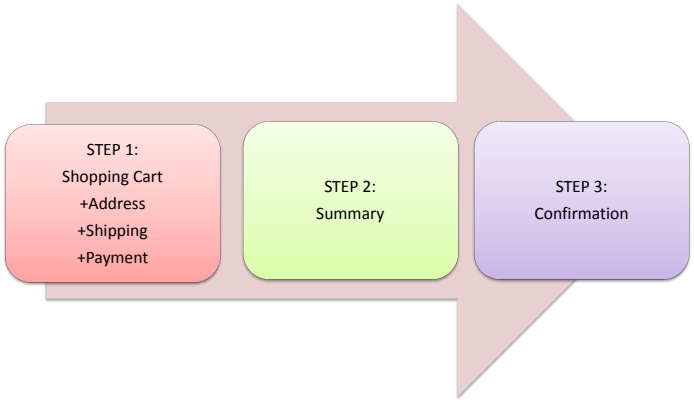

Fig. 2. PrimeLife Checkout three steps solution.

[2] To perform this step, the webshop needs to transfer all of its validity checks to PLC. This may seem like a heavy burden, but it has two advantages: The user will get a clear overview, which data she has filled in and is going to share and the user does not disclose any of her data until she finally confirms to complete the order. A thorough evaluation can be found in [WP410], section 5.2.

The major advantage of the PLC solution presented in this section is that all data will only be transferred at the end of the process in one data container and only if the user finishes the whole process. The webshop cannot score the user and select payment methods by the score value without the user's consent. If the user cancels the process at any time, no data will be transferred to the server.

Some would argue the disadvantage of the PLC is that by putting all of the fields the user has to fill out on one screen, the screen is getting to complex, and the user may be overwhelmed. They might argue that an Amazon like step-by-step solution is easier to understand. However, two points can be raised to defend PLC: First, users get a clear overview what data is required for the transaction from the beginning. The information is not hidden in the different steps, which are only accessible, if the user has filled out all fields in the steps before correctly. Second, while only a very small number of user tests have been conducted so far, the complexity of the screen was never an issue in the test results.

2.1 Step 1: Shopping Cart

In the first step, the user has to enter all necessary data to perform the purchase as shown in Figure 3. She is informed that she is in step 1 out of 3 and that no data will be transferred to the webshop until, she confirms the data transfer in the next step. The user will also get a view on her current shopping cart with the option to change the amount of the selected items.

Details about Figure 3 can be found in section 3.

2.2 Step 2: Summary

In step 2, the PLC will display all the data that have been collected in step 1 again in the same layout without the option to modify them as shown in Figure 4. The user has the opportunity to save the data that she entered in step 1 plus information to whom the data may be transferred for what purposes, to her privacy settings. She can check if all data that she has entered are correct and confirm the purchase and data disclosure by clicking on the "Order and Transfer Data →" link or go back and make changes by clicking on "← Return to Shopping Cart".

The goal of this step is to give the user a final view on her purchase, what data will be transferred to whom for what purposes, before finally confirming the purchase, and data transfer.

2.3 Step 3: Confirmation

In step 3, the PLC confirms the purchase. It also notifies the user that the entered data have been transferred to the service providers listed in the "My Data" field and in the bar on the right side. The user has the opportunity to save the privacy settings for future use and reference.

