

## Short Public Report

**1. Name and version of the IT-based service:**

CARGLASS Data Exchange with Insurance Companies. Based on the functionality of the version available in November 2014.

**2. Provider of the IT-based service:**

Company Name:



CARGLASS GmbH

Address:

Godorfer Hauptstr. 175, 50997 Cologne, Germany

Contact Person:

Manfred Moos

**3. Time frame of evaluation:**

June 2014 – November 2014

**4. EuroPriSe Experts who evaluated the IT-based service:**

Name of the Legal Expert:

Marco Schröder

Address of the Legal Expert:

c/o 2B Advice GmbH  
Joseph-Schumpeter Allee 25  
53227 Bonn

Name of the Technical Expert:

Hajo Bickenbach

Address of the Technical Expert:

c/o 2B Advice GmbH  
Joseph-Schumpeter Allee 25  
53227 Bonn

**5. Certification Authority:**

Name: EuroPriSe Certification Authority

Address: Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

E-Mail: [contact@european-privacy-seal.eu](mailto:contact@european-privacy-seal.eu)

**6. Specification of Target of Evaluation (ToE):**

The scope of the certification comprises the following elements:

- CARGLASS's technical interface through the GDV (German Insurance Association) for the purposes of:

- Coverage inquiry (S1)
- Forwarding of damage data / invoice to insurance companies (S2)
- CARGLASS's direct technical interface to the insurance company (2 insurance companies)
- Web application "Extranet," provided it is being used by CARGLASS as an interface for the input of (potential) customer data by the insurance company (S3)
- Obtaining declarations of consent through various customer contact options
- Security mechanisms utilized during transfer (encryption, credential management)

The following elements at CARGLASS fall outside the scope of certification:

- Application branch (operative order fulfillment)
- Oracle ERP Business Suite including database
- Invoicing and reminders
- Web application "Extranet" (see exception above)

The following third-party elements are also outside the scope of certification:

- Hardware or software used by the GDV or insurance companies
- Data transmission over networks of third parties

#### 7. **General description of the IT-based service:**

CARGLASS GmbH deals exclusively in the repair or replacement of glass panels in automobiles coupled with a very long warranty for their installation services. In the scope of these services, CARGLASS strives to relieve the customer of as much of the necessary work involved in such repairs as possible. This also includes communication with insurance companies which are often called upon for glass repairs.

As part of order processing, this communication serves three different purposes:

1. The performance of a coverage inquiry in order to be able to directly bill the insurance on the basis of the received information and to spare the customer the effort of settlement with the insurance company.
2. The transfer of customer damage reports. These are generated during processing, signed by the customer, and sent in his or her name to the insurance company (including assurance of assignment) in the context of order processing and accounting.
3. Additionally, insurance companies may have interest in handling as many of their customers' glass damages through CARGLASS GmbH as possible. To this end, they can "register" customers with CARGLASS GmbH themselves if the customers contact their insurance company initially.

The respectively required declarations of consent are dealt with in a uniform way for all customer contact options by the order processing "Branch," an in-house development of CARGLASS GmbH which is only part of the ToE with regard to this function.

The insurance interfaces are a largely automated process and handle communication between CARGLASS and insurance companies in the background as part of order processing. The data which will be transferred are extracted out of the order processing data and automatically transmitted. This prevents accidental excessive data transfers.

An exception exists in the case of transfer of customer data from insurance companies or agents to CARGLASS GmbH for the purpose of the "registration" of their client as a potential customer. In this case, the employee of the insurance company (e.g. a call center agent who takes the customer's call) will transfer the customer data over the web application "Extranet."

### **Online Coverage Inquiry:**

In the event of an insurance claim, it can be determined through an online inquiry whether an existing policy with the insurance company covers the given claim and whether the customer has to pay a deductible.

If a customer refuses the retrieval of a coverage inquiry, he or she may thus be handled as a direct payer. Settlement with the insurance company is then his or her personal responsibility.

At this point the coverage inquiry is not performed.

