Das Verfahrensverzeichnis.

Das wahrscheinlich wichtigste Formular, das die DSGVO verlangt!

Dieses Verzeichnis muss mit großer Wahrscheinlichkeit **jedes Unternehmen erstellen** und der Datenschutzbehörde vorweisen können. Daher beschäftigen wir uns heute ganz intensiv damit. Und präsentieren Ihnen eine Mustervorlage und geben Hinweise, wo was auszufüllen ist.

Eigentlich gäbe es in der DSGVO eine **Ausnahmeregel, die kleinen Firmen** diese Arbeit wohl ersparen sollte (weniger als 250 Mitarbeiter, kein Risiko für die Rechte der Betroffenen, nur gelegentliche Verarbeitung), aber laut Experten sind **die Formulierungen so unklar**, dass man besser diese Vorlage ausfüllt, um Stress mit der Behörde und letztlich auch die angedrohten (Millionen-)Strafen auf jeden Fall zu verhindern.

Im Verfahrensverzeichnis geht es darum, allgemein **zu dokumentieren, wo welche Daten anfallen, was man damit macht** (weitergeben?), wie lange man sie speichert etc.
Und sich auch technische und organisatorische Maßnahmen zur Datensicherung überlegt und diese ebenfalls niederschreibt. Experten vergleichen daher die DSGVO mit der ISO-Zertifizierung. Wo man sich ebenfalls die Prozesse ansieht und diese dokumentiert. Und durch das genaue Hinsehen entdeckt man potentielle Fehlerquellen und wird dadurch besser. Und reduziert somit das Risiko, dass die Daten gestohlen werden können, Fehler bei der Beauskunftung/ beim Löschwunsch passieren etc.

Das Verfahrensverzeichnis besteht aus 4 Blöcken:
A. Stammdatenblatt: Allgemeine Angaben
B. Datenverarbeitungen/Datenverarbeitungszwecke
C. Detailangaben zu den einzelnen Datenverarbeitungszwecken
D. Allgemeine Beschreibung organisatorisch-technischer Maßnahmen

Unter A), also im Stammdatenblatt, füllen Sie die **Kontaktdaten des Verantwortlichen** aus.
Spannende Frage dabei ist, ob Sie einen **Datenschutzverantwortlichen** (manchmal ist auch vom DS-Beauftragten die Rede) benötigen oder nur einen Datenschutzkoordinator einsetzen (der intern die Umsetzung der DSGVO vorantreibt und der Ansprechpartner intern und nach außen gegenüber der Behörde ist). Damit beschäftigen wir uns im nächsten Newsletter.

Unter **Position B)** füllen Sie aus, **bei welchen Verarbeitungen Daten anfallen.** Etwa beim Marketing (Newsletter), bei der Geschäftsabwicklung & im Rechnungswesen (Kundinnen und Kunden), in der Personalverwaltung (Mitarbeiterinnen und Mitarbeiter) usw.
Außerdem müssen Sie hier bekanntgeben, ob eine **Datenschutz-Folgenabschätzung** gemacht wurde. Wer eine solche machen muss und wer nicht, damit beschäftigen wir uns in einem der nächsten Newsletter.

Unter **Position C)** geben Sie Details zu **JEDER einzelnen Datenverarbeitung** (die Sie unter B aufgelistet haben) **an:** Welche Daten werden erfasst („Datenkategorien"), ob Sie sensible Daten verarbeiten („Datenkategorien nach Art. 9 bzw. 10 DSGVO") und wem Sie die Daten weitergeben. Was genau diese Datenkategorien sind, darüber informieren wir in einem der nächsten Newsletter.

Das Ergebnis für so eine Tabelle schaut dann in etwa so aus:

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO[10], strafrechtlich relevant iSd Art 10 DSGVO[11]	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden Im Anlassfall	Inkassounternehmen Im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
1	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	X	X	X	X	X	X	X	X	X	X
	2	Anschrift	Nein	X	X	X	X	X	X	X	X	X	X
	3	Kontaktdaten (Tel., Mail,Fax)	Nein	X	X	X	X	X	X	X	X	X	X
	4	Firmenbuchdaten	Nein	X	X	X	X	X	X	X	X	X	X
	5	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		X		X						
	6	Bankverbindungen	Nein	X	X	X	X	X	X	X	X	X	
	7	Kreditkartennummern und -unternehmen	Nein	X	X	X	X						
	8	UID-Nummer	Nein	X	X	X	X	X	X	X	X	X	
	9	Namen der Kontaktpersonen	Nein	X	X	X	X	X	X	X	X	X	X
	10	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.)	Nein	X	X	X	X	X	X	X	X	X	X
	11	Vertragstexte und Geschäftskorrespondenzen		X	X	X	X	X	X	X		X	

Graphik aus dem Muster-Verfahrensverzeichnis der WKO entnommen.

Danach geben Sie noch an, **wann eine Löschung erfolgt** („Aufbewahrung auf jeden Fall 7 Jahre aufgrund gesetzlicher Pflicht"; „bis zur Beendigung von Gewährleistungs- oder Garantiefristen" usw.)
Tipp: Sollte ein Löschwunsch einer Person einlangen, müssen Sie diesen nicht (komplett) erfüllen, wenn dies einer gesetzlichen (z.B. steuerliche Aufbewahrung etc.) oder vertraglichen Pflicht (Gewährleistung, Garantie etc.) widerspricht.
Am Ende von Position C) geben Sie noch die **Empfängerkategorien** an (also an wen Sie Daten weitergeben) und ob sich diese in einem Drittstaat oder bei einer internationalen Organisation befinden.

Unter **Position D)** beschreiben Sie Ihre **technischen und organisatorischen Maßnahmen**, die Sie setzen, um die gespeicherten Daten zu sichern.
Hier sind **5 Punkte** zu überlegen und zu dokumentieren – wobei hier immer abzuschätzen ist, was im Einzelfall zumutbar ist. Hier wird man bei größeren Firmen einen strengeren Maßstab anlegen als gegenüber EPUs.

a) Vertraulichkeit
Das könnte etwa umfassen:
Zutrittskontrolle (mechanisch oder Portier), Sicherheitstür, versperrbare Schränke etc.,
Zugangskontrolle (PC, Festplatten mit Passwort gesichert, Daten verschlüsselt etc.),
Zugriffskontrolle (wie verhindern Sie unbefugtes Lesen, Kopieren, Ändern, Löschen von Daten?).

b) Integrität:
Das könnte umfassen:
Eingabekontrolle (Klärung, ob und von wem Daten eingegeben, verändert, entfernt wurden – etwa durch Protokollierung, Dokumentenmanagement etc.)

Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Ändern, Löschen bei elektronischer Übertragung oder Transport z.B. durch Verschlüsselung, VPN-Übertragung (virtual private networks), digitale Signatur etc.
Zum Thema VPN bzw. E-Mail-Übertragung verweisen wir auf unseren entsprechenden Beitrag Nummer 1 in diesem Newsletter.

c) Verfügbarkeit und Belastbarkeit:
Unter diesem Punkt versteht man, dass Maßnahmen **zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust** getroffen wurden, also eine Backup-Strategie, Virenschutz, Firewall etc.
Wie man – auch mit einfachen, kostenlosen Programmen – ein Sicherungskonzept umsetzen kann, können Sie im bereits erschienenen **Beitrag „Praxistipp: Wie gegen Datenverlust schützen" nachlesen. Und zwar hier …**

d) Pseudonymisierung und Verschlüsselung:
Unter Pseudonymisierung versteht man das **Anonymisieren** von Daten: Falls möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten aus einer Datenanwendung entfernt und gesondert aufbewahrt. Also etwa die Sozialversicherungsnummer ausgelagert.
Betreffend Verschlüsselung sei auf das Windows-eigene Programm **Bitlocker** verwiesen.

e) Evaluierungsmaßnahmen:
Darunter fallen Datenschutz-Management (etwa Risikoanalyse, Datenschutz-Folgenabschätzung), aber auch regelmäßige Audits (ob sich etwas verändert hat, um Formulare, Prozesse anzupassen) sowie regelmäßige Mitarbeiter-**Schulungen.**

Sie sehen also, eine mächtige Aufgabe, die da vor Ihnen liegt. Wahrscheinlich erfordert es mehrere Anläufe, bis Sie alle Ihre Datenverarbeitungsprozesse eruiert und alle Details dazu „zusammengetragen" haben. Umso wichtiger ist es, dass Sie umgehend damit beginnen.
Im nächsten Newsletter beschäftigen wir uns mit den **weiteren Formularen**, die wir ausfüllen bzw. vorrätig haben müssen (Meldung an Behörde bei Data-Breach, also Hacker-Angriff, etc.) und was sich auf **der Homepage durch die DSGVO ändern muss.**

Die **Vorlage** des Verfahrensverzeichnisses **finden Sie hier** zum Herunterladen.

Quellen: B2B-Projekte Mag. Günter Wagner, Praxishandbuch „Das österreichische Versicherungsvermittlerrecht", Kommentare von Rechtsanwalt Mag. Stephan Novotny und Datenschutzexperte Mag. Georg Markus Kainz, Vorlagen der WKO zur DSGVO