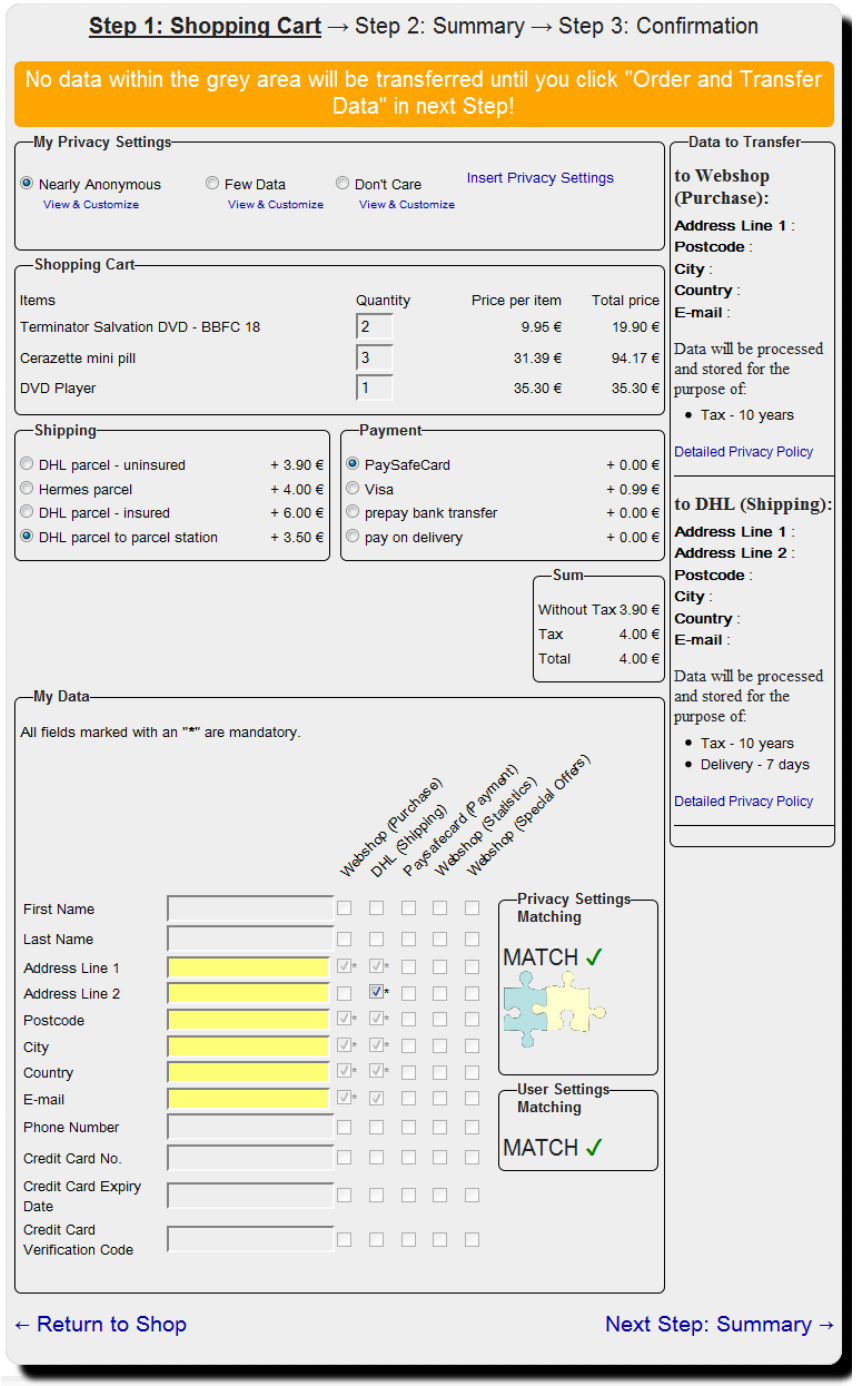

Fig. 3. Step 1: Shopping Cart.

