



Short Public Report

1 Name and version of the IT-based service:

Lidl Zentrale Kassenprüfungssoftware (Version: 5.4 April 2016)
Central Cash Register Audit Software

2 Provider of the IT-based service:

Company Name:

Lidl Stiftung & Co. KG

Address:

Stiftsbergstr. 1
74167 Neckarsulm

Contact Persons:

Mr. Brosch, Mr. Masuda

3 Time frame of evaluation:

December 2013 – May 2016

4 EuroPriSe Experts who evaluated the IT-based service:

Name of the Legal/Technical Expert:

Prof. Dr. Friedrich Holl

Address of the Legal/Technical Expert:

Hektorstraße 7
10711 Berlin

5 Certification body:

Name: EuroPriSe Certification Authority

Address: Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

eMail: contact@european-privacy-seal.eu

6 Specification of Target of Evaluation (ToE):

The components of the IT-service:

- automated detail analysis,
- manual cash ratio analysis,
- the keeping of logs as responsible agency.

The components of the corresponding processes:

- preparing the POS data for evaluation,
- the processes of POS audit,
- the retransmission of the data to the distribution company / sales agency,
- Notification of Lidl Stiftung on accomplished / not accomplished measures.

Components not included in the certification:

- Programming the central cash register audit software because it is carried out by another company in order.
- The basic Lidl Stiftung management information system as data supply to the central cash register audit including its back-up, recovery and archive.

7 General description of the IT-based service:

The central cash register audit software is used to analyze the POS data to detect manipulation in the POS payment process. To this end, scenarios are used that map now known or probable or possible fraud incidents. These scenarios, based on experienced thresholds values, are used to do fraud cash register using actual POS data of Lidl stores. In addition, an individual ratio analysis is performed that uses exceedances as basic parameters for an analysis of possible violations.

These analyzes are implemented on a database resulting from the daily transmitted data to Lidl Stiftung & Co. KG (Lidl Stiftung) from all stores. It is also used for different management processes and evaluations. The database basically processes only pseudonymous data; a direct reference to individuals does not exist at this POS data. Personal information can be restored later and exclusively in the case that manipulation can be detected with probability bordering on certainty.

If the result of the audit is such a strong suspicion of fraud (but it must be substantial sums), data is de-anonymized to real people in the companies, and the respective incident is examined further. It then may lead to consequences in law, on side of employment or even on criminal acts.

To lead back the evaluated data on real people only can be done outside the Lidl Stiftung, exclusively in the responsible organizational unit. Thus, the final rating and evaluation remains in the hands of the direct supervisor. With this in the assessment of the case, not only the formal (mathematical) conditions, but also personal circumstances will be considered in each individual case.

The central cash register audit is performed by the audit department of Lidl Stiftung. Thus, the test is carried out by a neutral body, which is not responsible to any key figures. Only the auditors of the central cash register audit are responsible for performing the defined testing processes. The evaluation is performed without the background of performance control and is also not used for identifying training needs of employees etc. To ensure a corporate group wide uniform and comparable quality, all standardized tests are carried out according to specifications of the concept of central cash register audit.

The audit is distinguished in an automated detail analysis and a manual ratio analysis, provided with the basic figures of the management information system for the evaluation. The basic data are all lines (positions) of the receipts in the audit period from all operators of the company to be evaluated.

The audit department performs the regular evaluations of the companies using the central cash register audit software. If new manipulation scenarios for future automated detail analysis are identified, these scenarios must be approved jointly by several departments of Lidl Stiftung. In addition to regular evaluations, in a concrete case of suspicion a store- or user-by-case verification of the cashiering behavior can be applied.

8 Transnational issues:

In medium term the cash register analysis is introduced in all countries where Lidl Stiftung companies operate. Currently (January 2016) it is used in the following countries.

1. Belgium
2. Bulgaria
3. Denmark
4. Finland
5. France
6. Greece
7. United Kingdom
8. Ireland
9. Croatia
10. Malta
11. Northern Ireland
12. Poland
13. Portugal
14. Romania
15. Sweden
16. Slovakia
17. Slovenia
18. Spain
19. Czech Republic
20. Hungary
21. Cyprus

22. Switzerland

Except Switzerland all countries are EU member states, where EU law is to be applied, and no transnational framework must be considered. When using the central cash register audit software in Switzerland, the provisions of Switzerland Data Protection Act [DGCH] meet the requirements of the Privacy Compliance EU Directive (Directive 95/46/EC) to third countries. In this regard, the use of the central cash register audit software in Switzerland is also conform with data protection regulations.

