Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

Auftraggeber (Verantwortlicher)

Abwasserverband Untere Döllnitz
Mannschatzer Str.38
04758 Oschatz

Auftragnehmer (Auftragsdatenverarbeiter)

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Entleerung von privaten abflusslosen Sammelgruben und Kleinkläranlagen im Entsorgungsgebiet des Abwasserverbandes „Untere Döllnitz“

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland wird dem Auftraggeber angezeigt und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags:

Der Vertrag beginnt am __.__.____ und wird auf unbestimmte Zeit geschlossen.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,

- die Einschränkung,
- das Löschen,
- die Vernichtung.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

- Kundendaten
- Lieferantendaten
- Persönliche Daten von Beschäftigten der Firma
- Daten über Mitarbeiter von Dienstleistern
- Grundsätzlich alle vom Auftraggeber übergebenen Daten.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Grundsätzlich alle vom Auftraggeber an den Auftragnehmer übermittelte Daten von natürlichen Personen.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen und sind ohne diese Dokumentation nicht gültig.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Alle Kontrollen werden einen Monat vorher angekündigt. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

Fr. Garbe, Fr. Stoltenberg, Hr. Streubel, Hr. Jahn, Hr. Garbe, Fr. Häschel

_____

_____

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

_____

_____

(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

E-Mail, Fax, Telefon

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

_____

(Stelle des Auftraggebers)

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung und mit zweimonatiger Vorankündigung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen

Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
Das im Anhang „Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen“ beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:
Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vertragsstrafen

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

11. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

_____

Datum

_____ _____

Auftraggeber Auftragnehmer

Beilage Vereinbarung Datenvereinbarung

Anlage - Technisch-organisatorische Maßnahmen (TOM) zur Einhaltung der EU-DSGVO

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

Der Auftraggeber sowie der Auftragnehmer erkennen die in Anlage 1 aufgeführten TOM als Standard an und streben diese an.

1. Pseudonymisierung

• Zur internen Zuordnung werden soweit möglich und sinnvoll Kundennummern verwendet statt Namen,

• Protokollierungen des IT-Systems erfolgen anhand der Benutzernummer,

• Nach Möglichkeit Trennung von Kundenstammdaten und Kundenvorgangsdaten.

2. Verschlüsselung

• Verschlüsselungsmethoden werden stets auf dem aktuellen Stand der Technik gehalten,

• Mobilgeräte kommunizieren mit dem internen Netzwerk ausschließlich über eine verschlüsselte VPN-Verbindung,

• E-Mails mit sensiblem Inhalt werden stets verschlüsselt (Z.B. Zusendung verschlüsselter Gehaltsabrechnung per E-Mail).

• Hochvertrauliche Daten werden nach Möglichkeit in verschlüsselter Form gespeichert,

• Öffentlich zugängliche Webseiten verfügen stets über eine ausreichend starke https Verschlüsselung,

• Angebotene Apps verfügen über eine ausreichend starke Verschlüsselung.

3. Vertraulichkeit

• Es existieren abgestufte Schließkreise mit unterschiedlichen Zutrittsberechtigungen,

• Zentrale IT-Komponenten sind in besonders geschützten Räumen untergebracht,

• Sensible Bereiche werden videoüberwacht,

• Das Hauptgebäude wird durch eine Einbruchmeldeanlage gesichert,

• Authentifizierung mit sicherem Passwort und Userkennung,

• Anzahl der Administratoren auf das „Notwendigste" reduziert,

• Es besteht ein Prozess für die Vergabe, Änderung und den Entzug von

IT-Berechtigungen,

• Für alle relevanten Anwendungen bestehen Berechtigungskonzepte, die nach dem Need-to-Know-Prinzip erstellt wurden,

• Zugriffsmöglichkeiten auf Daten werden auf das erforderliche Maß beschränkt,

• Verwaltung der Berechtigungen ausschließlich durch Systemadministratoren,

• Regelungen zur sicheren Löschung / Entsorgung / Vernichtung von Datenträgern und Dokumenten,

• Sichere Aufbewahrung von Datenträgern im Server-Raum und im Tresor,

• Verbot der Nutzung von Geschäftsdaten auf privaten Rechnern,

• Nur zweckgebundene Verarbeitung personenbezogener Daten,

• Einsatz von Anti-Viren-Software,

• Einsatz einer Software-Firewall.

4. Integrität

• Berechtigungs- und Zugriffskonzepte (siehe oben),

• Wesentliche Dokumente und Vorlagen werden möglichst unter Angabe der vorgenommenen Änderungen versioniert,

• Eingaben, Änderungen und Löschungen von Daten bzw. Dokumenten mit erhöhtem Schutzbedarf werden protokolliert,

• Es gibt interne Regelungen und Anleitungen für die Eingabe von Daten,

• Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).

5. Verfügbarkeit

• Unterbrechungsfreie Stromversorgung für zentrale IT-Systeme,

• Gewährleistung räumlicher Sicherheit (z.B. Brandmeldeanlage, Klimaanlage, Feuerlöscher usw.),

• Zentrale IT-Komponenten sind nicht unter sanitären Anlagen untergebracht,

• Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen,

• Schutzsteckdosenleisten in Serverräumen,

• Regelmäßige Wartung der Sicherheitstechnik,

• Virenschutz und Firewall-Systeme werden stets aktuell gehalten,

• Daten werden täglich inkrementell und wöchentlich vollumfänglich gesichert,

• Es werden regelmäßig Rücksicherungstests durchgeführt,

• Veränderungen an IT-Systemen durchlaufen stets einen standarisierten IT-Change-Prozess,

• Für wichtige IT-Systeme existiert ein SLA-Monitoring,

6. Belastbarkeit

• Für wichtige IT-Systeme werden ausreichend Ressourcen (Performance, Speicherkapazitäten,

Kapazitätsreserven für Spitzenlasten) zur Verfügung gestellt,

• Die Leitungskapazitäten des internen Netzwerks und der Internetverbindung werden

überwacht und an die Erfordernisse angepasst,

• Für hochverfügbare Webangebote werden Load-Balancer eingesetzt.

7. Physischer oder technischer Zwischenfall

• Es besteht ein Datensicherungs-Konzept,

• wichtige Datenbestände werden redundant vorgehalten,

• Es werden regelmäßig Notfalltests durchgeführt,

• Ein Prozess für den Umgang mit Incidents (Vorfällen) ist definiert,

• Es besteht ein Konzept zum Umgang mit Datenpannen.

8. Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

• Der Schutzbedarf der eingesetzten Anwendungen wird jährlich überprüft,

• Vorab definierte Soll-Schutz-Maßnahmen werden regelmäßig überprüft,

• Es finden in regelmäßigen Abständen interne Adaptierungen statt,

• Datenschutzvorfälle werden stets dokumentiert und ausgewertet,

• Es existiert ein Informationssicherheitsmanagement,

• Beteiligung des Datenschutzbeauftragten beim Abschluss neuer Vereinbarungen zur

Auftragsverarbeitung sowie diesbezügliche Kontrollhandlungen des Datenschutzbeauftragten.

Datum, ….. Unterschrift: