Kurzgutachten

Rezertifizierungs-Nr. EP-S-DZ2LYR

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

   Zentrale Kassenprüfungssoftware (ZKP); Version 8.1, Funktionsstand August 2021.

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:

   02.01.2021 – 21.10.2021.

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
- **Neu**: Hinzuziehung von Videobildmaterialien, sofern zulässig und vorhanden.

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 inkl. dessen Back-Up, Recovery und Archivierung
- Die Videosysteme.

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 pseudonyme **Bedienernummer**, die Rückschlüsse auf Beschäftigte zulässt. 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 gegenübergesetzt, 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 wird im Hinblick auf folgende Kennzahlen:

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

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.

Neu ist die Möglichkeit, **Videobildmaterial** hinzuzuziehen, sofern für die jeweilige Regionalgesellschaft vorhanden und dies zulässig ist. Ein „Videomasterkonzept" legt pro Gesellschaft etwa die rechtlichen Anforderungen an eine Videoüberwachung fest, z.B. Infoschilder, zulässige Kamerafokussierung, Speicherdauer etc. Ist eine Videoüberwachung von Beschäftigten an Kassierplätzen zulässig und liegt Material vor, kann dies von den ZKP-Prüfern bei bestimmten Manipulationsszenarien angefragt werden. Die Freigabe erfolgt durch den Datenschutzbeauftragten der Regionalgesellschaft. Die Prüfer erhalten dann einen Remote-Zugriff auf das diesbezügliche Videosystem. Der Zugriff auf konkrete Bilddaten ist gemäß der Anweisung anhand der Daten des Kassierbons (Filiale, Kasse, Datum, Uhrzeit) bestimmt und darauf beschränkt. In den Videodaten sind die Kassiererplätze während der Überprüfung konform zum Videomasterkonzept übrigens immer ausgeblendet, indem die Bilddaten im Bereich von Kopf und Oberkörper verpixelt bzw. gegraut werden. Nur im Falle der Auswertung werden die Bilddaten dann entpixelt bzw. entgraut. Im Falle einer Weiterverwendung vor Gericht können Bilddaten von Unbeteiligten wieder verpixelt/gegraut 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 gelöscht.

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 Gesellschaften, für welche die ZKP angewendet wird, sitzen in der EU und in Drittstaaten. Daten, die per ZKP verarbeitet werden, sind pseudonymisierte Beschäftigtendaten einer Regionalgesellschaft in den nachfolgend aufgeführten Ländern (08/2021):

1. Serbien (neu)	15. Belgien
2. Deutschland	16. Niederlande
3. Frankreich	17. Österreich
4. Malta	18. Ungarn
5. Griechenland	19. Polen
6. Zypern	20. Tschechien
7. Spanien	21. Slowakei
8. Portugal	22. Slowenien
9. England	23. Kroatien
10. Irland	24. Rumänien
11. Nordirland	25. Bulgarien
12. Dänemark	26. Litauen
13. Finnland	27. Schweiz
14. Schweden	28. USA

Das Competence Center der Lidl Stiftung und die Schwarz IT GmbH & Co KG (SIT) sind in Deutschland ansässig. Ein weiteres Competence Center ist in Bulgarien. Die Subunternehmen Snowflake und Microsoft sitzen in den Niederlanden mit Bezug zu Konzernmüttern in Drittstaaten (USA).

9. Verwendete Tools:

MicroStrategy 2020, Frondend und Teradata, Backend.

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

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

- Das Konzept Zentrale Kassenprüfung wurde aktualisiert.
- Es wurde eine neue Kennzahl Rabatt eingeführt.
- Es wurde ein neuer Prozess zur Einbindung von Videodaten als erweiterte Sachverhaltserforschung beschrieben.
- Es wurden Änderungen eingefügt, die sich auf die Migration der IT-Systeme in eine Cloudlösung (Microsoft Azure) beziehen.
- Als Alternative zur Fuhrenpost werden Berichte per E-Mail versendet.
- Das Handbuch zur Bedienung wurde aktualisiert
- Das Dokument der technischen Konzeption wurde aktualisiert.
- Das Verfahrensverzeichnis wurde aktualisiert.
- Während der Evaluation fand eine Migration der ZKP Systeme in eine Azure Cloud-Umgebung in ein Rechenzentrum von Microsoft in Amsterdam statt. Die Bondaten werden in der Microsoft Azure Cloud verarbeitet. Die Server sind im Unterauftrag der SIT in einem Microsoft-Rechenzentrum in Amsterdam untergebracht. Die Firma Snowflake übernimmt im Auftrag der SIT dort den Cloud Data Warehouse Service, ebenfalls vom Standort Amsterdam.
- Das Competence Center in Neckarsulm ist unverändert. Neu ist der Einsatz eines Competence Centers in Bulgarien, welches den gleichen Richtlinien und Anweisungen unterliegt, wie das in Neckarsulm.
- Die ZKP wird weiterhin in den bekannten Regionalgesellschaften angewendet. Neu ist die Regionalgesellschaft in Serbien (EU-Beitrittskandidat).

