



Short Public Report

Recertification No. **EP-S- DZ2LYR**

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

LIDL Central Cash Auditing (ZKP); version 7, functional status October 2018.

2. Manufacturer or vendor of the IT product / Provider of the IT-based service:

Company Name: Lidl Stiftung & Co. KG (Lidl Foundation)

Address: Stiftsbergstr. 1, 74167 Neckarsulm, Germany

Contact Person: Mr. Satoru Masuda, Chief Technical Officer of
Lidl Stiftung & Co. KG

3. Time frame of evaluation:

July 2018 – October 2018

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

Name of the Legal Expert: Dr. Irene Karper

Address of the Legal Expert: Konsul-Smidt-Str. 88a, 28217 Bremen, Germany
c/o datenschutz cert GmbH

Name of the Technical Expert: Dr. Irene Karper

Address of the Technical Expert: Konsul-Smidt-Str. 88a, 28217 Bremen, Germany
c/o datenschutz cert GmbH

5. Certification Authority:

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 ZKP is used to evaluate checkout processes for potential manipulations, fraud and fraudulent scenarios. By using the ZKP, typical scenarios are uncovered using certain key figures and threshold values.

The service includes the following components:

- Automated and manual cash audit – as a processor
- Keeping of logs – as a controller

The service includes the following processes:

- Receive cash desk data from sales company (controller) and prepare it for the cash audit
- Cash audit process
- Return result data to the sales company
- Notification of the Lidl Foundation about measures taken / not taken

The ToE does not include the following aspects:

- Programming the cash register software (since it is carried out by another company).
- The archiving of POS data in the e-journal is no longer part of the data processing of the ZKP and is therefore not part of the target of evaluation.
- The Management Information System (MIS), which provides data to the ZKP, including its back-up, recovery and archiving.

7. General description of the IT product or IT-based service:

ZKP is **both an IT product and an IT-based service**. For the analyses, LIDL Stiftung & Co. KG receives daily data from the cashiers' receipts from all affiliated branches and Customer Care analyses these in regular cycles with the help of the ZKP. The analysed data are system and

billing data (receipt), as well as a **pseudonym (operator number)** that allows the user of ZKP (sales company) who is the controller of the processing to identify the respective employee. The Lidl Foundation itself cannot identify employees by means of their operator numbers.

The analysis is performed exclusively by an auditor of the Lidl Foundation and is carried out both automatically and manually. Invoices are **automatically analysed** on the basis of key figures or scenarios that represent an initial suspicion of manipulation. These key figures or scenarios are supplemented over time on the basis of recent experiences. Scenarios are contrasted with thresholds that exclude minor fraudulent acts. Only when the threshold value is exceeded, the system provides information on a possible fraud case. In a manual plausibility check, the auditor then looks for evidence that may exonerate the employee.

The auditor also checks the data **manually**, looking for suspicious information. The data of the operators at the cash register system of the respective sales company are tested (pseudonymised) at the invoice level ("drill-down"). Again, thresholds are applied. Not only manipulations can be detected, but also new manipulation methods can be identified. In this sense, the ZKP also serves to point out further weak points or manipulation scenarios (previously unknown). These can then later be included in the automated ZKP provided this has been approved by a revisory board consisting of representatives of the departments of audits, sales, technology and data protection. Scenarios may be removed if it turns out that they are not relevant anymore.

The cash register processes of the ZKP are analysed with regard to the following key figures:

- Money return
- Cancellation
- Billing cancel
- Invoice provision
- Deposit
- Prices
- Subscriptions and cancellations
- Small invoice (defined single invoice)

These metrics represent the typical cases currently known in which manipulation could occur. Each sales company in a country is audited up to twice per year as a **random sample**. There is a technical regulation that a company can be selected for analysis no more than twice a year. These regular checks are carried out by the audit department of Lidl Foundation by means of ZKP.

If the ZKP detects a suspicion of manipulation, the affected regional sales company is informed and a group-wide standardised process for further clarification and settlement is set in motion. This can lead to personnel measures upon confirmation of the suspicions. Concretely, the abnormalities in the audit report (result data) are provided to the competent sales manager. These data include the copies of the concerned receipts. The sales manager examines the individual case for accuracy and plausibility. In doing so, s/he explores all known explanations for the identified abnormalities / deviations (e.g. operator errors). The audit is documented in templates. If the suspicion corroborates, the sales manager initiates further action if necessary. The distribution manager as the competent supervisor is indirectly involved and only receives information about the number of audit reports and the name of the responsible sales manager. He is not informed about the names of the concerned employee(s). The Lidl Foundation does not receive information about the names of the concerned employee(s) either, but only information on the result of the plausibility check performed by the sales manager. Personal data relating to identified abnormalities may only be transferred to third parties for the purpose of crime investigation and/or if necessary for labour court proceedings. In such a case, personal data may be transmitted to a police department, an investigating law enforcement agency, lawyers and the competent court.

