

---

Praxistipps IT

# Datenschutz in der Praxis

Umsetzung der EU-DSGVO für WP und StB

Rouven Friederich / Andreas Schneider



# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>9</b>
<b>2</b>	<b>Prozesse in Steuerberatungskanzleien und Wirtschaftsprüferpraxen</b> .....	<b>13</b>
<b>2.1</b>	<b>Dienstleister der Kanzlei</b> .....	<b>15</b>
<b>2.2</b>	<b>BDSG oder DSGVO – Was gilt denn nun?</b> .....	<b>16</b>
<b>2.3</b>	<b>Auftragsannahme</b> .....	<b>18</b>
2.3.1	Rechtmäßigkeit der Verarbeitung .....	18
2.3.2	Informationspflicht der Kanzlei .....	23
2.3.3	Informationspflichten der Mandanten .....	25
2.3.4	Verschwiegenheitspflicht .....	26
2.3.5	Einwilligungserklärung.....	28
2.3.6	Datenschutzerklärung.....	32
2.3.7	Verarbeitungsverzeichnis.....	33
2.3.8	Datenschutzfolgeabschätzung .....	35
<b>2.4</b>	<b>Mandatsbeendigung</b> .....	<b>37</b>
<b>2.5</b>	<b>Personalbeschaffung</b> .....	<b>39</b>
<b>2.6</b>	<b>Einwilligungserklärungen bei Beschäftigungs- verhältnissen</b> .....	<b>44</b>
<b>2.7</b>	<b>Personalausritte</b> .....	<b>45</b>
<b>2.8</b>	<b>Leistungsprozesse der Kanzlei</b> .....	<b>47</b>
2.8.1	Lohn- und Gehaltsbuchhaltung.....	47
2.8.2	Finanzbuchhaltung .....	55
2.8.3	Sonstige Steuerberatungsleistungen .....	57
<b>2.9</b>	<b>Durchsuchung und Beschlagnahme</b> .....	<b>59</b>
<b>2.10</b>	<b>Datenpannen</b> .....	<b>59</b>

<b>3</b>	<b>Schutz von personenbezogenen Daten</b>	<b>61</b>
<b>3.1</b>	<b>Datenschutz durch technische und organisatorische Maßnahmen</b>	<b>61</b>
3.1.1	Risikobewertung	61
3.1.2	Privacy by Design / Privacy by Default	64
3.1.3	Technische und organisatorische Maßnahmen (TOMs)	65
<b>3.2</b>	<b>Fahrplan für die Praxis</b>	<b>70</b>
3.2.1	Ist-Aufnahme der Datenflüsse	71
3.2.2	Durchführung der Risikobewertung	72
3.2.3	Ableitung der TOMs	73
3.2.4	Dokumentation der Bearbeitungsschritte	74
<b>3.3</b>	<b>Löschkonzept</b>	<b>74</b>
3.3.1	Aufstellung der gesetzlichen Aufbewahrungsfristen	74
3.3.2	Zusammenfassung und Gruppierung der Datenarten	75
3.3.3	Löschung von personenbezogenen Daten	75
<b>3.4</b>	<b>Meldung von Datenschutzverstößen</b>	<b>79</b>
<b>3.5</b>	<b>Datenschutzrichtlinie</b>	<b>80</b>
<b>4</b>	<b>Datenschutzbeauftragter</b>	<b>82</b>
<b>4.1</b>	<b>Bestellung und Voraussetzungen des Datenschutzbeauftragten</b>	<b>82</b>
4.1.1	Betriebliche Datenschutzbeauftragte	82
4.1.2	Externe Datenschutzbeauftragte	83
<b>4.2</b>	<b>Aufgaben des Datenschutzbeauftragten</b>	<b>84</b>
<b>4.3</b>	<b>Haftung des Datenschutzbeauftragten</b>	<b>85</b>
<b>4.4</b>	<b>Zusammenarbeit mit Aufsichtsbehörden</b>	<b>86</b>
<b>5</b>	<b>Landesämter für Datenschutz</b>	<b>87</b>
<b>5.1</b>	<b>Aufgaben und Befugnisse der Aufsichtsbehörden</b>	<b>87</b>
<b>5.2</b>	<b>Fragebögen der Behörden</b>	<b>88</b>
5.2.1	Struktur und Verantwortlichkeit im Unternehmen	88
5.2.2	Verzeichnis der Verarbeitungstätigkeiten	89
5.2.3	Einbindung externer Dienstleister	89

---

5.2.4	Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte.....	89
5.2.5	Verantwortlichkeit, Umgang mit Risiken.....	90
5.2.6	Datenschutzverletzungen.....	91
<b>6</b>	<b>Fazit.....</b>	<b>92</b>
	<b>Stichwortverzeichnis.....</b>	<b>109</b>