12. Änderungen der rechtlichen oder technischen Anforderungen

Durch die Migration der ZKP Systeme in die Microsoft Azure Cloud sind die Anforderungen der Rechtsprechung des EuGHs in der Rs. C-311/18 „Schrems II" sowie die entsprechenden Auslegungen der Aufsichtsbehörden, insbesondere die des Europäischen

Datenschutzausschusses (EDSA)[1] umzusetzen. Die technischen Anforderungen an die ZKP bleiben dadurch jedoch unverändert. Die Anforderungen an die Datenverarbeitung mittels der ZKP zum Beschäftigtendatenschutz inklusive der Weiterverarbeitung von Videobildmaterialien sind unverändert.

13. Ergebnisse der Evaluierung:

Transparenz

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

Auftragsverarbeitung

Der Einsatz der ZKP erfolgt im Auftrag der Regionalgesellschaft / Landesgesellschaft als verantwortliche Stelle. Die Lidl Stiftung GmbH & Co. KG ist Auftragnehmer dieser Datenverarbeitung. Sie hat die Lidl Bulgaria EQOD & CO. KD für das zweite Competence Center unterbeauftragt sowie ferner für den IT-Support die Schwarz IT GmbH & Co KG (SIT). Die SIT wiederum hat die Microsoft Ireland Operations Limited und die Microsoft Deutschland GmbH mit dem Hosting und Housing der Rechenzentren unterbeauftragt. Die Snowflake Inc. USA übernimmt im Unterauftrag der SIT den Cloud Data Warehouse Service, der durch die Snowflake Computing Netherlands B.V. am Standort Amsterdam erfolgt, wo sich auch das Rechenzentrum (Microsoft) befindet.

Der Einsatz der ZKP im Rahmen der **Auftragsverarbeitung** gegenüber den Regionalgesellschaften sowie gegenüber der SIT und der Lidl Bulgaria EQOD & CO. KD ist **konzernweit einheitlich** umgesetzt. Für alle Unternehmen der Lidl Gruppe gibt es einen einheitlichen Rahmenvertrag zur Auftragsverarbeitung, der durch sogenannte DViA zu speziellen Leistungen ergänzt werden kann. Im Rahmen der Evaluation wurden die Vertragskonvolute geprüft, die konform zu Art. 28 DSGVO sind.

Ebenfalls geprüft wurden die Vertragskonvolute der SIT mit Microsoft und Snowflake, die alle Anforderungen erfüllen. Sie beruhen auf Data Protection Addendums und

[1] Abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_en (Stand: Oktober 2021).

Standardvertragsklauseln. Aufgrund des zwischenzeitlich erlassenen Durchführungsbeschlusses (EU) 2021/914 liegen neue Standardvertragsklauseln vor, die im Rahmen der Übergangsfrist angewendet werden.

Generelle Zulässigkeit der ZKP-Verarbeitung von Beschäftigtendaten

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 milderes Mittel ist nicht ersichtlich. Insbesondere liefe eine Anonymisierung von Beschäftigtendaten in der ZKP dem Zweck zuwider, Manipulationen und Straftaten 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 Kassiervorgänge 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.

Beschäftigtendaten und Öffnungsklauseln der DSGVO

Die ZKP verarbeitet Beschäftigtendaten i.S.d. Art. 88 DSGVO in Form der Kassierdaten (Bons), Kassierernummer, und ggf. im Einzelfall anhand von Videobilddaten des Kassierarbeitsplatzes während der Arbeitszeit. Somit kommen nationale Regelungen oder Kollektivvereinbarungen als Ermächtigungsgrundlage in Betracht. Sofern Beschäftigte in EU-Staaten betroffen sind, in denen die Staaten von der **Öffnungsklausel des Art. 88 DSGVO** Gebrauch gemacht haben, kommen länderspezifische 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)[2]. 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

---

2 Eine Einwilligung der Beschäftigten als Rechtsgrundlage nach § 26 Abs. 2 BDSG scheidet hingegen aufgrund des Über-/Unterordnungsverhältnisses zwischen den Arbeitgebern als Nutznießer der ZKP-Daten und den betroffenen Beschäftigten regelmäßig aus, siehe z.B. für Deutschland das Kurzpapier Nr. 14 Beschäftigtendatenschutz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 24.09.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf., Seite 1f. (Stand Oktober 2021)

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 wurden[3]. 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 lassen[4]. 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 (Fraud Detection) und der Prozessoptimierung der Analyse durch Aufzeigen eventueller weiterer Schwachstellen sowie der zeitlichen Entlastung der Verkaufsleiter durch automatisierte Prozesse dient – und weniger den strafverfolgenden Interessen. Bondatenanalysen haben daher regelmäßig keinen repressiven Charakter[5]. Eine repressive Verfolgung wäre 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 Offizialdelikt 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 an[6]. Danach ist eine (offene) Überwachung, die sich nicht gegen

---

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

4 ebenda.

