Data-Protection-Service

. . . DER SICHERE WEG

Datenschutz im Unternehmen

Konsequenzen bei Nichterfüllung

Richtige Umsetzung

Vortrag Landes Innung SH-HH Rollladen und Sonnenschutz 16.02.2023

André Schombel
Externer Datenschutzbeauftragter
www.data-protection-service.de
a.schombel@data-protection-service.de
Tel: 040- 97 07 19 15

Seit dem 25.05.2018 gilt in ganz Europa ein neues Datenschutzrecht.

Zentrale Botschaft des Bundesdatenschutz-Gesetzes: (BDSG)

Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Zentrale Botschaft der Datenschutzgrundverordnung: (DSGVO)

Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen

Datenschutz im Unternehmen

Data-Protection-Service
. . . DER SICHERE WEG

Der Datenschutz umfasst laut DSGVO…

… die Verarbeitung von personenbezogenen Daten in Unternehmen.

… gilt nur für Daten von natürlichen Personen (Menschen), nicht für juristische Personen (GmbH, AG, Vereine)

… jegliche Erfassung, Speicherung, Verarbeitung sowie Löschung und das Sperren von personenbezogenen Daten.

Wo? In Datenbanken oder Computer oder Listen, Notizen, Formulare, Reparaturaufträgen, Dienstleistungs-nachweise sowie in einem Dateisystem (Datei, Ordner, Kalender)

… dies betrifft Kunden, Mitarbeiter, Vertragspartner etc. als auch Steuerdaten, Gesundheitsdaten

Datenschutz im Unternehmen

Data-Protection-Service
. . . DER SICHERE WEG

Beispiel: Elektronische Arbeitszeiterfassung

1. Kein Erahnen der Erkrankung durch den Facharztstempel
2. Zusätzliche Daten, weil Mini Jobber die KKH nennen müssen
3. AU-Bescheinigung nach Hinweis der erkrankten Personen elektronisch bei der KKH anfordern.
4. Unternehmen müssen mit Papierunterlagen als auch mit digitalen Bescheinigungen arbeiten. (TOM´s erforderlich)
5. Verarbeitungsverzeichnis muss entsprechend angepasst werden
6. Veröffentlichung an Schaubrettern (Schichtpläne) nur mit Einverständnis des Mitarbeiters
7. Keine unerlaubte Weitergabe an Dritte (Kunden, Kollegen)

Datenschutz im Unternehmen

Data-Protection-Service
. . . DER SICHERE WEG

Unbedachte und eigentlich unverfänglich wirkende Aussagen zur Krankmeldung, verstoßen gegen den Datenschutz

Unbedachte Aussagen zu Krankmeldungen

„Frau Müller fällt diese Woche aus gesundheitlichen Gründen aus, daher übernimmt solange Herr Meyer ihre Aufgaben.“

FALSCH

Arbeitgeber oder Vorgesetze gibt weiter, dass Frau Müller krank ist und wie lange die voraussichtliche Arbeitsunfähigkeit besteht

Unkonkrete Formulierungen zu nutzen

„Frau Müller ist für diese Woche nicht im Haus.“

RICHTIG

Diese allgemeine Aussage lässt keine konkreten Rückschlüsse auf den Gesundheitszustand der Angestellten zu und schützt somit deren Privatsphäre

Datenschutz im Unternehmen

Data-Protection-Service
. . . DER SICHERE WEG

Konsequenzen bei Datenschutz Verstößen

Geldbußen für DSGVO-Verstöße

und für Verletzungen anderer Datenschutzgesetze

Deutschl... | Suchen

Datum	€ Bußgeld	Empfänger	Land	Vergehen
26.01.2023	9.000 €	Universitätsklinikum Magdeburg	DE	Unterlassen der Informationspflicht über Datendiebstahl durch Klinikmitarbeiterin »Details
21.09.2022	50.000 €	Unbekanntes Bauunternehmen	DE	Unzulässige Einsichtnahme in Grundbuch für Kaufangebot von Bauland. »Details
21.09.2022	5.000 €	Vermessungsingenieur	DE	Unzulässige Einsichtnahme in Grundbuch für Kaufangebot von Bauland. »Details
20.09.2022	525.000 €	Tochtergesellschaft eines E-Commerce-Konzerns	DE	Interessenkonflikt des betrieblichen Datenschutzbeauftragten. »Details
28.07.2022	900.000 €	Hannoversche Volksbank	DE	Auswertung von Kundendaten ohne Rechtsgrundlage. »Details

Ein Verstoß gegen die Regeln und Pflichten der DSGVO kann ein Bußgeld nach sich ziehen.

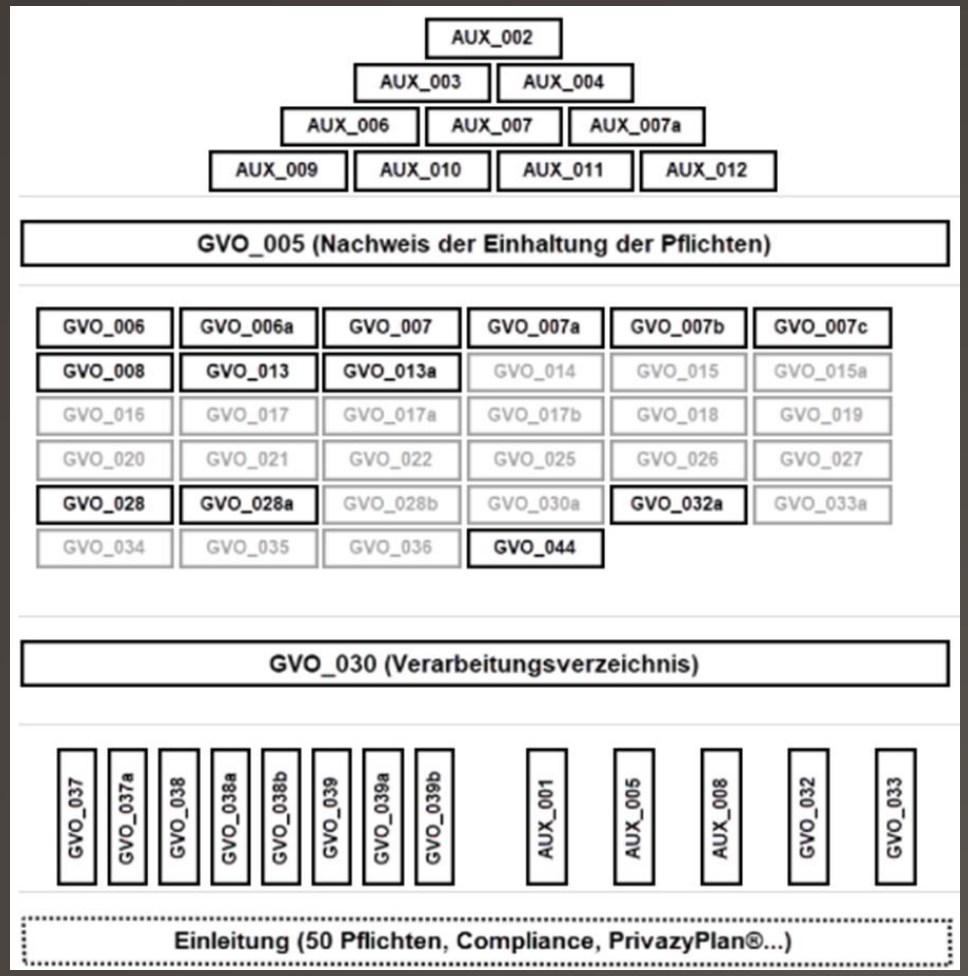
Quelle: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

27.01.2022	10.110 €	Autohandel	DE	Übermittlung eines Gesundheitsdatums eines Beschäftigten an über 3.000 Kunden ohne Rechtsgrundlage. »Details

Umsetzung des Datenschutzes im Unternehmen

Data-Protection-Service
. . . DER SICHERE WEG

Die Analogie zum Hausbau zeigt die Reihenfolge auf, in der die Pflichten bearbeitet werden sollten.



Ein Haus baut man von unten nach oben. Genauso ist es mit den datenschutzrechtlichen Pflichten.

Die Baugrube

Datenschutz verstehen

Umsetzung des Datenschutzes im Unternehmen

Bußgeldrelevante Regeln und Pflichten der DSGVO /BDSG

Data-Protection-Service
. . . DER SICHERE WEG

14.3 Pflichten in tabellarischer Form

Anhang

Für einen besseren Überblick können Sie sich diese Seite ausdrucken (weitere Tipps für einen guten Überblick gibt es auf Seite 12).
Wo können Sie die Arbeitsergebnisse speichern, wenn sie diese Pflichten erfüllen? Wir empfehlen die Verzeichnisstruktur der PrivazyPlan.zip auf Seite 29.

