



Kurzgutachten

Rezertifizierungs-Nr. EP-S-DZ2LYR

1. Name und Version des IT Produkts und IT-basierenden Service:

Zentrale Kassenprüfungssoftware (ZKP); Version 7, Funktionsstand Oktober 2018.

2. Entwickler oder Betreiber des IT-Produktes / IT-basierten Services:

Firmenname: Lidl Stiftung & Co. KG

Adresse: Stiftsbergstr. 1, 74167 Neckarsulm, Bundesrepublik Deutschland

Kontaktperson: Herr Satoru Masuda, Chief Technical Officer der
Lidl Stiftung & Co. KG

3. Zeitrahmen der Evaluation:

Juli 2018 – Oktober 2018

4. EuroPriSe Experten, die das IT-Produkt/den IT-basierenden Service evaluiert haben:

Name der rechtlichen Expertin: Dr. Irene Karper

Adresse der rechtlichen Expertin: Konsul-Smidt-Str. 88a, 28217 Bremen, Deutschland,
c/o datenschutz cert GmbH

Name der technischen Expertin: Dr. Irene Karper

Adresse der technischen Expertin: Konsul-Smidt-Str. 88a, 28217 Bremen,
Deutschland, c/o datenschutz cert GmbH

5. Zertifizierungsstelle:

Name: EuroPriSe Certification Authority

Adresse: Joseph-Schumpeter-Allee 25
53227 Bonn
Deutschland

eMail: contact@european-privacy-seal.eu

6. Spezifikation des Zertifizierungsgegenstandes (ToE)

Die ZKP wird zur Analyse der Kassendaten im Kassierprozess – insbesondere im Einzelhandel - eingesetzt und dient der Auswertung von Kassiervorgängen auf potentielle Manipulationen, Betrugs- und Unterschlagungsszenarien. Anhand der ZKP werden typische Szenarien mittels bestimmter Kennzahlen und Schwellwerte aufgedeckt und verhindert.

Zum Dienst gehören folgende Komponenten:

- automatisierte und manuelle Kassenprüfung (IT-System)
- Führen von Logs als verantwortliche Stelle

Zum Dienst gehören folgende Prozesse:

- Vorbereitung der Kassendaten für die Prüfung
- Prozess der Kassenprüfung
- Rückübermittlung der Daten an die Vertriebsgesellschaft/Verkaufsstelle
- Benachrichtigung der Lidl Stiftung über durchgeführte/nicht durchgeführte Maßnahmen

Nicht zum ToE gehören hingegen folgende Aspekte:

- Programmierung der Kassenprüfungssoftware, da diese im Auftrag durch ein anderes Unternehmen durchgeführt wird.
- Die Archivierung von Kassendaten im e-Journal gehört nicht mehr zur Datenverarbeitung der ZKP und ist daher auch nicht mehr Evaluationsgegenstand.
- Das Managementinformationssystem (MIS) als Datenlieferant der ZKP incl. dessen, Back-Up, Recovery und Archivierung.

7. Kurzbeschreibung des IT-Produkts und IT-basierten Service:

Die ZKP ist sowohl ein IT-Produkt als auch ein IT-basierter Service. Es steht jedoch keine Software als Vermarktungsgegenstand im Vordergrund, sondern die Auswertung und die daraus folgenden Prozesse, sofern sich ein Manipulationsverdacht erhärtet. Für die Analysen erhält die LIDL Stiftung & Co. KG weltweit aus allen eingebundenen Filialen täglich Daten der Kassierbons und der Bereich Customer Care analysiert diese in regelmäßigen Zyklen mit Hilfe der ZKP. Bei den analysierten Daten handelt es sich um System- und Abrechnungsdaten (Bondaten), sowie ferner eine **Bedienernummer**, die Rückschlüsse auf Beschäftigte zulässt. Dabei sind alle Daten, die die Lidl Stiftung aus den Filialen erhält, durch Nummern **pseudonymisiert**. Die Lidl Stiftung selbst kann keine Zuordnung zu einem bestimmten Beschäftigten vornehmen.

