IT-Sicherheitsrechtstag 2018

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Berlin, 25.10.2018

Der Übergang zur EU-DSGVO

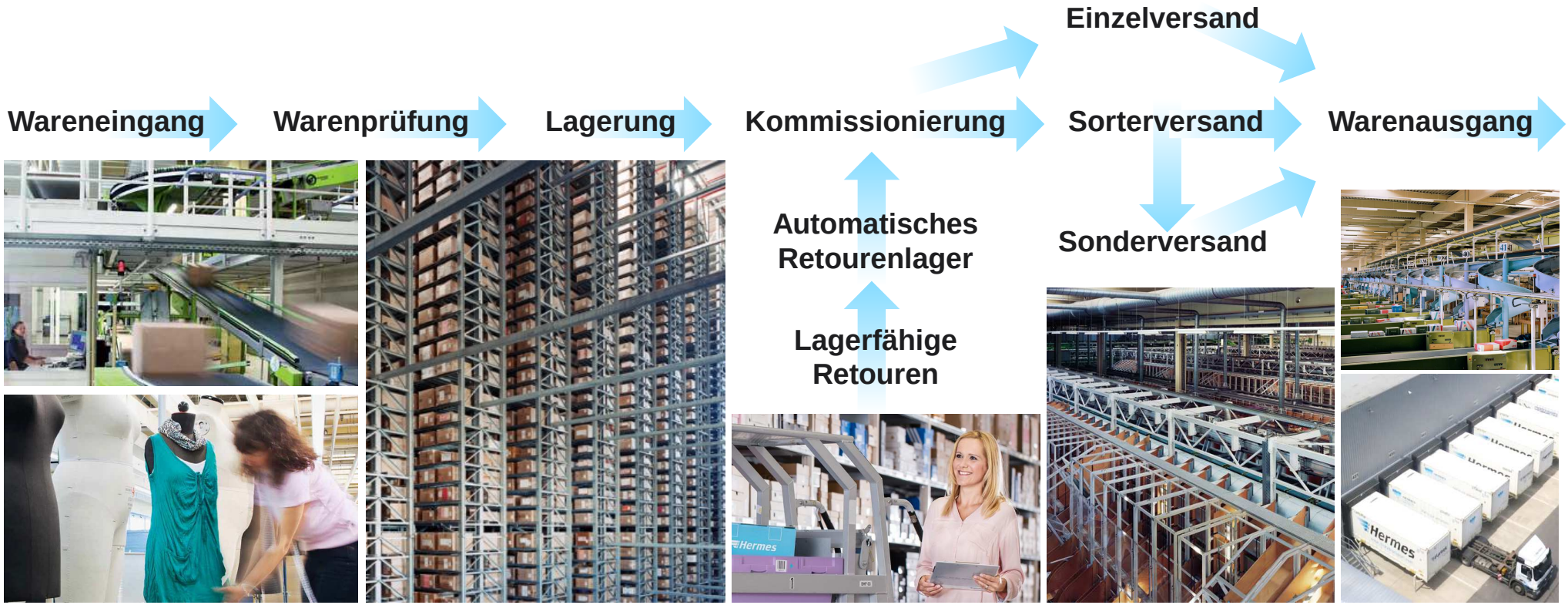
Frank Helle

Datenschutzbeauftragter

Hermes Fulfilment GmbH

Unsere Wertschöpfungskette beginnt ab Wareneingang, darauf folgt die Prüfung und Einlagerung und ab Sendungseingang die Kommissionierung, Sortierung und Warenausgang

Wertschöpfungskette – exemplarisch für die Paketlogistik



Quelle HF

Als Fulfilment Dienstleister deckt unser Leistungsportfolio Lagerlogistik, Retouren-abwicklung, Transport Management und Consulting ab

Leistungsportfolio

Lagerlogistik

- Flexible und skalierbare Lagerhaltung
- Inbound und Outbound Management
- Warehouse Management System
- Qualitätskontrolle
- Value Added Services