Pflichten aufgrund von Persönlichkeitsrechten

Im Kapitel 2 werden alle „typischen" Persönlichkeitsrechte erklärt:

2.1	Bei Erhebung von Daten ausführlich informieren [GVO_013]	Artikel 13 (1,2)	41
2.2	Zweckänderung vorab mitteilen [GVO_013a]	Artikel 13 (3)	47
2.3	Bei Erhebung von Daten über Dritte informieren [GVO_014]	Artikel 14	51
2.4	Auskunft erteilen [GVO_015]	Artikel 15 (1,2)	56
2.5	Datenkopie aushändigen [GVO_015a]	Artikel 15 (3,4)	59
2.6	Berichtigung ermöglichen [GVO_016]	Artikel 16	71
2.7	Löschen aus betrieblichen Gründen [GVO_017]	Artikel 17 (1)	73
2.8	Löschen auf Verlangen der betroffenen Person [GVO_017a]	Artikel 17 (1)	76
2.9	Löschen veröffentlichter Daten („Recht auf Vergessenwerden") [GVO_017b]	Artikel 17 (2)	79
2.10	Einschränkung der Verarbeitung [GVO_018]	Artikel 18	82
2.11	Korrektur bei Dritten (Nachberichtigung) [GVO_019]	Artikel 19	86
2.12	Datenübertragbarkeit ermöglichen [GVO_020]	Artikel 20	90
2.13	Widerspruchsrecht einräumen [GVO_021]	Artikel 21	95
2.14	Automatisierte Entscheidung vermeiden [GVO_022]	Artikel 22	99

Pflichten zu Dokumentationen und Nachweisen

Im Kapitel 3 geht es um den allgemeinen „Dokumentationsaufwand":

3.1	Nachweis der Einhaltung der „Grundsätze" [GVO_005]	Artikel 5 (2)	104
3.2	Datenschutzfreundliche Technikgestaltung und Voreinstellungen [GVO_025]	Artikel 25	108
3.3	Verarbeitungsverzeichnis des Verantwortlichen [GVO_030]	Artikel 30 (1)	112
3.4	Verarbeitungsverzeichnis des Auftragsverarbeiters [GVO_030a]	Artikel 30 (2)	118

Pflichten zu Rechtmäßigkeit und Einwilligung

Im Kapitel 4 wird die Rechtmäßigkeit (inkl. zahlreicher Einwilligungs-Aspekten) erklärt:

4.1	Datenverarbeitungen brauchen eine Rechtsgrundlage [GVO_006]	Artikel 6 (1)	124
4.2	Zweckänderungen müssen sorgsam geprüft werden [GVO_006a]	Artikel 6 (4)	140
4.3	Einwilligungen müssen dauerhaft nachweisbar sein [GVO_007]	Artikel 7 (1)	145
4.4	Einwilligungstexte müssen klar erkennbar und gut verständlich sein [GVO_007a]	Artikel 7 (2)	149
4.5	Einwilligung muss jederzeit (und einfach) widerrufbar sein [GVO_007b]	Artikel 7 (3)	151
4.6	Die Freiwilligkeit von Einwilligungen muss unbestreitbar sein [GVO_007c]	Artikel 7 (4)	154
4.7	Einwilligungen von Kindern durch Eltern legitimieren [GVO_008]	Artikel 8 (2)	158

Pflichten zu Sicherheit und Datenschutzverletzungen

Im Kapitel 5 wird die Informationssicherheit erläutert und Datenschutzverletzungen behandelt:

5.1	Informations-Sicherheits-Managementsystem einrichten [GVO_032]	Artikel 32 (1)	161
5.2	Beschäftigte Personen sind konkret anzuweisen [GVO_032a]	Artikel 32 (4)	168
5.3	Datenschutzverletzungen dauerhaft dokumentieren [GVO_033]	Artikel 33 (5)	173
5.4	Datenschutzverletzungen an Aufsichtsbehörde melden [GVO_033a]	Artikel 33 (1)	177
5.5	Betroffene Person über Datenschutzverletzung benachrichtigen [GVO_034]	Artikel 34 (1)	181

Pflichten zur Datenschutz-Folgenabschätzung und Konsultation

Im Kapitel 6 werden die Folgen eine Datenverarbeitung abgeschätzt und ggf. die Aufsichtsbehörde einbezogen:

6.1	Datenschutz-Folgenabschätzung [GVO_035]	Artikel 35	185
6.2	Konsultation der Aufsichtsbehörde [GVO_036]	Artikel 36	192

Pflichten in Hinblick auf andere Verantwortliche

Im Kapitel 7 dreht sich alles um verschiedene Formen des „Outsourcings":

7.1	Gemeinsame Verantwortlichkeit [GVO_026]	Artikel 26	195
7.2	EU-Vertreter benennen [GVO_027]	Artikel 27	208
7.3	Auftragsverarbeitung detailliert regeln [GVO_028]	Artikel 28	211
7.4	Auftragsverarbeitung streng nach Weisung durchführen [GVO_028a]	Artikel 28 (3a)	218
7.5	Auftragsdatenverarbeitung aus BDSG übernehmen [GVO_028b]	Artikel 28 (3)	225
7.6	Datentransfer an Drittländer ist stark reglementiert [GVO_044]	Artikel 44	227

Pflichten zur Benennung eines Datenschutzbeauftragten etc.

Im Kapitel 8 wird die betriebliche Einbindung des Datenschutzbeauftragten (DSB) beschrieben und seine Aufgaben erläutert:

8.1	Benennung eines Datenschutzbeauftragten [GVO_037]	Artikel 37 (1)	241
8.2	Bekanntmachung des Datenschutzbeauftragten [GVO_037a]	Artikel 37 (7)	248
8.3	Frühzeitige Einbindung des Datenschutzbeauftragten [GVO_038]	Artikel 38 (1)	251
8.4	Unterstützung des Datenschutzbeauftragten [GVO_038a]	Artikel 38 (2)	254
8.5	DSB als Anlaufstelle für betroffene Personen [GVO_038b]	Artikel 38 (4)	256
8.6	Unterrichtung und Beratung hinsichtlich der Pflichten [GVO_039]	Artikel 39 (1a)	258
8.7	Überwachung der Einhaltung von Datenschutzvorschriften [GVO_039a]	Artikel 39 (1b)	260
8.8	Anlaufstelle für Aufsichtsbehörde und Zusammenarbeit [GVO_039b]	Artikel 39 (1e)	263

Pflichten aus sonstigen Datenschutzvorschriften

Im Kapitel 9 geht es um datenschutzrelevante Vorschriften aus anderen Gesetzen. Die hier genannten Beispiele können für Unternehmen in Deutschland relevant sein:

9.6.1	Berufliche Schweigepflicht [STGB_203]	§ 203 StGB	278
9.6.2	Unzumutbare Werbe-Belästigungen [UWG_007]	§ 7 UWG	279
9.6.3	Jugendschutz in Telemedien nicht kommerzialisieren [TTDSG_020]	§ 20 TTDSG	281
9.6.4	Privatsphäre im Webbrowser etc. [TTDSG_025]	§ 25 TTDSG	282

Pflichten durch das neue Bundesdatenschutzgesetz

Im Kapitel 10 geht es um datenschutzrelevante Vorschriften, die der deutsche Gesetzgeber aufgrund der Öffnungsklauseln nutzt. Die hier genannten Pflichten sind speziell für Unternehmen in Deutschland relevant:

~~10.1~~	~~OBSOLET: Videoüberwachungen kenntlich machen~~	~~§ 4 Abs. 2~~	~~287~~
~~10.2~~	~~OBSOLET: Identifizierte Personen von Videoüberwachung informieren [BDSG_004a]~~	~~§ 4 Abs. 4~~	~~288~~
10.3	Sicherheitsmaßnahmen bei sensiblen Daten [BDSG_022]	§ 22 Abs. 2	289
10.4	Sensible Forschungsdaten anonymisieren [BDSG_027]	§ 27 Abs. 3	291
10.5	Auskunftei muss EU-Darlehensgebern Auskunft geben [BDSG_030]	§ 30 Abs. 1	293
10.6	Abgelehnte Finanzierung muss Auskunftei als Grundlage nennen [BDSG_030a]	§ 30 Abs. 2	294
10.7	Verweigerung von Auskünften dokumentieren etc. [BDSG_034]	§ 34	295
10.8	Verarbeitungs-Einschränkung anstelle Löschung kommunizieren [BDSG_035]	§ 35 Abs. 2	297

„Weiche" Pflichten (die nicht bußgeldbewehrt sind, sondern eher „Strategien" darstellen)

Im Kapitel 12.1.7 wird eine Reihe von **Strategien** erwähnt, die der Datenschutzbeauftragte ebenfalls überwachen könnte.