Die Analyse wird ausschließlich durch einen Revisor der Lidl Stiftung durchgeführt und erfolgt automatisch sowie manuell. **Automatisch analysiert** werden Bondaten anhand von

Kennzahlen bzw. Szenarien, die einen Anfangsverdacht für Manipulationen repräsentieren. Diese Kennzahlen bzw. Szenarien werden fortlaufend anhand aktueller Erfahrungen ergänzt. Szenarien werden Schwellwerten gegenübergestellt, die Bagatellhandlungen ausgrenzen. Erst bei Überschreitung des Schwellwertes erfolgt eine Anzeige im System für einen möglichen Betrugsfall. Anschließend führt der Revisor eine manuelle Plausibilitätsprüfung der ausgegebenen Bons durch, was zur Entlastung der zunächst auffälligen Bedienernummer führen kann. Ferner wird vom Revisor eine **manuelle Kennzahlenanalyse** durchgeführt, in welcher nach Auffälligkeiten gesucht wird. Die Daten der Bediener am Kassensystem dieser Gesellschaft werden (pseudonymisiert) auf Bonebene geprüft (sog. „drill-down“). Auch hierbei werden Schwellwerte angesetzt. Dabei können nicht nur Manipulationen aufgedeckt werden, sondern auch neue Manipulationsmethoden identifiziert werden. In diesem Sinne dient die ZKP auch dem Aufzeigen weiterer Schwachstellen bzw. Manipulationsszenarien. Diese können dann später in die automatische ZKP aufgenommen oder bei Nicht-Relevanz auch entfernt werden, sofern dies durch ein Entscheidungsgremium aus den Fachbereichen Revision, Vertrieb, Technik und Datenschutz freigegeben wurde.

Geprüft werden die Kassenprozesse der ZKP im Hinblick auf folgende Kennzahlen:

- Geldrückgabe
- Storno
- Bonabbruch
- Bonrückstellung
- Pfand
- Preisanzeige
- An- und Abmeldungen
- Kleinstbon (definierter Einzelbon)

Diese Kennzahlen stellen die derzeit bekannten typischen Fälle dar, in denen eine Manipulation erfolgen könnte. Jede Gesellschaft eines Landes wird bis zu 2x pro Kalenderjahr als **Stichprobe** durch die Revision geprüft. Es existiert hierzu eine technische Reglementierung, dass eine Gesellschaft max. 2x pro Kalenderjahr für eine Analyse ausgewählt werden kann. In besonderen Ausnahmefällen kann eine Filiale über den definierten Prüfungsumfang hinaus geprüft werden, nämlich bei einer räumlichen Zuordnung der Filiale zu einer anderen Gesellschaft. Diese regelmäßigen Prüfungen werden durch die Revision mit der ZKP durchgeführt.

Ermittelt die ZKP einen Manipulationsverdacht, wird die betroffene Regionalgesellschaft informiert und diese setzt einen **konzernweit standardisierten Prozess** zur weiteren Aufklärung und Abwicklung in Gang. Dies kann bei Bestätigung der Verdachtsmomente zu

personellen Maßnahmen führen. Konkret werden die Auffälligkeiten im Prüfbericht dem Verkaufsleiter inklusive der Kopien der Bons zur Verfügung gestellt, der den Einzelfall auf Richtigkeit und Plausibilität prüft. Dabei erforscht er alle bekannten Möglichkeiten einer Erklärung für die Abweichungen (z.B. Bedienerfehler). Die Prüfung wird in Formblättern dokumentiert. Erhärtet sich der Verdacht, leitet der Verkaufsleiter ggf. Maßnahmen ein. Der Vertriebsleiter als Vorgesetzter ist mittelbar eingebunden und erhält nur Informationen über die Anzahl der Prüfberichte und den Namen des zuständigen Verkaufsleiters. Er erhält keine Namen der betroffenen Person. Auch die Lidl Stiftung erhält diese nicht. Die dortige Revision erhält lediglich das Ergebnis der Plausibilitätsprüfung ohne Namen als Feedback. Die Datenübermittlung an Dritte ist nur bei Straftaten und Arbeitsgerichtsprozessen zulässig. Daten dürfen in diesem Fall an eine polizeiliche Dienststelle bzw. ermittelnde Strafverfolgungsbehörde und Anwälte übermittelt werden.

Mittels der ZKP werden zudem **Statistik-Berichte** erstellt, die keinerlei personenbezogene Daten aufweisen.

Alle **Prüfprozesse** werden elektronisch **geloggt**, um die Einhaltung des definierten Prüfungsumfangs durch die ZKP zu kontrollieren. Die Prüfung der Log-Dateien erfolgt durch den Datenschutzbeauftragten der Lidl Stiftung. Die Prüfung erfolgt innerhalb eines Monats nach Ende des Kalenderjahres. Die Supervisoren aus der Revision haben im Rahmen der Sorgfaltspflicht Einsicht in die Log-Dateien. Diese führen ebenfalls eine stichprobenartige Kontrolle durch. Die Speicherdauer der Log-Dateien beträgt 13 Monate. Danach werden die Daten systemseitig automatisiert abgelöscht.

