Bayerisches Landesamt für
Datenschutzaufsicht

Datenschutz-Checkliste

für Soloselbstständige und Kleinstunternehmen aus dem Handel

Rahmenbedingungen

Die vorliegende Checkliste soll eine praxisnahe Orientierung für Kleinstunternehmen und Soloselbstständige aus dem Bereich Handel zur Umsetzung der datenschutzrechtlichen Anforderungen unter der Datenschutz-grundverordnung (DS-GVO) geben. Dabei werden folgende Rahmenbedingungen zugrunde gelegt:

- Unternehmen aus dem Bereich Handel
- keine oder nur wenige Mitarbeiter (max. 9)
- ggf. stationärer Handel
- Eigene Unternehmens-Webseite
- B2B, teils auch B2C
- keine Hochrisikoverarbeitung (z. B. kein KI-Startup, das datengetriebenes Profiling betreibt)
- hauptsächlich Nutzung von IT-Diensten (auch Cloud) und Standardkommunikation

Praxis-Check für Soloselbstständige und Kleinstunternehmen aus dem Bereich Handel

INHALT

1. Verzeichnis der Verarbeitungstätigkeiten (VVT)

Das Verzeichnis der Verarbeitungstätigkeiten (VVT) nach Art. 30 DS-GVO soll einen Überblick über den eigenen Umgang mit personenbezogenen Daten geben und auch schon erste zu klärende datenschutzrechtliche Anforderungen wie Löschfristen oder Datentransfers in sog. Drittländer (z. B. USA) benennen. Zugleich weisen insbesondere in bestimmten Sektoren sowie Unternehmenstypen die VVTs ein hohes Maß an Standardisierung auf – daher haben wir für einige typische Verarbeitungstätigkeiten für Soloselbstständige und Kleinstunternehmen aus dem Bereich Handel Muster erstellt (Anlage A).

Jeder Eintrag im VVT entspricht einer „Verarbeitungstätigkeit", bestehend aus:

- Zweck der Verarbeitung (Wieso werden personenbezogene Daten verarbeitet?)
- Mittel der Verarbeitung (Welche Art von automatisierter Verarbeitung wird eingesetzt, z. B. welche Software?)
- Welche Personengruppe ist von der Verarbeitung betroffen (z. B. Kunden, Mitarbeiter, Geschäftspartner)?
- Welche Datenkategorien werden verarbeitet (z. B. Adressdaten, Videoaufnahmen, Zahlungsdaten)?
- Wann sind die personenbezogenen Daten nicht mehr erforderlich und müssen gelöscht werden (z. B. acht Jahre bei Rechnungen)?
- Werden personenbezogene Daten in Nicht-EU-Länder übermittelt, und wenn ja, in welche?

2. Rechtsgrundlagen im VVT

Jede Verarbeitung personenbezogener Daten braucht eine Rechtsgrundlage (Art. 6 DS-GVO). Im Bereich Handel wird meist entweder eine vertragliche Rechtsgrundlage oder eine sog. Interessensabwägung verwendet. Für eine schlanke Datenschutz-Compliance können die Rechtsgrundlagen direkt an das VVT angefügt werden (Anhang A).

Einige mögliche Rechtsgrundlagen:

- ☐ Einwilligung
- ☐ Vertragliche Grundlage
- ☐ Gesetzliche Verpflichtung
- ☐ Interessenabwägung

3. Datenschutz-Folgenabschätzung (DSFA)

Schwellwertprüfung zur DSFA: Die DS-GVO erfordert bei Hochrisikoverarbeitungen die Durchführung einer Datenschutzfolgenabschätzung, die systematisch Risiken beurteilt und eindämmt. Bei der typischen Tätigkeit von Soloselbstständige und Kleinstunternehmen aus dem Bereich Handel auf Grundlage des exemplarischen

VVT in Anlage A ist eine DSFA in der Regel nicht erforderlich[1]; dies kann in einer formfreien Erweiterung dort beispielsweise wie dargestellt auch direkt vermerkt werden.

