



Prüfdokumentation IITR Compliance Kit 2.0

Unabhängig
Staatlich befugt
Beeidet

IITR Datenschutz GmbH

Ansprechpartner	Dr. Sebastian Kraska	
Auditoren	Dipl.-Ing. Dr. Peter Gelber, Zivilingenieur für Informatik Dipl.-Ing. Wolfgang Fiala, Zivilingenieur für Informatik	
Datum	13.07.2019	
Örtlichkeit	Büros der Auditoren	
Prüf-Schwerpunkte	Nr	Beschreibung
	1	Überprüfung des „Compliance Kit 2.0“, bestehend aus dem Handbuch „01-01-01-DE Datenschutzhandbuch“.
	2	Überprüfung des „Compliance Kit 2.0“, bestehend aus 92 Vorlagen beginnend mit „01-02-01 DE Uebersicht Datenverarbeitungsverfahren.docx“ und endend mit „09-03-01 DE Datenschutz-Review.docx“.
	3	PrüfSchwerpunkt: Entsprechen die Dokumente den Vorgaben der DSGVO?
	4	PrüfSchwerpunkt: Gibt es Widersprüche zwischen dem Inhalt des Dokuments und der DSGVO?
	5	PrüfSchwerpunkt: Enthält die DSGVO Bestimmungen, die zwar zum aktuellen Kapitel gehören aber in der Vorlage nicht enthalten sind?
Auditergebnis	Datum	Bestätigungsvermerk
	Urkunden	Der positive Abschluss des Audits wird von den Auditoren mit der Urkunden <ul style="list-style-type: none">• 06/2019 ohne Einschränkungen bestätigt,

Wien, am 08.08.2019

/Dipl.-Ing. Wolfgang Fiala



/Dipl.-Ing. Dr. Peter Gelber/



INHALTSVERZEICHNIS

1	ALLGEMEINES - DSGVO	9
1.1	Zweck des Datenschutzmanagementsystems	9
1.2	Prozesse und Wechselwirkung	9
1.3	Anwendung/Geltungsbereich und Freigabe	9
2	PROZESSORIENTIERUNG	12
2.1	Prozesse	12
2.2	PDCA	12
3	GRUNDSÄTZE BEIM UMGANG MIT PERSONENBEZOGENEN DATEN	14
3.1.1	Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz	14
3.1.2	Zweckbindung	15
3.1.3	Datenminimierung	15
3.1.4	Richtigkeit	16
3.1.5	Speicherbegrenzung	16
3.1.6	Integrität, Vertraulichkeit und Verfügbarkeit	16
4	KONTEXT UND INTERESSIERTE PARTEIEN	19
4.1	Verstehen der Organisation und Ihres Kontextes	19
4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien	19
5	FÜHRUNG UND VERANTWORTUNG	21
5.1	Verpflichtung	21
5.2	Politik	21
5.3	Rollen, Verantwortlichkeiten und Befugnisse	22
6	PLANUNG	25
6.1	Risikomanagement	25
6.2	Datenschutzbestimmungen /-ziele und Planung	26
7	UNTERSTÜTZUNG	28
7.1	Ressourcen	28
7.2	Kompetenzen	28
7.3	Bewusstsein	30



Prüfdokumentation IITR Compliance Kit 2.0

Unabhängig
Staatlich befugt
Beeidet

7.4	Kommunikation.....	31
7.5	Dokumentierte Informationen	32
8	DATENVERARBEITUNG.....	34
8.1	Schutzmaßnahmen	34
8.1.1	Technische und organisatorische Schutzmaßnahmen	34
8.1.2	Verarbeitungsbezogene Schutzmaßnahmen	36
8.2	Verarbeitungstätigkeiten	37
8.2.1	Transparenz der Verarbeitung	37
8.2.2	Verzeichnis der Verarbeitungstätigkeiten	37
8.2.3	Verantwortlichkeiten für die Verarbeitungstätigkeiten	39
8.2.4	Verarbeitungstätigkeiten durch externen Dienstleister	40
8.2.5	Verarbeitungstätigkeiten im Auftrag als Dienstleister	41
8.2.6	Gemeinsam verantwortlich für die Verarbeitungstätigkeiten.....	42
8.3	Rechte der Betroffenen	43
8.3.1	Informationspflicht.....	43
8.3.2	Auskunftsrecht.....	44
8.3.3	Berichtigung, Einschränkung und Löschung.....	45
8.3.4	Datenübertragung.....	46
8.3.5	Einwilligung zur Datenverarbeitung.....	47
8.4	Beanstandungsverfahren	48
8.4.1	Inhalt des aktuellen Handbuch-Kapitels.....	48
8.4.2	Prüfung des Handbuch-Inhalts	48
8.4.3	Prüfung der zugeordneten Vorlagen	48
8.5	Datenschutz-Folgenabschätzung.....	48
8.5.1	Inhalt des aktuellen Handbuch-Kapitels.....	48
8.5.2	Prüfung des Handbuch-Inhalts	49
8.5.3	Prüfung der zugeordneten Vorlagen	49
8.6	Datenschutzverletzung und Meldepflicht	49
8.6.1	Inhalt des aktuellen Handbuch-Kapitels.....	49
8.6.2	Prüfung des Handbuch-Inhalts	50
8.6.3	Prüfung der zugeordneten Vorlagen	50
8.7	Unternehmensspezifischer Datenschutz.....	51
8.7.1	Datenschutz im Personalbereich	51
8.7.1.1	Bewerbungsprozess	51
8.7.1.2	Verpflichtung der Beschäftigten.....	52
8.7.1.3	Schulung der Beschäftigten	53
8.7.1.4	Definition der mit der Datenverarbeitung Beschäftigten.....	54
8.7.1.5	Personalakten	54
8.7.1.6	Datenverarbeitungssysteme im Personalbereich.....	55
8.7.1.7	Nutzung von Fotos oder Filmaufnahmen der Beschäftigten.....	56



Prüfdokumentation IITR Compliance Kit 2.0

Unabhängig
Staatlich befugt
Beeidet

8.7.2	Datenschutz im IT-Bereich	57
8.7.2.1	Besondere Verpflichtung der IT-Administratoren	57
8.7.2.2	Fernzugriff auf Systeme.....	58
8.7.2.3	Fernzugriff auf von Mitarbeitern genutzter Hardware.....	58
8.7.2.4	Lokale Administrationsrechte.....	59
8.7.2.5	Nutzung von Unternehmenshardware außerhalb des Unternehmens	59
8.7.2.6	Unternehmensfremde Hardware.....	60
8.7.2.7	Private Nutzung der unternehmenseigenen Hardware.....	61
8.7.2.8	Nutzung der Kommunikationsmittel für private Zwecke.....	61
8.7.2.9	Gäste-WLAN	63
8.7.2.10	Videoüberwachung	63
8.7.2.11	Datenverarbeitungssysteme im IT-Bereich	65
8.7.3	Datenschutz im Vertrieb und Marketing.....	66
8.7.3.1	Homepage	66
8.7.3.2	Homepage-Tracking.....	66
8.7.3.3	Nutzung der Kundendaten für Werbezwecke.....	67
8.7.3.4	Nutzung von Social Media Plattformen.....	68
8.7.3.5	Datenverarbeitungssysteme im Vertrieb und Marketing	69
8.7.4	Datenschutz im Einkauf.....	70
8.7.4.1	Lieferanten- und Dienstleisterdaten.....	70
8.7.4.2	Datenübermittlung oder Zugriffgewährung.....	70
8.7.4.3	Datenverarbeitungssysteme im Beschaffungsbereich	71
9	BEWERTUNG DER LEISTUNG	74
9.1	Überwachung, Messung, Analyse und Bewertung.....	74
9.1.1	Inhalt des aktuellen Handbuch-Kapitels.....	74
9.1.2	Prüfung des Handbuch-Inhalts	74
9.1.3	Prüfung der im Handbuch mitgeltenden Dokumente / Vorlagen:.....	74
9.2	Internes Audit	74
9.2.1	Inhalt des aktuellen Handbuch-Kapitels.....	74
9.2.2	Prüfung des Handbuch-Inhalts	75
9.2.3	Prüfung der im Handbuch mitgeltenden Dokumente / Vorlagen:.....	75
9.3	Datenschutz-Review	75
9.3.1	Inhalt des aktuellen Handbuch-Kapitels.....	75
9.3.2	Prüfung des Handbuch-Inhalts	76
9.3.3	Prüfung der im Handbuch mitgeltenden Dokumente / Vorlagen:.....	76
10	VERBESSERUNG	78
10.1	Nichtkonformität und Korrekturmaßnahmen.....	78
10.1.1	Inhalt des aktuellen Handbuch-Kapitels.....	78
10.1.2	Prüfung des Handbuch-Inhalts.....	78
10.1.3	Prüfung der im Handbuch mitgeltenden Dokumente / Vorlagen:	78



Prüfdokumentation IITR Compliance Kit 2.0

10.2 Vorbeugende Maßnahmen / Präventivmaßnahmen	78
10.2.1 Inhalt des aktuellen Handbuch-Kapitels	78
10.2.2 Prüfung des Handbuch-Inhalts.....	78
10.2.3 Prüfung der im Handbuch mitgeltenden Dokumente / Vorlagen:	78
10.3 Ständige Verbesserung.....	79
10.3.1 Inhalt des aktuellen Handbuch-Kapitels.....	79
10.3.2 Prüfung des Handbuch-Inhalts.....	79
10.3.3 Prüfung der im Handbuch mitgeltenden Dokumente / Vorlagen:	79
II IMPRESSUM.....	80