If not already performed before closure of the contract, the inquiry is performed without consent upon closure of the contract in all cases where the customer claims insurance coverage. This is done on the basis of a legitimate interest of CARGLASS.

The coverage inquiry is always performed fundamentally in the same way, namely by the transmission of an unambiguous identifier (license plate and possibly insurance number) in a request and, in response, the transmission of coverage information and possibly a deductible. This is performed either using a service provided by the GDV or directly with the insurance company.

### **Glass damage report and billing**

The customer whose insurance shall pay the damages must furnish a damage report for the insurance company such that it accepts the costs. The customer must therefore settle the balances resulting from their contract with CARGLASS and subsequently submit a glass damage report in order to request reimbursement from the insurance company.

A glass damage report is recorded and it is noted on the print-out that an assurance of assignment shall take place. The customer confirms this with a signature and the result is sent to the insurance company via the GDV and charges are settled directly with the insurance company.

### **Customer data in advance from the insurance company**

In the special case where the customer first contacts his or her insurance company to discuss the repair of damages, the insurance company can “register” the customer with CARGLASS through the web application “Extranet.”

In this case, an employee of the insurance company (e.g. the call center agent who takes the customer’s call) will enter these data into a web form which is available in a password-protected area of the CARGLASS Extranet (<https://www.carglass4partners.de/>).

## **8. Transnational issues:**

The data are transferred from Carglass branches in Germany to insurance companies in Germany. No transfers across national borders take place.

## **9. Tools used by the provider of the IT-based service:**

- IBM MQSeries Message Queue Client
- Microsoft Windows Server
- Microsoft Internet Information Server
- Oracle EBusiness Suite with development environment

## **10. Edition of EuroPriSe Criteria used for the evaluation:**

EuroPriSe Criteria (November 2011)

## **11. Evaluation results:**

### **Fundamental aspects of processing**

CARGLASS offers customers the option to let CARGLASS handle the charges through the customer's insurance company. The necessary coverage inquiries for this purpose are handled in the interfaces which have been examined for this certification. Insurance companies can arrange appointments for repairs quickly and easily for insurance holders if they so wish. The arrangement of repair orders by customer request is handled through the web interface which has been examined for this certification.

### **Processed personal data**

The processing of personal data is limited to those data which are necessary for monetary processing and underwriting. In particular, direct transfers to insurance companies are completely free of secondary data; the data which shall be transferred are only available until the successful transfer is ensured.

### **Fundamental technical setup**

Pseudonyms are used for inquiries in all cases. The license plate number is used as the pseudonymous label. In addition, in the two cases in which the inquiry does not take place over the GDV interface, the insurance number is used.

### **Transparency and description**

The interfaces for coverage inquiries are technically documented and implemented in CARGLASS's order system. Only the necessary data to confirm insurance coverage for the damages are exchanged over the interface. The alteration or use of the interface by individual employees is not possible. Before performing the coverage inquiry, the employee must obtain the consent of the customer. This is documented in CARGLASS's order system. The customer is thus informed which data is transmitted to what places for the purposes of the coverage inquiry.

The web interface for the referral of insurance holders has an informative, comprehensively written data protection statement. The users (insurance employees) have access to an extensive brochure about usage of the web interface in line with data protection standards. Only fields which are absolutely necessary for the referral are marked as mandatory.

### **Legal basis**

The coverage inquiry is, depending on the configuration of the order, justified by the consent of the data subject or absolutely necessary for the fulfillment of the contract with the data subject. The usage of personal data for settlement and processing of the repair order is required for the execution of the contract with the data subject. The usage of personal data of the data subject during the referral of a repair order by the insurance company is covered by the consent of the data subject.

### **Extent of data processing**

The coverage inquiry takes place over the interface through the use of pseudonyms. During referral of repair orders, the mandatory entries are limited to the name and necessary contact details to make an appointment. Pictures of the damage can be uploaded; employees of the insurance company are informed that no personal data other than the

representation of the damage may be visible. Information is only recorded in text fields if it is necessary for the performance of the repairs. The insurance employees are explicitly informed of this in the brochure for the web interface.