Before use in other countries, the special needs required by the respective national data protection acts must be examined and the audit system must be adapted. In countries where the level of data protection is less than that of the EU (for example, United States of America), it has to be checked, which data may be collected in spite of this problem, which may be processed, and especially which data is allowed to be sent back to use the certified system accordingly.

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

MicroStrategy, TeraData, Oracle

Name: L-AS193 / 194; Manufacturer: HP; Operating System: SUSE Linux ES 11 SP1

Software: MicroStrategy

Version Number: 9.0.2

Type: Application Server

Name: L-AS221; Manufacturer: HP; Operating System: Win2008 R2;

Software: Oracle

Version Number: 11 Release 2

Type: Database Server

Name: L-AS195 - 196; Manufacturer: HP; Operating System: SUSE Linux ES 11 SP1

Software: MicroStrategy

Version Number: 9.0.2

Type: Web Server

Name: INT-TD11 - 22; Manufacturer: Teradata; Operating System: SUSE Linux ES 10

Software: Teradata

Version Number: 12:10

Type: Database Server

10 Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria_Vers_2013; EuroPriSe Commentary May 2014

11 Evaluation results:

The behavioral control of employees is a major problem in business. Besides the internal problem that exuberant control is limiting the freedom of choice and possibly the decision necessity of employees, it may also negatively affect the work atmosphere. Monitoring also includes, especially in large companies, a socio-political dimension which has to be considered, too. Thus, a company's image will be damaged, for example, if employment law measures are taken, if it is only the "theft" of a roll that was left. A dimension that also has to be looked at is data protection, which, of course, also counts in companies and warrants the right of informational self-determination and the protection against misuse of personal data, also for employees.

The cash register analysis of Lidl Stiftung is such a behavioral control that is used to evaluate which employee has manipulated the cashiering process and, with this infected or inflicts a monetary loss to the company. It is legally indisputable that companies may examine employees if they cheat on their employers or steal; an employer must not even accept that employees take away the smallest amounts / values.

Of course, the implementation of such a behavioral control has also to consider the legitimate interests of employees in the exclusion from such a control. Therefore, a permanent control of all employees is strictly prohibited; they also may not violate against the general moral laws (for example, video surveillance in locker rooms), etc. Certain limits and guidelines are also to be complied with. In this respect, such a system must be “designed” to achieve the data protection laws, for example, and/or the legal regulations regarding the participation of employees (Works Constitution) to be permissible.

The data protection audit of Lidl Stiftung cash register analysis showed the following results:

The Lidl Stiftung cash register analysis can be operated permissibly from a data protection perspective. As already stated above, the employer has a legitimate interest to prevent manipulation and fraud and to realize this with appropriate, possible technical means. The legitimate interests of employees to the exclusion of these measures have to be considered also. This means in the present case that it should be tried to filter out only those people from the available database that have really manipulated almost certainly, and thus possibly committed a crime. This is implemented in the Lidl system in an excellent way, because relatively high thresholds must be crossed and the scenarios under which the data is checked, are secured. That means, manipulations have been carried out in the way of the scenarios or would at least be possible if employees proceed accordingly. Furthermore, a personal reference will only be made if it can be traced over a professional inspection by audit staff next to the automatic conclusion that a manipulation was found. The Lidl Stiftung as an employer here approvingly accepts that employees harm the company and pursues exclusively manipulations that exceed a rather high value. Thereby, the potential number of offenders is severely limited and reduced to the person of which it can be assumed with great certainty that they have manipulated.

Through the process further additional safeguards are defined to prevent innocent people to be accused. Thus, the manipulations have to be brought into line with the on-site conditions. This is to prevent that particular local conditions lead to unjustified accusations, because they could not be intercepted by the automated and personal plausibility checks.

By the use of pseudonymisation of the data to be evaluated, the entire system additionally fulfils data protection law aspects. In the first step, the data only can be filtered to the patterns that emerge in cashing in (a) Lidl branch store(s). These patterns may be assigned to operator numbers, but not to real people. That disadvantages arise by these analyzes, particularly for employees who neither have manipulated nor are accused in any other form, is unlikely to happen. In addition, the records may be used only for testing manipulation incidents. A use for other purposes is completely excluded.

