

Umsetzung von Datenschutz für Dokumente

GSE Enterprise Documents, Neuss, 21.9.2017

M. Ruland



Das Unternehmen



DATEV eG

Hauptsitz: Nürnberg

Gründung: 1966

Geschäftsjahr 2016

■ Umsatz: 928 Mio. Euro

■ Mitarbeiter: 7.005

■ Mitglieder: 40.501

■ Einzige berufsständische EDV-Dienstleistungsorganisation in Europa für

- Steuerberater
- Rechtsanwälte
- Wirtschaftsprüfer

Klassische Druck- und Versanddienstleistungen



Druck- und Versanddienstleistungen

Outsourcing

Tägliche Verarbeitung

z. B. Rechnungen, Mahnungen, Konto- und Depotauszüge

Monatliche Verarbeitungen

z. B. Lohnabrechnungen, Mahnungen, Back-Up-Services (Hot Standby)

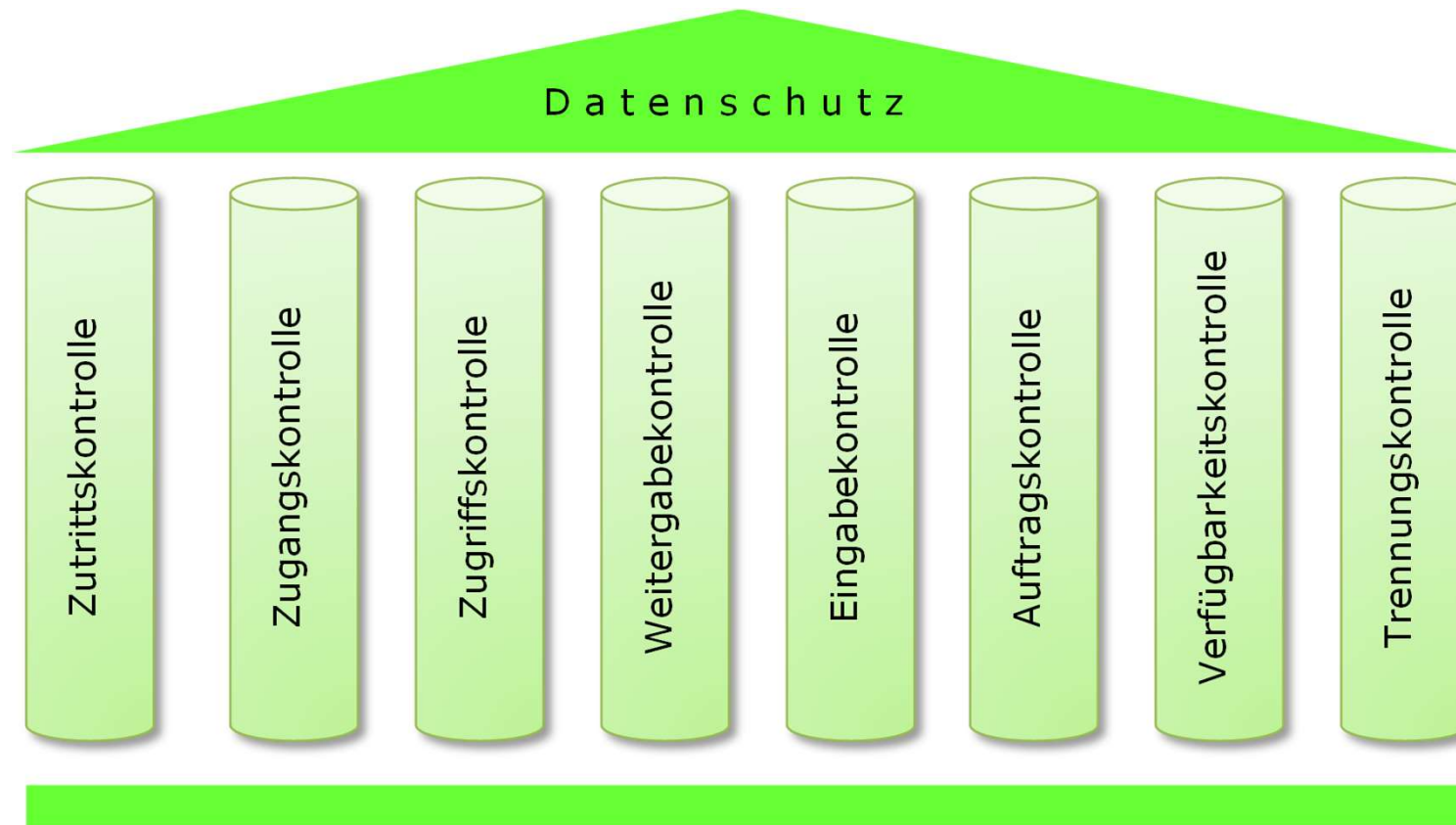
Einmalige Verarbeitungen

z. B. Jahreskonto- und Depotauszüge, Jahresbescheide

Basis Druckanwendung

z. B. Mailing-Aktionen, statische Dokumente (Offsetdruck)

Kontrollziele des Datenschutzes (Anlage zu § 9 Satz 1 BDSG)



Zutrittskontrolle

- Unbefugten ist der **Zutritt zu den Datenverarbeitungsanlagen**, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.
- **Technische und organisatorische Maßnahmen:**
 - Mehrere, unterschiedliche Sicherheitsbereiche
 - Einzelschleusen mit Lichtbildabgleich
 - „Rund um die Uhr“-Überwachung durch Mitarbeiter des Sicherheitsdienstes (zwei ständig besetzte Sicherheitszentralen)
 - Authentisierung mit personenbezogenen Mitarbeiterausweisen über elektronische Erfassungssysteme automatisiert und lückenlos
 - Geregelter Workflow zur Genehmigung, Verwaltung und Löschung von Zutrittsberechtigungen
 - Periodische Überprüfung und Bestätigung der Notwendigkeit von Zutrittsberechtigungen von Mitarbeitern durch Vorgesetzte