4. Videoüberwachung

Videoüberwachung bspw. im Laden oder außerhalb Betriebszeiten im Lager: Bei einer Videoüberwachung zur Aufklärung von Diebstählen oder von Sachbeschädigungen sowie zur Abschreckung ist gerade für kleine Handelsunternehmen, insbesondere bei denen diese Risiken schnell existenzbedrohend werden können, i. d. R. auf Grundlage einer Interessenabwägung zugunsten der Unternehmen datenschutzrechtlich möglich[2].

Checkliste:

- ☐ Datenminimierung (erforderliche Bereiche ggf. auch durch Verpixelung/Aufzeichnungszeiten festlegen)
- ☐ Sicherstellung, dass keine Beschäftigten überwacht werden (z. B. Sozialräume, Lagerbereiche)
- ☐ Hinweisschilder (mit Benennung Zweck und Kontaktdaten)[3]
- ☐ Festlegung Löschfristen (z. B. 72 Stunden bei Überwachung von Laden, der i. d. R. werktäglich betreten wird)

5. Pflicht zur Bestellung eines Datenschutzbeauftragten

Keine DSB-Bestellpflicht nach Bundesdatenschutzgesetz (BDSG)/DS-GVO: Ein betrieblicher Datenschutzbeauftragter unterstützt kompetent bei der Umsetzung der DS-GVO insbesondere bei Verarbeitungen mit erhöhten Risiken. Bei Soloselbstständigen und Kleinstunternehmen aus dem Bereich Handel sind jedoch i. d. R. die Voraussetzungen der Bestellpflicht nach DS-GVO[4] (z. B. Kerntätigkeit ist systematische Überwachung) und nach BDSG[5] (z. B. 20 Personen die sich ständig mit automatisierter Verarbeitung personenbezogener Daten beschäftigen) nicht erfüllt.

Bestellpflicht Datenschutzbeauftragter:

- ☐ Nein
- ☐ Ja. Begründung: _____

[1] Siehe beispielsweise die sog. Muss-Liste der deutschen Datenschutzaufsichtsbehörden für Unternehmen unter https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
[2] Ausführliche Informationen finden sich unter https://www.lda.bayern.de/de/thema_videoueberwachung.html
[3] Muster für Hinweisschilder (https://www.lda.bayern.de/de/thema_videoueberwachung.html; am Ende).
[4] siehe Art. 37 DS-GVO
[5] siehe §38 BDSG

6. Webshop

Die Webseite bzw. der Webshop (ggf. über ein vorgefertigtes Baukastensystem) wird (so die Annahme im einfachsten Fall) bei einem in der EU/EWR ansässigen Hoster betrieben.

Checkliste:

- ☐ Vertrag zur Auftragsverarbeitung (z. B. nach Vorlage[6] des Anbieters) abgeschlossen
- ☐ Technische und organisatorische Maßnahmen (auch im Vertrag mit Dienstleister) vereinbart und umgesetzt (Anlage TOM)

7. E-Mail-Kommunikation

Das E-Mail-Konto wird (ggf. sogar über den gleichen Hoster wie die Webseite) betrieben.

Checkliste:

- ☐ Vertrag zur Auftragsverarbeitung (z. B. nach Vorlage des Anbieters) abgeschlossen (ggf. bereits in Punkt 6 erfolgt)
- ☐ Technische und organisatorische Maßnahmen (auch im Vertrag mit Dienstleister) vereinbart und umgesetzt (vgl. auch Anlage TOM)

8. Office-Produkte aus der Cloud

Nutzung von Cloud-Office-Produkten (hier die Annahme: Drittlandstransfer in die USA abgesichert durch den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US Data Protection Framework[7]). Die Sicherheit der Verarbeitung nach Art. 32 DS-GVO bei Speicherung von Dateien und die Nutzung von Office-Produkten wird über die Standard-Maßnahmen der Cloud-Plattform abgesichert.