Alle **Mitarbeiter** wurden über den Einsatz der ZKP konzernweit **informiert**. Erhärtet sich der Verdacht einer Straftat, wird die betroffene Person über die Einleitung von arbeitsrechtlichen und/oder strafrechtlichen Maßnahmen informiert. Diese Information wird individuell für den jeweiligen Einzelfall erstellt. Auch die **Kollektivrechte** der Beschäftigten werden gewahrt. Der Einsatz der ZKP in Gesellschaften/Filialen mit Betriebsrat ist ohne dessen Zustimmung unzulässig.

8. Transnationale Rahmenbedingungen:

Die Analysen im Rahmen der ZKP bilden ein standardisiertes Prüfkonzept, welches konzernweit immer gleich angewandt wird und dadurch eine vergleichbare Qualität bewirken soll.

Seit der letzten Zertifizierung findet die ZKP in zusätzlichen Ländern Anwendung. Zum Auditzeitpunkt wird sie in Filialen folgenden Ländern durchgeführt (Stand: Oktober 2018):

Deutschland	Nordirland	Tschechien
Frankreich	Dänemark	Slowakei
Malta	Finnland	Slowenien
Griechenland	Schweden	Kroatien
Zypern	Belgien	Rumänien
Spanien	Niederlande	Bulgarien
Portugal	Österreich	Litauen
England	Ungarn	Schweiz
Irland	Polen	USA

Daten, die pseudonymisiert an die Lidl Stiftung übermittelt werden, sind Beschäftigtendaten der dort angestellten Personen. Daten aus den Filialen in den USA oder der Schweiz tangieren ausschließlich Beschäftigte aus dem jeweiligen Land. Alle Daten der ZKP werden dabei räumlich-physikalisch innerhalb Deutschlands verarbeitet.

9. Verwendete Tools:

MicroStrategy, Versionsnummer 10.3 und Teradata, Versionsnummer 15.10.

10. Version der für die Evaluation genutzten EuroPriSe Kriterien:

Grundlage der EuroPriSe-Evaluation ist der EuroPriSe-Kriterienkatalog in der Version aus Januar 2017. Ferner wurde der EuroPriSe-Kommentar aus 05/2017 genutzt.

11. Änderungen / Ergänzungen des IT-Produkts / des IT-basierenden Services seit der letzten (Re-)Zertifizierung

Der ZKP ist gegenüber der letzten Zertifizierung in wenigen Punkten aktualisiert worden. Folgende Prozesse wurden verändert / neu eingeführt:

- IT-Provider: Schwarz IT GmbH & Co. KG (SIT)
- Housing bei der noris network AG in Nürnberg
- Neue Szenarien in der automatischen Detailanalyse: Mehrfache Preisanzeigen in Folge, Geldrückgabe nicht autorisierungspflichtig und Mehrfache Rückgabe mit gleichem Originalbon
- Neue Kennzahl in der Manuellen Kennzahlenanalyse: Gesamtanzahl manuelle Geldrückgaben
- Automatische Detailanalyse: Anzeige aller Bons der auffälligen Bedienernummer zum Prüfthema
- Automatische Detailanalyse: Einschränkung von Szenarien durch zusätzliche Schwellenwerte
- Change Management: Beschreibung Einspielung Schwellenwerte hinzugefügt
- Einspielung Schwellenwerte per Webinterface anstatt Excel-Tabelle

- Start Analyse
- Technische Reglementierung zur Beladung von Gesellschaften eingeführt
- Personalleiter und Datenschutzbeauftragter Land als Stellvertreter des Verwaltungsleiters definiert
- Prüfung Log-Dateien durch DSB Lidl Stiftung anstatt durch DSB Regionalgesellschaft. Hierdurch entfällt die Checkliste F5
- Anpassung Mitarbeiterinformation nach DSGVO
- Layoutanpassungen

12. Änderungen der rechtlichen oder technischen Anforderungen

Die ZKP wurde in datenschutzrechtlicher Sicht an die Anforderungen der DSGVO angepasst. Insbesondere wurden Mitarbeiterinformationen gemäß Art. 12ff. DSGVO erstellt und an Beschäftigte konzernweit ausgegeben. Zudem wurde das Verzeichnis der Verarbeitungstätigkeiten über die ZKP aktualisiert und es wurde eine Datenschutzfolgeabschätzung erstellt. Ferner wurden die Verträge zur Auftragsverarbeitung an die DSGVO angepasst und konzernweit aktualisiert. In technischer Hinsicht ist der Umzug in das Rechenzentrum der Noris Network AG in Nürnberg (Housing) relevant. Ferner wurden Server, Datenbanken und Betriebssystem aktualisiert.