5 So auch Gola in: Gola, Handbuch Beschäftigtendatenschutz, 8. Auflage 2019, Rn. 1401 und1406.

6 Gola in: Gola, Handbuch Beschäftigtendatenschutz, 8. Auflage 2019, Rn. 1401 und1406; Forst in: Auerhammer, DSGVO BDSG Kommentar, 7. Auflage 2020, § 26 BDSG, Rn. 68.

bestimmte Beschäftigte richtet, nicht dauerhaft ist und die der Verhinderung von Verstößen dient, auch ohne einen Verdacht zulässig[7]. 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."*[8]

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 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 Kassiervorgänge 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 Kassiervorgänge 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

---

7 So auch das BAG Urteil vom 28. März 2019, Az. 8 AZR 421/17, a.A.: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/datenschutzbeauftragter-von-baden-wuerttemberg-kritisiert-urteil-des-bundesarbeitsgerichts/ (Stand Oktober 2021).

8 Bundestagsdrucksache 16/13657, 16. Wahlperiode, Seite 21, abrufbar unter https://dip21.bundestag.de/dip21/btd/16/136/1613657.pdf (abrufbar Oktober 2021).

DSGVO zu beachten ist. Eine Kollektivvereinbarung kann daher nur dann einen Erlaubnistatbestand darstellen, wenn sie die Vorgaben der DSGVO weiterhin erfüllt[9].

Datenübermittlung an Drittländer

Durch den Einsatz der ZKP in der Umgebung von Microsoft und Snowflake ist ein potentieller Drittstaatenbezug gegeben. Vertraglich ist der Datenschutz zwischen der SIT und den durch US-amerikanische Konzerne gesteuerten Unternehmen Microsoft und Snowflake in DPA´s und Standardvertragsklauseln (SCC) geregelt. Durch das Urteil des EuGHs in der Rs. C-311/18 „Schrems II" ist jedoch statuiert, dass dies alleine nicht mehr ausreicht. Um für die von der Verarbeitung der ZKP betroffenen Beschäftigten in der EU ein angemessenes Datenschutzniveau im Lichte der EU-Grundrechte-Charta und im Hinblick auf Art. 46 Abs. 1 DSGVO zu bewirken, bedarf es zusätzlicher geeigneter Garantien, u.a. für die Durchsetzbarkeit von Rechten und wirksamen Rechtsbehelfen der Betroffenen. Landesdatenschutzbehörden sowie der EDSA haben in Handlungshilfen u.a. eine Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten vorgeschlagen. Aus Sicht der EuroPriSe-Expertin sind die Vorgaben für die ZKP vollumfänglich erfüllt. Die Verarbeitung der Bedienerdaten ist auf ein geringstmögliches Maß reduziert. Die Bedienerdaten sind pseudonymisiert und können nur unter Anwendung erheblicher Aufwände und Missachtung von technischen und organisatorischen Maßnahmen de-pseudonymisiert werden, wovon nicht auszugehen ist. Die Daten unterliegen ferner dem vertraglichen Schutz des DPA und dortigen Sanktionsmöglichkeiten der Vertragspartner und den dort geregelten zusätzlichen Garantien für Betroffene. Die Lidl Stiftung weist zudem in Transfer Impact Assessments (TIA) nach, dass für eine potentielle Drittstaatenübermittlung geeignete Garantien i.S.d. Art. 46 DSGVO vorliegen, welche das Risiko für den Schutz aller personenbezogenen Daten in der ZKP minimieren. Die TIAs sind schlüssig und nachvollziehbar. Die EuroPriSe-Expertin erkennt diesen risikominimierenden Ansatz an. Das Risiko der Betroffenen ist durch die oben benannten Maßnahmen deutlich reduziert.

Informationssicherheit

Der Zugriff auf die ZKP erfolgt innerhalb einer **gesicherten IT-Umgebung** der Lidl Stiftung in den Competence Centern in Deutschland und Bulgarien. Die Server und Datenbanken sind in

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

einem gemäß ISO/IEC 27001-zertifizierten Rechenzentrum von Microsoft in Amsterdam, Niederlande untergebracht.