Checkliste:

- ☐ Vertrag zur Auftragsverarbeitung (z. B. nach Vorlage des Anbieters) abgeschlossen
- ☐ Die Datenübermittlung in die USA wird beim konkreten Unternehmen über das EU-US Data Protection Framework (DPF) sichergestellt (Voraussetzung: Cloud-Anbieter ist in der DPF-Liste des US-Handelsministeriums aufgeführt, siehe https://www.dataprivacyframework.gov/list).[8]
- ☐ Technische und organisatorische Maßnahmen (auch im Vertrag mit Dienstleister) vereinbart und umgesetzt (Anlage TOM)

[6] Eine Vorlage zum selbstständigen Abgleich findet sich auch auf der Website des BayLDA unter https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf

[7] Vgl. Art. 45 DS-GVO

[8] Die meisten großen Cloud-Anbieter aus den USA sind in der DPF-Liste eingetragen; sofern das nicht der Fall ist, müssen Übermittlungen in die USA auf andere Garantien gestützt werden, z. B. sog. Standardvertragsklauseln der EU-Kommission (Näheres unter https://www.lda.bayern.de/de/thema_uebermittlung_personenbezogener_daten_in_drittlaender.html)

9. Messenger-Verwendung

Die Kommunikation mit Geschäftspartnern erfolgt über einen Messenger.

Checkliste:

- ☐ Auswahl eines geeigneten Messengers mit Ende-zu-Ende-Verschlüsselung
- ☐ Verarbeitung von Smartphone-Kontaktdaten zum Nutzerabgleich durch Messenger-Anbieter ist diesbezüglich datenschutzkonform (z. B. Auswahlmöglichkeit einzelner Kontakte) oder der selektive Zugriff ist von Seiten des Smartphones konfigurierbar

10. Betroffenenrechte

Der Umgang mit datenschutzrechtlichen Betroffenenrechtenkann bei Soloselbstständigen und Kleinstunternehmen aus dem Bereich Handel kann reaktiv ausgestaltet werden, d.h. es kann abgewartet werden, bis eine Anfrage ggf. überhaupt gestellt wird anstatt bspw. Abläufe und Dokumente im Vorfeld zu definieren.

Checkliste:

- ☐ Es ist bekannt, dass es Betroffenenrechte wie bspw. Auskunfts-, Berichtigungs- oder Löschrechte gibt[9]
- ☐ Kontaktdaten für Betroffenenrechte an geeigneter Stelle, bspw. auf Webseite veröffentlicht
- ☐ Information der Beschäftigten über interne Ansprechpartner im Fall der Geldendmachung von Betroffenenrechten

11. Prozess zur Meldung von Sicherheitsvorfällen

Der Umgang mit datenschutzrechtlichen Meldeverpflichtungen bei Soloselbstständigen und Kleinstunternehmen aus dem Bereich Handel kann reaktiv ausgestaltet werden, d.h. es kann abgewartet werden, ob ggf. überhaupt ein meldepflichtiger Vorfall aufritt anstatt bspw. Abläufe und Dokumente im Vorfeld zu definieren.

Checkliste:

- ☐ Meldeformular des BayLDA unter www.lda.bayern.de/datenpanne ist bekannt
- ☐ Im Falle eines Sicherheitsvorfalls ist dort eine geführte Meldung abzusetzen, die alle erforderlichen Informationen abfragt

[9] Information für Verantwortliche z. B. zur Auskunft: https://www.lda.bayern.de/media/themen/Infoblatt_fuer-verantwortliche_zu_auskunft.pdf, zur Löschung: https://www.lda.bayern.de/de/thema_loeschung.html

12. Tracking auf Website

Webtracking nur mit Einwilligung. Neben der DS-GVO gilt auf Webseiten noch das Telekommunikation- Digitale-Dienste-Datenschutzgesetz (TDDDG). Dieses gilt insbesondere für den Einsatz von Cookies, sog. Zähl-Pixeln und anderen Methoden zur Reichweitenmessung und geht von einer grundsätzlichen Pflicht zur Einwilligung aus. Diese kann über ein sog. Cookie-Banner eingeholt werden.