13. Ergebnisse der Evaluierung:

Die Benutzung von ZKP ist intuitiv. Revisoren können anhand der Verarbeitungsschritte jederzeit sehen, welche Daten sich in welchem Workflow-Stand befinden. Dem Anwender stehen **aussagekräftige Produktdokumentationen** und Vorlagen zur Verfügung. Auch die **Informationsrechte der Beschäftigten** sind gewahrt.

Der Einsatz der ZKP im Rahmen der **Auftragsverarbeitung** ist vertraglich konform zu Art. 28 DSGVO geregelt und konzernweit einheitlich umgesetzt.

Der Einsatz erfolgt innerhalb einer **gesicherten IT-Umgebung** der Lidl Stiftung. Die Server und Datenbanken sind in einem gemäß ISO/IEC 27001-zertifizierten Rechenzentrum in Deutschland untergebracht.

Von besonderer Relevanz ist die **datenschutzrechtliche Zulässigkeit** der Verarbeitung personenbezogener Beschäftigtendaten. Für die Verarbeitung der beschäftigtenbezogenen Pseudonyme mittels der ZKP ist zunächst **Art. 6 Abs. 1 lit. f DSGVO** relevant. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein

Kind handelt. Dabei stehen die Interessen der Beschäftigten, nicht einer **Verhaltenskontrolle** sowie dem Verdacht einer Straftat unterzogen zu werden, den Interessen der Unternehmen gegenüber, Manipulationen und Straftaten und die daraus entstehenden wirtschaftlichen Schäden zu verhindern und aufzuklären. Die Datenverarbeitung und Analyse der ZKP fokussiert sich auf die nachträgliche Kontrolle des Kassiervorgangs, mithin auf ein Verhalten von Beschäftigten während der Kassiertätigkeit. Zwar sind die Beschäftigten in den Arbeitsverträgen und Rundschreiben hinreichend informiert worden über die ZKP, so dass keine verdeckte Überwachung vorliegt. Gleichwohl kann die bloße Tatsache, dass der Kassiervorgang mittels eines automatischen Systems auf Auffälligkeiten hin analysiert wird, einen **Überwachungsdruck** bei den betroffenen Beschäftigten auslösen und die Entfaltung des Persönlichkeitsrechts am Arbeitsplatz beeinträchtigen. Dabei ist jedoch zu berücksichtigen, dass die Überwachung der ZKP nicht flächendeckend oder auf Vorrat durchgeführt wird, sondern dass lediglich Stichproben genommen werden. Jede Gesellschaft eines Landes wird lediglich bis zu 2x pro Kalenderjahr als Stichprobe durch die Revision geprüft. Zusätzliche Analysen sind systemseitig reglementiert. Die Prüfung deckt ferner nur 24 Wochen einer Jahreskassiertätigkeit pro Bediener ab und nicht die gesamte Jahreskassiertätigkeit. Der Stichprobenumfang bei der manuellen Kennzahlenanalyse ist in der Standardeinstellung der ZKP zudem auf 15% gesetzt, so dass nicht mehr als 15% der Beschäftigten der jeweiligen Regionalgesellschaft geprüft werden, wobei die Verteilung der Stichprobe auf die definierten Kennzahlen je nach Manipulationsergebnis variabel sein kann. Der Stichprobenumfang von 15% stellt einen Maximalwert dar. Soweit die Anzahl der Manipulationsfälle mit Beginn der Prüfungshandlung nachhaltig (z.B. für die Dauer von 2 Jahren) rückgängig sein sollte, hat eine Verringerung des Stichprobenumfangs zu erfolgen. Der jeweils zuständige Fachbereich hat dem Entscheidungsgremium ZKP diese Tatsache unverzüglich mitzuteilen, damit der Veränderungsprozess angestoßen werden kann. Ferner werden ausschließlich **pseudonymisierte Daten** analysiert. Erst bei konkretem Verdachtsmoment, der innerorganisatorisch nochmals auf Schlüssigkeit außerhalb der elektronischen Datenverarbeitung geprüft wird, werden die Daten de-pseudonymisiert und durch den Vorgesetzten einem bestimmten Beschäftigten zugeordnet. In der dann folgenden Datenverarbeitung, die außerhalb der ZKP erfolgt, sind weitere organisatorische Maßnahmen eingebaut, die falsche Verdächtigungen und Rufschädigungen des Betroffenen möglichst ausschließen sollen. Der Betroffene wird zudem über die internen Ermittlungen informiert und kann sich dazu äußern. Sodann wird die gesamte Datenanalyse mittels der ZKP in die Hände einer neutralen Sachverwaltung bei der Lidl Stiftung gelegt, die ungebunden

gegenüber den Regionalgesellschaften und Märkten handelt und welche die Identität der betroffenen Beschäftigten nicht kennt.