Moreover, there is a separation between Lidl branch stores and Lidl Stiftung. Thus, the assignment “employee / operator number” can be made exclusively in the Lidl branch store, as this relationship is only known here. Operator numbers are assigned to employees only locally in the Lidl branch stores. Elsewhere this relationship cannot be traced. In a case in which a suspicion has occurred, a person belonging to an operator number only can be found in the Lidl branch store. An improper use of the database of the cash register analysis should be impossible, with very high probability.

From a technical / organizational perspective, the system of cash register analysis is to be assessed also very positively. The storage and the calculations are done on a server in the high security data center of Lidl Stiftung. This protection goes beyond a level which would be necessary for such a system, in particular due to the use of pseudonymisation.

From a data protection point of view, it could be found that the cash register analysis was designed and implemented in a very good manner. The design approach of Lidl Stiftung resulted in a system that takes into account the interests of people affected by the system to a large extent without severely restricting company's interests. With the cash register analysis employees are indicated who cause great financial loss for the company. Those who have not performed manipulations are not stronger bothered in their rights than is absolutely necessary.

12 Data flow:

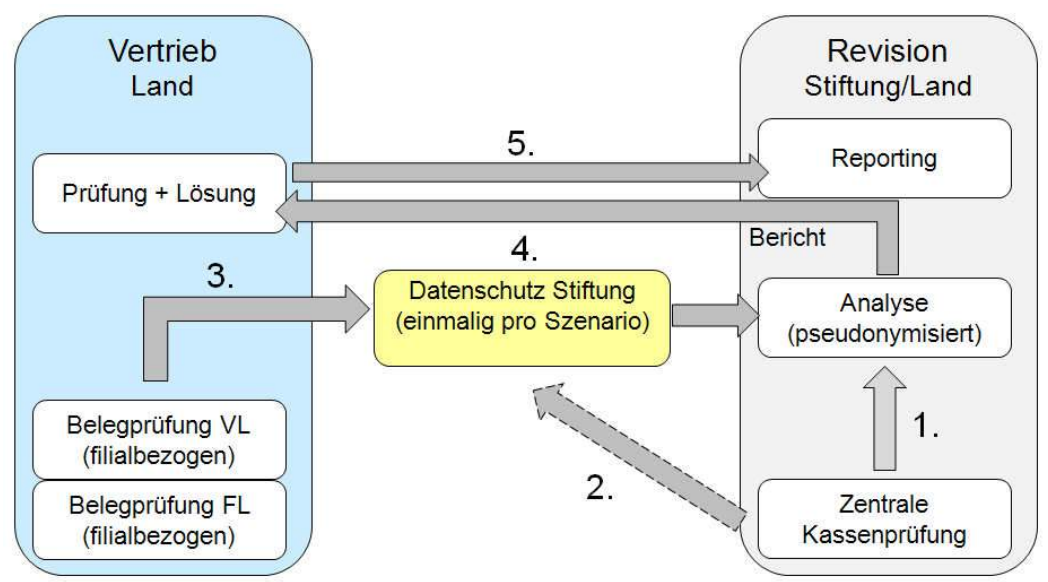


Figure 1: Complete Process

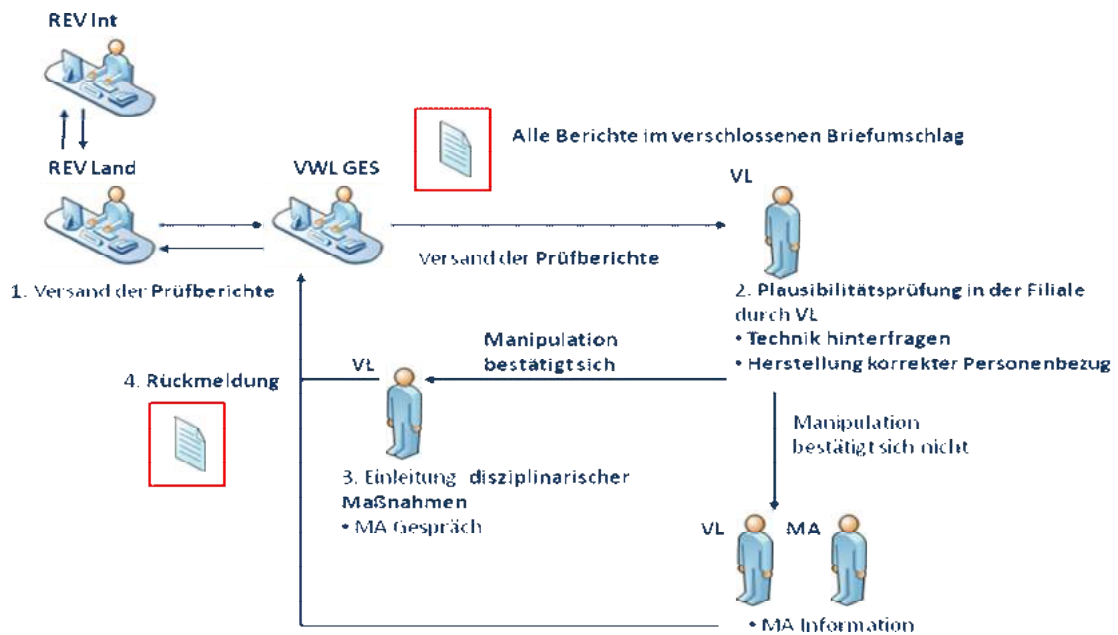


Figure 2: Communication process under suspicion of manipulation

13 Privacy-enhancing functionalities:

The central cash register audit of Lidl Stiftung achieves a high level of proportionality in the use of the system. Therefore, an employer cannot be expected to accept, embezzlement, fraud, etc., even if this is only for small amounts. Filtering out such violations is extremely difficult, because the deviations from which such behavior could be developed have considerable scattering width. This then results in the problem that next to the fraudsters innocent employees / staff come to the fore. Apart from the basic problem to be suspected as an impostor, it even may be difficult for an innocent person to prove his / her innocence because not every proof is available.

To work around this problem, or at least to alleviate it, Lidl Stiftung accepts violations, to certain thresholds, depending on the selected scenario. This matches fewer people, because with these limits, potential violations with small amounts are not selected. This reduces the selection to those where significant differences can be found from the normal range. This again increases the probability of having found a true perpetrator.