Checkliste Inhalte Datenschutzerklärung:

- ☐ Name und Kontaktdaten des Verantwortlichen
- ☐ Beschreibung der Zwecke der Datenverarbeitung (Betrieb Webseite, Webshop, Tracking-Tools, Werbenetzwerke, …) und Angabe der Rechtsgrundlage(n) (z. B. Interessenabwägung)
- ☐ Auflistung der verarbeiteten personenbezogenen Daten (z. B. IP-Adresse, Name, E-Mail-Adresse)
- ☐ Information über Empfänger oder Kategorien von Empfängern (z. B.: Hosting-Provider, Zahlungsdienstleister, Drittanbieter (z. B. für Tracking, Werbung))
- ☐ Angabe, ob eine Übermittlung in ein Drittland außerhalb der EU/des EWR stattfindet sowie Nennung der Garantien für die Übermittlung (z. B. EU-US Data Protection Framework)
- ☐ Hinweise zu Betroffenenrechten nach DS-GVO (z. B. Recht auf Auskunft, siehe auch oben, Ziffer 10)
- ☐ Verwendung einer klaren und einfachen Sprache

Checkliste Einwilligungsbanner:

- ☐ Einwilligung wird (wenn nötig) mit einfacher Sprache eingeholt, bevor bspw. Cookies gesetzt werden
- ☐ Gleichwertige Möglichkeit, keine Einwilligung zu erteilen, auf erster Ebene und nicht „versteckt" in tieferen Dialogschichten
- ☐ Vollständige Information über:
  - Zugriff auf die Endeinrichtung / Auslesen von Informationen (z. B. Cookie xy wird gesetzt)
  - Zweck der Verarbeitung, Kategorien von Empfängern (z. B. beim Einsatz von Werbenetzwerken oder Trackingdienstleistern), Drittstaatentransfers
- ☐ Hinweis auf das Widerrufsrecht[10]

[10] § 25 Abs. 1 Satz 2 TDDDG i. V. m. Art. 7 Abs. 3 Satz 1 DS-GVO

13. (E-Mail-)Werbung

Im Bereich Endkunden wird Werbung an Bestandskunden sowie Interessierte mittels E-Mail sowie teils mit postalischen Schreiben durchgeführt.

Checkliste:

- ☐ Double-Opt-In (eingegebene Mailadresse muss vom Kunden in einer zugesandten Anmelde-Mail bestätigt werden) bei elektronischer Werbung auf Basis einer Einwilligung (bspw. Checkbox auf Webseite). Einfache Möglichkeit des Widerrufs ist umgesetzt.
- ☐ Widerspruchsmöglichkeit bei elektronischer Werbung von Bestandskunden sowie bei postalischer Werbung ist umgesetzt

14. Informationspflichten

Betroffene Personen sind verständlich über die Verarbeitung ihrer Daten zu informieren. Wenn die Daten direkt von der Person stammen[11], muss dies im Zeitpunkt der Datenerhebung erfolgen.
Typische Situationen, in denen die Information auf Basis von Verarbeitungen des im Rahmen dieser Handreichung vorgestellten VVT (Anhang A) zu erteilen ist, sind somit u. a.:

- Aufnahme von Kundendaten bei einer Bestellung o. ä. auf der Website
- Aufnahme von Kundendaten bei einer Bestellung, bei Ausstellung einer Kundenkarte o.ä. im persönlichen Kontakt (z. B. im Laden)

Werden die Daten nicht bei der betroffenen Person selbst erhoben[12], sondern bei einer anderen Person/Stelle (z. B. bei Verwendung von Adressdaten von Dritten zu Werbezwecken), muss die Information in der Regel an die betroffene Person spätestens innerhalb eines Monats erteilt werden.