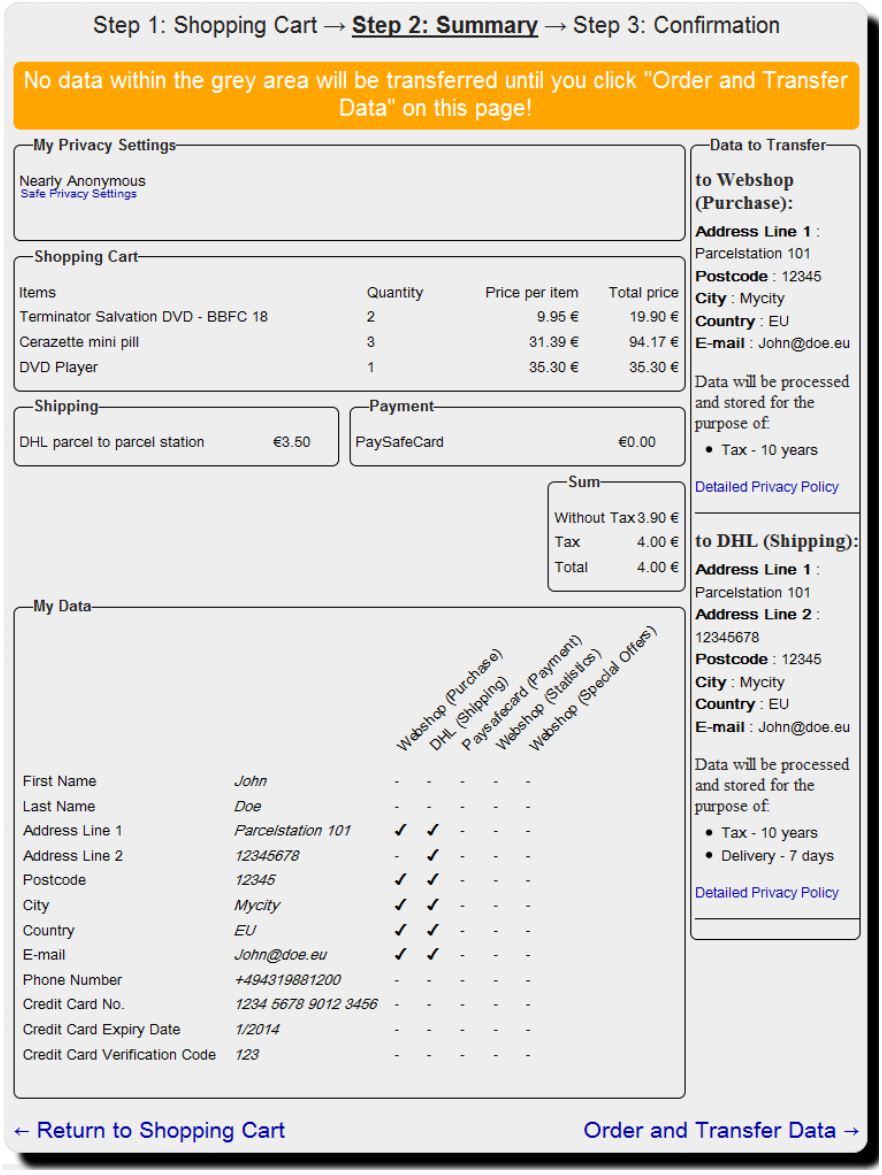

Fig. 4. Step 2: Summary.

3 Components of the PLC

In this section, we provide a short description of the components of the PLC.

At the top of the PLC user interface, there is an overview of all steps where the current step is displayed in bold and underlined font. In step 1, the user gets the information that no personal data entered within the grey area will be transferred until the user finally clicks "Order and Transfer Data". In step 3, this box will show the confirmation that the data have been transferred to the recipients listed in the right bar, see Figures 3, 4.

3.1 My Privacy Settings

An important part of the PLC is the "My Privacy Settings" box illustrated in Figure 5 where the user selects her preferred privacy settings. There are three predefined settings available: "Nearly Anonymous", "Few Data" and "Don't Care". In addition, there is a field for the user to insert her privacy settings with the help of a policy editor.

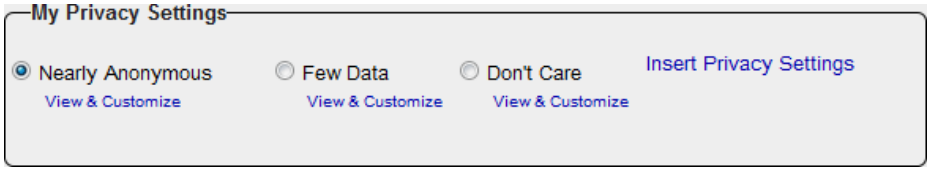

Fig. 5. "My Privacy Settings".