Durch diese Maßnahmen und die Gesamt-Organisation der ZKP ist gewährleistet, dass nicht alle Beschäftigten permanent unter einen Generalverdacht der Manipulation gestellt werden. Zu berücksichtigen ist auch, dass mittels der ZKP-Analyse ein Verdachtsmoment, der durch eine manuelle Analyse des Verhaltens im Markt entsteht, gegengeprüft wird und diese Gegenprüfung zur Entlastung des Betroffenen beitragen kann. Vor allem aber ist eine Beeinträchtigung der Beschäftigten auf ein so gering wie mögliches Maß reduziert, ohne dass der Zweck der Aufdeckung von Manipulationen und Straftaten gefährdet wird. Es ist nicht ersichtlich, dass das Interesse der Beschäftigten gegenüber den Interessen der Unternehmen überwiegt. Durch Betrug, Diebstahl und Unterschlagung entstehen dem **Einzelhandel** jährlich Schäden in Millionenhöhe. Nach Art. 88 Abs. 1 DSGVO ist der Schutz des Eigentums der Arbeitgeber oder der Kunden ein legitimer Zweck. Die Unternehmen haben folglich ein berechtigtes, wirtschaftliches Interesse daran, dass Manipulationen und Straftaten zu ihren Lasten mittels der ZKP verhindert und aufgeklärt werden, um hieraus ggf. Regressansprüche oder ggf. arbeitsrechtliche Konsequenzen, wie Kündigung oder Abmahnung herzuleiten. Auch können Strafverfolgungsbehörden eingeschaltet werden. Die Ergebnisse der ZKP liefern dann für gerichtliche Verfahren Indizien oder gar Beweise und unterstützen somit die Beweisführung. Dabei ist die ZKP-Analyse bereits so voreingestellt, dass sie nur ab einer **Bagatellgrenze** Ergebnisse anzeigt. Dabei darf der Verdacht zur Manipulation im Prüfbericht nur dargestellt werden, wenn eine Manipulationssumme in Höhe von 25,- EURO erreicht wurde. Hinzu kommt, dass die Analyse der ZKP nur dann einen Vorfall anzeigt, wenn die definierten Schwellwerte überschritten werden. Die Unternehmen werden folglich mittels der ZKP nicht unterhalb dieser Bagatellgrenze und der Schwellwerte tätig, wenngleich sich auch hier Straftaten und wirtschaftliche Schäden ergeben können. Ein milderer Mittel ist nicht ersichtlich. Insbesondere liefe eine Anonymisierung von Beschäftigtendaten in der ZKP dem Zweck zuwider, Manipulationen und Strafen auch verfolgen zu können und hieraus Regress oder arbeitsrechtliche Konsequenzen nehmen zu können. Wenn die ZKP in der Analyse einen Verdachtsmoment bestätigt, ist es für das Unternehmen nicht hinnehmbar, diesen nicht auch verfolgen zu dürfen. Andere Kontrollmöglichkeiten, wie etwa die manuelle Auswertung aller Kassivorgänge durch den Marktleiter, sind personell und wirtschaftlich nicht vertretbar und wären zudem mit einem höheren Überwachungsdruck gegenüber den Beschäftigten verbunden. Die ZKP ist daher zur Wahrung der berechtigten Interessen der Unternehmen erforderlich.

