Drescher.
Druck und Dienstleistung

Datenschutz – und Datensicherheitsbestimmungen (nach § 9 BDSG und § 78a SGB X)

Allgemeine Informationen zum Unternehmen

Gesellschaftsform und Eigentümerstruktur Ihres Unternehmens.

Unter der Eppe-Drescher Beteiligungsverwaltung GmbH - Eigentümer Roland Eppe - strukturiert sich die Drescher-Gruppe wie folgt:

Drescher Full-Service-Versand GmbH (100%)

Geschäftsführung	Roland Eppe, Klaus Vollmer
Produktionsleitung	Felix Römer
Kaufmännische Leitung	Hans Miller
Datenschutzbeauftragter	Marcus Pegoski

Unternehmenskennzahlen

Umsätze	2014	2015	2016
Umsatz Full-Service Versand GmbH	29,9 Mio. €	30,0 Mio. €	30,10 Mio. €
Anzahl Mitarbeiter	175	175	173

Produktionsstätten/Geschäftsstellen

Produktionsstätten :	Geschäftsstellen:
77656 Offenburg	82205 Gilching (München)
	71229 Leonberg
Nachod (CZ)	
Gorzow (PL)	

Druckproduktspektrum mit dem jeweiligen Anteil am Gesamtdruckvolumen

- Endlosdruck und Druckveredelung, Offsetdruck 20 %
- Direktmarketing-Fullservice, Fullfillment 35 %
- Dokumenten-Management 35 %
- Etiketten 10 %

Maßnahmen zur Qualitätssicherung (z.B. Zertifizierungen etc.).

- Zertifizierung nach ISO 9001 : 2015
  Zertifikat gültig bis 11.01.2020
- Zertifizierung nach ISO 14001:2015
  Zertifikat gültig bis 04.01.2021
- Zertifizierung nach ISO/IEC 27001:2013
  Zertifikat gültig bis 25.10.2020

- Zertifizierung nach FSC-Produktkettennachweis
  Zertifikat gültig bis 10.06.2019
- Qualitätsbeauftragter: Jörg Trenz
- Datenschutz:
  Alle Mitarbeiterinnen und Mitarbeiter von Drescher wurden über die Bestimmungen des Bundesdatenschutzes (§ 5 BDSG) belehrt und verpflichten sich
  in einer schriftlich abverlangten Datenschutzerklärung, sich an diese zu halten.

Referenzen	
• Commerz Finanz GmbH	Kontoauszugsversand monatlich
• Allianz Deutschland AG	Kunden- und Vertreterkommunikation
• LBBW Berlin Invest GmbH	Kontoauszugsversand laufend
• ZVK Kommunaler Versorgungsverband BW	Versicherungsnachweise
• Airbus, Hamburg	Verdienstabrechnungen, Portallösung
• Bausparkasse Schwäbisch Hall	Anträge, Mailing Back-up Partner etc.
• Hallesche Krankenversicherung	Anträge etc.
• AOK Baden-Württemberg, Bayern, Nordost	Mitgliederkommunikation
• Union Investment	PrePress
• Dekra Prüfgesellschaft	Prüfberichte
• Burda Direct	Kundenkommunikation, Etiketten
• Fidelity International	Print + Mail-Kommunikation
• Wüstenrot & Württembergische AG	Kundenkommunikation
• DG-Verlag	Kundenkommunikation
• Deutscher Sparkassenverlag	Kundenkommunikation
• BMW AG,	Print + Mail-Kommunikation
• Esprit Europe GmbH	Full-Service Mailings
• Gardena GmbH	Katalogproduktion + Versand
• Webasto Gruppe	Web-to-Print international
• Uni Credit Bank AG	Kundenkommunikation, Mailings
• KKH Hannover	Sozialwahlunterlagen
• Ärzte ohne Grenzen	Fundraising – Mailings
• Kaufland AG	Lohn- und Gehaltsabrechnungsversand
• Metro / Real AG	Lohn- und Gehaltsabrechnungsversand
• Ärztekammer Berlin	Dokumentenversand
• Santander Consumer Bank	Dokumentenversand
• Schüco Fenster AG	Rechnungsoutsourcing

u.v.m.

Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit bei der Drescher Full-Service Versand GmbH um das erforderliche Schutzniveau für die Verarbeitung und Nutzung von Daten zu gewährleisten

Nach § 11 Abs. 2 S. 2 BDSG und § 80 SGB X sind die technischen und organisatorischen Datenschutzmaßnahmenschriftlich festzulegen.

Folgende technische und organisatorische Maßnahmen (Anlage zu § 9 BDSG) werden zwischen dem AUFTRAGGEBER und dem AUFTRAGNEHMER verbindlich festgelegt. § 11 Abs. 4 BDSG bleibt unberührt.

1) Zutrittskontrolle

Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren:

- Protokollierung der Zu- und Abgänge von Mitarbeitern über Elektronische Zutrittskontrolle (Transponder mit Protokollierung), Elektronische Erfassung und Abspeicherung der Zutrittszeiten, Datenaufbewahrung 3 Monate.

- Protokollierung der Zu- und Abgänge von unternehmensfremden Personen. Schriftliche Erfassung der Zutrittszeit über Betriebszutrittsprotokoll

- Zentraler Empfangsbereich vorhanden, besetzt von 8-17 Uhr, geführt durch Assistenz der Geschäftsführung. Nur in diesem Zeitraum ist der Betriebszutritt für Besucher möglich.

- Ausgabe von Besucherausweisen

- Aufenthalt von Fremden im gesamten Unternehmensgebäuden nur in Anwesenheit von Mitarbeitern

- Festlegung der zutrittsberechtigten Personen zu Gebäude / Rechenzentrum / Serverraum mit definierter Schlüsselregelung. Festlegung erfolgt durch Geschäftsführung. Autorisiert sind Systemadministratoren.

- Rechenzentrum / Serverräume neben Transponderterminal durch Sicherheitsschloss abgesichert

- Abschließen des Gebäudes nach Arbeitsschluss durch verantwortlichen Schichtführer, sowie anschließende Gebäudesicherung durch Alarmanlage. Auslösung des Alarms wird an die Polizei und die Werksleitung gemeldet.

- Videoüberwachung im Eingangsbereich, Zugriff durch Assistenz der Geschäftsführung, keine Datenspeicherung. Dient zur Identifizierung der Personen, welche Zutritt zum Gebäude erlangen möchten.

- Im Hause Drescher existieren drei Sicherheitsbereiche: Der Sicherheitsbereich 1 ist für alle Mitarbeiter mit gültigem Transponder zugänglich. Im Sicherheitsbereich 2 werden sensible Daten verarbeitet (Laserbereich, Intelligente Kuvertierung), dieser Bereich ist nur mit den Transpondern der Mitarbeiter zugänglich, welche in diesem Bereich arbeiten oder diesen Bereich kontrollieren. Im Sicherheitsbereich 3 (EDV) stehen die IT-Anlagen.
- Zu diesem Bereich haben nur Mitarbeiter der IT und die Projektleitung Zutritt. Der Serverraum ist zusätzlich verschlossen.

- Fachgerechte und alarmgesicherte Notausgänge, welche nur von Innen zu öffnen sind.

- Notebooks werden ausschließlich in abgeschlossenen Räumen vorgehalten.

- Es existiert ein Safe zur Aufbewahrung von Liquiden Mitteln und Datenträgern mit personenbezogenen Daten, zu welchen lediglich die Assistenz der Geschäftsführung Zugriff hat. (2 Personen)

2) Zugangskontrolle

Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können insbesondere durch den Einsatz von dem Stand der Technik entsprechenden Verschlüsselungsverfahren:

- FTP over SSL, Secure FTP (SSH) und unverschlüsseltes FTP, PGP und VPN.

