Praxistips für Businesskunden von Preisl Computer zur Vorbereitung und Umsetzung der DSGVO bis Mai 2018 - Vorschläge und Wegweiser!

Sie können in dieser Reihenfolge vorgehen und sich eine Liste/Aufstellung erarbeiten, diese dient dann bereits als sehr gute Vorlage für das **zu erstellende Verarbeitungsverzeichnis.** Am besten mit z.B. Word oder Excel erstellen und befüllen/ergänzen. (Auch Mitarbeiter befragen/einbinden!)

Inhalt der Liste – welche Daten werden überhaupt, wie und wo / von wem / warum verarbeitet?

Welche personenbezogenen Daten verarbeiten Sie? – eine Aufzählung – bitte ergänzen!
z.B. gespeichert, ausgedruckt, Formulare, versendet, empfangen (Fax/Post/Mail), archiviert
diese in Anwendung, Kategorien, Personengruppen und Zweck der Verwendung aufteilen : z.b.

Verarbeitung#: Kategorie personenbezogener Daten / Personengruppen -> Verwendungszweck:

Verarbeitung1: Auftragsverwaltungs-Software/Faktura/Lager/Bestellungen/ERP:
Name, Anschrift, Emailadresse **von Kunden** -> für Angebote, Rechnungen, Kundenbetreuung
Name Kontaktperson, Mails und Handynummer **Lieferanten** -> für Bestellungen, Reklamationen
Verarbeitung2: Lohnverrechnung Mitarbeiter:
Name, Anschrift, Geburtsdatum **der Mitarbeiter** -> für Lohnverrechnung, Sozialversicherung
Sozialversicherungsnummern **der Mitarbeiter** -> für Lohnverrechnung, Sozialversicherung
Bankkontodaten **der Mitarbeiter** -> für Gehaltsauszahlungen
Telefon Nummer eines Angehörigen der Mitarbeiter **(Dritte)** > für Notfälle und Unfälle
usw. .....ergänzen !
Verarbeitung3: Email- und sonstige (Tele)-Kommunikation für den Geschäftsbetrieb:
Namen, Emailadressen, Tel. Nummern, sowie Mails und SMS, als auch Briefe von Bewerbern, Mitarbeitern, Lieferanten, Kunden, sonstigen Dritten -> für die Geschäftskommunikation
Verarbeitung xy: Onlineshop, Vereinsverwaltung, Patientenkartei, CRM, usw. – bitte anpassen!

Weitere Orte und Typen von personenbezogenen „Datensammlungen“ bitte nicht vergessen:
z.b. Telefonlisten, Geburtstagskalender, „Coockies“ auf Webseiten, Onlineshop, Kontaktformular auf Webseite, IP-Adressen auf Webservern, in allen Email Programmen (Quelltext), in Firewall / Antiviren Logs und Reports, Zeiterfassungs-Systeme, Videoüberwachung, KFZ-Kennzeichen, Zugangskontrollen z.b. mit Fingerprint, Anrufbeantworter, Telefonanlagen, Fahrtenschreiber (LKW / Busse), SMS, Facebook – sofern geschäftlich verwendet, PRIVATGERÄTE von Mitarbeitern, etc.,

Mit / auf welchen Geräten sind Daten, schriftliche Ordner/Belege, Kästen, Internet, Cloud?
Handys – (Kontakte, SMS, Mails), Tablets, PCs, Server, Fax, Backup, Archiv, in der „Cloud“, Notebooks / privateMitarbeitergeräte oder private Cloud-Speicher?

Wie lange müssen die personenbezogene Daten tatsächlich aufbewahrt werden?
(z.b. anhand einer gesetzliche Verpflichtung), bzw. wann verfällt der Verwendungszweck?
Zeitdauer pro Kategorie/Personengruppe anführen / ergänzen + geplante Löschungsintervalle!