Sofern Beschäftigte in EU-Staaten betroffen sind, in denen die Staaten von der **Öffnungsklausel des Art. 88 DSGVO** Gebrauch gemacht haben, kommen länderspezifischen Regelungen als Rechtsgrundlage in Betracht. Etwa ist für Deutschland **§ 26 Abs. 1 BDSG** relevant, welcher sich auf das (vertragliche) Beschäftigungsverhältnis bezieht (Satz 1) und auf die Aufdeckung von Straftaten im Beschäftigungsverhältnis (Satz 2)¹. Diese beiden Rechtsgrundlagen sind im Hinblick auf die ZKP voneinander abzugrenzen. Nach § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Nach § 26 Abs. 1 S. 2 BDSG dürfen personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Der Wortlaut des § 26 Abs. 1 S. 2 BDSG weist in der Praxis Auslegungsschwierigkeiten auf, die auch durch die Gesetzesbegründung sowie durch zwischenzeitliche Kommentierungen der Fachliteratur nicht behoben wurden². Etwa bleibt weiterhin unklar, ob § 26 Abs. 1 S. 2 BDSG neben den repressiven Zwecken der Aufdeckung von Straftaten auch präventive Zwecke zur Verhinderung selbiger erfassen soll, zumal sich in Gemengelagen die Zweckbestimmungen oftmals nicht trennen lassen³. Im vorliegenden Fall liegt aber genau eine solche **Gemengelage** verschiedener Zwecke vor, denn die ZKP verfolgt sowohl repressive als auch präventive Zwecke. Dabei liegt jedoch zu diesem Zeitpunkt der Datenverarbeitung mittels der ZKP kein konkreter Tatverdacht vor, sondern lediglich Kennzahlen, die in der weiteren Datenverarbeitung außerhalb der ZKP ausgewertet und weiter erforscht werden müssen. Die Datenverarbeitungsprozesse der ZKP können daher mangels eines konkreten Tatverdachts nicht auf § 26 Abs. 1 S. 2 BDSG als Rechtsgrundlage gestützt werden. Es kann jedoch festgestellt werden, dass die ZKP auch – und sogar eher – der Prävention / Verhinderung von Manipulationen und der Prozessoptimierung der Analyse

¹ Eine Einwilligung der Beschäftigten als Rechtsgrundlage nach § 26 Abs. 2 BDSG scheidet hingegen kategorisch aufgrund des Über-/Unterordnungsverhältnisses zwischen den Arbeitgebern als Nutznießer der ZKP-Daten und den betroffenen Beschäftigten aus.

² Karper in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 1.Auflage, Kap. F, Rn. 48 m.w.N.

³ ebenda.

durch Aufzeigen eventueller weiterer Schwachstellen sowie der zeitlichen Entlastung der Verkaufsleiter durch automatisierte Prozesse dient – und weniger den strafverfolgenden Interessen. Letztere sind zudem mit der ZKP nicht zu realisieren, da sie völlig außerhalb des ToE erfolgen und weitere Nachforschungen und Prüfprozesse der Revision, des Vorgesetzten und der Strafverfolgungsbehörden voraussetzen. Unterhalb der benannten Bagatellgrenze und der Schwellwerte gibt die ZKP zudem keine Kennzahlen heraus, auch wenn in diesen Fällen ggf. Straftaten vorliegen würden. Selbst bei einem durch die ZKP anfänglich ermittelten und durch Nachforschung des Vorgesetzten erhärtetem Verdacht einer Straftat erfolgt in vielen Fällen keine Strafanzeige (sofern kein Officialdelikt vorliegt), da dies letztendlich für den Konzern unwirtschaftlich ist.

Die wohl herrschende Ansicht sieht für die Datenverarbeitung im Rahmen von präventiven Maßnahmen, die noch keine konkreten Verdachtsmomente voraussetzen, § 26 Abs. 1 S. 1 BDSG als Rechtsgrundlage an⁴. Danach ist eine (offene) Überwachung, die sich nicht gegen bestimmte Beschäftigte richtet, nicht dauerhaft ist und die der Verhinderung von Verstößen dient, auch ohne einen Verdacht zulässig⁵. Für diese Ansicht spricht zudem die Gesetzesbegründung des damaligen § 32 BDSG a.F., der im Wortlaut des § 26 BDSG jedoch unverändert ist: *„Nach der Einstellung darf der Arbeitgeber sich bei seinen Beschäftigten über Umstände informieren oder Daten verwenden, um seine vertraglichen Pflichten gegenüber den Beschäftigten erfüllen zu können, z. B. Pflichten im Zusammenhang mit der Personalverwaltung, Lohn- und Gehaltsabrechnung. Das gilt auch, wenn der Arbeitgeber seine im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses bestehenden Rechte wahrnimmt, z. B. durch Ausübung des Weisungsrechts oder durch Kontrollen der Leistung oder des Verhaltens des Beschäftigten. Nach Satz 1 ist deshalb z. B. auch die Zulässigkeit solcher Maßnahmen zu beurteilen, die zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen, erforderlich sind.“*⁶

Nach Ansicht der EuroPriSe-Expertin ist diese Ansicht vorzugswürdig. Danach ist aufgrund des überwiegend präventiven Charakters des Systems **§ 26 Abs. 1 Satz 1 BDSG** anwendbar. Es

⁴ Stamer/Kuhnke in: Plath, DSGVO BDSG Kommentar, 3. Auflage 2018, § 26 BDSG, Rn. 77b m.w.N. Bereits zu § 32 BDSG a.F. vertreten diese Meinung u.a. Simitis, BDSG, § 32 Rn. 103; Gola/Schomerus, BDSG, § 32 Rn. 39; Taeger/Gabel, BDSG, § 32 Rn. 48.