Altogether, the extent of the data processing can be evaluated as markedly low.

### **Sensitive data types**

Special types of data do not appear in the interfaces for coverage inquiry or settlement.

Special types of data are not fundamentally necessary. However, one cannot rule out that certain individual circumstances can make such information necessary during referral, if for instance the repair must be performed on site at the data subject's location and the health of the data subject must be considered. Such information may only be recorded in absolutely exceptional cases with the express consent of the data subject. The insurance employees are explicitly informed of this in the brochure for the web interface.

During the referral of repair orders, one cannot rule out that insurance employees record special types of data in text fields in justified individual cases. The circumstances in which this is permissible are described in the brochure for users of the web interface.

### **Special requirements during the processing steps**

Before the coverage inquiry, service center employees must ask the data subject for his or her consent. This is depicted and ensured through a corresponding dialogue step in the repair administration system. The question text is set in the system.

For referral of repair orders, the consent of the data subject must be obtained by the insurance employees. This is also made clear in the brochure for the use of the web interface.

### **Technical measures**

On the level of security technology, CARGLASS enforces an appropriate security level through the following measures:

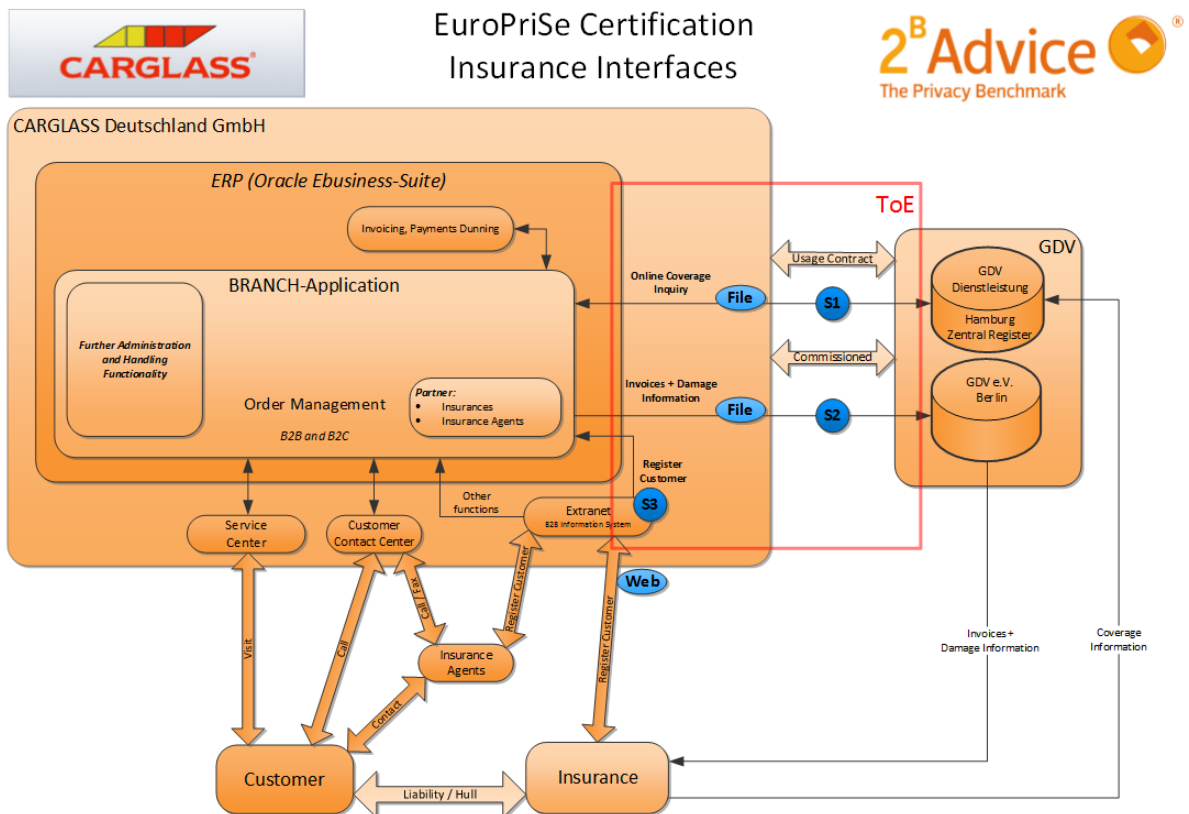
- Encryption of data transfer meets the state of the art continually and consistently,