Checkliste:

- ☐ Informationen bei Datenerhebung im Laden (z. B. Bestellung, Kundenkarte) mittels Aushangs, Informationsblatt oder im Bestell-/Vertragsformular selbst
- ☐ Informationen bei Datenerhebung im Webshop über Webseite in Datenschutzerklärung
- ☐ Bei Verwendung von Daten Dritter Informationen entsprechend eines geeigneten Kommunikationsmittels (z. B. E-Mail)

[11] Siehe Art. 13 DS-GVO
[12] Siehe Art. 14 DS-GVO

15. Verwendung von Künstlicher Intelligenz

Künstliche Intelligenz wird (so die Annahme in dieser Handreichung) bei Soloselbstständigen und Kleinstunternehmen aus dem Bereich Handel für das Verfassen von Textentwürfen bspw. für Soziale Netzwerke oder für Briefe/E-Mails eingesetzt. Dazu werden Cloud-Dienste (KI as a Service) verwendet, die mittels Webanwendung des KI-Anbieters durch Eingabe von Textanfragen (Prompts) sowie ggf. dem Hochladen einzelner Dokumente (z. B. als PDF) genutzt werden.

Checkliste:

- ☐ Vertrag zur Auftragsverarbeitung (z. B. nach Vorlage des Anbieters) abgeschlossen[13]
- ☐ Geprüft, dass die eigenen Eingabe- und Ausgabedaten vom KI-Anbieter nicht für eigene Zwecke wie die Produktverbesserung verwendet werden[14]
- ☐ Sollte ein KI-as-a-Service nur ohne personenbezogene Daten genutzt werden, dann sind die eigenen Mitarbeiter diesbezüglich zu schulen
- ☐ Es werden (von Beschäftigten) bei der Verarbeitung von personenbezogenen Daten keine KI-Cloud-Dienste verwendet, die nur für die private Nutzung vorgesehen sind (sog. „Schatten-KI")
- ☐ Es ist (allen Beschäftigten) bekannt, dass insbesondere Generative KI bei der Erzeugung von Texten mitunter unrichtige Fakten ausgibt (umgangssprachlich sog. „Halluzinationen")
- ☐ Hinweis: Über den konkreten Einsatz eines KI-Tools muss in den Informationspflichten nach Art. 12 ff. DS-GVO nicht zwangsläufig öffentlich informiert werden[15]

[13] Dies sind meist kostenpflichtige Varianten von KI-Anwendungen, die kostenlos nur für Endverbraucher nutzbar sind, die aber mitunter mit ihren Daten „zahlen".
[14] Bei Verträgen zur Auftragsverarbeitung sollte das i.d.R. ausgeschlossen sein. Mitunter gibt es Cloud-Dienste, die dies über eine Konfiguration (z. B. Schieberegler in Weboberfläche) erst unterbinden.
[15] Die DS-GVO sieht keine Informationspflichten für die Erzeugung von KI-generierten Text-/Bildinhalten derart vor, dass deren Ursprung mittels KI den betroffenen Personen kenntlich gemacht werden müsste. Auch ist momentan unklar, ob Art. 50 KI-VO (Transparenzpflichten bei KI-generierten Inhalten) dann greift, wenn ein Mensch eine KI-Ausgabe prüft und dann bspw. selbst „von Hand" in ein soziales Netzwerk einstellt – derartige Fragen würden dann von der für die für die KI-VO zuständige Aufsichtsbehörde, die zum Zeitpunkt der Veröffentlichung dieser Handreichung in Deutschland von nicht fest steht, zu beantworten sein.