The standard privacy settings are predefined and always the same. The user has the option to use her customized privacy settings by using the "Insert Privacy Settings" link. The names of the privacy settings should indicate how much personal information the user is willing to disclose:

- "Nearly Anonymous" is the most restrictive setting where the user wants to reveal as little personally identifiable information as possible, i.e., she desires to act anonymously. In web transactions, complete anonymity is hard to obtain or measure. This is why we have called this setting "Nearly Anonymous", to prevent a false sense of safety in users.
- With "Few Data" the shop, the shipping company and the payment provider will only get the data necessary to perform the transaction, by default. So the default of "Few Data" is identical with the "Nearly Anonymous" settings. The difference to "Nearly Anonymous" is that a user can agree to transfer more data than necessary in the "Nearly Anonymous" case. This might enable the user to e.g. select a different payment provider. Additional purposes for data collection and data usage such as marketing are disabled by default within this setting.

– The setting “Don’t Care” disables all restrictions. The user can configure to disclose her data without being warned by the system that the webshop’s privacy policy does not match with her privacy settings.

3.2 My Data

The “My Data” box shown in Figure 6 contains text fields in which the user can enter personal data requested by the service provider. It also contains a matrix in which the user can use checkboxes to select which data should be transferred to whom for what purposes.

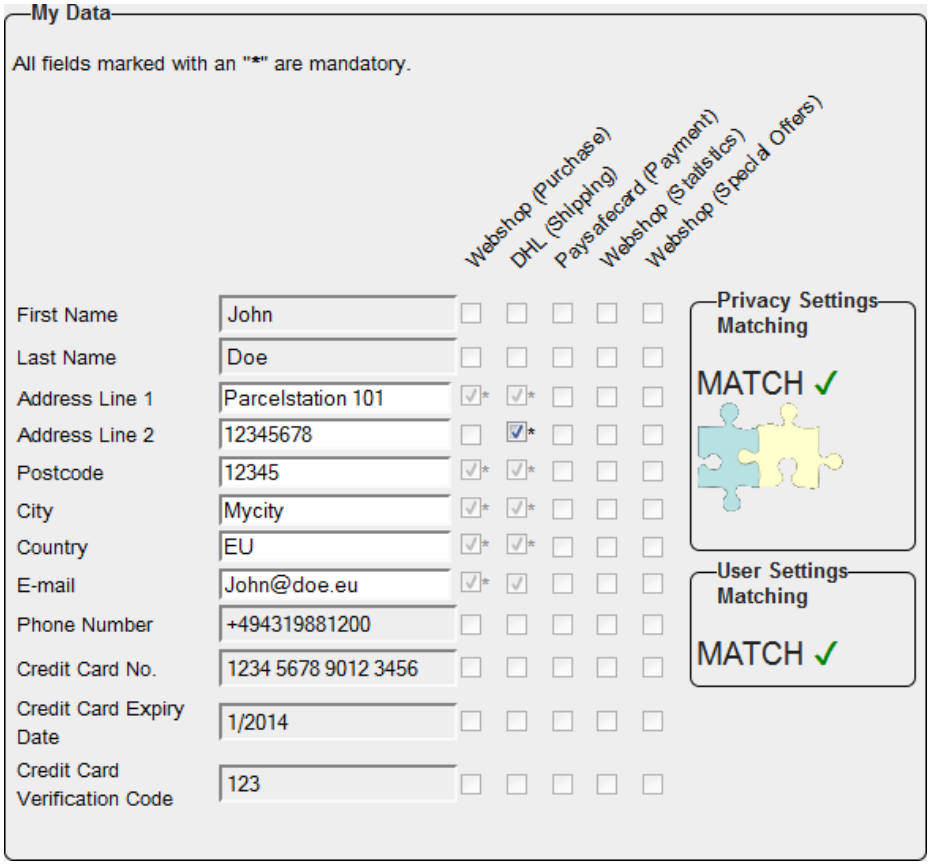

Fig. 6. “My Data” field including matching results.