The ZKP also produces **statistical reports** that do not contain any personal data.

All **inspection processes** are **logged** electronically to control the compliance of the ZKP with the defined scope of the audit. The examination of the log files is carried out by the data protection officer of the Lidl Foundation. The examination takes place within one month after the end of a calendar year. Supervisors from the audit department have access to the log files as part of due diligence. They perform random checks on the log data. The storage period of the log files is 13 months. Thereafter, data are automatically deleted by the system.

All employees are informed about the use of ZKP across the Lidl Group. If the suspicion of a criminal offense arises, the data subject is informed of the initiation of employment and / or criminal law measures. This information is created individually for each individual case. The collective rights of employees will also be respected. The use of ZKP in companies / branches with a works council is not permitted without the council's consent.

8. Transnational issues:

The analyses within the scope of the ZKP form a standardized audit concept, which is always applied uniformly throughout the Lidl Group and is therefore expected to produce comparable quality. Since the last certification, the ZKP has been introduced in additional countries. Currently, it is used in the following countries:

Germany	Northern Ireland	Czech Republic
France	Denmark	Slovakia
Malta	Finland	Slovenia
Greece	Sweden	Croatia
Cyprus	Belgium	Romania
Spain	Netherlands	Bulgaria
Portugal	Austria	Lithuania
England	Hungary	Switzerland
Irland	Poland	USA

The information that is transmitted to the Lidl Foundation in a pseudonymised form is personal data of the respective employees of the different sales companies. Data from the branches in the US or Switzerland affect only employees from the respective country. The data processing related to ZKP takes place in Germany.

9. Tools used by the manufacturer of the IT product / provider of the IT-based service: MicroStrategy, v. 10.3 and Teradata, v. 15.10.

10. Edition of EuroPriSe Criteria used for the evaluation:

The basis of the EuroPriSe evaluation is the EuroPriSe criteria catalogue in the version from January 2017. Furthermore, the EuroPriSe commentary from 05/2017 was used.

11. Modifications / Amendments of the IT product or IT-based service since the last (re)certification

The ZKP has been updated compared to the last certification in a few points. The following processes have been changed / newly introduced:

- IT-Provider: Schwarz IT GmbH & Co. KG (SIT)
- Housing at noris network AG, Nuremberg, Germany

- New scenarios in the automated detailed analysis: multiple price announcements in a row, money return not subject to authorisation and multiple return with the same original receipt
- New measure in the manual measure analysis: total number of manual returns
- Automatic detail analysis: Display of all receipts of the conspicuous operator number for the inspection topic
- Automatic detail analysis: restriction of scenarios by additional thresholds
- Change Management: Description recording thresholds added
- Import of thresholds via web interface rather than via an Excel spreadsheet
- Start analysis
- Technical regulation introduced to load sales companies
- HR Manager and Data Protection Officer Country defined as Deputy Chief Executive Officer
- Review of audit log files by DSB Lidl Foundation rather than by DSB Regional Company.
- Adaptation of employee information according to GDPR
- Layout Adjustments

12. Changes in the legal and/or technical situation

In terms of data protection law, the ZKP was adapted to the requirements of the GDPR. In particular, information pursuant to Art. 12ff. GDPR was documented and issued to employees throughout the Lidl Group. In addition, the records of processing activities for the ZKP were updated and a privacy impact assessment was prepared. In addition, the order processing (controller-processor) contracts were updated in light of Art. 28 GDPR throughout the Lidl Group. From a technical point of view, the movement to the data centre of Noris Network AG in Nuremberg (Housing) is relevant. Furthermore, servers, databases and operating system were updated.

13. Evaluation results:

The use of ZKP is intuitive. Auditors can see at any time which data is in which workflow state. The user is provided with **meaningful product documentation** and templates. The **information rights of employees** are also respected.