14. Datenfluss:

Der Datenfluss der ZKP lässt sich wie folgt darstellen:

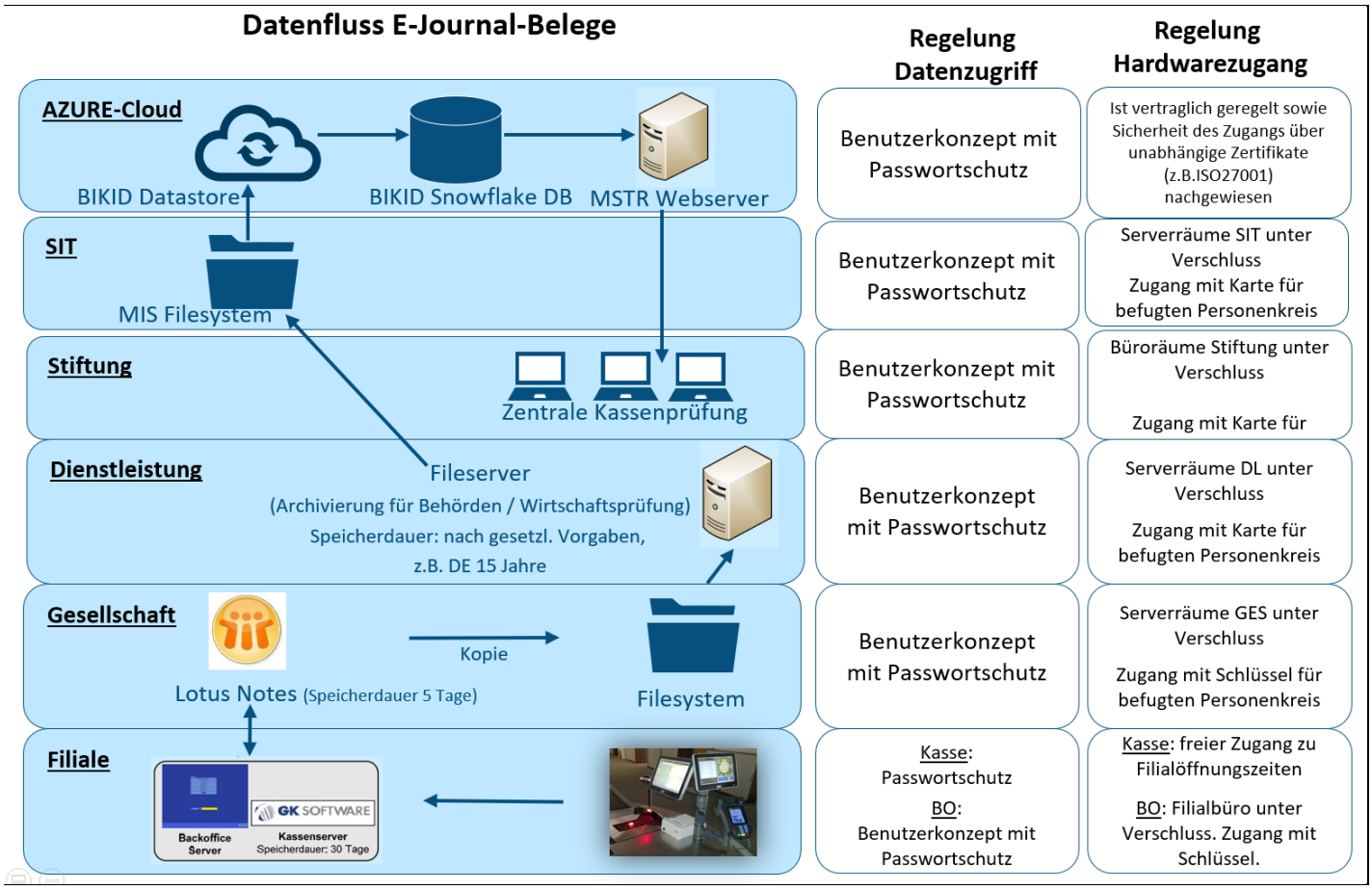

Abbildung 1: Datenfluss (Legende: „BO" = Backoffice", „SIT" = Schwarz IT)

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 Beschäftigtendaten 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.

16. Bereiche, die besondere Aufmerksamkeit der Benutzer erfordern:

Nicht erforderlich.

17. Ausgleich von Schwächen:

Nicht erforderlich.

18. Übersicht der Bewertung der Anforderungen:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	Excellent	Der Umfang der Datenverarbeitung mittels ZKP ist auf die notwendigen personenbezogenen Daten minimiert. Es werden anhand der Bedienernummer 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.
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, 21.10.2021	Dr. Irene Karper	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Bremen, 21.10.2021	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.

		Sebastian Meissner Digitally signed by Sebastian Meissner DN: cn=Sebastian Meissner, o=EuroPriSe GmbH, ou=EuroPriSe CA, email=meissner@european-privacy-seal.eu, c=DE Date: 2021.12.14 11:03:46 +01'00'
Place, Date	Name of Certification Authority	Signature