Technische und organisatorische Maßnahmen (TOMs) (Art. 5 Abs. 1 lit. f, 24, 25, 28 und 32 DSGVO)

Druckwerkstatt Handels GmbH, Hosnedlgasse 16b, 1220 Wien
Tel.: +43-1-285 88 09, E-Mail: info@druckwerkstatt.at, www.druckwerkstatt.at

Gründungsjahr (GmbH): 2005
Geschäftsführer: Robert Bincik
UID Nummer: ATU61398357
Firmensitz: Wien, Firmenbuchnummer: 257392v
Firmengericht: Handelsgericht Wien; Behörde gem. ECG: MBA XXI. Wien
Weitere Aufsichtsbehörde: Gewerbebehörde der Drucker- und Druckformenhersteller
Mitglied der WKO Wien: Fachgruppe Druck & LG Handelsagenten

Datenschutz-Kontakt
E-Mail: datenschutz@druckwerkstatt.at
Telefon: +43 1 285 88 09

Ein formell bestellter Datenschutzbeauftragter ist derzeit nicht benannt (nicht verpflichtend). Die datenschutzrechtliche Verantwortung obliegt der Geschäftsführung.

Fassung vom 05.03.2026

1. Allgemeines, Geltungsbereich, Ziele

Diese technischen und organisatorischen Maßnahmen (TOMs) gelten für alle Verarbeitungstätigkeiten der Druckwerkstatt Handels GmbH, insbesondere für:

- Kunden- und Interessentenverwaltung, Lieferantenverwaltung, Finanzbuchhaltung, Personalverwaltung, Bewerbermanagement,
- Webshop, Produktions- und Druckdaten (inkl. Lettershop/Adressverarbeitung), IT-/Cloud-/FTP-Systeme, E-Mail-Kommunikation, Uploadportale, Videoüberwachung.

Ziel ist die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 DSGVO) sowie die Erfüllung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO.

2. Organisation & Verantwortlichkeiten

- **Verantwortlicher & Datenschutzkoordination:** Geschäftsführung der Druckwerkstatt Handels GmbH (kein formeller Datenschutzbeauftragter erforderlich).
- **Vertraulichkeitsverpflichtung:** Alle Mitarbeitenden haben eine Verschwiegenheits-/Datenschutzklausel im Dienstvertrag oder separat unterschrieben.

Rollen und Zuständigkeiten:

- **Geschäftsführung:** Gesamtverantwortung, Freigabe von Richtlinien, Entscheidungen über DSFA.
- **IT:** Betrieb der Systeme, technische Sicherheit, Benutzerverwaltung.
- **HR:** Personalakten, Bewerberdaten, Umsetzung von HR-bezogenen Lösch- und Aufbewahrungsfristen.
- **Vertrieb/Projektmanagement:** Kunden- und Druckdaten im Rahmen von Angeboten, Aufträgen und Reklamationen.
- **Produktion/Vorstufe:** Bearbeitung von Druck- und Adressdaten (Auftragsverarbeitung).

Prozesse:

- Dokumentierter Prozess für Betroffenenrechte (Auskunft, Berichtigung, Löschung etc.) inkl. Fristenkontrolle und Dokumentation.
- Dokumentierter Prozess für Meldung und Behandlung von Datenschutzpannen (interner Meldeweg, Bewertung, ggf. Meldung an Behörde/Betroffene).
- Regelmäßige Überprüfung und Aktualisierung von Verarbeitungsverzeichnis, DSFAs und TOMs (mindestens alle 2–3 Jahre oder anlassbezogen, z. B. bei größeren Systemänderungen).

3. Schulung & Awareness

- Onboarding-Schulung für neue Mitarbeitende zu Grundzügen der DSGVO, Umgang mit Kundendaten, internen Zuständigkeiten und Meldewegen.
- Regelmäßige Auffrischungsschulungen zu Phishing, Passwortsicherheit, Umgang mit sensiblen Daten, Erkennen von Verdachtsfällen.
- Spezielle Schulungen für IT (System-/Netzwerksicherheit, Updates) sowie Vorstufe/Lettershop (Adressverarbeitung, Löschfristen, Auftragsverarbeitung).

4. Physische Sicherheit (Zutrittskontrolle)

- Gebäudezugang zu Büro- und Produktionsflächen nur für Mitarbeitende und autorisierte Personen (Schließsystem, Schlüsselverwaltung).
- Besucher in der Produktion werden begleitet durch den Betrieb geführt
- Server- und Technikräume sind separat gesichert; Zutritt nur für IT und Geschäftsführung.
- Papierakten mit besonders schützenswerten Daten (insbesondere Personalakten, Finanzunterlagen) werden in abschließbaren Schränken aufbewahrt.
- Videoüberwachung ausgewählter Bereiche zur Sicherung von Personen und Sachwerten; klare Kennzeichnung durch Hinweisschilder, keine Überwachung von Sanitär- oder Sozialbereichen.