Werden personenbezogene Daten weitergegeben, wenn ja, welche Daten und an wen/wohin:
z. B. an Schwesterfirma, Lieferanten, Steuerberater, Banken, Leasing, Inkasso, Versicherungen, etc. (z.B. Inkassobüro im Anlassfall), Lieferanten im Gewährleistungsfall / Garantiefall; gehen Daten in ein Eu-Drittland, wenn ja, welches?

Whatsapp in Verwendung? – Achtung: nach momentaner Lage riskant!
ALLE auf Handys gespeicherten Kontakte werden hier standardmäßig an Facebook übermittelt – hierfür bräuchten Sie **von jedem** gespeicherten Kontakt eine Einwilligung/Zustimmung hierfür!

Werden personenbezogene Daten durch „Auftragsverarbeiter" verarbeitet?
Beispiele für Auftragsverarbeiter sind:
Lohnverrechnungsbüro / Steuerberater
EDV –System der Schwester/Mutterfirma/Tochterfirma wird verwendet,
externe, ev. **auch nur gelegentliche** EDV Betreuung oder Fernwartung durch Softwarefirmen

Auftragsverarbeitung im Internet - gehostete Server und Anwendungen in der Cloud wie z.B.
Cloud Backups, Dropbox, Onedrive, Google Drive, Google Calendar, Skype, Office 365 / Outlook - Exchange Online, Icloud, GMX, Google Mail, Ebay, Amazon Marketplace, etc., etc.

Gibt es schriftliche, konkrete und datenschutzkonforme Verträge mit Ihren Anbietern?
Gibt es mit jedem der in Frage kommenden Auftragsverarbeiter einen schriftlichen Vertrag oder entsprechend angepasste Nutzungsbedingungen bei z.B. Google, Microsoft, Facebook, etc. – Denn: Sie sind trotzdem immer der Verantwortliche für Ihre gespeicherten Daten bei Datenschutzproblemen/Pannen! *Vermutlich (noch) nicht! --------> nachholen / einholen.*

Sind Sie berechtigt , alle von Ihnen aufgelisteten Daten zu verarbeiten oder weiterzugeben?
1. Für Daten die für die Erfüllung eines Vertrages, z.b. Kaufvertrages notwendig sind haben Sie eine rechtliche Grundlage und Berechtigung und brauchen dafür keine separate Einwilligung.
Sie haben aber eine Informationspflicht! (Siehe Datenschutzerklärung – auf diese verweisen!)

2. Verarbeitungen personenbezogener Daten, für die Sie keine rechtliche Grundlage haben, dürfen Sie verarbeiten sofern Sie eine Einwilligung dafür haben (idealerweise schriftlich)!
z.b. Email Adresse für Newsletter-Versand, Geburtsdatum für Geburtstagsglückwünsche, etc.

3. Sensible Daten: Hier brauchen Sie prinzipiell eine freiwillige und ausdrückliche schriftliche Einwilligung, Personenbezogene Daten von Kindern unter 14 Jahren – sind gänzlich sensibel.

--> **Einwilligungs-Schreiben / Formulare aufsetzen** inkl. Belehrung über die Rechte der Betroffenen (Widerruf, Recht auf Löschung, Berichtigung, Übertragung, etc.) weisen Sie auf ev. vorhandene AUFTRAGSVERARBEITER oder DATENEMPFÄNGER hin!

--> Die Einwilligungen einholen (+ alte personenbezogene Daten „ausmisten!")

Sofern eine rechtmäßige Einwilligung bereits besteht, muß diese nicht erneut eingeholt werden. Achtung: Es besteht aber ein **Kopplungsverbot**, für jeden **einzelnen** Verarbeitungszweck braucht es auch eine einzelne Einwilligung!