- Vereinbarter Standard: TLS 1.2 mit 256-Bit-AES und RSA Verschlüsselung

- Identifikation und Authentifikation gegenüber dem Datenverarbeitungssystem (Kennwort/Passwort)
- Richtlinien zum sicheren und ordnungsgemäßen Umgang mit Passwörtern: Persönlich, keine Weitergabe, mind. 8 Stellen, Kombination aus allen Kategorien Ziffern, Großbuchstaben, Kleinbuchstaben und Sonderzeichen, Zugangssperre nach vier Fehlversuchen. Automatische Freischaltung der Zugangssperre nach 60 Minuten. Im Krankheitsfall/Abwesenheit des Berichtigungsinhabers, Freischaltung der notwendigen Daten durch Administrator.

- Passwörter können alle 24 Stunden durch den Benutzer selbst, oder durch systemseitige Aufforderung (kurz vor Ablauf der 90-tägigen Gültigkeitsdauer) geändert werden.
- Passworthistorie: Der Nutzer darf ein Passwort frühestens nach Ablauf von 24 Zyklen erneut vergeben.

- Sicherung der Bildschirmarbeitsplätze nach Abwesenheit (durch Anweisung und automatisiert)

- Softwareschutz gegen Verletzung der Systemintegrität (Software: Snapshoot)

- Regelmäßige Softwareaktualisierungen (z.B. bei Virenscanner, Firewall und eingesetzte Betriebssoftware). Virenscanner: stündliche Prüfung nach Updates für eingesetzte Software. Monatliche Prüfung, ob automatische Funktionen in gewünschter Form arbeiten.

2.1) Maßnahmen zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die Ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können

- Eindeutige Zugangskennungen, keine Sammelkonten (z.B Azubi).

- Festlegung eines Benutzerprofils mit Vergabe von Schreib- und Leserechten (differenziert)

- Erstellung eines Berechtigungskonzeptes mit Administrationsrechten und Verwaltung sowie Kontrolle der Zugriffe durch Systemadministrator

- Vergabe von Administratorrechten für Serversysteme besitzen 2 Administratoren. Diese Personen besitzen uneingeschränkte Rechte über Serversysteme und werden durch EDV-Leitung im Bedarfsfall kontrolliert.

- Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern

- Monatliche Kontrolle der Gültigkeit der Berechtigungen und bei Bedarf (z.B. Ausscheiden eines Mitarbeiters)

3) Zugriffskontrolle

Maßnahmen die verhindern, dass Sozialdaten bei der Verarbeitung, Nutzung sowie nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, insbesondere durch den Einsatz von dem Stand der Technik entsprechenden Verschlüsselungsverfahren

- FTP over SSL, Secure FTP (SSH) und unverschlüsseltes FTP, PGP und VPN.

- Vereinbarter Standard: TLS 1.2 mit 256-Bit-AES und RSA Verschlüsselung

- Festplattenschlösser an den Arbeitsstationen

- BIOS-Passwort zum Schutz vor unbefugtem Zugriff

- Zugriff auf interne System von externen Standorten über VPN-Verbindung ohne Datentransferoption

- Verschlüsselung der Kundendatenbanken (Access). Kunde bestimmt, ob dessen Kundendaten verschlüsselt übertragen und in welcher Weise diese im System abgelegt werden.

- Abschottung interner Netze gegen Zugriffe von außen (Firewall: Typ watchguard) – Aktualisierungshäufigkeit: kontinuierliche Sicherheitsupdates, Betriebssystem / Firmware nach Aufforderung des Wartungsunternehmens

- Organisation der Datenträgerverwaltung, Absicherung der Bereiche, in denen Datenträger verarbeitet und aufbewahrt werden. Dies erfolgt lediglich in der EDV. Die Datenträger werden nach Verwendung an den Kunden zurückgegeben. Zwischenzeitlich erfolgt die Aufbewahrung in abgeschlossenen Sicherheitsschränken oder im Safe. Vorgehensweise in Arbeitsanweisung definiert.