5. Zugangskontrolle (Authentifizierung)

- Personalisierte Benutzerkonten für alle relevanten Systeme (Windows-Login, Microsoft 365, Paginanet, Webshop-Backend etc.).
- Keine geteilten Standard-Accounts, wo vermeidbar; separate Admin-Konten ausschließlich für Administrationszwecke.
- Passwort-Richtlinien: Mindestlänge für Clients 12 Zeichen, Stand März 26), Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen; regelmäßiger Wechsel (alle 180 Tage) und bei Verdacht auf Kompromittierung.
- Fernzugriffe ausschließlich über gesicherte VPN- und RDP-Verbindungen; Konfiguration und Zugangsdaten werden verschlüsselt gespeichert und durch ein Masterpasswort-Konzept zusätzlich geschützt.
- Einsatz von Mehrfaktor-Authentifizierung (MFA) für besonders kritische Zugänge (z. B. M365-Admin, Remote-Zugänge, ggf. Backup-Konsole)

6. Zugriffskontrolle (Berechtigungen, Need-to-know)

Die Vergabe von Berechtigungen erfolgt nach dem Need-to-know-Prinzip:

- Rollenbasierte Berechtigungskonzepte in Paginanet, Finanzbuchhaltung, HR-Systemen und Dateiservern.
- Trennung von Kunden-, Lieferanten-, Bewerber- und Mitarbeiterdaten durch eigene Bereiche/Ordner und Systemmodule.
- HR- und Bewerberdaten: Zugriff ausschließlich für HR, Geschäftsführung und unmittelbar in Auswahlprozesse eingebundene Personen.
- Regelmäßige Überprüfung und Bereinigung von Berechtigungen (z. B. bei Funktionswechseln, Austritten).

7. Weitergabekontrolle (Übertragung & Empfänger)

- E-Mail-Verkehr über TLS-verschlüsselte Verbindungen (Microsoft 365), soweit technisch möglich.
- Externe Datenübertragung über HTTPS, SFTP/FTPS oder VPN (Uploadportal, FTP-Server, externe Dienstleister).
- Uploadportal mit Token-basierten Einmallinks, begrenzter Gültigkeit und Einschränkung der Downloadanzahl; Beschränkung auf definierte Dateitypen (Whitelist).
- Übermittlung personenbezogener Daten an Auftragsverarbeiter nur auf Grundlage von Auftragsverarbeitungsverträgen (AVV) gemäß Art. 28 DSGVO.
- Bei Dienstleistern mit möglicher Drittlandanbindung (z. B. Microsoft, Cloud-Dienste): Einsatz von EU-Standardvertragsklauseln

8. Eingabekontrolle (Protokollierung & Nachvollziehbarkeit)

- System- und Sicherheitslogging auf Servern, VPN, Firewall, FTP/Uploadsystemen (soweit technisch möglich).
- Protokollierung von Anmeldeereignissen, Fehlversuchen und administrativen Tätigkeiten in kritischen Systemen.
- Nachvollziehbarkeit von Änderungen an Stammdaten (z. B. Kunden- und Lieferantendaten) durch Protokollfunktionen im ERP-System, soweit vorhanden.
- Dokumentation von Freigaben und Qualitätsprüfungen im Produktions- und Lettershop-Prozess (z. B. Freigabe-E-Mails, Freigabeprotokolle).

9. Auftragskontrolle (Auftragsverarbeiter-Management)

- Abschluss von Auftragsverarbeitungsverträgen (AVV) gemäß Art. 28 DSGVO mit allen relevanten Dienstleistern (z. B. Steuerberater/Lohnverrechnung, CloudLab/Magento-Hosting, Microsoft 365, Wasabi, Brevo).
- Klare vertragliche Regelung der Weisungsgebundenheit und der getroffenen TOMs beim Dienstleister.

- Prüfung von Zertifizierungen und Sicherheitsnachweisen der Dienstleister (z. B. ISO 27001, SOC-Reports, Rechenzentrumsstandards).
- Anlassbezogene oder stichprobenartige Überprüfung der Vertragspartner (z. B. bei Änderungen der Dienste, Vorfällen oder neuen Systemen).