⁵ Stamer/Kuhnke in: Plath, DSGVO BDSG Kommentar, 3. Auflage 2018, § 26 BDSG, Rn. 77d m.w.N. auch zur Rechtsprechung des BAG.

⁶ Bundestagsdrucksache 16/13657, 16. Wahlperiode, Seite 21, auch abrufbar unter <http://dip21.bundestag.de/dip21/btd/16/136/1613657.pdf> .

kommt daher für die Anwendung der ZKP im Rahmen des Beschäftigungsverhältnisses auf die Erforderlichkeit und Verhältnismäßigkeit an. Diese Aspekte wurden bereits oben im Rahmen der Interessenabwägung ausführlich dargestellt, so dass auf die dortigen Aussagen verwiesen wird. Andere, gleich geeignete Maßnahmen der Auswertung der Kassivorgänge sind nicht ersichtlich, insbesondere scheidet eine Beobachtung durch z.B. Detektive aus, da dadurch eine Pseudonymisierung der Daten gefährdet wäre. Beschäftigte sind über den Einsatz der ZKP informiert. Eine Dauerüberwachung oder eine Vollkontrolle aller Beschäftigten oder aller Kassivorgänge ist damit nicht verbunden. Dies wird durch die beschriebenen Mechanismen der periodischen Stichproben, der Pseudonymisierung, des neutralen Sachwalters und der Bagatell- und Schwellwertgrenzen sichergestellt. Die Maßnahme ist insgesamt erforderlich, verhältnismäßig und datenschutzrechtlich nicht zu beanstanden.

Schließlich können **Kollektivregelungen** eine Rechtsgrundlage darstellen und die Zulässigkeit im Lichte des Art. 88 DSGVO konkretisieren. Diese stellen etwa in der BRD nach § 26 Abs. 4 BDSG eine Rechtsgrundlage der Verarbeitung von Beschäftigtendaten dar, wobei Art.88 DSGVO zu beachten ist. Eine Kollektivvereinbarung kann daher nur dann einen Erlaubnistatbestand darstellen, wenn sie die Vorgaben der DSGVO weiterhin erfüllt⁷.

⁷ Rossow in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 1.Auflage, Kap. C, Rn. 430 m.w.N.

14. Datenfluss:

Der Datenfluss des ZKP lässt sich wie folgt darstellen:

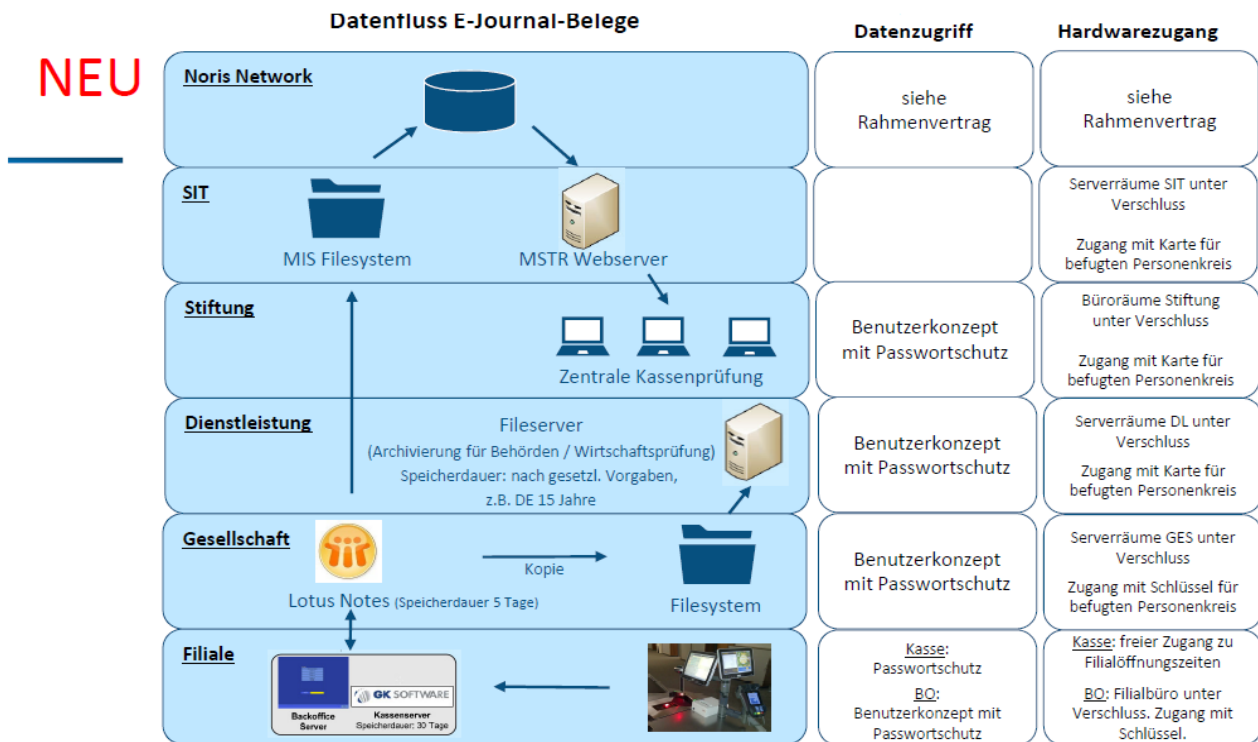


Abbildung 1: Datenfluss (Legende: „BO“ = Backoffice“)

15. Datenschutz-fördernde Funktionalitäten:

- Die seitens der Lidl Stiftung & Co. KG stetig weiterentwickelten und umgesetzten Datenschutz- und Sicherheitsmaßnahmen entsprechen vorbildlich dem Privacy-by-Design Grundsatz. Dabei gelingt es, die ZKP so einzusetzen, dass das größtmögliche Maß des Schutzes der Beschäftigendaten ausgeschöpft und gleichwohl die Effizienz zur Aufklärung und Verhinderung von Schäden zulasten der Unternehmen gesichert wird. Die ZKP erreicht dies u.a. durch Pseudonymisierung des Datensatzes, durch ein mehrstufiges Prüfungskonzept, durch Einbindung der Lidl Stiftung als neutralen Revisor und durch immer aktuelle Manipulationsszenarien und Schwellwerte, die eine Bagatellisierung ausschließen.
- Das Rechenzentrum, in welchem sich die Systeme der ZKP befinden, weist ein hohes Maß an physikalischer Sicherheit auf und ist zertifiziert; für die ohnehin nur als Pseudonym zu bewertenden Daten wird dadurch ein vorbildlich hohes Schutzniveau realisiert.

16. Bereiche, die besondere Aufmerksamkeit der Benutzer erfordern:

Nicht erforderlich.

17. Ausgleich von Schwächen:


Nicht erforderlich.


18. Übersicht der Bewertung der Anforderungen:

<i>EuroPriSe Requirement</i>	<i>Decision</i>	<i>Remarks</i>
Data Avoidance and Minimisation	Excellent	Der Umfang der Datenverarbeitung mittels ZKP ist auf die notwendigen personenbezogenen Daten minimiert. Es werden anhand der Bedienernummer ausschließlich Pseudonyme verwendet. Ferner werden mittels der ZKP nur Stichproben aus der gesamten Datenmenge für einen bestimmten, eingegrenzten Zeitraum von 12 Wochen erhoben. Reports für Gesellschaften enthalten keine personenbeziehbaren Daten. Damit werden im größtmöglichen Maß die Möglichkeiten einer Reduzierung der Datenverarbeitungsprozesse ausgeschöpft.
Transparency	Excellent	Die Benutzung ist intuitiv; Dokumentationen sind aktuell; es ist zu jeder Zeit zu erkennen, welche Daten sich in welchem Workflow befinden.
Technical-Organisational Measures	Adequate	Das Rechenzentrum, in welchem sich die Systeme der ZKP befinden, weist ein hohes Maß an physikalischer Sicherheit auf und ist zertifiziert; für die ohnehin nur als Pseudonym zu bewertenden Daten wird dadurch ein vorbildlich hohes Schutzniveau realisiert.
Data Subjects' Rights	adequate	Das Vorgehen zur Information der Beschäftigten über die ZKP und deren Datenschutz-Rechte insgesamt ist konzernweit standardisiert.

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
-------------	---------------------------------	-----------