Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
1. Organisationskontrolle					
1.1	**Ist ein Betriebsrat vorhanden?**			✓	
1.2	**Werden personenbezogene Daten verarbeitet? / Welche?**	✓			Die Art der verwendeten Daten und der betroffenen Personen ergeben sich aus den jeweils angehängen AVA
1.3	**Wie viele Mitarbeiter sind mit der Verarbeitung personenbezogener Daten befasst?**				25
1.4	**Wie ist die Vertretung im Urlaubs-/Krankheitsfall sichergestellt?**	✓			Vertretungsregelung im Urlaubsantrag - Übergabe offener Punkte vor dem Urlaub
1.5	**Wird der BSI-Grundschutz umgesetzt?**	✓			
1.6	**Ist das Unternehmen zertifiziert? Wenn ja, wann, durch wen, für was (z.B. ISO)?**		✓		
1.7	**Werden einschlägige Verfahren/best practises genutzt (z.B. ITIL, COBIT)? In welcher Verfahrenstiefe/in welcher Version?**		✓		
1.8	**Wurde ein qualifizierter Datenschutzbeauftragter bestellt (gem. Art. 37 DSGVO)**	✓			zum 01.03.2015 Herr Thomas Brausch Am Wissenschaftspark 32 54296 Trier Tel: 0651 96629-132 Mail: Thomas.Brausch@bit-Informatik.de
1.8.1	Erstellt der DSB regelmäßige Datenschutzberichte?	✓			JA
1.8.2	Wenn ja, wann zuletzt und mit welchem Ergebnis?	✓			17.01.2018, siehe Tätigkeitsbericht. Dieser kann per mail angefordert werden

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
1.9	**Verfügt das Unternehmen über eine eigene Revision?**		✓		
1.9.1	Werden Prüfungen zum Datenschutz durchgeführt und Prüfberichte erstellt?			✓	
1.9.2	Wenn ja, wann zuletzt und mit welchem Ergebnis?			✓	
1.10	**Wurde ein qualifizierter IT-Sicherheitsbeauftragter für das Unternehmen bestellt? Welcher Zeitanteil ist bei diesem Mitarbeiter für das IT-Sicherheitsmanagement eingeplant?**	✓			10%
1.11	**Gibt es aktuelle, verbindliche Sicherheitskonzepte und eine Sicherheitsrichtlinie (Security Policy)?**	✓			
1.12	**Existiert ein geeignetes Anweisungswesen (Arbeits-/ Verfahrensanweisungen)?**	✓			
1.13	**Existiert ein Datenschutzkonzept?**	✓			
1.14	**Sind die Arbeitsplätze durch entsprechende Stellenbeschreibungen beschrieben?**		✓		
1.15	**Existiert ein schriftliches Programmeinsatzverfahren?**	✓			
1.16	**Sind die einschlägigen datenschutzrechtlichen Bestimmungen in einer aktuellen Fassung im Unternehmen bekannt? Wie wird dies sichergestellt?**	✓			Regelmäßige Belehrung der Mitarbeiter über datenschutzrechtliche Bestimmungen

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
1.17	**Werden die Mitarbeiter auf den Datenschutz (gemäß Art. 47 (2) n) und ggf. weitere Geheimhaltungsgrundsätze (z.B. Bankgeheimnis) verpflichtet und regelmäßig unterwiesen und wird dies dokumentiert?**	✓			Verpflichtung und regelmäßige Belehrung der Mitarbeiter über datenschutz- und bankrechtliche Bestimmungen
1.18	**Liegt ein Verzeichnis von Verarbeitunstätigkeiten für das Unternehmen(gem. Art. 30 DSGVO) vor und werden diese zeitnah gepflegt?**	✓			
1.19	**Werden DV-Anlagen durch Fremdfirmen mit genutzt? Wie ist die logisch und physikalische Trennung sichergestellt?**		✓		
1.20	**Existiert eine ausreichende Funktionstrennung bzw. wird ein 4-Augen-Prinzip eingehalten?**	✓			
1.21	**Finden regelmäßige Hinweise, Schulungen, Ermahnungen o.ä. statt um das Problembewusstsein zu fördern?**	✓			
1.22	**Werden gelegentliche unvermutete Kontrollen der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen durchgeführt? Wie oft, in welchem Umfang, mit welchen Ergebnissen in der Vergangenheit?**	✓			einmalige komplette Überprüfung der Arbeitsplätze auf offene personenbezogene Daten (verschiedene Personen mussten auf einen Verstoß hingewiesen werden - eine erneute Kontrolle zeigte, dass das Problem behoben war), Rechner der Mitarbeiter auf aktualität des Virenscanners (ohne Verstöße), regelmäßige Prüfung der Vorgaben zur Zutrittskrontrolle (ohne Verstöße)
2. Zutrittskontrolle					
2.1	**Wie sind die Räume des Unternehmens durch geeignete Sicherheitsmaßnahmen gegen unbefugten Zutritt geschützt (z.B. Chipkarte mit Kartenleser, 24 Std. Pförtner, Fensterverglasung, Schlüsselkarteien, Videoüberwachung, Besucherbuch, Zutrittskonzepte, Alarmanlage, Werkschutz, Absicherung Lichtschächte etc.,…)?**	✓			Chipkarte mit Kartenleser, 3-fach Fensterverglasung, abgeschlossene Fenster, Alarmanlage mit Anbindung an Sicherheitszentrale
2.2	**Wie sind besonders schutzwürdige Systeme (z.B. zentrale IT-Systeme) vor unberechtigtem Zutritt geschützt?**	✓			Schutzwürdige Systeme befinden sich in einem eigenen Raum, der durch eine eigene schlüsselgebundene Schliessanlage gesichert ist. Der Zutritt ist auf wenige Personen eingeschränkt.
2.3	**Wie wird der Zutritt protokolliert und kontrolliert (Zeiterfassung, Schichtbuch, Software-Protokolle, …)?**	✓			Zutritte werden per Liste protokolliert; regelmäßige Prüfung dieser Listen