The use of ZKP in the context of **Commissioned Data Processing** is regulated by a contract in accordance with Art. 28 GDPR and uniformly implemented throughout the Lidl Group.

The deployment takes place within a **secure IT environment** of the Lidl Foundation. The servers and databases are housed in an ISO / IEC 27001 certified data centre in Germany.

Of particular relevance is the lawful processing of the employees' personal data. For the processing of employment-related pseudonyms by means of the ZKP, Art. 6 para. 1 lit. f GDPR is relevant. Accordingly, processing is lawful where it is necessary to safeguard the legitimate interests of the controller or a third party and does not outweigh the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data. The interest of the employees not to be subject to performance monitoring as well as to wrongful suspicions of criminal offenses are to be balanced with the interests of the sales companies to prevent and investigate manipulations, criminal offenses and economic damages. The data processing and analysis of the ZKP focuses on the subsequent control of the cashier process, and thus on the behaviour of employees during the cashier activity. The employees are informed about the ZKP in the employment contracts and via circular letters. Nevertheless, the mere fact that the checkout process is analysed for abnormalities by means of an automatic system can trigger **monitoring pressure** and impair the development of personal rights in the workplace. However, it has to be taken into account that employees are not monitored by means of ZKP on a permanent basis, but that monitoring is limited as follows, as a rule: Each company in a country is reviewed as a random sample by the auditors only up to twice a year. In addition, the total audit may only cover 24 weeks of cashier activities per operator and not the entire annual proceedings. The sample size in the manual analysis is also set to 15% in the standard setting of the ZKP so that no more than 15% of the employees of the respective regional company are audited, whereby the distribution of the sample to the defined key figures may be variable depending on the manipulation result. The sample size of 15% represents a maximum value. Furthermore, only **pseudonymized data** is analyzed. Only when there is a concrete suspicion, which is again checked for conclusiveness outside of electronic data processing within the organisation, the data is de-pseudonymised and assigned by the sales manager (superior) to a specific employee. In the following data processing, which takes place outside of the ZKP, further organisational measures are to be observed, which are to exclude false suspicion and reputational damage of the data subject as far as possible. The data subject is also informed about the internal investigation and can comment on it. Then the entire data analysis by means of the ZKP is placed into the hands of a neutral department at the Lidl Foundation, which acts unbound to the regional sales companies and markets and which does not know the identity of the affected employees.

These measures and the overall organisation of the ZKP ensure that not all employees are permanently placed under a general suspicion of manipulation. It should also be borne in mind

that the ZKP analysis can refute a suspicion created by a manual analysis of behaviour in the market and help to relieve the person concerned. Above all, however, negative impacts on employees are reduced to as low a level as possible without jeopardising the purpose of detecting tampering and criminal offenses. It is not apparent that the interests of employees outweigh the interests of the sales companies. Through fraud, theft and embezzlement, the retail industry incurs millions in damages every year. According to Art. 88 (1) GDPR, the protection of the employer's property is a legitimate purpose. The sales companies therefore have a legitimate, economic interest in preventing and investigating manipulations and offenses at their expense by means of the ZKP in order to derive recourse claims or possibly employment-related consequences, such as dismissal or warning and/or to engage law enforcement agencies. The ZKP analysis is already present in such a way that it only displays results, if a minimum threshold is reached / exceeded, although this may lead to economic damage. The suspicion of manipulation in the audit report may only be presented if a manipulation sum of at least 25, - € has been achieved. The manipulation sum can be lower in exceptional cases. A less severe means is not apparent. In particular, the anonymization of employment data in the ZKP would run counter to the purpose of being able to prosecute manipulations and penalties and of taking recourse or employment law consequences from this. If the ZKP confirms a suspicion in the analysis, it is unacceptable for the company not to pursue it. Other control options, such as the manual evaluation of all cashier transactions by the manager of a store, are not justifiable in terms of personnel efforts and cost and would, moreover, result in even higher monitoring pressure on the employees. The ZKP is therefore required to safeguard the legitimate interests of sales companies.