- Schriftliche Regelung zum Kopieren von Daten (lediglich eine Sicherheitskopie erlaubt) Sicherheitskopie wird bei Dateneingang über Datenträger im Netzwerk abgelegt oder bei elektr. Dateneingang ist die Datenursprungsquelle Speicherort der Sicherheitskopie. Schriftlich formuliert über auftragsbezogenen Betriebsauftrag an die EDV.

- Deaktivierung bzw. Sicherstellung von USB-Anschlüssen durch Beschränkung auf Leserechte entnehmbarer Medien (Wechselmedien); sämtliche Schnittstellen sind deaktiviert, lediglich in der EDV gibt es die Möglichkeit, Wechseldatenträger anzuschließen bzw. einzulegen; auch dort aber nur Leserecht.

- Schriftliche Regelung zur E-Mail- und Internet-Nutzung Mitarbeitern ist die Private Nutzung des Internets während der Arbeitszeit verboten. Internetzugang nur bei betrieblicher Notwendigkeit freigeschalten. Ausdrückliches Verbot unbefugten Datentransfers. Zugangsverbot zu pornografischen oder gesetzlich bedenklichen Seiten

- Hinweis, dass bei Verdacht auf Verstößen der Internetzugang kontrolliert wird.

- Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Abteilungsleitung / Geschäftsleitung)

- Meldung über Datenverlust schriftlich an Administrator, Prüfung des tatsächlichen Datenverlusts und Wiederherstellung durch Administrator nach Anweisung der betreffenden Abteilungsleitung bzw. GF

4) Weitergabekontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, insbesondere durch den Einsatz von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

- FTP over SSL, Secure FTP (SSH) und unverschlüsseltes FTP, PGP und VPN.

- Standard: TLS 1.2 mit 256-Bit-AES und RSA Verschlüsselung

- Transport von Datenträger mit personenbezogenen Daten nur via hauseigenen Kurier Dokumentation auf Lieferschein. Daten sind vor unbefugtem Zugriff geschützt (Verschlüsselung)

- Generelle Verschlüsselung von personenbezogenen Daten des Auftraggebers bei der Weitergabe

- Verschlüsselung bezüglich gesichertem E-Mail-Versand auf Wunsch möglich

- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger über zertifiziertes Entsorgungsunternehmen im Standardprozess

- Vertragliche Regelungen zur Fernwartung mit Vertraulichkeitsvereinbarung, u.a. mit eingeschränkten Berechtigungen, Protokollierung der Datenübermittlung und nur unter Aufsicht eines internen Administrators.

- Datenschutzgerechte Vernichtung von Datenträgern und Fehldrucken mit eindeutigen Arbeitsanweisungen

- Ausgabe von Datenträger mit personenbezogenen Daten nur an autorisierte Personen dieser Abteilung EDV, bzw. hauseigenem Kurier

- Einlagerung von Back-up-Bändern inhouse

- Mit Subunternehmern, welche vom Auftraggeber autorisierten Zugriff zu personenbezogenem Datenmaterial des Auftraggebers erhalten, werden nach § 11 BDSG Datenschutzvereinbarungen geschlossen. Es werden hierbei dieselben Anforderungen an den Subunternehmer gestellt, welche auch für den Auftragnehmer gelten. Durch die Durchführung einer Fernwartung ist es nur in seltenen Fällen nötig, dass der Subunternehmer Zugriff zu Datenmaterial erhält.

4.1) sicher zu stellen, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Personenbezogenen Daten / Sozialdaten durch Einrichtung der Datenübertragung vorgesehen ist

- Auftragnehmer stellt verschlüsselten FTP-Server zur Datenübertragung zur Verfügung, zu welchem

ein Log-IN (Benutzer / Passwort) erforderlich ist.

- Datenübernahme auf FTP-Server automatisiert möglich.

- Datenübertragung in Log-file protokolliert

5) Eingabekontrolle

Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des Auftraggebers lt. Datenschutzvereinbarung und Leistungsbeschreibung.