1.)	Beschäftige schulen und zur Vertraulichkeit verpflichten [AUX_001]	326
2.)	Beschäftigte unterliegen einer Regelung zur Privatnutzung [AUX_002]	326
3.)	Beschäftigte unterzeichnen EDV-Nutzungsvereinbarung [AUX_003]	327
4.)	Datenschutz beim Betriebsrat regeln [AUX_004]	328
5.)	Grundlegende Anforderungen an Websites und Apps [AUX_005]	328
6.)	Erstellen und veröffentlichen von Fotos durch Journalisten [AUX_006]	330
7.)	Stammblatt einer jeden Verarbeitung erzeugen [AUX_007]	330
8.)	Stammblätter sind komplett bearbeitet [AUX_007a]	330
9.)	Datenschutz-Managementsystem einrichten [AUX_008]	330
10.)	Bring your own device ("BYOD") [AUX_009]	331
11.)	Lösch-Konzept (Akten, Datenträger, Löschverlangen) [AUX_010]	332
12.)	Transparenztext einer jeden Verarbeitung erstellen [AUX_011]	332
13.)	Korrekter Umgang mit Videoüberwachungen [AUX_012]	333

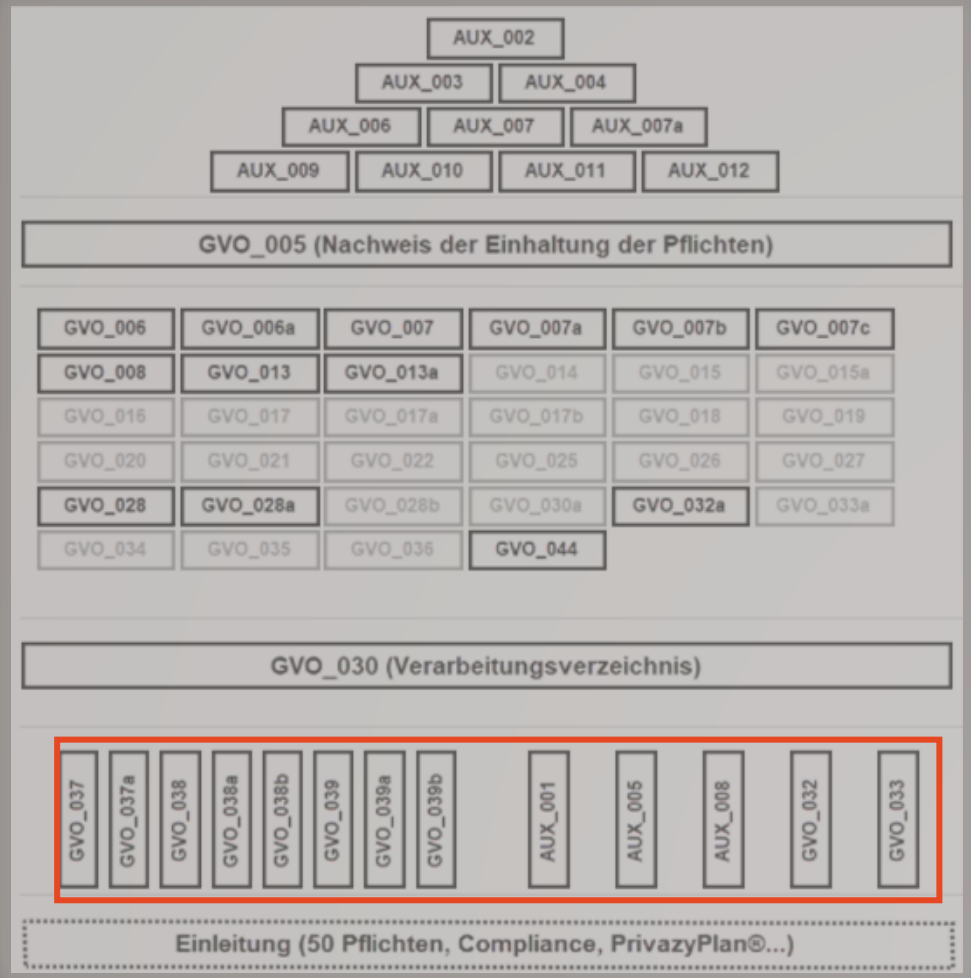
Umsetzung des Datenschutzes im Unternehmen

1. Benennung Datenschutzbeauftragten
2. Datenschutz Management System einrichten
3. Beschäftigte sensibilisieren und zur Vertraulichkeit verpflichten
4. Regelungen der Privatnutzung (Mail, Internet, etc.)
5. Grundlegende Anforderungen an Websites und Apps

Das Fundament

Compliance (regelgetreuer Datenschutz)

Der rechtskonforme und redliche Umgang mit personenbezogenen Daten ist gefordert. Das nennt sich "Compliance"... und ist eine dauerhafte Anstrengung.



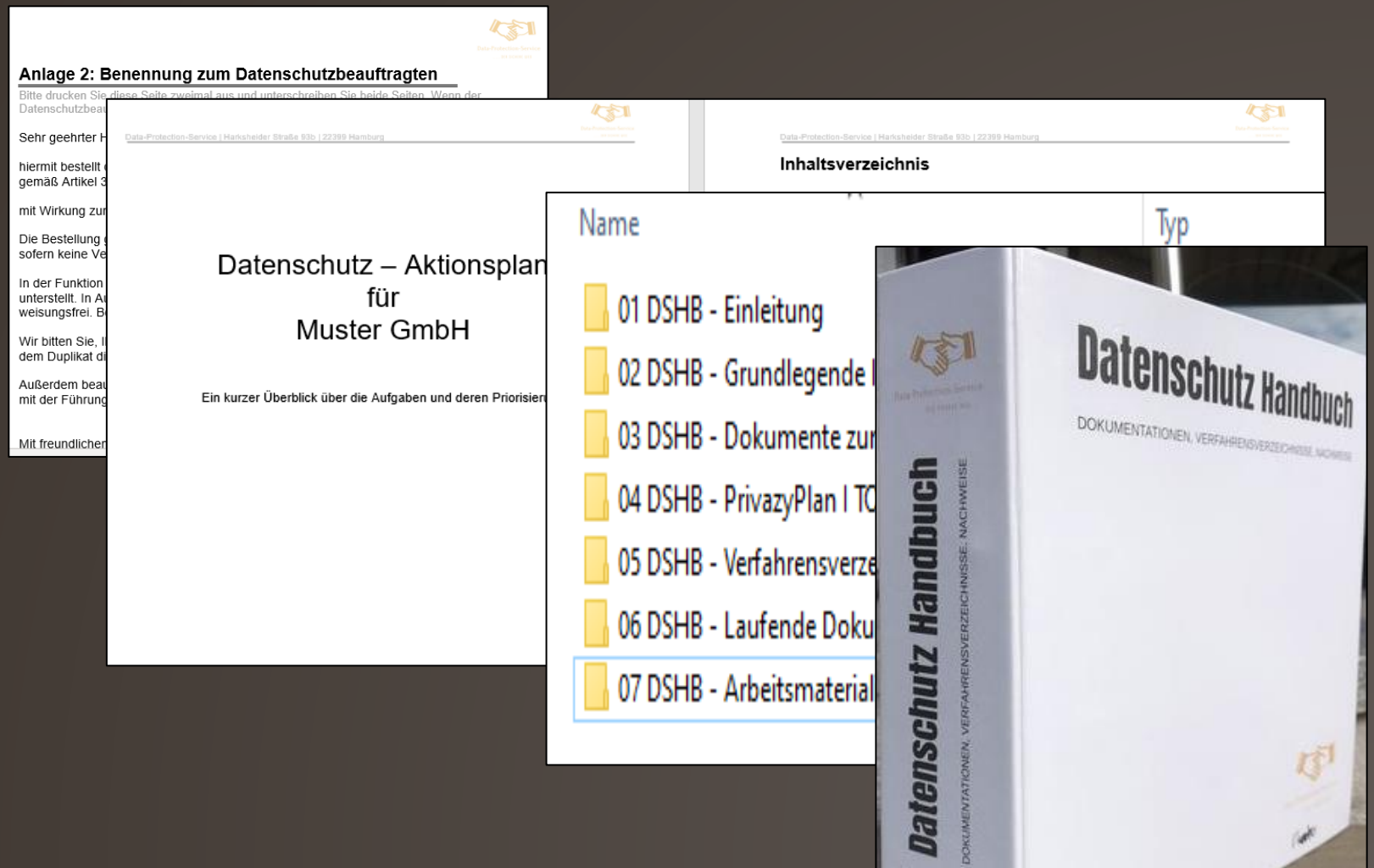
Umsetzung des Datenschutzes im Unternehmen

1. Benennung Datenschutzbeauftragten
2. Datenschutz Management System einrichten
3. Beschäftigte sensibilisieren und zur Vertraulichkeit verpflichten
4. Regelungen der Privatnutzung (Mail, Internet, etc.)
5. Grundlegende Anforderungen an Websites und Apps

Das Fundament

Compliance (regelgetreuer Datenschutz)

Der rechtskonforme und redliche Umgang mit personenbezogenen Daten ist gefordert. Das nennt sich "Compliance"... und ist eine dauerhafte Anstrengung.



Umsetzung des Datenschutzes im Unternehmen

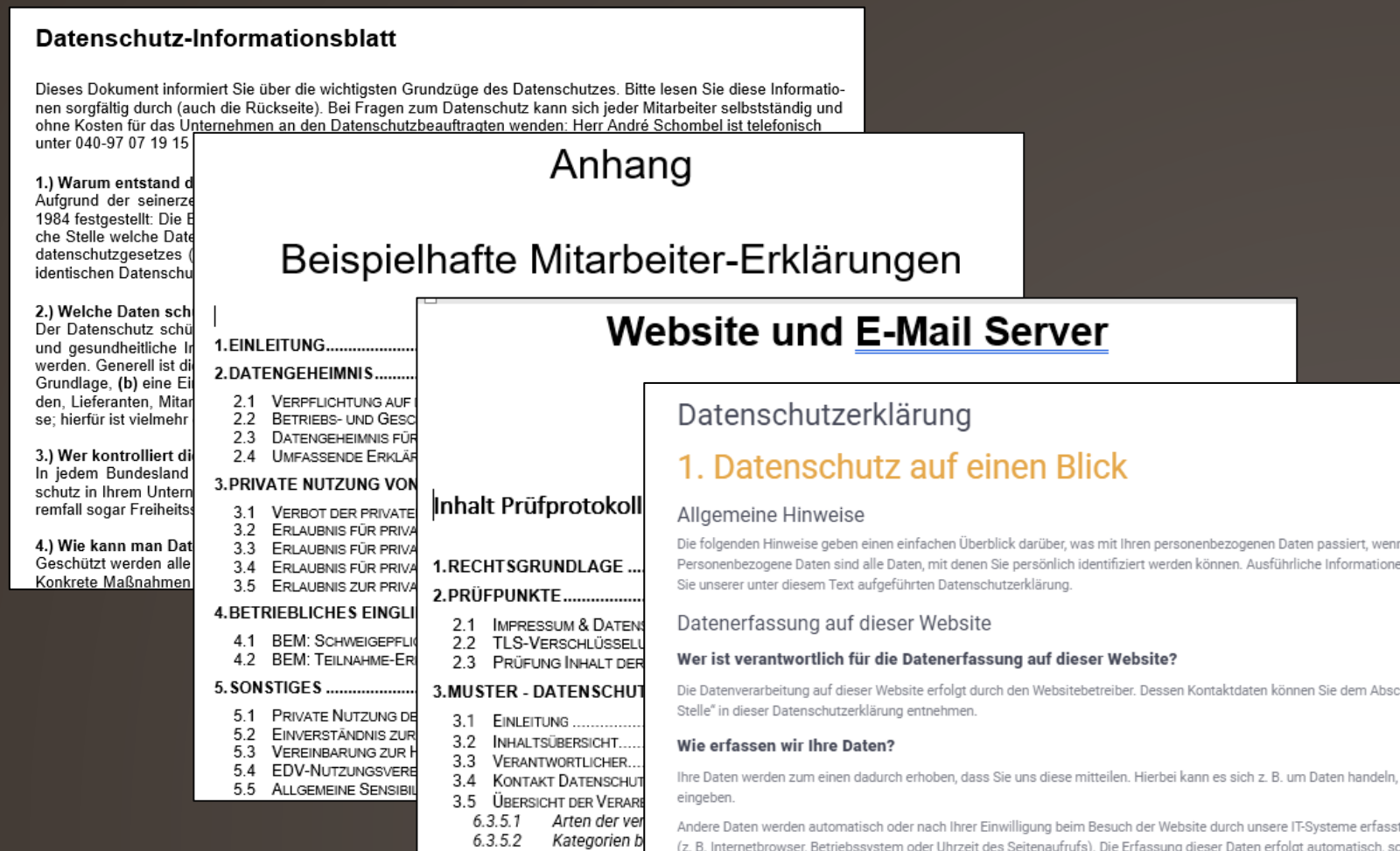
1. Benennung Datenschutzbeauftragten
2. Datenschutz Management System einrichten
3. Beschäftigte sensibilisieren und zur Vertraulichkeit verpflichten
4. Regelungen der Privatnutzung (Mail, Internet, etc.)
5. Grundlegende Anforderungen an Websites und Apps

Data-Protection-Service
. . . DER SICHERE WEG

Das Fundament

Compliance (regelgetreuer Datenschutz)

Der rechtskonforme und redliche Umgang mit personenbezogenen Daten ist gefordert. Das nennt sich "Compliance"... und ist eine dauerhafte Anstrengung.



Umsetzung des Datenschutzes im Unternehmen

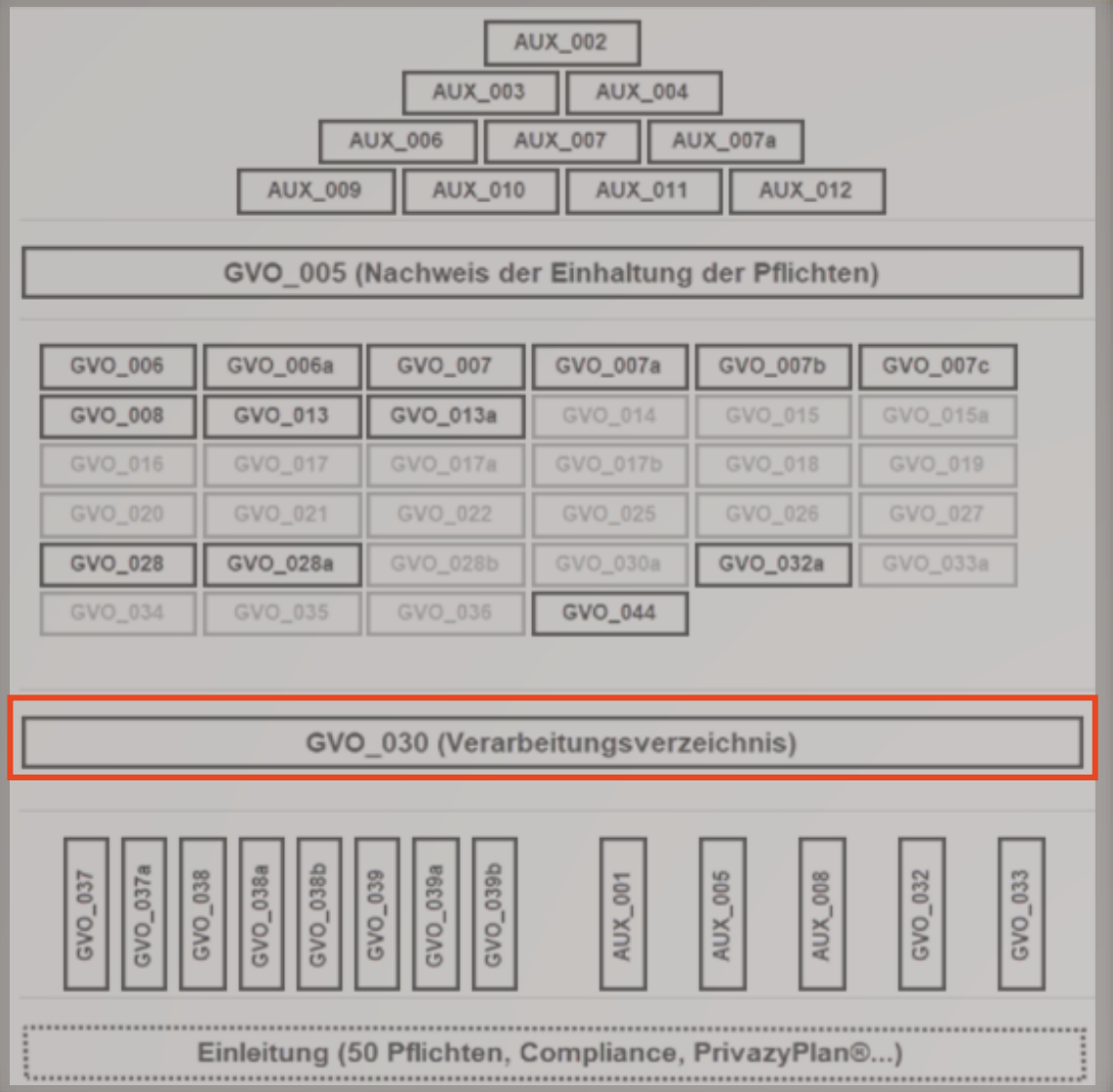
1. Verarbeitungsverzeichnis des Verantwortlichen

Data-Protection-Service
DER SICHERE WEG

Die Bodenplatte

Basis für alle anderen Pflichten

Dokumentation aller Verarbeitungen von personenbezogenen Daten im sogenannten "Verarbeitungsverzeichnis".



Umsetzung des Datenschutzes im Unternehmen

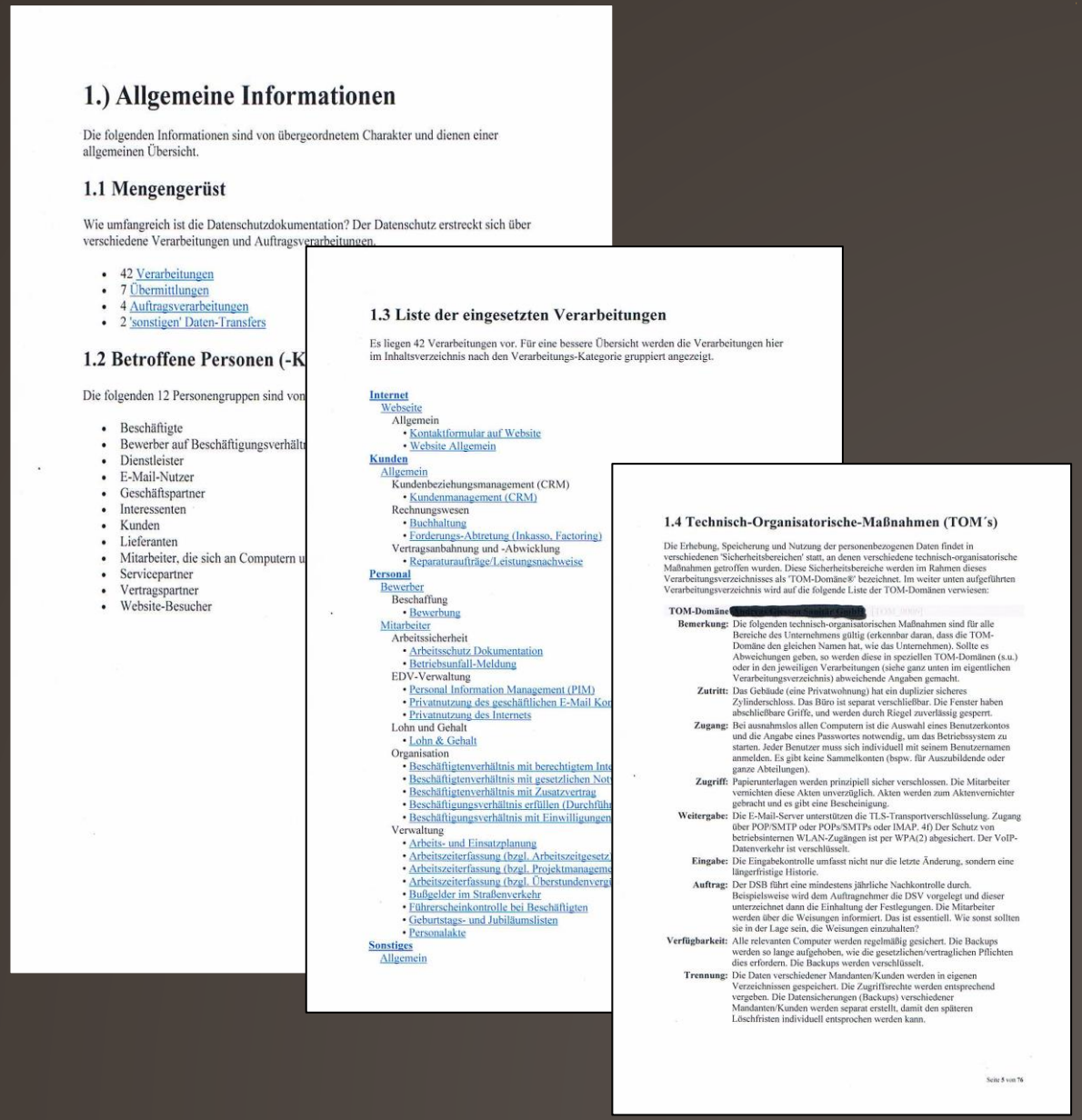
1. Verarbeitungsverzeichnis des Verantwortlichen

Data-Protection-Service
. . . DER SICHERE WEG

Die Bodenplatte

Basis für alle anderen Pflichten

Dokumentation aller Verarbeitungen von personenbezogenen Daten im sogenannten "Verarbeitungsverzeichnis".



1.) Allgemeine Informationen

Die folgenden Informationen sind von übergeordnetem Charakter und dienen einer allgemeinen Übersicht.

1.1 Mengengerüst

Wie umfangreich ist die Datenschutzdokumentation? Der Datenschutz erstreckt sich über verschiedene Verarbeitungen und Auftragsverarbeitungen.

- 42 Verarbeitungen
- 7 Übermittlungen
- 4 Auftragsverarbeitungen
- 2 'sonstigen' Daten-Transfers

1.2 Betroffene Personen (-K

Die folgenden 12 Personengruppen sind von

- Beschäftigte
- Bewerber auf Beschäftigungsverhält
- Dienstleister
- E-Mail-Nutzer
- Geschäftspartner
- Interessenten
- Kunden
- Lieferanten
- Mitarbeiter, die sich an Computern u
- Servicepartner
- Vertragspartner
- Website-Besucher

1.3 Liste der eingesetzten Verarbeitungen

Es liegen 42 Verarbeitungen vor. Für eine bessere Übersicht werden die Verarbeitungen hier im Inhaltsverzeichnis nach den Verarbeitungs-Kategorie gruppiert angezeigt.

Internet
Webseite
Allgemein
• Kontaktformular auf Website
• Website Allgemein
Kunden
Allgemein
Kundenbeziehungsmanagement (CRM)
• Kundenmanagement (CRM)
Rechnungswesen
• Buchhaltung
• Forderungs-Abtretung (Inkasso, Factoring)
Vertragsanbahnung und -Abwicklung
• Reparaturaufträge/Leistungsnachweise
Personal
Bewerber
Beschaffung
• Bewerbung
Mitarbeiter
Arbeitssicherheit
• Arbeitsschutz Dokumentation
• Betriebsunfall-Meldung
EDV-Verwaltung
• Personal Information Management (PIM)
• Privatnutzung des geschäftlichen E-Mail Kon
• Privatnutzung des Internets
Lohn und Gehalt
• Lohn & Gehalt
Organisation
• Beschäftigtenverhältnis mit berechtigtem Inte
• Beschäftigtenverhältnis mit gesetzlichen Not
• Beschäftigtenverhältnis mit Zusatzvertrag
• Beschäftigungsverhältnis erfüllen (Durchführ
• Beschäftigungsverhältnis mit Einwilligungen
Verwaltung
• Arbeits- und Einsatzplanung
• Arbeitszeiterfassung (bzgl. Arbeitszeitgesetz
• Arbeitszeiterfassung (bzgl. Projektmanageme
• Arbeitszeiterfassung (bzgl. Überstundenvergü
• Bußgelder im Straßenverkehr
• Führerscheinkontrolle bei Beschäftigten
• Geburtstags- und Jubiläumslisten
• Personalakte
Sonstiges
Allgemein

1.4 Technisch-Organisatorische-Maßnahmen (TOM´s)

Die Erhebung, Speicherung und Nutzung der personenbezogenen Daten findet in verschiedenen 'Sicherheitsbereichen' statt, an denen verschiedene technisch-organisatorische Maßnahmen getroffen wurden. Diese Sicherheitsbereiche werden im Rahmen dieses Verarbeitungsverzeichnisses als 'TOM-Domäne®' bezeichnet. Im weiter unten aufgeführten Verarbeitungsverzeichnis wird auf die folgende Liste der TOM-Domänen verwiesen:

TOM-Domäne [redacted]

Bemerkung: Die folgenden technisch-organisatorischen Maßnahmen sind für alle Bereiche des Unternehmens gültig (erkennbar daran, dass die TOM-Domäne den gleichen Namen hat, wie das Unternehmen). Sollte es Abweichungen geben, so werden diese in speziellen TOM-Domänen (s.u.) oder in den jeweiligen Verarbeitungen (siehe ganz unten im eigentlichen Verarbeitungsverzeichnis) abweichende Angaben gemacht.

Zutritt: Das Gebäude (eine Privatwohnung) hat ein duplizier sicheres Zylinderschloss. Das Büro ist separat verschließbar. Die Fenster haben abschließbare Griffe, und werden durch Riegel zuverlässig gesperrt.

Zugang: Bei ausnahmslos allen Computern ist die Auswahl eines Benutzerkontos und die Angabe eines Passwortes notwendig, um das Betriebssystem zu starten. Jeder Benutzer muss sich individuell mit seinem Benutzernamen anmelden. Es gibt keine Sammelkonten (bspw. für Auszubildende oder ganze Abteilungen).

Zugriff: Papierunterlagen werden prinzipiell sicher verschlossen. Die Mitarbeiter vernichten diese Akten unverzüglich. Akten werden zum Aktenvernichter gebracht und es gibt eine Bescheinigung.

Weitergabe: Die E-Mail-Server unterstützen die TLS-Transportverschlüsselung. Zugang über POP/SMTP oder POPs/SMTPs oder IMAP. 4f) Der Schutz von betriebsinternen WLAN-Zugängen ist per WPA(2) abgesichert. Der VoIP-Datenverkehr ist verschlüsselt.

Eingabe: Die Eingabekontrolle umfasst nicht nur die letzte Änderung, sondern eine längerfristige Historie.

Auftrag: Der DSB führt eine mindestens jährliche Nachkontrolle durch. Beispielsweise wird dem Auftragnehmer die DSV vorgelegt und dieser unterzeichnet dann die Einhaltung der Festlegungen. Die Mitarbeiter werden über die Weisungen informiert. Das ist essentiell. Wie sonst sollten sie in der Lage sein, die Weisungen einzuhalten?

Verfügbarkeit: Alle relevanten Computer werden regelmäßig gesichert. Die Backups werden so lange aufgehoben, wie die gesetzlichen/vertraglichen Pflichten dies erfordern. Die Backups werden verschlüsselt.

Trennung: Die Daten verschiedener Mandanten/Kunden werden in eigenen Verzeichnissen gespeichert. Die Zugriffsrechte werden entsprechend vergeben. Die Datensicherungen (Backups) verschiedener Mandanten/Kunden werden separat erstellt, damit den späteren Löschfristen individuell entsprochen werden kann.

Seite 5 von 76

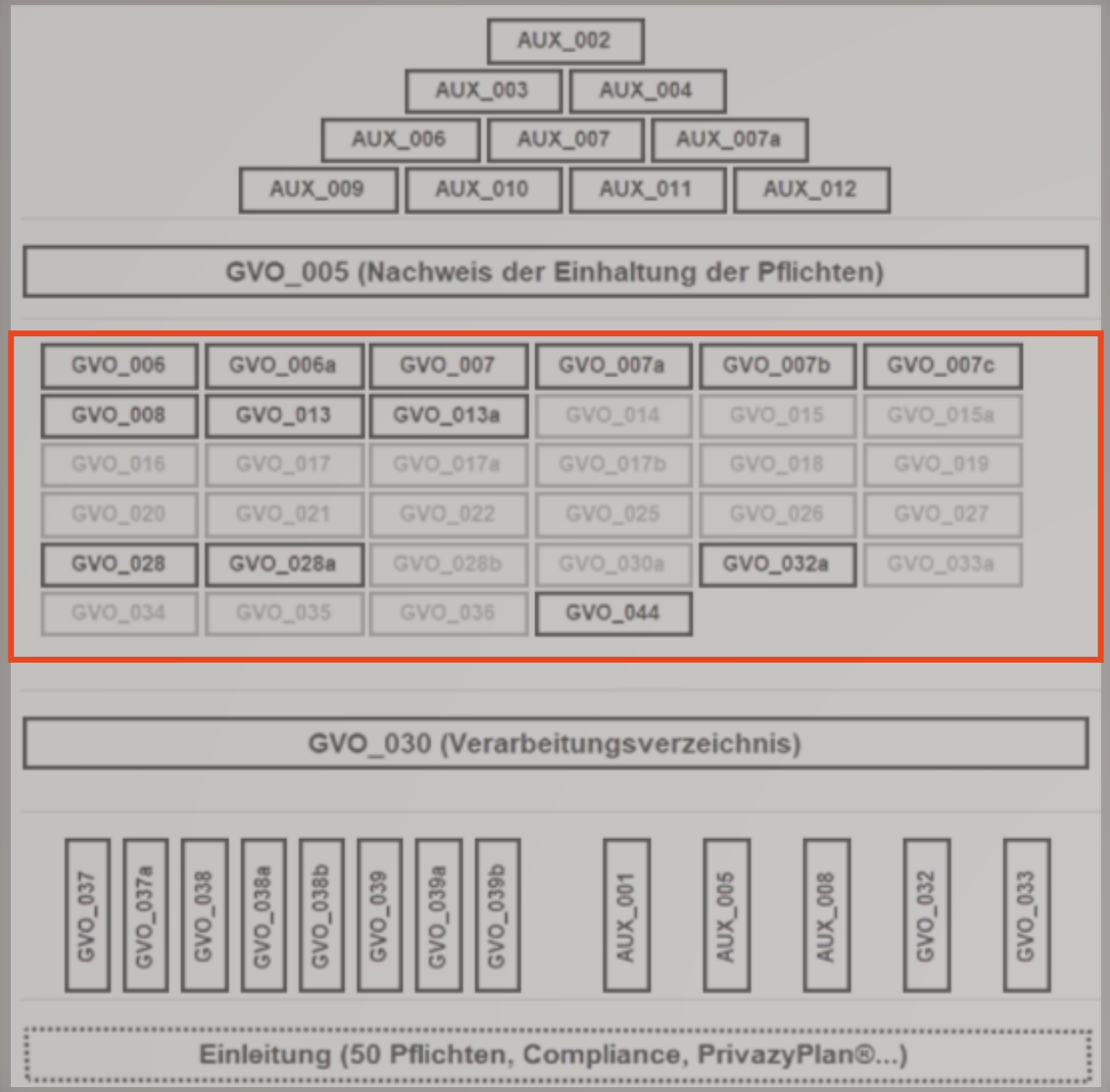
Umsetzung des Datenschutzes im Unternehmen

1. Verarbeitungen kennen
2. Rechtsgrundlage und Zweck der Datenverarbeitung
3. Ausführlich über die Datenerhebung informieren
4. Auftragsdatenverarbeitungen abschließen

Die Mauern

Mauern der einzelnen Räume

Jeder "Raum" ist eine "Verarbeitung" von personenbezogenen Daten. Diese Pflichten müssen also auf jede (Daten-) Verarbeitung angewendet werden.



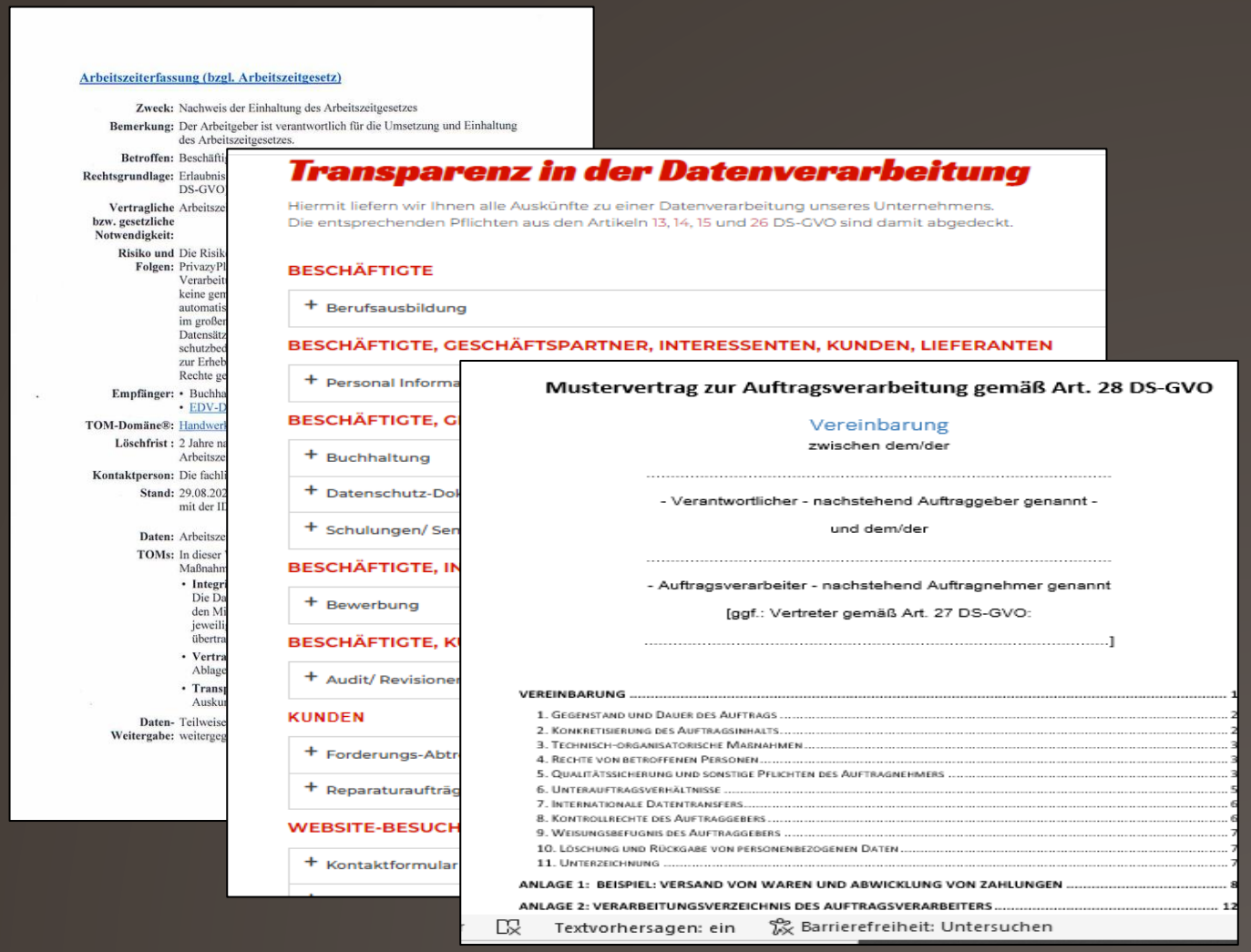
Umsetzung des Datenschutzes im Unternehmen

1. Verarbeitungen kennen
2. Rechtsgrundlage und Zweck der Datenverarbeitung
3. Ausführlich über die Datenerhebung informieren
4. Auftragsdatenverarbeitungen abschließen

Die Mauern

Mauern der einzelnen Räume

Jeder "Raum" ist eine "Verarbeitung" von personenbezogenen Daten. Diese Pflichten müssen also auf jede (Daten-) Verarbeitung angewendet werden.



Arbeitszeiterfassung (bzgl. Arbeitszeitgesetz)

Zweck: Nachweis der Einhaltung des Arbeitszeitgesetzes

Bemerkung: Der Arbeitgeber ist verantwortlich für die Umsetzung und Einhaltung des Arbeitszeitgesetzes.

Betroffen: Beschäfti

Rechtsgrundlage: Erlaubnis DS-GVO

Vertragliche bzw. gesetzliche Notwendigkeit: Arbeitsze

Risiko und Folgen: Die Risik PrivazyPl Verarbeit keine gen automatis im großer Datensätz schutzbed zur Erheb Rechte ge

Empfänger: • Buchha • EDV-D

TOM-Domäne®: Handwerk

Löschfrist : 2 Jahre na Arbeitsze

Kontaktperson: Die fachli

Stand: 29.08.202 mit der II

Daten: Arbeitsze

TOMs: In dieser Maßnahm
- **Integri** Die Da den Mi jeweili übertra
- **Vertra** Ablage
- **Transp** Auskun

Daten-Weitergabe: Teilweise weitergeg

Transparenz in der Datenverarbeitung

Hiermit liefern wir Ihnen alle Auskünfte zu einer Datenverarbeitung unseres Unternehmens.
Die entsprechenden Pflichten aus den Artikeln 13, 14, 15 und 26 DS-GVO sind damit abgedeckt.

BESCHÄFTIGTE

+ Berufsausbildung

BESCHÄFTIGTE, GESCHÄFTSPARTNER, INTERESSENTEN, KUNDEN, LIEFERANTEN

+ Personal Informa

BESCHÄFTIGTE, G

+ Buchhaltung
+ Datenschutz-Dok
+ Schulungen/ Sen

BESCHÄFTIGTE, IN

+ Bewerbung

BESCHÄFTIGTE, K

+ Audit/ Revisione

KUNDEN

+ Forderungs-Abtr
+ Reparaturauftrag

WEBSITE-BESUCH

+ Kontaktformular

Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung
zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

VEREINBARUNG 1
1. Gegenstand und Dauer des Auftrags 2
2. Konkretisierung des Auftragsinhalts 2
3. Technisch-organisatorische Maßnahmen 3
4. Rechte von betroffenen Personen 3
5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 3
6. Unterauftragsverhältnisse 5
7. Internationale Datentransfers 6
8. Kontrollrechte des Auftraggebers 6
9. Weisungsbefugnis des Auftraggebers 7
10. Löschung und Rückgabe von personenbezogenen Daten 7
11. Unterzeichnung 7
ANLAGE 1: BEISPIEL: VERSAND VON WAREN UND ABWICKLUNG VON ZAHLUNGEN 8
ANLAGE 2: VERARBEITUNGSVERZEICHNIS DES AUFTRAGSVERARBEITERS 12

Textvorhersagen: ein Barrierefreiheit: Untersuchen

Umsetzung des Datenschutzes im Unternehmen

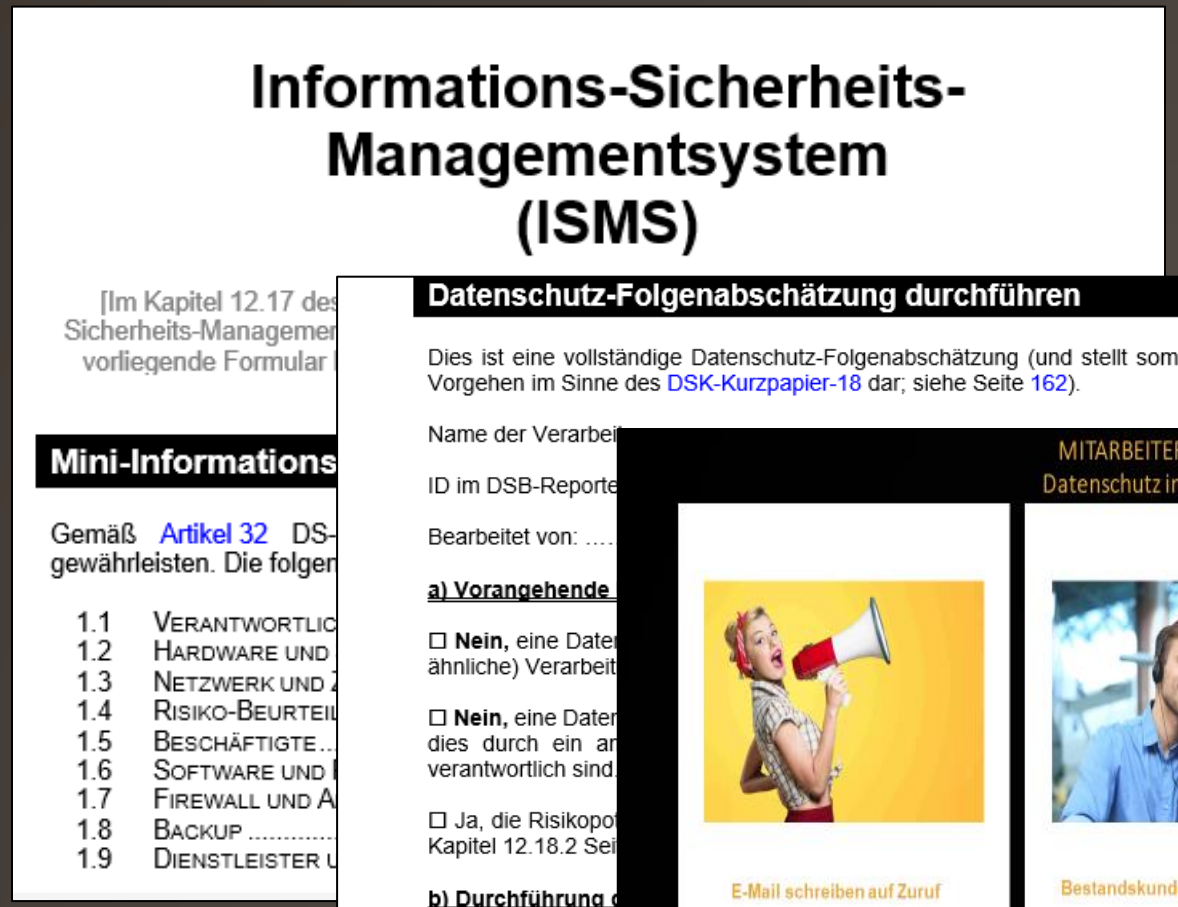
1. IT-Sicherheit (ISMS)
2. Risikoanalyse & Folgeabschätzungen
3. Mitarbeiterschulungen

Externer Datenschutzbeauftragter

Die Mauern

Mauern der einzelnen Räume

Jeder "Raum" ist eine "Verarbeitung" von personenbezogenen Daten. Diese Pflichten müssen also auf jede (Daten-) Verarbeitung angewendet werden.



Umsetzung des Datenschutzes im Unternehmen

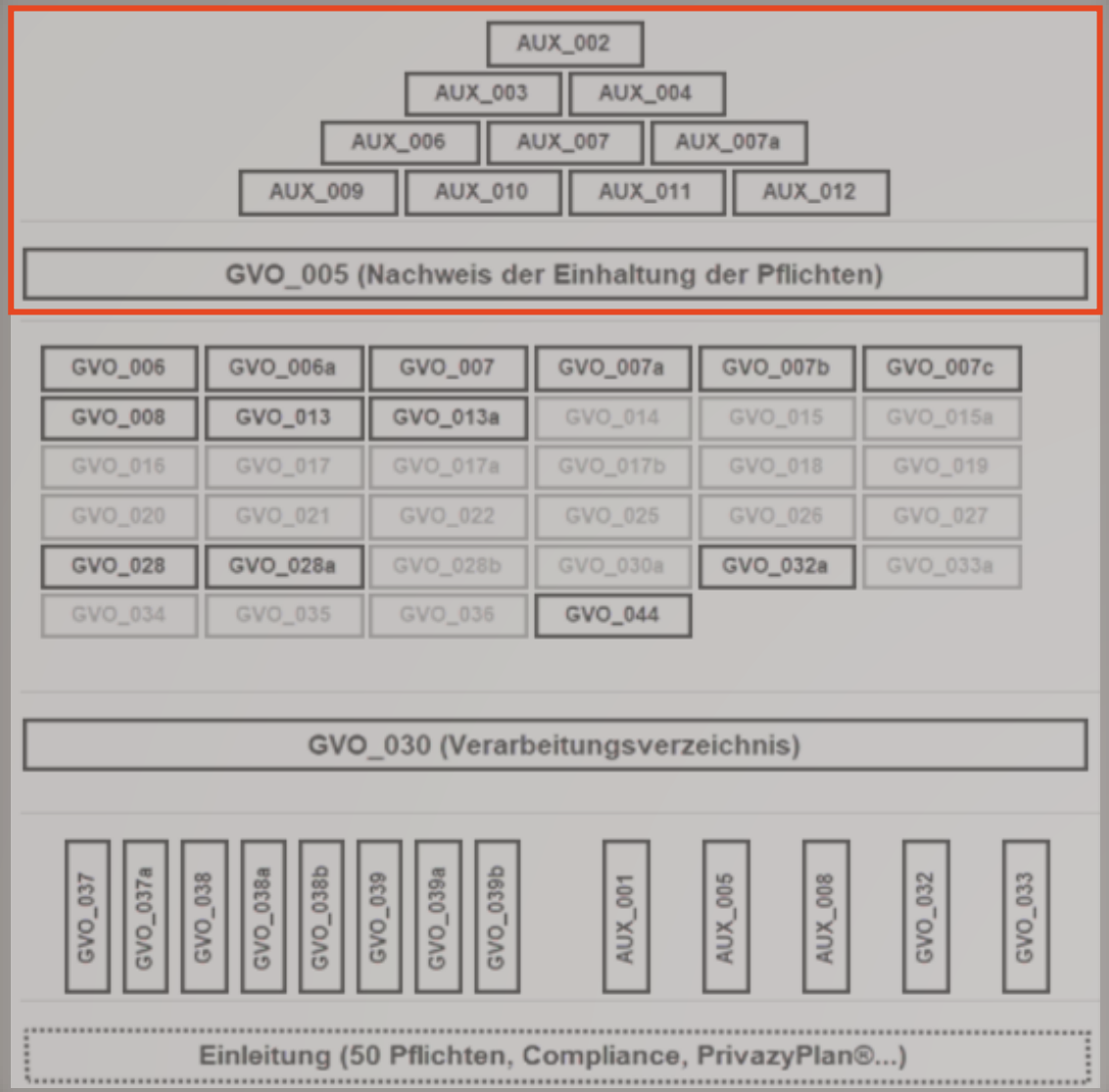
Externer Datenschutzbeauftragter

1. Jahresbericht
2. Pflichtüberwachung
3. Nachweis der Grundsätze

Das Dach

Nachweis und Pflichtüberwachung

Wenn alle anderen bußgeldbewehrten Pflichten erfüllt sind, dann wird darüber ein schriftlicher Nachweis erbracht.



Umsetzung des Datenschutzes im Unternehmen

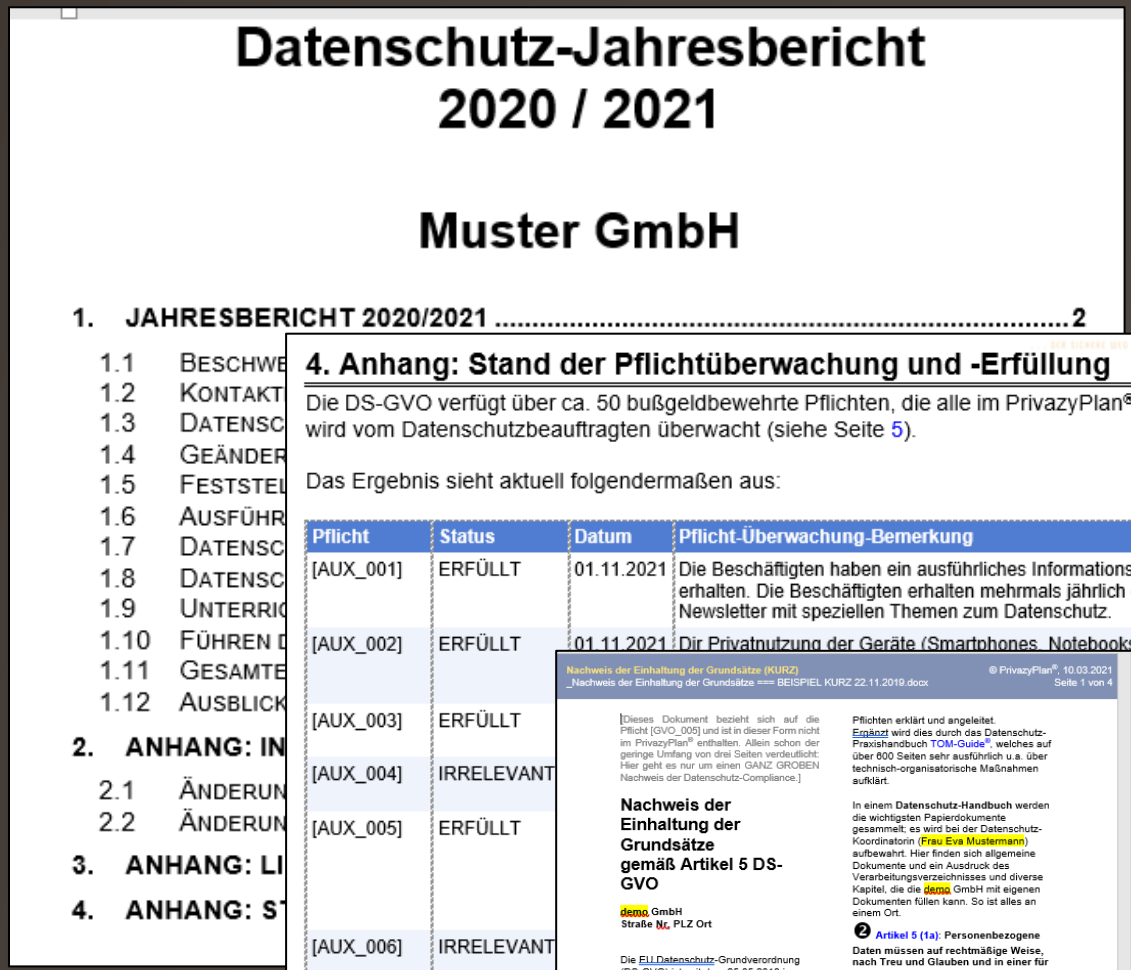
1. Jahresbericht
2. Pflichtüberwachung
3. Nachweis der Grundsätze

Externer Datenschutzbeauftragter

Das Dach

Nachweis und Pflichtüberwachung

Wenn alle anderen bußgeldbewehrten Pflichten erfüllt sind, dann wird darüber ein schriftlicher Nachweis erbracht.



Datenschutz-Jahresbericht 2020 / 2021

Muster GmbH

1. JAHRESBERICHT 2020/2021 2
   - 1.1 BESCHWE
   - 1.2 KONTAKT
   - 1.3 DATENSC
   - 1.4 GEÄNDER
   - 1.5 FESTSTEL
   - 1.6 AUSFÜHR
   - 1.7 DATENSC
   - 1.8 DATENSC
   - 1.9 UNTERRIC
   - 1.10 FÜHREN D
   - 1.11 GESAMTE
   - 1.12 AUSBLICK
2. ANHANG: IN
   - 2.1 ÄNDERUN
   - 2.2 ÄNDERUN
3. ANHANG: LI
4. ANHANG: S

4. Anhang: Stand der Pflichtüberwachung und -Erfüllung

Die DS-GVO verfügt über ca. 50 bußgeldbewehrte Pflichten, die alle im PrivazyPlan® erläutert wurden. Diese Einhaltung d
wird vom Datenschutzbeauftragten überwacht (siehe Seite 5).

Das Ergebnis sieht aktuell folgendermaßen aus:

Pflicht	Status	Datum	Pflicht-Überwachung-Bemerkung	Tätigkeit	Pflicht-Beschreibung
[AUX_001]	ERFÜLLT	01.11.2021	Die Beschäftigten haben ein ausführliches Informationsblatt erhalten. Die Beschäftigten erhalten mehrmals jährlich einen Newsletter mit speziellen Themen zum Datenschutz.		BESCHÄFTIGTE SCHU VERTRAULICHKEIT VE
[AUX_002]	ERFÜLLT	01.11.2021	Dir Privatnutzung der Geräte (Smartphones, Notebooks, etc.)		BESCHÄFTIGTE UNTE
[AUX_003]	ERFÜLLT				
[AUX_004]	IRRELEVANT				
[AUX_005]	ERFÜLLT				
[AUX_006]	IRRELEVANT				
[AUX_007]	ERFÜLLT				

Nachweis der Einhaltung der Grundsätze (KURZ) © PrivazyPlan®, 10.03.2021
_Nachweis der Einhaltung der Grundsätze === BEISPIEL KURZ 22.11.2019.docx Seite 1 von 4

[Dieses Dokument bezieht sich auf die Pflicht [GVO_005] und ist in dieser Form nicht im PrivazyPlan® enthalten. Allein schon der geringe Umfang von drei Seiten verdeutlicht: Hier geht es nur um einen GANZ GROBEN Nachweis der Datenschutz-Compliance.]

Nachweis der Einhaltung der Grundsätze gemäß Artikel 5 DS-GVO

demo GmbH
Straße Nr. PLZ Ort

Die EU-Datenschutz-Grundverordnung (DS-GVO) ist seit dem 25.05.2018 in ganz Europa anzuwenden. Dort wird im Artikel 5 ein „Nachweis der Einhaltung der Grundsätze" gefordert.

❶ **Allgemeine Informationen**

Das Unternehmen fällt in den nicht-öffentlichen Bereich und unterliegt somit der EU-Datenschutz-Grundverordnung 2016/679 (DS-GVO).

Für die Beschäftigtendaten gilt der § 26 BDSG (in der Fassung vom

Pflichten erklärt und angeleitet.
Ergänzt wird dies durch das Datenschutz-Praxishandbuch TOM-Guide®, welches auf über 600 Seiten sehr ausführlich u.a. über technisch-organisatorische Maßnahmen aufklärt.

In einem **Datenschutz-Handbuch** werden die wichtigsten Papierdokumente gesammelt; es wird bei der Datenschutz-Koordinatorin (Frau Eva Mustermann) aufbewahrt. Hier finden sich allgemeine Dokumente und ein Ausdruck des Verarbeitungsverzeichnisses und diverse Kapitel, die die demo GmbH mit eigenen Dokumenten füllen kann. So ist alles an einem Ort.

❷ **Artikel 5 (1a): Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.**

Compliance: Das Unternehmen stellt die Compliance sicher, indem es die ca. 50 bußgeldbewehrten Pflichten mit Hilfe des PrivazyPlan® systematisch bearbeitet.

Die **Ergebnisse aller Maßnahmen** werden in einem Dateisystem mit ca. 50 Unterverzeichnissen gesammelt.

Die **Überwachung der Pflichten** erfolgt sowohl durch das Unternehmen selbst, als auch gemäß Artikel 39 (1b) durch den

Nachweis der Einhaltung der Grundsätze (KURZ)
_Nachweis der Einhaltung der Grundsätze === BEISPIEL KURZ 22.11.2019.d

und mit dem Datenschutzbeauftragten abgestimmt.

Die Rechtmäßigkeit von **Einwilligung** im Sinne der Artikel 7 und 8 und des § 26 BDSG wird durch spezielle Checklisten sichergestellt.

Die Beauftragung von **Auftragsverarbeitungen** gemäß Artikel 28 erfolgt stets mit einem entsprechenden Vertrag.

Im Falle von **Übermittlungen an Dritte** ist die jeweilige Rechtsgrundlage ebenfalls dokumentiert.

Bei Übermittlungen an **Drittländer** werden die Auflagen des Artikel 44 eingehalten.

Transparenz: Für jede Verarbeitung wird ein sehr ausführlicher „Transparenztext" erstellt, der zu 100% mit dem Verarbeitungsverzeichnis übereinstimmt. Hier werden alle Angaben gemäß der Artikel 13, 14, 15, 26 und 30 geliefert. Diese Texte werden den betroffenen Personen zur Verfügung gestellt (und ggf. auch im Internet publiziert).

Sollten Daten **bei Dritten erhoben** werden (ohne dass die betroffenen Personen davon wissen), so werden Sie gemäß Artikel 14 im Rahmen der Transparenztexte (siehe oben) darüber informiert.

Datenschutz ist verpflichtend für jedes Unternehmen!

Ich helfe gerne und beantworte
auch ihre Fragen.

Data-Protection-Service
. . . DER SICHERE WEG

André Schombel
Externer Datenschutzbeauftragter
www.data-protection-service.de
a.schombel@data-protection-service.de
Tel: 040- 97 07 19 15