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
2.4	**Wie lange ist nachvollziehbar, wer wann Zutritt erlangte?**	✓			Aufbewahrungsfrist für die Listen: 3 Jahre
2.5	**Bestehen entsprechende Zugangsregelungen auch für Backup- und Sicherungsstandorte/-räume?**	✓			
2.6	**Gibt es besondere Regelungen für das Reinigungspersonal und Wartungspersonal (Gebäudewartung, Software-/Hardware-Wartung etc.)?**	✓			
3. Zugangskontrolle					
3.1	**Existieren angemessene Regelungen zur Zugangskontrolle (Passwortsicherheit)?**	✓			
3.1.1	Hat das Passwort mindestens eine Länge von 8 Zeichen?	✓			
3.1.2	Ist ein Zeichenmix (Sonderzeichen, Ziffern, Buchstaben, Groß-/Kleinschreibung) vorgeschrieben und sind Trivialpassworte ausgeschlossen?	✓			
3.1.3	Wird ein Passwortwechsel erzwungen? Wenn ja, nach welcher Zeit (i.d.R. angemessen: ca. 90 Tage)?		✓		
3.1.4	Wird der Zugang bei mehr als drei fehlerhaften Anmeldeversuchen gesperrt?	✓			
3.2	**Hat jeder User eine eigene Zugangskennung zum System/zu den Verfahren?**	✓			
3.3	**Werden Administratorenpassworte geschützt?**	✓			

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
3.4	**Ist ein Zugriff auf die Systeme/Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, mobile Endgeräte etc.)?**		✓		
3.5	**Werden die Zugriffe auf Anwendungen und Systeme nachvollziehbar protokolliert?**		✓		Fernwartungen werden nur auf Verlangen erstellt und dem Kunden zur Verfügung gestellt.
3.5.1	Wenn ja, wie lange werden die Protokolle aufbewahrt?				
3.5.2	Wer hat Zugriff auf die Protokolle?				
3.6	**Werden Datenträger auf dem Transportweg verschlüsselt (z.B. CD, Mail)?**	✓			Sollten Datenträger versendet werden, werden diese als passwortgeschützte Zip-Files versendet; mails werden als sichere Notes-Mail versendet (nicht über das Internet). Internet-Mails: Hier werden die Anhänge als passwortgeschützte Zip-Files versendet
3.7	**Sind die Systeme/Anwendungen ausreichend durch eine Firewall gegen unberechtigte Zugriffe abgesichert?**	✓			
3.8	**Existieren besondere Regelungen, Arbeitsanweisungen für Zugriffe von extern?**			✓	Externe besitzen keinen Zugriff auf interne Systeme
4. Zugriffskontrolle					
4.1	**Existiert ein abgestuftes Berechtigungskonzept mit angemessenen Regelungen zur Zugriffskontrolle (z.B. Rollen, Funktionen, 4-Augen-Prinzip)?**	✓			
4.1.1	Werden einzelne den Funktionen entsprechende Rollen und Rechte vergeben?	✓			
4.1.2	Gibt es differenzierte Berechtigungen für lesenden und schreibenden (Änderung/Löschung) Zugriff?	✓			

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
4.1.3	Gibt es anwendungsbezogen vergebene Userrechte?	✓			
4.1.4	Werden die Zugriffe protokolliert?	✓			
4.1.5	Werden Zugriffsprotokolle aufbewahrt?	✓			
4.2	**Wie werden Datenträger aufbewahrt/gelagert (Verschluss in Schränken, Tresoren etc.)? Wer hat Zugriffsrechte (Schlüsselträger etc.)?**	✓			Gesondert abschliessbarer Stahlschrank; Administratoren und Geschäftsführung haben Zugriff
4.3	**Werden Sicherungsmedien getrennt verwahrt und besonders gesichert?**	✓			
4.4	**Sind die einschlägigen Aufbewahrungsfristen bekannt und werden sie beachtet?**	✓			
4.5	**Wie werden nicht mehr benötigte Daten qualifiziert gelöscht bzw. vernichtet?**	✓			
4.5.1	**Werden Datenträger bis zur Entsorgung entsprechend sicher verwahrt? (Zwischenlagerung wie)**	✓			
4.5.2	Wie wird die Vernichtung/Löschung protokolliert, überwacht und kontrolliert?		✓		
4.5.3	Wie erfolgte die Auswahl des Entsorgungsunternehmens (Referenzen)?	✓			kleinere Mengen: CD Schredder; Cross Cut 4*32 mm Papier-Schredder: Sicherheitsstufe 5 Größere Mengen in einem zertifizierten Unternehmen

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
4.5.4	Werden Entsorgungsbescheinigungen erstellt?	✓			Nur für größere Mengen

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
4.6	**Ist die Nutzung privater Datenträger verboten?**	✓			
4.7	**Wie wird die Trennung der Datenträger nach Auftraggebern gewährleistet?**	✓			Arbeitsanweisung und regelmäßige Schulung und Kontrolle
4.8	**Existieren gesonderte Regelungen für mobile Endgeräte?**	✓			
4.9	**Ist das Mitnehmen von dienstlichen Unterlagen geregelt bzw. verboten?**	✓			
4.10	**Wurden Wartungs- und Fernwartungsverträge mit Externen geschlossen und berücksichtigen diese u.a. Zutritt, Zugriff, Datenschutz und Geheimhaltung?**	✓			
4.10.1	Werden Fernwartungszugriffe protokolliert?	✓			Mit dem Kunden kann eine Aufzeichnungspflicht bei Fernwartung vereinbart werden
4.10.2	Wie lange werden Fernwartungsprotokolle aufbewahrt, durch wen sind sie auswertbar?	✓			Sofern eine Aufzeichnugnspflicht besteht, werden die Aufzeichnungen dem Kundfen zur Verfügung gestellt. Nicht mehr benötigte Aufzeichnungen werden gelöscht, sobald der Zweck der eigentlichen Fernwartung nicht mehr besteht.
5. Weitergabekontrolle					
5.1	**Werden Datenträger transportiert? Wenn ja, wohin und wie?**		✓		
5.2	**Wurden Transportregelungen schriftlich festgelegt (Berechtigte, Transportwege, Transportverfahren, Transportbehälter)?**			✓	
5.3	**Wie werden Transporte von Daten/Datenträgern gesichert, protokolliert und überwacht (Transportprotokolle, Verschlüsselung, Quittungsverfahren, Einschreiben etc.)?**			✓	

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
5.4	**Existieren gesonderte Regelungen für Heimarbeiter/Telearbeiter?**			✓	
6. Eingabekontrolle					
6.1	**Werden Datenveränderungen protokolliert?**	✓			
6.2	**Werden die Protokolle gem. Aufbewahrungsfristen gesichert?**	✓			
6.2.1	Wie lange sind die Protokolle auswertbar und von wem?	✓			gemäß gesetztlicher Aufbewahrungsfristen durch berechtigte Personen
7. Auftragskontrolle					
7.1	**Welche Referenzpartner nutzen die nachgefragten Dienstleistungen in einem ähnlichen Umfang?**	✓			über 200 Kreditinstitute
7.2	**Sind die nachgefragten Dienstleistungen zertifiziert?**			✓	
7.2.1	Wenn ja, wann, in welcher Version (Software/Hardware) und durch wen?			✓	
7.3	**Werden Subunternehmer eingesetzt?**		✓		
7.3.1	Wenn ja, sind diese in Deutschland ansässig/tätig?			✓	
7.3.2	Wurden die Subunternehmer auf den Datenschutz und zur Geheimhaltung vertraglich verpflichtet?			✓	

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
7.4	**Gibt es detaillierte schriftliche Regelungen der Auftragsverhältnisse und eine Formalisierung des gesamten Auftragsablaufs? Auch für Subunternehmer (z.B. Datenerfassung, Datenträgerentsorgung, Call Center, Reinigungsunternehmen, Wartungsunternehmen?**	✓			
8. Verfügbarkeitskontrolle					
8.1	**Existieren geeignete Backup- und Sicherungsverfahren für alle relevanten Systeme/Anwendungen?**	✓			
8.2	**Ist eine geeignete Datensicherung (Generationenprinzip oder Vergleichbares) realisiert? Welcher Zeitraum wird abgesichert?**	✓			Tagessicherung für 5 Tage rückwirkend Wochensicherung für 4 Wochen rückwirkend Monatssicherung für 3 Monate rückwirkend Jahressicherung
8.3	**Wird regelmäßig überprüft, ob eine Rekonstruktion gesicherter Daten tatsächlich und einwandfrei möglich ist?**	✓			
8.4	**Werden Sicherungsbestände räumlich getrennt aufbewahrt?**	✓			
8.5	**Wurden Notfallpläne erstellt?**	✓			
8.6	**Finden regelmäßige Tests zu Backup und Wiederanlauf statt? Wenn ja, in welchen zeitlichen Abständen?**	✓			alle 6 Monate
8.7	**Sind die Datensicherungen, Schutzbedarfe, Wiederanlaufpläne (wo notwendig) mit dem Auftraggeber abgestimmt und verzahnt?**	✓			
8.8	**Existiert eine aktuelle, einheitliche und konsistente Lösung zum Virenschutz?**	✓			
8.9	**Welche Brandschutzeinrichtungen existieren (Feuerlöscher in Server-/Technik-//Arbeitsräumen, Rauch- und Brandmelder, Sprinkleranlage, feuerfeste Schränke, Brandschutztüren etc.)?**	✓			Feuerlöscher, Rauchmelder, feuerfeste Schränke

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
8.10	**Besteht ein Rauchverbot in Server-, Technik- und Arbeitsräumen?**	✓			
8.11	**Sind Server-/Technikräume ausreichend klimatisiert sowie vor Wassereinbruch geschützt?**	✓			
8.12	**Ist eine unterbrechungsfreie Stromversorgung gewährleistet?**	✓			
9. Trennungsgebot					
9.1	**Ist für jede Bearbeitung personenbezogener Daten festgelegt, zu welchem Zweck sie erfolgt bzw. auf Grund welcher Rechtgrundlage und mit Hilfe welcher Verfahren die Bearbeitung erfolgt?**	✓			
9.2	**Wie wird sichergestellt, dass die Vertraulichkeit der Daten und Informationen zwischen den verschiedenen Auftraggebern gewahrt bleibt?**	✓			Speichern in getrennten Ordnern (Arbeitsanweisung), ausgedrucktes Material wird nicht ausgegeben sondern gemäß Datenschutzvorschriften vernichtet.
9.3	**Wird die Funktionstrennung (Produktion und Test) beachtet?**	✓			
9.4	**Werden Daten pseudonymisiert (z.B. Testdaten)?**	✓			
9.5	**Wird das Pseudonym-Zuordnungsmerkmal von den restlichen Daten getrennt?**	✓			
9.6	**Ist die Zweckbindung gewährleistet (werden Daten nur zum vereinbarten Zweck genutzt/verarbeitet)?**	✓			
9.7	**Überprüfung der technisch organisatorischen Massnahmen**	✓			September 2017

Checkliste Auftragsdatenverarbeitung

Umsetzung der technischen und organisatorischen Maßnahmen
(bit Informatik GmbH)

Erfüllung der Aufgaben nach Art. 32 DSGVO					
	Vorgabe	**trifft zu**	**trifft nicht zu**	**nicht relevant/ erforderlich**	**Ergebnis**
9.8	**Beanstandungen**				Keine
10. Datenschutz-Management					
10.1	**Existieren Richtlinien/Anweisung zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit**	✓			
10.2	**Wurde ein Datenschutzbeauftragter bestellt?**	✓			siehe 1.8
10.3	**Sind alle Mitarbeiter auf das Datengeheimnis verpflichtet?**	✓			
10.4	**Existieren hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten?**	✓			2 Schulungen pro Jahr
10.5	**Wir eine Übersicht der Verarbeitungstätigkeiten geführt?**	✓			
10.6	**Werden Datenschutzfolgenabschätzungen durchgeführt, soweit erforderlich?**	✓			
11. Incident-Response-Management					
11.1	**Existiert ein Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)**	✓			
11.2	**Existiert ein Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)**	✓			
12. Datenschutzfgreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)					
12.1				✓	
13. Gültigkeit					
13.1	**Diese TOM's gelten ab dem 15.05.2018** **Die TOM's wurden geprüft von Thomas Brausch, bit Inofrmatik GmbH**				