Text fields In the text fields, the user can enter the personal data requested. The fields are greyed out if data for that respective field are not requested by the

service provider, yellow if the information in the field is necessary for completing the transaction but not provided yet or filled out incorrectly, and white if the data are necessary and filled out correctly.

One issue with the use of colours relates to colour-blind users that cannot perceive the difference between a yellow and a grey field. A solution could be a symbol behind the text field, which indicates the status of the text field. This has not been implemented within PLC.

Checkboxes The checkboxes are arranged in a matrix with data fields as rows and the combination of data controllers and the respective purposes as columns. Every checkbox symbolises whether information from the user is disclosed to a data controller or not. If there is an asterisk next to a checkbox, the data field is mandatorily requested by the data controller. To successfully perform the purchase, the user has to give her consent to allow the respective processing by checking the checkbox next to the asterisk. Otherwise, there will be a mismatch between the "Privacy Settings" and the "Privacy Policy" of the data controllers in the involved column. In such a case the user may seek for a different option which does not require this type of data, e.g., to opt for an anonymous payment method or to choose a shipping provider who allows anonymous pickup of the shipped goods.

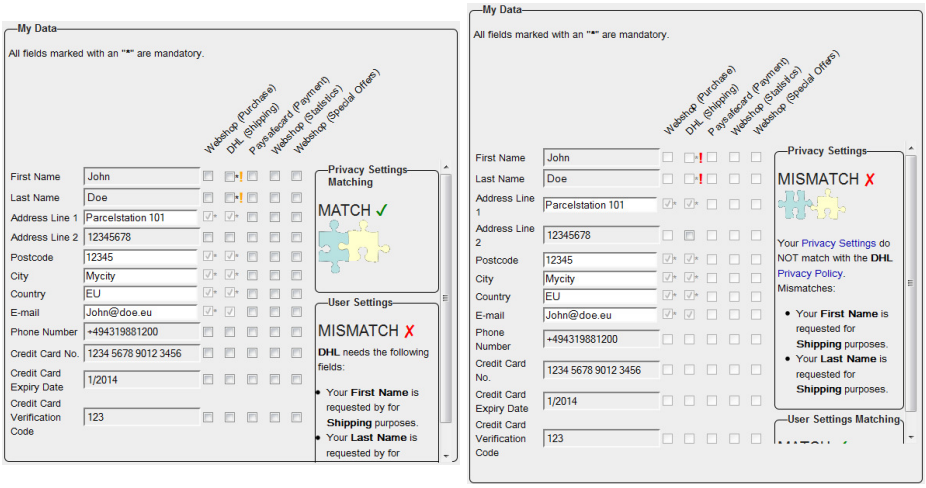

Fig. 7. Left: "My Data" field with a "User Settings" mismatch. Right: "My Data" field with a "Privacy Settings" mismatch.

Matching The PLC matches the "Privacy Settings" selected by the user with the "Privacy Policy" of the different data controllers. The choice of the "Privacy

Settings" determines the statuses of the checkboxes in the matrix. The "Privacy Policy" of the data controllers is compared with statuses of the checkboxes in the matrix. If both are matching, there will be a "MATCH ✓" in the box on the right side of the matrix, otherwise a "MISMATCH ✘". If the mismatch can be resolved by the user without changing her privacy settings, there will be an orange exclamation mark "!" on the right side of the checkbox where the mismatch is located and the mismatch will be displayed in the "User Settings Matching" box as illustrated in Figure 7. If the user has to change the Privacy Settings in order to resolve the conflict, the exclamation mark will be red and the mismatch will be displayed in the "Privacy Settings Matching" box as shown in Figure 7. The details of the mismatches are displayed in the boxes on the right side of the matrix. Visibility impaired persons can distinguish the different mismatches with the help of the text in the boxes. The user can only proceed with the shopping transaction if there are no mismatches.