The same applies to the use of scenarios. This achieves that there is no search after exceeding standard values, but only after the injury of values in relation to specific contexts that are already known as problem scenarios.

Overall, the system has been organized so that privacy gets a considerable weight and is therefore considered in all respects, in which personal data are concerned. Lidl Stiftung succeeded in implementing the, especially in the part of behavioral control of employees and staff, important principle of proportionality to a very good and professional extent. The central cash register audit was designed that both, the interests of the employer and the employee / persons concerned, are taken into account in an outstanding manner. The Lidl Stiftung receives a

tool to detect manipulation / tampering while cashiering – those affected can be sure that they will only be charged potentially if a manipulation suspected can be detected with probability bordering on certainty. This could be proved as a whole in the evaluation.

It has to be noted that the excellently chosen organizational framework can be performed by the system without any problems. The system can be used so privacy conducive because the relevant data protection laws are implemented by the Lidl Stiftung.

14 Issues demanding special user attention:

none

15 Compensation of weaknesses:

none

16 Decision table on relevant requirements:

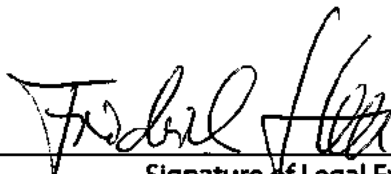
EuroPriSe Requirement	Decision	Remarks
Data Avoidance and Minimization	excellent	The central cash register audit only uses the minimum of required data.
Transparency	adequate	Documentation and in particular the statements concerned for the employees are informative, up-to-date and understandable.
Technical-Organizational Measures	adequate	Due to the design of the processing, which uses exclusively pseudonymous data, not very sophisticated technical and organizational measures must be implemented. In this respect, the measures taken can be rated as excellent in part, as the processing takes place in a high security data center. Overall, the technical organizational measures shall be assessed "adequate".
Data Subjects' Rights	adequate	The data subject's rights are implemented adequately in principle. Especially in the case that employees are blamed of having committed violations.

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.

Berlin 24.06.2016

Prof. Dr. Friedrich Holl



Place, Date

Name of Legal / Technical Expert

Signature of Legal Expert

Certification Result

The above-named IT product / 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