 - Grundsätzliche Begleitpflicht für Fremdleister und Verpflichtungserklärung auf das Datengeheimnis



Zugangskontrolle

- Es muss **verhindert** werden, dass Datenverarbeitungsanlagen von **unbefugten Dritten** genutzt werden können.
- **Technische und organisatorische Maßnahmen:**
 - Zugang nur über Zugangskontrollsystem (UserID und Passwort)
 - Absicherung des elektronischen Datenaustausches durch Prüfungen und technische Maßnahmen (VPN-Tunnel, Datenverschlüsselung via Automat bzw. SmartCard, Firewalls und Proxyserver)
 - Speziell ausgebildete und autorisierte Druckoperator an den Datenverarbeitungsanlagen
 - Projekt-Team (Kundenverantwortlicher Mitarbeiter, Kundenbetreuer in der Produktion und Entwickler) sorgen für korrekte Umsetzung der Anforderungen in der Verarbeitung



Zugriffskontrolle

- Es ist zu gewährleisten, dass **nur Berechtigte** ausgewählte Daten verarbeiten dürfen und eine **Manipulation** durch Unbefugte **ausgeschlossen** wird.
- **Technische und organisatorische Maßnahmen:**
 - Geregelter Workflow zur Genehmigung, Verwaltung und Löschung von Zugriffsberechtigungen
 - Alle aktiven Rechte eines Mitarbeiters werden in einer zentralen Rechtedatenbank bei IT-Sicherheit gespeichert
 - Periodische Überprüfung und Bestätigung der Notwendigkeit von Zugriffsberechtigungen von Mitarbeitern durch Vorgesetzte
 - Verschlüsselung der Daten bei der Datenübertragung
 - Grundsätzliches Fotografier- und Filmverbot
 - Penetrationstests für Anwendungen und Systeme vor Produktionsfreigabe
 - Verfilmung der Zugriffe auf die produktiven Druckdatensysteme