Overview of data transfer One main objective of the PLC is to visualise in a user-friendly manner what will be done with the data disclosed by the user. This is expressed by a list of all data the user has entered which shows all involved data controllers with all data fields (attributes) and field content (attribute values) that will be transmitted if the transaction is completed. The list is updated in real-time so that the user can immediately observe consequences of all her changes. To establish this, the "Data to Transfer" box on the right side of the user interface displays for each data controller what data will be disclosed for what purposes and what will be the data retention periods for the respective purposes, see Figure 8. Besides, links to the full privacy policies of the data controllers are provided to comply with the Art. 29 Working Party recommendation on multi-layered privacy policies [Par04]. The "Data to Transfer" box confirms the user input while the "My Data" box is used to input data.

4 Technical issues

This section deals with some technical issues of the PLC. Section 4.1 describes alternative ways how data of the user can be transferred to third party data controllers. Section 4.2 describes different options how PLC can be used and deals with some technical issues.

4.1 Direct data transfer

In the "classic" approach, the user transfers all her data to the webshop from the first step of the buying procedure onwards. If necessary, the webshop forwards the information to the other data providers, also called downstream data controllers [ABD+09]. The problem is that the webshop gets the complete data set of every user, including information not necessary to perform the transaction.

There are two alternatives to this "classic" approach. The first solution may be to transfer the necessary data directly to the third parties and other service providers (downstream data controllers), e.g., the shipping address directly to the shipping company and the payment data to the payment company. In this case, the webshop would just need a primary key for each process and the corresponding data provider. The second solution for such downstream controllers could be to encrypt the data with the public key of the downstream provider and then forward this to the provider via the webshop.

Neither of these options has been implemented in the PLC because the PLC is just a GUI-demonstrator, but in any implementation in a real life environment, it is an important design decision how to transfer the data to the downstream controllers and how to make this transparent to the user.

For example: A user wants to buy "The Blues Brothers" DVD at a webshop using the shipping services of DHL and the payment services of Visa Card. The webshop gets the information that the user wants to buy "The Blues Brothers", that the payment is done by Visa Card with the primary key 156345 and the shipping will be done by DHL with the primary key 95328. Visa gets the information that the user wants to pay €10, with credit card no. 1234-5678-9012-3456, valid until 10/2015 with card security code 987 to the owner of the primary key 156345. DHL gets the information that one parcel with the primary key 95328 has to be shipped to Holstenstr. 98, 24103 Kiel, Germany. Visa informs the webshop that €10 from primary key 156345 has been paid and will be transferred to the webshop. The webshop passes the DVD to DHL with the primary key 95328 and pays the shipping costs. DHL ships the DVD to the user.

This architecture enables the user to expose her private data to a minimal group of data providers. For each of these providers only a minimal set of data is exposed. This approach works under the assumption that the data providers have a privacy policy that does not allow forwarding data to another data provider with a foreign purpose and that the data providers obey to their own privacy policy.

Fig. 8. "Data to Transfer" box.

4.2 Low barriers for usage

The PLC could run directly from the website of the webshop or in a standalone program on the user's computer. All the users need is a web browser with JavaScript support. This lowers the barrier for users who do not know PLC and do not want to install anything from a third party on their computer or if their operating system is not supported. The output of PLC is also designed to be screen reader compatible, to enable visually handicapped people to use it, too.

Users can also install PLC directly from PrimeLife Website or another trusted party on their PC, so that there is no way of manipulation by the shop provider. The necessary data to perform the transaction has to be provided by the shop provider at the beginning of the transaction. This includes validation checks for the personal data of the user, additional costs for different shipping and payment methods and allowed payment and shipping methods. To transfer this data from the shop provider to the PLC a policy language similar to the PrimeLife Policy Language [ABD+09] is needed, which ensures that requirements and checks are performed correctly. All checks have to be done offline. If code is transferred that will be executed on the users' computers, it has to be ensured that this code runs in a sandbox like environment, without network or file access. The research of such a policy has not been done within the research of PLC. If data has to be transferred for a validation or availability check, the user has to give her informed consent to transfer the specific data. A user-interface-demonstration is available at [Kö10].