If ZKP is used in an EU Member State, which has made use of the opening clause of Art. 88 GDPR, country-specific regulations must be complied with. For example, in the Federal Republic of Germany, § 26 (1) of the Federal Data Protection Act (FDPA) is relevant, which refers to the (contractual) employment relationship (sentence 1) and to the detection of offenses during employment (sentence 2)¹. These two legal bases are to be distinguished from each other in terms of the ZKP. Pursuant to section 26 (1) sentence 1 FDPA, personal data may be processed by employers for employment purposes, as far as this is necessary for the

¹ On the other hand, the employees' consent must be ruled out as a potential legal basis due to the overlap / subordination relationship between the employers as the beneficiaries of the ZKP data and the employees concerned.

establishment, implementation or termination of the employment relationship. Pursuant to Section 26 (1) Sentence 2 FDPA, personal data of employees may only be processed for the detection of criminal offenses, if the factual evidence to be substantiated justifies the suspicion that the person concerned has committed an offense in the employment relationship, the processing is required to detect it and the legitimate interest of the employee in excluding the processing does not prevail, in particular its nature and extent are not disproportionate to the occasion. The wording of § 26 Abs. 1 S. 2 FDPA has in practice interpretation difficulties, which were not resolved by the statement of reasons as well as by interim comments of the literature². For example, it remains unclear whether Section 26 (1) sentence 2 FDPA seeks to detect not only the repressive purposes of detecting criminal offenses, but also preventive purposes for preventing them, especially since in mixed situations the purposes can often not be separated³. In the present case, however, precisely such a mixture of different purposes exists, because the ZKP pursues both repressive and preventive purposes. However, at this time of data processing by means of the ZKP there is no concrete suspicion, but only key figures that have to be evaluated and further researched in the further data processing outside the ZKP. Therefore, the data processing processes of the ZKP cannot be based on § 26 Abs. 1 S. 2 FDPA as a legal basis due to lack of a concrete suspicion. However, it can be stated that the ZKP also serves - and even more so - to prevent manipulation and process optimisation of the analysis by showing possible further weaknesses as well as relieving the sales manager of time by automated processes - and less the criminal prosecution interests. In addition, the latter can not be realised with the ZKP, since they are carried out entirely outside the ToE and require further investigation and review processes by the auditors, the supervisor and the law enforcement authorities. Also, the ZKP does not issue any figures below the designated the threshold values, even if in these cases criminal offenses exist. Even with a suspicion of a criminal offense initially determined by the ZKP and substantiated by research of the supervisor, in many cases there is no criminal complaint, as this is ultimately uneconomical for the Lidl Group and provided there is no official offense.

The prevailing view is that the processing of data in the context of preventive measures, which do not require any concrete suspicions, is based on § 26 (1) sentence 1 FDPA as the legal basis.

² Karper in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 1.Edition, Chapter. F, Sidemark 48 with further references.

³ *ibid.*

According to this, (open) supervision, which is not directed against specific employees, is not permanent and which serves to prevent violations, is permissible even without suspicion.

In the opinion of the EuroPriSe expert, this view is preferable. According to this, due to the predominantly preventive nature of the system, § 26 (1) sentence 1 FDPA is applicable. It is therefore important for the application of the ZKP in the context of the employment relationship to be necessary and proportionate. These aspects have already been described in detail above in the context of the balance of interests check so that reference is made to the statements made there. Other, equally suitable measures of the evaluation of the cashier operations are not apparent, in particular an observation by e.g. detectives, since this would jeopardise the pseudonymisation of the data. Employees are informed about the use of the ZKP. A permanent monitoring or a full control of all employees or all cashier operations does not take place. This is ensured by the described mechanisms of the periodic sampling, the pseudonymisation, the neutral administrator and the bagatelle and threshold limits. Overall, the measure is necessary, proportionate and not objectionable under data protection law.

Finally, collective agreements may constitute a legal basis and concretise the admissibility in the light of Art. 88 GDPR. In Germany, for example, these provide a legal basis for the processing of employee data in accordance with § 26 (4) FDPA, whereby Article 88 GDPR must be observed. Therefore, a collective agreement can only constitute a legal basis if it does not fall short of the provisions of the GDPR⁴.

⁴ Rossow in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 1.Edition, Chapter C, Sidemark 430 with further references.