10. Verfügbarkeitskontrolle & Notfallmanagement

- Regelmäßige Datensicherung von relevanten Systemen und Dateien (Fileserver, ERP, wichtige Datenbanken).
- Externe, verschlüsselte Backups (S3/Wasabi) mit definierten Aufbewahrungsfristen und zusätzlichen Mechanismen wie Immutability (Schreibschutz für eine definierte Zeitspanne).
- Backup- und Recovery-Strategie
- Regelmäßige Tests von Rücksicherungen (Restore-Tests), um die Funktionsfähigkeit der Backups sicherzustellen.
- Einsatz von Schutzmechanismen auf der Infrastruktur (Firewall, Viren-/Malware-Schutz, Intrusion Detection, Geoblocking).

11. Trennungsgebot (Daten- & Zwecktrennung)

- Systemseitige Trennung von Datenkategorien (Kunden, Lieferanten, Mitarbeitende, Bewerber) durch separate Module, Mandanten oder Ordnerstrukturen.
- Trennung von Test- und Produktivumgebungen; keine Nutzung von Echtdaten in Tests, soweit vermeidbar (Einsatz von Pseudonymisierung/Anonymisierung).
- Auftragsbezogene Trennung von Lettershop- und Kampagnendaten pro Kunde/Mailing, keine Vermischung von Adresslisten unterschiedlicher Auftraggeber.
- Technische und organisatorische Sicherstellung, dass personenbezogene Daten nur für die Zwecke verwendet werden, für die sie erhoben wurden (Zweckbindung).

12. Lösch- und Speicherfristen

Die im Verzeichnis der Verarbeitungstätigkeiten festgelegten Speicher- und Löschfristen werden systematisch in den Fachbereichen und IT-Systemen umgesetzt.

- Buchhaltungs- und Steuerunterlagen: Aufbewahrung gemäß gesetzlichen Vorgaben
- Bewerbungsunterlagen: Löschung in der Regel nach 6 Monaten bei Absage, verlängerte Aufbewahrung (z. B. bis 2 Jahre) nur mit Einwilligung.
- Produktions-/Druckdaten und Lettershop-Adressen: Speicherung nur so lange wie für Nachdrucke, Reklamationen oder Nachweispflichten erforderlich (max. 7 Jahre).
- Videoaufzeichnungen: Speicherdauer technisch möglichst kurz (72 Stunden bis max. 7 Tage), längere Speicherung nur im Anlassfall (Vorfall).

- E-Mails: Umsetzung von Konzepten zur Löschung/Archivierung, insbesondere für sensible Bereiche (z. B. Bewerbungen), z. B. 6-Monats-Regel, zusätzlich Archivierung von geschäftsrelevanten Kommunikationen im Rahmen der gesetzlichen Aufbewahrungspflichten.
- Uploadportal/FTP: automatische oder manuelle Löschung von hochgeladenen Daten nach definierten Fristen (z. B. wenige Tage bis Wochen), sofern die Daten nicht in den Produktions-Workflow übernommen und dort weiterverarbeitet werden.

13. Datenschutz durch Technikgestaltung & Voreinstellungen (Art. 25 DSGVO)

- Datenminimierung bei Erhebung und Verarbeitung: Es werden nur diejenigen personenbezogenen Daten erhoben, die für die jeweilige Verarbeitung erforderlich sind
- Voreinstellungen in Systemen sind grundsätzlich datenschutzfreundlich ausgerichtet (z. B. restriktive Standardberechtigungen, eingeschränkte Sichtbarkeit von Daten).
- Einsatz von Pseudonymisierung oder Anonymisierung wo diese technisch möglich und/oder sinnvoll ist.
- Berücksichtigung datenschutzrechtlicher Anforderungen bereits bei der Planung neuer Systeme und Prozesse (Privacy by Design/Default).

14. Überprüfung, Audits & Dokumentation

- Regelmäßige Reviews (mindestens alle 2–3 Jahre oder anlassbezogen) des Verzeichnisses der Verarbeitungstätigkeiten, der DSFAs und der TOMs.
- Interne Kontrollen, z. B. Stichprobenkontrolle von Zugriffsrechten, Umsetzung von Löschfristen, Einhaltung von Prozessen bei Bewerbungen, Lettershop, Videozugriff.
- Dokumentation der durchgeführten Überprüfungen (Datum, verantwortliche Person, Ergebnisse, ggf. beschlossene Maßnahmen).

Bei wesentlichen Änderungen (z. B. Einführung neuer Systeme, Wechsel wesentlicher Dienstleister) wird geprüft, ob DSFAs anzupassen oder neu zu