- Führung nachvollziehbarer Zugriffsberechtigungen, um Transparenz zu gewinnen, wer Dateneingaben bzw. -veränderungen vorgenommen hat.

- Dateneingabe in Bezug auf personenbezogene Daten erfolgt nur auf schriftliche Anweisung durch den Adresseigner. Eine Dateneingabe oder Datenveränderung erfolgt nur, wenn dies der Auftraggeber ausdrücklich und schriftlich anweist. Sollte dies der Fall sein, so wird protokolliert welche Person die Dateneingabe/Veränderung in welcher Form durchgeführt hat.

- Programmtechnische Registrierung der Benutzer und Uhrzeit der Dateneingabe

6) Auftragskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers sind im Auftrag und der evtl. Datenschutzvereinbarung definiert
- Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags
- Vorhandensein eines betrieblichen Datenschutzbeauftragten, welcher für die Datenschutzorganisation und für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse sorgt
- Auf Kundenwunsch kann im Vertrag eine verantwortliche Person beim Auftraggeber benannt werden, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber dem Dienstleister weisungsbefugt ist.
- Kontrolle der Einhaltung von Datensicherheitsbestimmungen, federführend durch den Datenschutzbeauftragten
- Meldung, auch bei Verdacht auf Verstößen, bezüglich der Datensicherheit der Daten des Auftraggebers

- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis und dessen Auffrischung über jährliche Schulungsmaßnahmen
- Trennung von Test- und Produktionsbetrieb

7) Verfügbarkeitskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backup- und Recovery-Konzept, enthält u.a.:

Recovery: - Softwareschutz gegen Verletzung der Systemintegrität (Software: Snapshoot)

- Regelmäßige Softwareaktualisierungen (siehe oben)

Backup: Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Abteilungsleitung / Geschäftsleitung)

- Meldung über Datenverlust schriftlich an Administrator

- Prüfung des tatsächlichen Datenverlusts

- Wiederherstellung durch Administrator nach Anweisung der betreffenden Abteilungsleitung bzw. GF

- Sichere und ordnungsgemäße Archivierung von Datenbeständen, auch für externe Unternehmen

Intern: Keine Datentrennung, Inhousedurchführung, tägliche Sicherung auf Band

Extern: Inhouseerstellung von Archiv-PDFs, Trennung von anderen Daten

- Unterbrechungsfreie Stromversorgung durch USV

- Notfallkonzepts bei akuter Gefahr eines Datenverlusts, z.B. durch Systemabsturz, Feuer, höhere Gewalt. Inhalt: Trennung des Betriebs in versch. Brandabschnitte, unverzügliche Abhilfe durch externes Systemhaus.

- Automatische Feuer- und Rauchmeldeanlagen mit Meldung an die zuständige Feuerwehr

- CO^2-Feuerlöschgeräte auf gesamten Betriebsgelände mit Wartung nach den gesetzlichen Vorschriften

- Überwachung von Betriebsparametern des Rechenzentrums (z.B. CPU, verfügbarer Speicher, Raumtemperatur des Rechenzentrums). Bei Abweichung vom Normwert werden die verantwortlichen Stellen (eigene EDV, externes Systemhaus) informiert und vorbeugende Maßnahmen eingeleitet.

- es existieren Raid-Systeme, externe Storagesysteme (SAN)

8) Trennungsgebot

Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Die Daten des Auftraggebers und anderer Mandanten werden von unterschiedlichen Mitarbeitern des Dienstleisters verarbeitet

- Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Mandanten Rechnung trägt

- Umsetzung und Dokumentation einer Funktionstrennung (z.B. Vier-Augen-Prinzip und Projektleiterorganisation) . Überwachung durch Qualitätsmanagementbeauftragten und jeweiligen Bereichsleiter.

- Kundendaten werden voneinander getrennt durch Ablage in unterschiedlichen Verzeichnissen mit unterschiedlichen Berechtigungen und getrennten Filesysteme

Stand (Datum) 01.11.2017

Drescher Full-Service Versand GmbH