14. Data flow:

The data flow of the ZKP can be represented as follows:

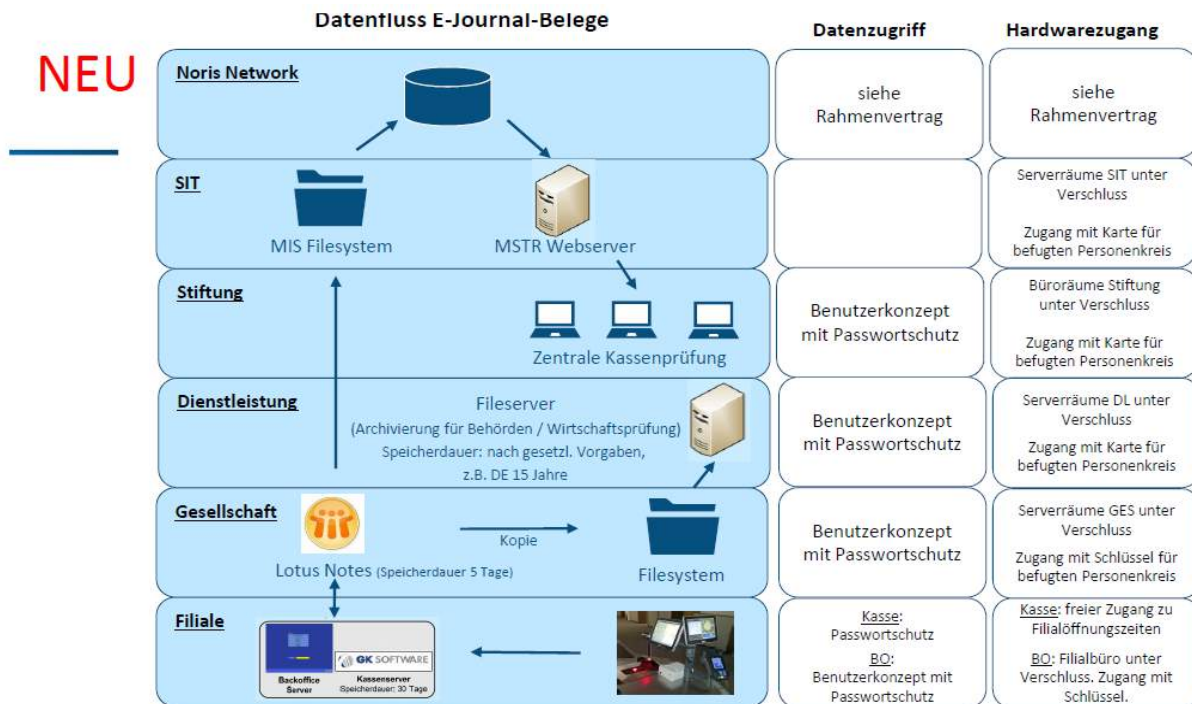


Abbildung 1: Datenfluss (Legende: „BO“ = Backoffice“)

15. Privacy-enhancing functionalities:

- The privacy and security measures that have been steadily developed and implemented by Lidl Stiftung & Co. KG are in line with the privacy-by-design principle. Lidl Stiftung succeeds in providing the ZKP service in such a way that the greatest possible extent of the protection of the employment data is guaranteed and nevertheless the efficiency for the clarification and prevention of damages is charged to the companies. The ZKP achieves this, inter alia, through pseudonymisation of the dataset, through a multi-stage audit concept, through the involvement of the Lidl Foundation as a neutral auditor, through always up-to-date manipulation scenarios and threshold values that exclude a trivialisation.
- The data centre in which the ZKP systems are located has a high degree of physical security and is certified. Thus, a high level of protection is realised.

16. Issues demanding special user attention:

Not applicable.

17. Compensation of weaknesses:


Not applicable.


18. Decision table on relevant requirements:

<i>EuroPriSe Requirement</i>	<i>Decision</i>	<i>Remarks</i>
Data Avoidance and Minimisation	excellent	The scope of data processing by ZKP is limited to the necessary personal data. Only pseudonyms are used (operator number). Furthermore, the ZKP only collects samples from the total data volume for a specific, limited period of 12 weeks. Reports for companies do not contain personally identifiable information.
Transparency	excellent	ZKP may be used intuitively. Relevant documentation is up to date. It is always visible which data is in which workflow.
Technical-Organisational Measures	adequate	The data centre in which the ZKP systems are located has a high degree of physical security and is certified. Thus, a high level of protection is realised.
Data Subjects' Rights	adequate	The procedure for informing employees about the ZKP and its data protection rights as a whole is standardised across the Group.

Experts' Statement

We affirm that the above-named IT product / 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.

Bremen, 28.12.2018	Dr. Irene Karper	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Bremen, 28.12.2018	Dr. Irene Karper	
Place, Date	Name of Technical Expert	Signature of Legal Expert

Recertification 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
-------------	---------------------------------	-----------