Anhang A: Verzeichnis der Verarbeitungstätigkeiten inkl. Compliance-Erweiterung

An-wendbar	Zweck	Mittel	Betroffene Personen-gruppen	Datenkategorien	Speicher-dauer[16]	Transfer Dritt-land?	Empfänger[17]	TOM	Rechtsgrundlage	DSFA erforder-lich?
☐	Kundenverwal-tung und Bestell-abwicklung	<Webseiten-software>	Kunden	Adressdaten, Verkaufsdaten	<ToDo>	Nein	Zahlungs-dienstleister Logistikdienstleister	Checkliste Technische und organisatorische Maßnahmen	Vertrag	Nein
☐	Buchhaltung und Rechnungsstel-lung	<Software zur Waren-wirtschaft>	Kunden	Adressdaten, Verkaufsdaten, Lieferdaten	<ToDo>	Nein	Steuerberater Banken Finanzamt		Vertrag	Nein
☐	Verwaltung von Lieferanten	<Software zur Waren-wirtschaft>	Lieferanten	Adressdaten, Einkaufsdaten, Lieferdaten	<ToDo>	Nein	Steuerberater Banken		Vertrag	Nein
☐	Marketing und Werbung	<Newsletter-System>	Kunden	Adressdaten, Verkaufsdaten	<ToDo>	Ja (USA)	E-Mail-Marketingan-bieter		Einwilligung	Nein
☐	Betrieb Web-seite/ Onlines-hops	<Baukasten Hoster>	Kunden	IP-Adressen Webseiten-besucher, Trackingdaten	<ToDo>	Nein	Hosting-Provider		Vertrag, Interes-senabwägung	Nein
☐	Verwaltung von Mitarbeiterdaten	<Software für Mitarbeiter-verwaltung>	Mitarbei-tende	Vertragsdaten, Lohnab-rechnungsdaten, Bewer-bungsdaten	<ToDo>	Nein	Sozialversicherungs-träger Finanzamt		Gesetzliche Grundlage, Vertrag	Nein
☐	Videoüberwa-chung im Ver-kaufsraum/Lager	<Netzwerk-fähige VÜ-An-lage>	Kunden, Mitarbei-tende	Videoaufzeichnungen	72 Stunden	Nein	Polizei, wenn erfor-derlich		Interessenabwä-gung	Nein
☐	Nutzung von Cloud-Infrastruk-tur-Diensten	<Software ei-nes Cloud-An-bieter>	Kunden, Lie-feranten, Mitarbei-tende	Adressdaten, Verkaufsdaten, Lieferdaten, Einkaufsdaten	<ToDo>	Ja (USA)	Cloud-Provider		Interessenabwä-gung	Nein
☐	Nutzung von Messenger-Diensten	<Eingesetzter Messenger>	Lieferanten	Telefonnummern, Kom-munikations-Metadaten	<ToDo>	Ja (USA)	Anbieter des Mess-enger-Dienstes		Interessenabwä-gung	Nein
☐	Social Media Nutzung	<Social Media Kanal>	Kunden, Sonstige	Kommentardaten	<ToDo>	Ja (USA)	Social-Media-Anbie-ter		Interessenabwä-gung	Nein

[16] Die rein datenschutzrechtliche Speicherdauer ergibt sich aus der Erforderlichkeit zur Erreichung des Zwecks (z. B. Versand Newsletter). Da es aber noch anderes rechtliche Aufbewahrungsfristen (z. B. Steuer-recht) gibt, können diese von der Datenschutzaufsichtsbehörde, die bei diesen keine eigene Expertise hat, nicht verlässlich im Rahmen einer Vorlage angegeben werden – insofern bitten wir die entsprechenden Werte ggf. mit einem Steuerberater o. ä. zu ermitteln.

[17] Es wird bei diesem Beispiel davon ausgegangen, dass es aufgrund der sehr kleinen Unternehmensstruktur keine internen Empfänger gibt.

Anhang B: Technische und organisatorische Maßnahmen

TOM 1: Verwendung von starken Passwörtern

Starke Passwörter sind entscheidend, um unbefugten Zugriff auf Systeme und Daten zu verhindern. Sie sollten komplex und ausreichend lang sein.