Weitergabekontrolle

- Es ist zu gewährleisten, dass **nur Berechtigte** personenbezogene Daten nachprüfbar **lesen, weitergeben und speichern** können.
- **Technische und organisatorische Maßnahmen:**
 - Umfassende Maßnahmen zur Absicherung beim elektronischen Datenaustausch (z. B. VPN-Technik)
 - Bereitstellung von Druckaufträgen, Zuordnung zu Druck- und Nachbereitungssystemen sowie Kontrolle des Materialflusses erfolgen über Drucksteuerungs-Software, deren Ablauf im Leitstand ständig überwacht wird
 - Vollständigkeit und Zusammengehörigkeit der Kundenaufträge werden über Barcodes bzw. Matrixcodes sichergestellt
 - Kommissionierung nach Vorgaben des Kunden
 - EDV-gestützte Ausgangsdokumentation
 - Eigene Abteilung für das Qualitätsmanagement (Prozessüberwachung/-optimierung)
 - Strenge Sicherheitsvorkehrungen gewährleisten, dass unbefugtes Entfernen von Datenträgern aus den Sicherheitsbereichen verhindert wird
 - Zentrale Entsorgung in einem eigens hierfür errichteten Wertstoffgebäude mit Schredder-Anlage; Entsorgungsgut mit schutzwürdigem Inhalt wird in verschlossenen Behältern transportiert



Eingabekontrolle

- Es ist zu gewährleisten, dass **Veränderungen an personenbezogenen Daten nachvollzogen** werden können.
- **Technische und organisatorische Maßnahmen:**
 - Laufende Protokollierung/Überwachung der Jobabläufe
 - Dateneingabe für Verarbeitung der Auftragsdaten ausschließlich nach vereinbartem Verfahren mit Auftraggeber
 - Verarbeitungsanstoß ausschließlich im vorgegebenen Weisungsrahmen des Auftraggebers gemäß festgelegtem Datenfahrplan
 - Ausführliches Protokollsystem beim Eingang der Daten und bei der maschinellen Verarbeitung und Überwachung durch Leitstand



Auftragskontrolle

- Es ist zu gewährleisten, dass **personenbezogene Daten** nur **entsprechend den Weisungen des Auftraggebers** verarbeitet werden können.
- **Technische und organisatorische Maßnahmen:**
 - Datenverarbeitung nur im Rahmen der Weisungen des Auftraggebers
 - Vollständig maschinelle Verarbeitungsprozesse
 - Automatische Jobnetze für Programmabläuffolgen
 - Keine Eingriffsmöglichkeit auf die Ablauffolge durch Konsoloperatoren
 - Keine Datenweitergabe oder auftragsbezogene Auskünfte an unbefugte Dritte
 - Leistungsprozesse werden im Rahmen von Service-Level-Agreements vertraglich festgelegt (z. B. Druckausführung, Nachbereitung, Mengen, Termine)
 - Zutritts-, Auskunfts- und Kontrollrecht für Auftraggeber zur Erfüllung der Überwachungspflicht beim Auftragnehmer
 - Vernichtung von „Fehlverhalten“ nach DIN 66399



Verfügbarkeitskontrolle

- Es ist zu gewährleisten, dass **personenbezogene Daten** gegen zufällige Zerstörung oder Verlust **geschützt** sind.
- **Technische und organisatorische Maßnahmen:**
 - Alle RZ-Komponenten, Drucksysteme und Nachbereitungsanlagen sind auf verschiedene Brandabschnitte (Brandabschnittskonzept) aufgeteilt
 - Datenanbindung der Produktionsstandorte ist redundant ausgelegt und erfolgt über räumlich getrennte Trassen
 - Backup-Lösungen für RZ-Komponenten, Drucksysteme und Nachbereitungsanlagen an anderen Standorten (IT-Notfallplan, Betriebsstättenkonzept)
 - 24/7 Stundenservice durch eigene Techniker bzw. Serviceverträge mit Herstellern der Produktionsanlagen für hohe Verfügbarkeit und Qualitätsniveau
 - Unterbrechungsfreie Stromversorgung an allen DATEV-Standorten
 - Automatische CO₂-Löschanlagen und Sprinkleranlage
 - Klimatisierung durch Kältezentralen



Trennungskontrolle

- Es ist zu gewährleisten, dass zu **unterschiedlichen Zwecken** erhobene Daten **getrennt verarbeitet** werden können.
- **Technische und organisatorische Maßnahmen:**
 - Prinzip der Funktionstrennung (Produktion/Test)
 - Funktionelle, organisatorische und räumliche Trennung in der Datenverarbeitung
 - Schutzwürdige Daten werden Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die Aufgabenerfüllung erforderlich ist
 - Datenaustausch zwischen Test- zu Produktionssystemen erfolgt durch entsprechende Werkzeuge und ist nachvollziehbar dokumentiert (Entwicklungs- und Produktionssysteme sind strikt getrennt)



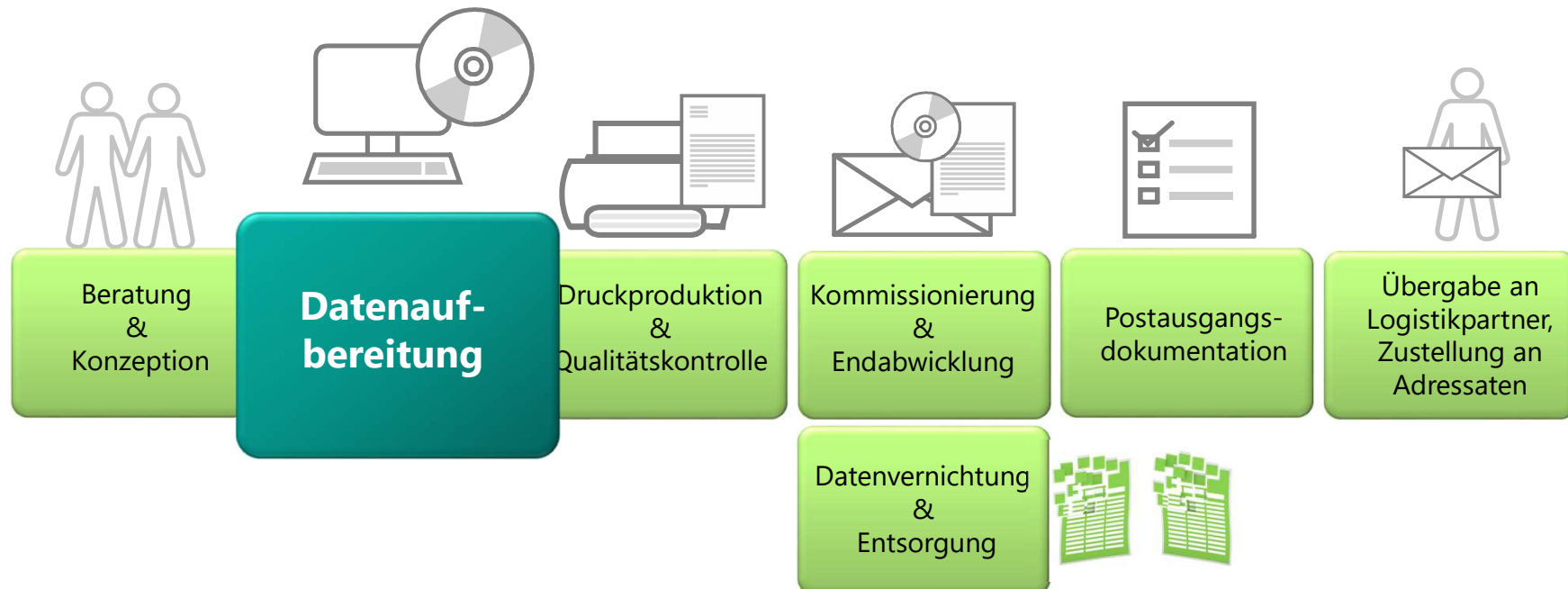
Konzeption

- Prinzip der Funktionstrennung (Produktion/Test)
- Trennung der Kunden untereinander
- Absicherung des elektronischen Datenaustausches durch Prüfungen und technische Maßnahmen (VPN-Tunnel, Datenverschlüsselung via Automat bzw. SmartCard, Firewalls und Proxyserver)



Datenbereitstellung, -überprüfung und -aufbereitung

- Verarbeitungsanstoß ausschließlich im vorgegebenen Weisungsrahmen des Auftraggebers gemäß festgelegtem Datenfahrplan
- Vollständig maschinelle Verarbeitungsprozesse
- Geregelter Workflow zur Genehmigung, Verwaltung und Löschung von Zugriffsberechtigungen
- Periodische Überprüfung und Bestätigung der Notwendigkeit von Zugriffsberechtigungen von Mitarbeitern durch Vorgesetzte