Informationspflichten – Datenschutzerklärung - bereits vor „Erheben/Aufnehmen“ von Daten!
Am besten eine Datenschutzerklärung aufsetzen, im Betrieb aufhängen & im Internet öffentlich zugänglich ebenfalls. Darin **möglichst transparent und einfach** beschreiben was mit personenbezogenen Daten in Ihrem Betrieb passiert und wie mit diesen umgegangen wird, wie lange sie gespeichert und wie sie geschützt werden, ebenso ob diese weitergegeben werden. Dazu **die Belehrung** über **die Rechte** der Betroffenen (jederzeit Widerruf, Recht auf Löschung, etc.)
Siehe als Beispiel meine eigene Datenschutzerklärung unter **http://www.preisl.at/datenschutz/**
Mein Tip: Weisen Sie auf Ihre Datenschutzerklärung bereits in jeder Email Signatur hin (Link)!

Risiko-Folgenabschätzungen:
Besteht bei z.b. Verlust oder „Hacken“ / Diebstahl ein besonders **hohes** Risiko für die Betroffenen?
Leider fehlt bis dato eine Black-/Whitelist der Datenschutzbehörde dazu.
Dann müssen Sie eine Risikofolgenabschätzung durchführen, bzw. ev. einen Datenschutzbeauftragten ernennen, bzw. ev. sogar eine vorherige Konsultation der Datenschutzbehörde einleiten. (Zusätzlich gilt Schadenersatzpflicht, Schmerzensgeld, etc.!)

Online Dienste / Webseiten/Onlinshops:
Diese an die notwendigen Gegebenheiten anpassen (Datenschutzerklärung, Cookies, Formulare mit Zustimmungsbuttons Belehrung Widerruf, etc.) Ev. AGBs anpassen an DSGVO / Datenschutz.

Verarbeitungsverzeichnis fertigstellen/erstellen:
Aus den erarbeiteten Ergebnissen erstellen Sie jetzt das sogenannte **Verarbeitungsverzeichnis**. Dieses muß bei Veränderungen dann auch laufend angepasst werden. Dieses Verzeichnis erstellen Sie zb mit Word oder Excel, es bleibt in Ihrem Haus und ist nur auf Verlangen der Datenschutzbehörde vorzulegen. Es **muß** noch Ihr Name als Verantwortlicher darin aufscheinen.

Erarbeiten und Dokumentation Ihrer „technisch-organisatorischen“ Maßnahmen:
Diese beschreibt alle getroffenen Maßnahmen um den Schutz der Daten zu gewährleisten.
Ich empfehle auch hier Word oder Excel zu verwenden und in sich zu gehen!

1., Welche Maßnahmen bestehen bereits? – 2., wo ist Handlungsbedarf, --> **nachbessern!**
Notieren Sie 1., wie solche angewendet und 2., **verbessert werden können**, grob unterteilt in:

Ihre technische Maßnahmen „am Stand der Technik“ zum Schutz personenbezogener Daten:
z.B.: Datensicherungen, möglichst genau beschreiben. Wie und wie oft, **verschlüsselt** ja/nein; Unterbrechungsfreie Stromversorgung, Überspannungsschutz, Internet Fallback, Proxy Server, Raidsysteme gegen Festplattenausfälle, regelmäßige Netzwerkwartung und Dokumentation, Freigabe- und NTFS- Berechtigungen auf Server, Arbeitsplätzen, NAS, in Softwareprogrammen, Verwendung von modernen Firewalls, Antivirenprogramme, Software-Sicherheitsupdates, Zutrittskontrollen (wer hat Zugang zu PCs, Handy, Serverraum, Switch, nur begleitet, etc.) Passwörter: Welche Passwörter, wie oft gewechselt, Komplexität, Sichere WIFI Verschlüsselung, Verschlüsselung: werden Daten verschlüsselt gespeichert, verschlüsselt übermittelt (Mail,/Web) Bildschirmschoner, Kennwörter, Pin / Fingerprint am Handy, Fernlöschfunktionen Handy/Tablets Hochwasserschutz, Brandschutz, Feuerlöscher, Alarmanlagen, Wachdienst, Videoüberwachung, Pseudonymisierung, Verpixelung, 2Faktor Authentisierung, Privacy by default, Privacy by Design,..
Im Idealfall korrekt, konkret, und im vorhandenen und praktizierten Umfang!