Checkliste:

- ☐ Vorgabe von Mindestanforderungen an Passwörter (z. B. Länge mind. 12 Stellen, Sonderzeichen)
- ☐ Änderung von Passwörtern bei Mitarbeiterwechsel oder Berechtigungsänderung
- ☐ Schulung der Beschäftigten zur Erstellung und Verwaltung starker Passwörter

TOM 2: Schutz durch Datenverschlüsselung

Die Verschlüsselung schützt personenbezogene Daten sowohl im Ruhezustand als auch während der Übertragung, um sie vor unbefugtem Zugriff zu sichern.

Checkliste:

- ☐ Verschlüsselung von personenbezogenen Daten im Ruhezustand (z. B. Festplattenvollverschlüsselung von Notebooks)
- ☐ Verschlüsselung von Daten während der Übertragung (z. B. HTTPS für Webseiten)
- ☐ Verschlüsselung von mobilen Daten (z. B. Backups auf USB-Stick)

TOM 3: Automatische Softwareupdates

Automatische Softwareupdates stellen sicher, dass alle Systeme und Anwendungen stets auf dem neuesten Stand sind, um Sicherheitslücken zu schließen und die IT-Sicherheit zu erhöhen.

Checkliste:

- ☐ Aktivierung automatischer Updates für Betriebssysteme und Anwendungen
- ☐ Regelmäßige Überprüfung der Update-Einstellungen und -Protokolle
- ☐ Unterrichtung der Beschäftigten zur Bedeutung von Softwareupdates

TOM 4 Zwei-Faktor-Authentifizierung (2FA) bei Cloud-Diensten

Die Implementierung von 2FA erhöht die Sicherheit beim Zugriff auf Cloud-Dienste mitunter erheblich, indem sie eine zusätzliche Authentifizierungsebene hinzufügt.

Checkliste:

- ☐ Aktivierung von 2FA für alle Cloud-Dienste, die personenbezogene Daten verarbeiten (z. B. mittels Smartphone App)
- ☐ Schulung der Beschäftigten zur Nutzung von 2FA und den verfügbaren Authentifizierungsmethoden
- ☐ Regelmäßige Überprüfung der 2FA-Einstellungen und -Protokolle.

TOM 5: Datensicherung mit Offline-Backups

Offline-Backups bieten zusätzlichen Schutz vor Datenverlust, insbesondere bei Cyberangriffen wie Ransomware, indem sie Daten an einem physischen Ort speichern, der nicht mit dem Netzwerk verbunden ist.

Checkliste:

- ☐ Erstellung von Offline-Backups auf externen Speichermedien (z. B. USB-Sticks, externe Festplatten)
- ☐ Regelmäßige Aktualisierung der Offline-Backups (z. B. monatlich).
- ☐ Sichere Aufbewahrung der Offline-Backups an einem geschützten Ort

TOM 6: Schulung und Sensibilisierung

Die Schulung (der Beschäftigten) ist entscheidend, um ein Bewusstsein für Sicherheitsrisiken zu schaffen

Checkliste:

- ☐ Regelmäßige Schulungen für Mitarbeiter zum Thema Datenschutz und IT-Sicherheit
- ☐ Sensibilisierung für Phishing und andere Cyber-Bedrohungen (E-Mail-Hacking, Website-Fakes)
- ☐ Nutzung von Informationsmaterialien (z. B. Handbücher, Leitfäden, Flyer, Broschüren)

TOM 7: Datenminimierung

Die Datenminimierung bedeutet, nur die Daten zu erheben, die für den jeweiligen Zweck notwendig sind. Dies reduziert das Risiko von Datenmissbrauch und erleichtert die Einhaltung der DS-GVO („Was nicht mehr da ist, kann nicht gehackt werden").