5 Evaluation

The PLC has shown some strength in discussions with other researchers, e.g. the "Data to Transfer" section was well accepted. It is an easy way to make transparent to the customers what data will be transferred for which purpose to whom.

The three-step design is also a big step forward to bring privacy to the users. Most webshops are designed to make it as easy as possible for the customer to buy something. The goal is to lose a minimal amount of customers during the checkout process. Nevertheless, easy is not equal to transparent. Nowadays transparency becomes a more and more important issue for customer in times of phishing, identity theft, and massive data warehousing.

On the other hand, the PLC has some weaknesses. One of the major weaknesses are the checkboxes in the "My Data" section. There are too many checkboxes. It is difficult for users to understand what to do with all of these boxes. Users may not understand that they are giving their consent by clicking a checkbox to transfer data.

Another problem is that the user has too many choices. Many of the combinations of choices that are possible to select in the GUI make no sense and will lead to some kind of error. It would help the user a lot if the GUI would prevent the selection of senseless combinations. It may also help if all payment/shipping

providers that not compatible with the chosen "MyPrivacySettings" would be hidden or visually disabled. E.g., rows with unused fields like the credit card number are even displayed, when they are not needed. In addition, unused columns are displayed even if they are not used e.g. when the user has selected nearly anonymous, a column for marketing purposes makes no sense.

In addition, an automatic mismatch solver would probably help the users to deal with the PLC-Interface. Moreover, it has to be taken into account that the interface should make it easier to select a privacy friendly solution than giving the consent into privacy unfriendly data processing.

There has been an evaluation of the PLC done by Staffan Gustavsson, but with just five participants, so the results are not very reliable. It can be found in [WP410], section 5.2.

6 Conclusion

PLC introduces a new way for the checkout process in three steps that makes the whole process more transparent for the users compared with other multiple step processes. The concept may influence the design of real life webshops, if privacy becomes a selling point, beside the price.

If privacy becomes a selling point, there is a good chance that privacy-aware webshops are going to include something like the "Data to Transfer" box into their website because this would support the intelligibility of their privacy policy. The other parts of PLC contain many valuable ideas, but need some reworking before they can be transferred into productive systems.

The next step is to make privacy more transparent and comparable in a way that webshops start to compete not just with the price, but also in terms of who is guaranteeing the best privacy and making this process transparent to the potential customers.

References

ABD+09. Claudio A. Ardagna, Laurent Bussard, Sabrina De Capitani Di, Gregory Neven, Stefano Paraboschi, Eros Pedrini, Stefan Preiss, Dave Raggett, Pierangela Samarati, Slim Trabelsi, and Mario Verdicchio. Primelife policy language. Available online: `http://www.w3.org/2009/policy-ws/papers/Trabelisi.pdf`, 2009. 4.1, 4.2

Kö10. Ulrich König. Primelife checkout livedemo. Available online: `http://www.primelife.eu/images/stories/releases/checkout/PrimeLifeMockUp_3_2.html` or `http://is.gd/e3AFr`, 04 2010. 4.2

LEP+01. Peter Loosemore, Christian Egelhaaf, Erik Peeters, Sune Jakobsson, Kostas Zygourakis, and Niamh Quinn. Technology assessment of middleware for telecommunications. *Eurescom Project P910*, April, 2001. Available online: `http://www.eurescom.eu/~pub/deliverables/documents/P900-series/P910/TI_5/p910ti5.pdf`. 1, 2

Par04. Article 29 Data Protection Working Party. Opinion on more harmonised information provisions. Available online: `http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf`, November 2004. 3.2

WP410. WP4.3. UI prototypes: Policy administration and presentation - version 2. In Simone Fischer-Hübner and Harald Zwingelberg, editors, *PrimeLife Deliverable 4.3.2*. PrimeLife, `http://www.primelife.eu/results/documents`, June 2010. 2, 2, 5