Retourenabwicklung

- Internationale Retouren-rückführung
- Retouren-bearbeitung
- Verwertung und Recycling
- Reparatur
- Ersatzteilhandling
- Eigene Reinigung
- Entsorgung

Transport Management

- Internationale Paketdistribution
- 1- & 2-Mann-Handling
- Carrier-management
- Direktversand

Consulting

- Prozess-optimierung
- Standortplanung
- Solution Design
- Verpackungs-management

Schutzbedürftige Datenkategorien

~60 Mio. Kundendaten der Händler

Kunden-Stammdaten, Zahlungsdaten, Zahlungswegedaten, Daten zur Warenbestellung und Bestellabwicklung, Lieferungsdaten

Beschäftigtendaten
von über 5400 Beschäftigten

Prozessdaten, Leistungsdaten (Prämie), Personal & Gehaltsdaten, Zeitdaten
……..

Vom BDSG zur EU-DSGVO in der Hermes Fulfilment

Quelle: Piaxabay

Vorgehen

Herausforderungen

Aktueller Stand

Vom BDSG zur EU-DSGVO in der Hermes Fulfilment

Umfangreiche Themen implizieren zunächst den “Großprojekt-Ansatz”

- **Ressourcenbedarf**
- **Konkurrenz zu laufenden Projekten**
- **Zeitdruck**
- **Zwang zur Umsetzung**

- **laufender Reorganisationsprozess**
- **Umbau Organisationsstrukturen**
- **grundlegende Veränderungen von Geschäftsprozessen**
- **Veränderungen strategischer Ausrichtungen**

Wir lösen den Konflikt durch

Ermittlung der für die Gesellschaft relevanten Themen
Adressierung der Einzelthemen an Verantwortliche der Fachbereiche mit Handlungsempfehlung
Unterstützungsleistungen durch DSB, ISO und Experten
Bericht über Fortschritte in Routinen mit GF, bei Erfordernis Eskalation
Einbindung unseres Vorgehens in das Status-Audit des Konzerns

1. Identifikation der relevanten Themen 1/2

	Themenübersicht DSGVO (nicht relevante Themen)					
BEREICH	THEMA	To Do	Wer	Zeitraum /Termi	Status	Bemerkung
	Inkasso	nein				für HF nicht relevant
	Scoring	nein				für HF ni
	Einzelfallentscheidung	nein				
	Printwerbemittel	nein				relevant
	Datenschutzhinweise in Printwebemitteln	nein				ür HF nicht relevant
	Profilbildung im Datawarehouse	nein				für HF nicht relevant
	Aktive Zahlungsartensteuerung	nein				für HF nicht relevant
	Adresshandel	nei				für HF nicht relevant
	Zahlungsarteneinschränkung					für HF nicht relevant
	Einwilligungen (Endkunden)					für HF nicht relevant
	Auskunft	nein				für HF nicht relevant
	Inform	nein				für HF nicht relevant
		nein				für HF nicht relevant
	Drittländer	nein				für HF nicht relevant
	übertragbarkeit	nein - wenn dann über Auftraggeber				für HF nicht relevant

nicht relevant

1. Identifikation der relevanten Themen 2/2

- Initialbelehrung (zzgl. zeitnahe Schulung)
- Schulungskonzept, e-Learnings
- Informationsunterlage für Beschäftigte
- Prozess Umgang mit Datenpannen Information und Prozess
- Speicherung von Bewerberdaten
- Einwilligungen im Beschäftigungsverhältnis
- kleines Konzernprivileg
- Auftragsdatenverarbeitung (ADV)
- pb Daten / anonyme Daten / Pseudonymisierung
- Verzeichnis von Verarbeitungstätigkeiten / DFS
- Webseite - Klärung Verantwortlichkeiten und DSGVO-konforme Gestaltung
- DS durch Technik und ds-freundliche Voreinstellungen
- Videobeobachtung
- Löschkonzept / Recht auf Löschung / Recht auf Auskunft / Berichtigung