Checkliste:

- ☐ Erhebung nur der notwendigen Daten für spezifische Zwecke
- ☐ Regelmäßige Überprüfung der Datenbestände auf Relevanz
- ☐ Insbesondere Löschung nicht mehr benötigter Daten, für die keine gesetzlichen Aufbewahrungspflichten mehr bestehen

TOM 8: Security Basics

Technische Sicherheitsmaßnahmen schützen die IT-Infrastruktur vor Bedrohungen und Angriffen. Dazu gehören klassische Maßnahmen wie Firewalls, Antiviren-Software und regelmäßige Software-Updates.

Checkliste:

- ☐ Einsatz von Firewalls und Antiviren-Software
- ☐ Regelmäßige Software-Updates und Patch-Management
- ☐ Nutzung von sicheren Netzwerken (z. B. Verschlüsselte VPN für Remote-Zugriffe bspw. aus dem Home Office)

Hinweise zur Handreichung:

Diese Handreichung soll die Erwartungen des BayLDA an die Datenschutz-Compliance für Soloselbstständige und Kleinstunternehmen im Bereich Handel an die sog. Datenschutz-Compliance bei nicht-öffentlichen Stellen in Bayern aufzeigen. Unter diesem Begriff „Compliance" wird die Einhaltung gesetzlicher Vorgaben und eigener Richtlinien zum Schutz personenbezogener Daten verstanden. Ziel ist es, sicherzustellen, dass die Verarbeitung solcher Daten im Einklang mit Datenschutzgesetzen – insbesondere der Datenschutz-Grundverordnung (DS-GVO) – erfolgt. Während Großunternehmen sowie Unternehmen mit risikobehafteten datengetriebenen Geschäftsmodellen hierbei mitunter umfangreichere Aufbaustrukturen sowie Prozessabläufe (z. B. Betroffenenrechte bei einem Energieunternehmen mit angebundenem Inkasso; Start-Up mit Profiling-Diensten) umsetzen müssen, ist eine Datenschutz-Compliance bei Kleinstunternehmen, die keine erhöhten Risiken bei der Verarbeitung personenbezogenen Daten besitzen, i. d. R. mittels standardisierter und eher schematischer Vorgaben zu erreichen. Diese Handreichung zeigt Lösungsansätze und datenschutzgerechte Umsetzungsmaßnahmen an Hand typisierter und schematisch abgebildeter Verarbeitungen auf und soll so die besonderen Bedürfnisse von Kleinstunternehmen berücksichtigen und zur Rechtssicherheit beitragen. Sollten weitere Verarbeitungen durchgeführt werden, die nicht in dieser Handreichung gelistet sind, stehen für weitere Abklärungen, die Beratungsmöglichkeiten des BayLDA unter www.lda.bayern.de/beratung zur Verfügung.

Zum Hintergrund der Handreichung:

Das BayLDA hat seit Ende 2024 mit der IHK Bayern eine Datenschutz-Austausch und Informationsreihe zum Thema Datenschutz und Rechtssicherheit gestartet. Diese Handreichung soll demnach bayerischen Soloselbstständigen und Kleinstunternehmen im Bereich Handel helfen, die datenschutzrechtlichen Anforderungen praxisnah umzusetzen. Das vorliegende Dokument wird in der vorliegenden Version 0.9 bewusst als anpassungsfähiger Stand verstanden – Verbesserungsvorschläge sowie Feedback aus der Sicht der Zielgruppe dieses Dokuments nimmt das BayLDA gerne unter poststelle@lda.bayern.de entgegen.

Stand: 13.05.2025 (Version 0.9)

Aktuelle Version zum Download:
https://www.lda.bayern.de/checkliste_handel

Herausgeber und Kontakt:
Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Promenade 18 | 91522 Ansbach
www.lda.bayern.de | Tel.: 0981 180093-100
poststelle@lda.bayern.de

Titelbild: KI-generiert
Checklisten-Icon: KI-generiert