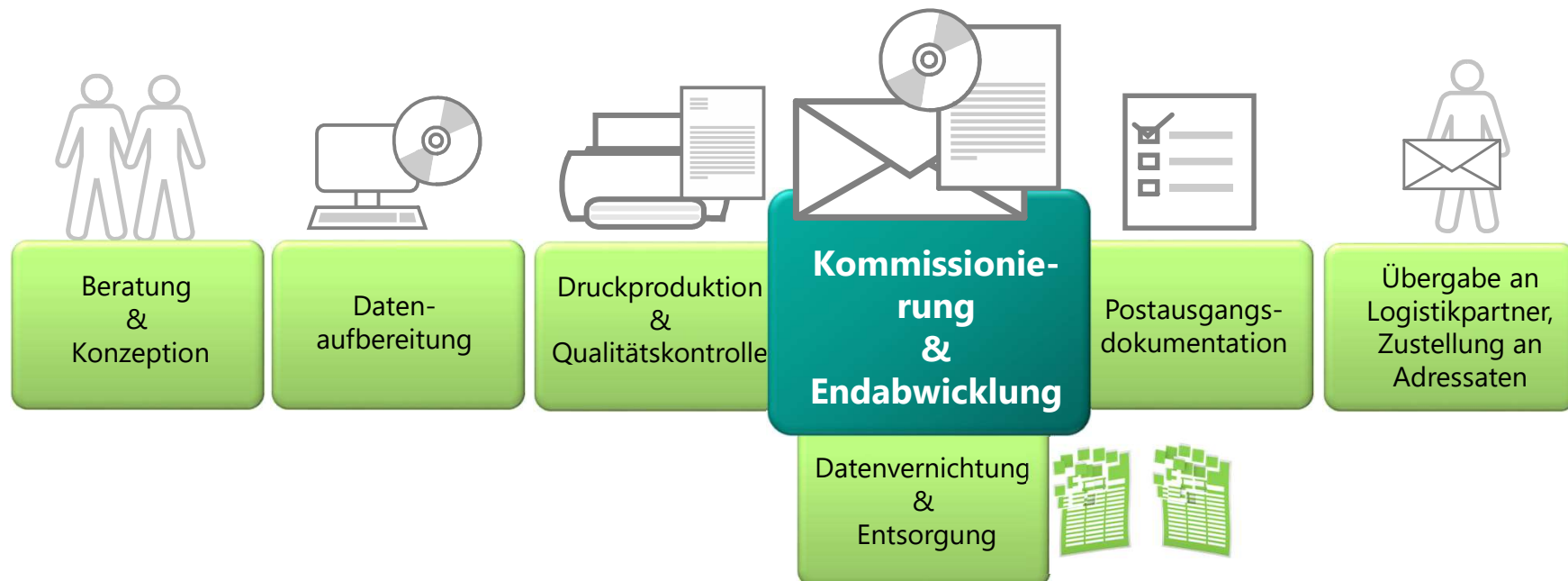
Druckproduktion und Qualitätskontrolle

- Verfilmung der Zugriffe auf die produktiven Druckdatensysteme
- Bereitstellung von Druckaufträgen, Zuordnung zu Druck- und Nachbereitungssystemen sowie Kontrolle des Materialflusses erfolgen über Drucksteuerungs-Software, deren Ablauf im Leitstand ständig überwacht wird
- Speziell ausgebildete und autorisierte Druckoperator an den Datenverarbeitungsanlagen
- Vollständig maschinelle Verarbeitungsprozesse
- Automatische Jobnetze für Programmabläufen



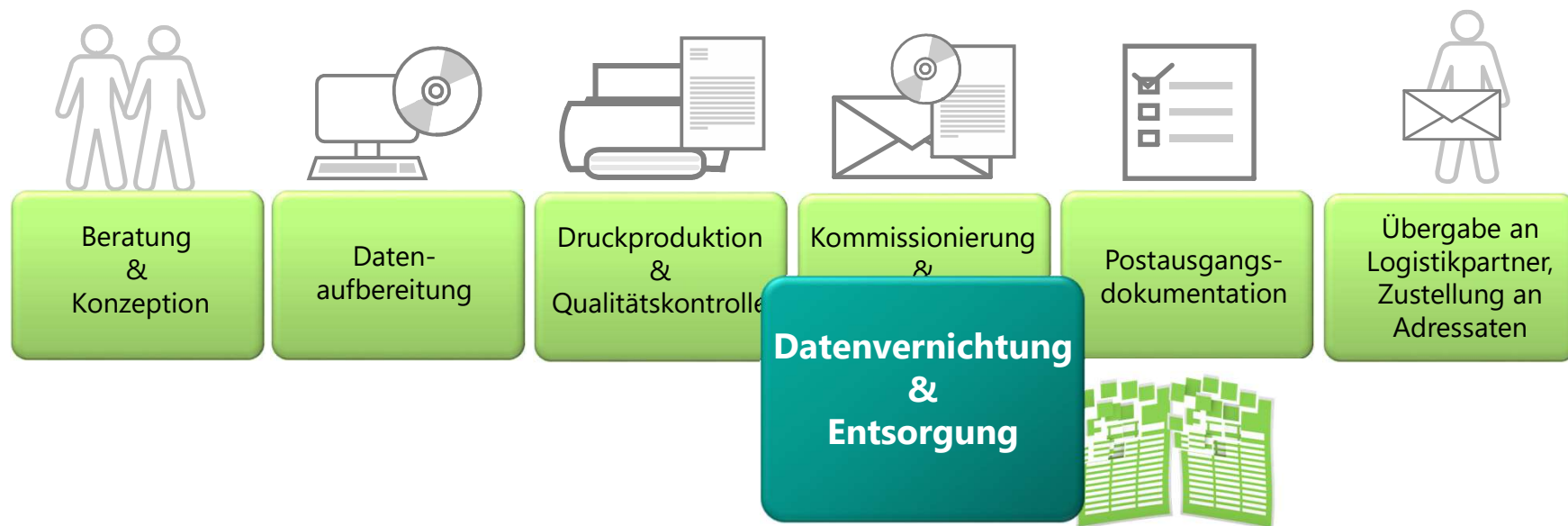
Kommissionierung und Endabwicklung

- Vollständigkeit und Zusammengehörigkeit der Kundenaufträge werden über Barcodes bzw. Matrixcodes sichergestellt
- Kommissionierung nach Vorgaben des Kunden



Datenvernichtung & Entsorgung

- Entsorgung nach DIN 66399 Schutzklasse 3 und Sicherheitsstufe 4
 - Schutzklasse 3: Sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten
 - Sicherheitsstufe 4: Reproduktion der auf ihnen wiedergegebenen Daten nur unter außergewöhnlich hohem Aufwand möglich
- Interne und externe Audits zur Einhaltung der DIN 66399
- Entsorgungsgut mit schutzwürdigem Inhalt wird in verschlossenen Behältern transportiert















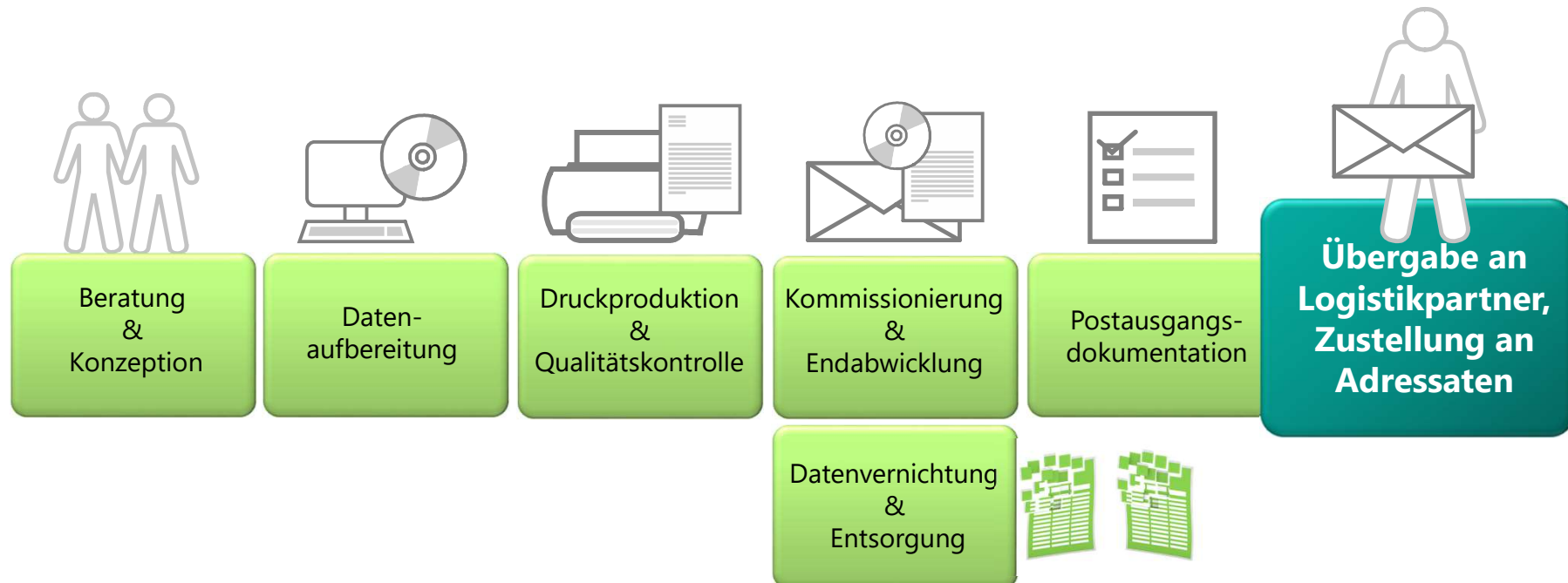
Postausgangsdokumentation

- EDV-gestützte Ausgangsdokumentation
- Eigene Abteilung für das Qualitätsmanagement (Prozessüberwachung/-optimierung)



Versandmanagement

- Mehrere, unterschiedliche Sicherheitsbereiche
- Einzelschleusen mit Lichtbildabgleich
- „Rund um die Uhr“-Überwachung durch Mitarbeiter des Sicherheitsdienstes (zwei ständig besetzte Sicherheitszentralen)



Zertifikatsübersicht



DAS **SERVICE-MANAGEMENT** WURDE
NACH **ISO 20000**
UND DAS
QUALITÄTSMANAGEMENT
NACH **ISO 9001**
ZERTIFIZIERT

DAS **DATEV-
INFORMATIONSSICHERHEITS-
MANAGEMENTSYSTEM**
WURDE NACH
ISO 27001
ZERTIFIZIERT

DAS **DATENSCHUTZ-
MANAGEMENT** BEI
DATEV WURDE NACH
§9A BDSG
ZERTIFIZIERT

DIE DIENSTLEISTUNG
„**LODAS / LOHN UND
GEHALT**“ WURDE
NACH
ISAE 3402
ZERTIFIZIERT

DIE **VERNICHTUNG**
VON
DATENTRÄGERN BEI
DATEV WURDE NACH
**DIN SPEC
66399**
ZERTIFIZIERT

In 2017:

TESTAT NACH
IDW PS 951
„**NACHWEIS ÜBER DIE
ERFÜLLUNG
DER MA-RISK (AT 9)
ANFORDERUNGEN**“

Bleiben Sie auf der sicheren Seite!

- ISO 27001
 - Nachweis für einen IT-Verbund, dass Standardsicherheitsmaßnahmen nach ISO 27001 umgesetzt wurden
- DQS Datenschutzzertifikat
 - Zertifizierung von Managementsystemen für die Umsetzung strenger Datenschutzvorgaben
- Service- und Qualitätsmanagement
 - Zertifizierungen nach ISO 20000-1 und ISO 9001 im Druck-, Logistik- und Servicezentrum
- SAS 70 Type II / ISAE 3402
 - Internationaler Prüfungsstandard, der die Wirksamkeit des internen Kontrollsystems (IKS) von Dienstleistungsorganisationen beurteilt
- DIN SPEC 66399
 - Vorgabe für Prozesse der Datenträgervernichtung von Maschinen und Einrichtungen, damit eine Reproduktion von schutzbedürftige Informationen nicht möglich ist
- Zertifikate nach ETSI TS 102 042 und der Policy "NCP+„
 - Nachweis für die Bereitstellung von fortgeschrittenen Signatur-zertifikaten und Verschlüsselungszertifikaten
- Testat nach IDW PS 951
 - Nachweis über die Erfüllung der MA-Risk (AT9) Anforderungen



Zukunft gestalten. Gemeinsam.