2. Adressierung der Anforderungen an Fachabteilungen / Status
(Auszug / Beispiele)

Zuordnung zum Fachbereich → Person → Abmeldung Erledigung / Kontrolle

Themenbereich	Beteiligte FB	Status	
Initialbelehrung (zzgl. zeitnahe Schulung) Schulungsangebote, Informationsunterlage Rechte der Betroffenen (Beschäftigten) Art. 15,16,20 DSGVO	HR / DSB	Initialbelehrung angepasst Mitarbeiterinformation bereitgestellt an HR bzw. über FK	✓
Speicherung von Bewerberdaten	HR	Anpassung Bewerberportal durch AN/ DL (mehrere Konzernfirmen) angepasst	✓
Prozess Umgang mit Datenpannen Information und Prozess	SI / DSB	Anpassung Incidentprozess Aufnahme in Krisenprozesse	✓
Verzeichnis von Verarbeitungstätigkeiten / DFS	FB-Verantwortlicher / DSB, DSK	Nutzung konzerneinheitliches Tool, Verarbeitungen initial erstellt, wesentliche Anpassungen (z.B. Rechts-grundlagen) bis XX/2018, Operationalisierung/Reviewprozess mit Fachbereichen bis XX / 2018	✓

Hermes

4. Support durch Datenschutz Konzern und Rechtsabteilung der ottogroup

Self-Assessment

54 Fragen zu den wesentlichen Themenbereiche der DSGVO

Struktur Self-Assessment

Frage-Nr.	Inhalt	Brand/ Rechtseinheit	Antw.	Kommentar gem. Self Assessment Bogen
04	Gibt es in Ihrem Unternehmen eine Richtlinie zum Datenschutz? Wenn ja: stellen Sie uns diese bitte zur Verfügung.	Hermes Fulfilment GmbH	Nein	Status: in Erarbeitung / Abstimmung - Richtlinie zum Datenschutz wurde erstellt und befindet sich aktuell in der Abstimmung mit dem BR und in der Finalisierung - zu 95% erledigt. Termin GF 24.07.2017 Anlage: 4_Entwurf_2017_06_16_HF_RL_Datenschutz_2017.pd4.pdf

umsetzbar bis 25.05.18? (Stand Feb 2018)	umsetzbar bis 25.05.18? (neu)	Erfüllungs-grad in % (bis Feb 20	Erfüllungs-grad in % (neu)	Anmerkung	Anmerkung (neu)	Status (per Feb 2018)	Status (neu)
Ja!	Ja!	100%	100%	Die RL wurde an Führungskräfte der ersten Berichtsebene durch die GF kommuniziert.Weiterhin erfolgten Hinweise über die Bildschirme und das Intranet sowie direkte Schulungen au		erledigt	erledigt

Beispiele der Fragen im Self-Assessment

Frage-Nr.	Inhalt
01	Ist eine Person im Unternehmen benannt, die explizit für den Datenschutz zuständig ist (z.B. ein Datenschutzbeauftragter oder -koordinator?
02	Gibt es in Ihrem Unternehmen ein Organigramm? Wenn ja: stellen Sie uns dieses bitte zur Verfügung.
03	Ist in Ihrem Unternehmen bereits eine (interne oder behördliche) Prüfung zum Datenschutz in den vergangenen 5 Jahren durchgeführt worden? Wenn ja: stellen Sie uns das Ergebnis bitte zur Verfügung.
04	Gibt es in Ihrem Unternehmen eine Richtlinie zum Datenschutz? Wenn ja: stellen Sie uns diese bitte zur Verfügung.
05	Gibt es weitere Richtlinien in Ihrem Unternehmen mit Bezug zum Datenschutz? Wenn ja: stellen Sie uns diese bitte zur Verfügung.
06	Existiert in Ihrem Unternehmen ein Datenschutzmanagementsystem? Wenn ja: stellen Sie uns eine Zusammenfassung
07	Sind in in Ihrem Unternehmen die Anforderungen aus der Konzernrichtlinie Informationssicherheit vollständig umgesetzt worden?
08	Existiert in Ihrem Unternehmen eine Richtlinie zur Informationssicherheit? Wenn ja: stellen Sie uns diese bitte zur Verfügung.
09	Gibt es Verschwiegenheitserklärungen in Ihrem Unternehmen? Wenn ja: stellen Sie uns diese bitte zur Verfügung.
10	Ist sichergestellt, daß auch externe Mitarbeiter (z.B. Freiberufler, Werkstudenten) Verschwiegenheitserklärungen unterschreiben und damit auf das Datengeheimis verpflichet werden?
11	Existiert in Ihrem Unternehmen ein Konzept, wenn es zu Datenpannen kommt (beispielsweise zum Verlust, zur Vernichtung oder Veränderung personenbezogener Daten)?
12	Wird der Datenschutz (Datenschutzbeauftragter oder Datenschutzkoordinator) bei der Änderung oder Neu-Aufnahme von Datenverarbeitungstätigkeiten aktiv für deren Prüfung mit einbezogen?
13	Besteht hierzu (siehe Frage 12) innerhalb Ihres Hauses ein organisatorischer Prozess? Wenn ja: stellen Sie uns die entsprechende Dokumentation bitte zur Verfügung.
14	Führt Ihr Unternehmen ein Verzeichnis, in dem alle Verarbeitungstätigkeiten in Bezug auf personenbezogene Daten aufgeführt sind? Wenn ja: stellen Sie uns dieses bitte zur Verfügung.

Hermes

Validierung Self-Assessment

Validierung der Antworten durch WP in einem eintägigen Audit

Richtlinien

Prozesse

Stichproben

Dokumentation der TOM

Verarbeitungsübersicht

Meldeprozesse

Initialbelehrung

Schulungskonzept …….

Quelle: Pixabay

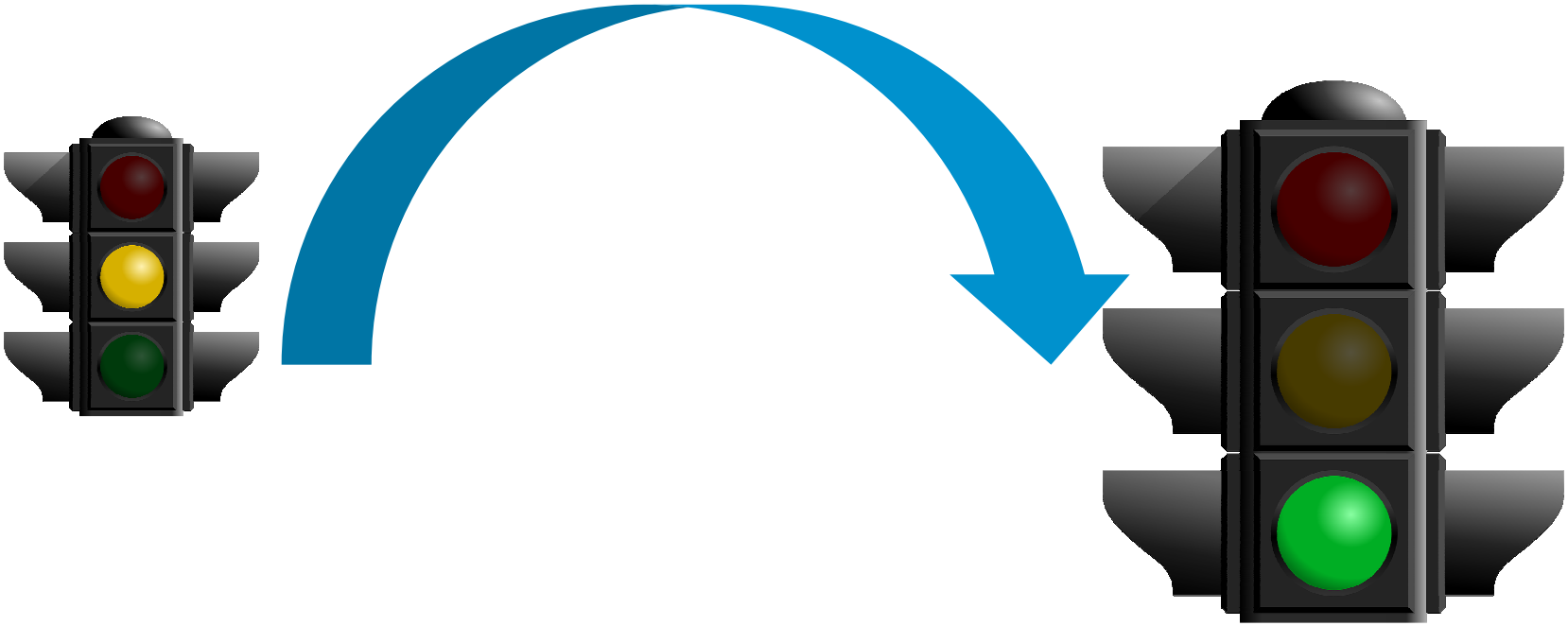
Berichterstattung zur DS-GVO Umsetzung (permanentes Reporting)

Auszug (Struktur)

Handlungsstrang	Status *(in Bearbeitung / Abgeschlossen)*	Für noch nicht abgeschlossene Handlungsstränge:		
		Datum der geplanten Finalisierung (tt/mm/jj)	**Maßnahmenverant-wortlicher/ Funktion**	**Kurze Erläuterungen zu den noch offenen Punkten sowie geplanten Maßnahmen**
1. Datenschutzbeauftragter und Datenschutzorganisation	abgeschlossen			Gem. Validierung des Self-Assessments durch PWC
2. Datenschutzmanagement-System (DSMS) und Governance	in Bearbeitung	XX.XX.XXXX	XXXXXXXXXXXXXXX	Überarbeitung Richtlinie Datenschutz und IT-Sicherheit Schulungen laufen permanent (erledigt) Mitarbeiterinformation zum Datenschutz (erledigt)
3. Incident-Management	in Bearbeitung	XX.XX.XXXX	XXXXXXXXXXXXXXX	Anpassung der Prozessbeschreibung –Intranet (T: XX.XX.2018) Sensibilisierung der FK zum Meldeprozess (T: XX.XX.2018) Klassifizierungs- und Meldeprozesse für Incidents anpassen für die verschiedenen Support-Dienstleister (UHD) Meldeprozesse für Sicherheitsvorfälle angepasst (erledigt) Trainingsmaßnahmen geplant (erledigt)
4. Verarbeitungsverzeichnis	in Bearbeitung	XX.XX.XXXX danach permanenter Prozess in Routinen mit FB-Verantwortlichen	XXXXXXXXXXXXXXX XXXXXXXXXXXXXXX und FB-Verantwortliche	Initiale Erfassung und initiale Prüfung durch DSB der Verfahren (erledigt) Identifikation FB-Verantwortliche Planung und erste Durchführung von Review-Terminen zur Qualitätssicherung Permanente Operationalisierung mit den Fachbereichen

Fazit

DSGVO - Readiness → DSGVO



Frank Helle
Datenschutzbeauftragter
Hermes Fulfilment GmbH
Bannwarthstr. 5
22179 Hamburg
Tel. +49 40 646041 -8635

Frank.Helle@hermes-europe.de
www.hermesworld.com/fulfilment