- its own redundant computer centers and server systems with appropriate connectivity with each other and with the outside, access protection and physically secure construction,
- segmentation of the internal network and limitation of possible access to data functions which are impermissible for the relevant location,
- usage of up-to-date firewall systems and secure network technologies for linkage to external locations (MPLS) and to the alternative computer center (dedicated fiberglass cables),
- active monitoring of all relevant components and regular patches and updates,
- implementation of an emergency and outage concept with a strategic orientation toward increasingly automated processes in the scope of the necessary system redundancy for this goal.

When commissioned service providers are engaged, Carglass ensures that the necessary contracts are available and that the commissioned service provider is controlled.

12. Data flow:



13. Privacy-enhancing functionalities:

*How does the IT-based service enhance privacy?*

The actual transmission mechanism is completely automated, which ensures that the data-protection-compliant function of the system cannot be compromised by improper intrusions. In addition, for the only situation in which data (before transfer to the insurance companies) can be transferred manually through the Extranet to CARGLASS by insurance employees, there is an extensive brochure which informs users excellently about all relevant data protection aspects and facilitates a competent and constantly informed usage. In particular, the brochure informs the user of the Extranet that entries and referrals through the interface S3 may only be performed with the agreement of the insurance holder. For all optional fields, the brochure contains extensive information about the types of data, the situations, and the purposes for which the field can be used. In cases of uncertainty, the brochure contains the contact data of the data protection officer who is responsible for ensuring that the measures detailed in the brochure are com-

plied with. The brochure is available to all users of the interface S3 at -  
<https://www.carglass4partners.de/datenschutz/merkblatt.html>.

14. Issues demanding special user attention:

There are no circumstances in which S1 or S2 require special caution from their users.

The interface S3 contains optional fields, whose usage and purpose are transparently explained in an application brochure for the users of the Extranet.

15. Compensation of weaknesses:

N/A

16. Decision table on relevant requirements:

<b><i>EuroPriSe Requirement</i></b>	<b><i>Decision</i></b>	<b><i>Remarks</i></b>
Data Avoidance and Minimisation Datenvermeidung und -sparsamkeit	<i>adequate</i> <i>adäquat</i>	Only data which are directly connected to and necessary for the processing are transmitted.
Transparency Transparenz	<i>excellent</i> <i>exzellent</i>	User access by CARGLASS and insurance employees is avoided as much as possible. For all cases in which this is required, the highest possible transparency is provided for. The extensive and easily comprehensible brochure for the usage of the interface S3 by insurance employees especially promotes the data-protection-compliant application of the referral interface.
Technical-Organisational Measures Technisch-organisatorische Maßnahmen	<i>adequate</i> <i>adäquat</i>	Strong protection of the transmission routes, technically secure limitation to the necessary functionality, and a continuously up-to-date state of the network security components.
Data Subjects' Rights Rechte des Betroffenen	<i>adequate</i> <i>adäquat</i>	Collection of data and consent declarations, but the rights of the data subject are always transparently safeguarded for the customer.

## **Experts' Statement**

We affirm that the above-named IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

---

Place, Date	Name of Legal Expert	Signature of Legal Expert
-------------	----------------------	---------------------------

---

Place, Date	Name of Technical Expert	Signature of Technical Expert
-------------	--------------------------	-------------------------------

## **Certification Result**

The above-named IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

---

Place, Date	Name of Certification Authority	Signature
-------------	---------------------------------	-----------