Ihre organisatorischen Maßnahmen zum Schutz personenbezogener Daten können sein z.B.:

Laufende Mitarbeiter-**Sensibilisierung** und –**Schulung** in IT Sicherheit **UND** deren Dokumentation.

Richtlinien und Vorgaben für Mitarbeiter z.b. Geheimhaltungspflichten, Verbot unerlaubter Softwaredownloads oder privater Daten auf Firmengeräten, Verbot private (Mail)-Nutzung, etc. eine „Clean Desk" – Policy (aufgeräumter Schreibtisch, versperrte Akten, am PC abgemeldet), Handys, Notebooks, Home-Office Geräte passwortgeschützt, HomeOffice - VPN nur verschlüsselt!

Vorbereitete Pläne für sofortige Routinemaßnahmen bei Mitarbeiterwechsel/-ausscheiden. Schlüsselverwaltung Büros und Serverräume, Online, versperrbare Kästen, Archive mit Belegen Notfallpläne in Katastrophenfällen oder bei Hackerangriffen, Diebstahl, Verlust, udgl,

Regelmäßige Testrücksicherungen aus Backups,
Zugriffskontrollen (werden Zugriffe protokolliert und überwacht?)
Überwachung von Eindringungsversuchen (z.b. mittels moderner Firewalls)

Sorgfältige Auswahl **nur zuverlässiger Auftragsverarbeiter** und deren laufende Kontrolle.
Dokumentation aller einlangenden Datenschutzanfragen, z.B. Auskunft-, Löschanfragen
Pläne zu und Dokumentation bei Sicherheitsvorfällen, etc.

Umso schutzwürdiger die Daten sind, umso mehr Maßnahmen sollten Sie ergreifen!

Jetzt hätten Sie laut Fahrplan auch die organisatorisch technischen Maßnahmen dokumentiert und müssen möglicherweise in einigen Bereichen nachbessern! **Auch diese Dokumentation** bleibt bei Ihnen und ist der Datenschutzbehörde nur auf Verlangen vorzulegen.

Abschließend rate ich eine DSGVO TO-DO Liste anzulegen, und auf einem Kalender „DSGVO" zu vermerken, welche Maßnahmen regelmäßig ab Inkrafttreten routinemäßig erledigt werden möchten. Inhalt z.B. Excel Tabellenblatt: (diese samt Datum in einer Spalte „erledigt" abarbeiten.)
z.b.:
Täglich: Backups kontrollieren, auffällige Sicherheitsereignisse protokollieren/ Chef(in) melden.
Wöchentlich: externe Backups auswechseln, Vidoüberwachungen entgültig löschen, ev. Datenschutzanfragen beantworten + dokumentieren, gab es Mitarbeiterwechsel / Maßnahmen?
Monatlich: Sicherheitsupdates, Firewall Logs, Antivirenprogramme überprüfen, Passwörter / Wlan Schlüssel ändern, etc, defekte oder ausgeschiedene Geräte und Datenträger VERNICHTEN.
¼ jährlich zb. Testrücksicherung aus Backup, Verarbeitungsverzeichnis und Toms aktualisieren, alte Mails & SMS löschen, Mitarbeiter Sensibilisierung & Schulung, Selbstevaluierung – ob Verbesserungsmaßnahmen beim Datenschutz möglich und umsetzbar sind? -> Umsetzen!
Jährlich: z.B. am Jahresbeginn: **Kalender DSGVO** – Termine eintragen, Belege vernichten / entsorgen, alte Daten löschen, Budget Planung Datenschutzmaßnahmen, etc.

Ich hoffe, mit dieser Anleitung haben Sie einen brauchbaren Wegweiser zur DSGVO-Umsetzung erhalten. Dies ist keine rechtsverbindliche -/gültige Information, Fehler und Irrtümer vorbehalten!

Mit besten Grüßen, Preisl Computer - Hermann Preisl.