AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 ABS. 3 DSGVO

Auftraggeber (Verantwortlicher):

Vorname und Nachname des Kooperationspartners | Nummer des Kooperationspartners

Firma

Straße, Hausnummer | PLZ, Ort

Auftragnehmer (Auftragsverarbeiter):
ThomasLloyd Global Asset Management GmbH
Hanauer Landstraße 291b
60314 Frankfurt am Main
Deutschland

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:
Regelmäßig wiederkehrende Durchführung von Mailing-Aktionen gemäß jeweiligem Einzelauftrag; Mailings an Kunden und Interessenten des Verantwortlichen (Adressen werden vom Verantwortlichen überlassen), Prüfung der Adressdaten auf Versandfähigkeit, Dublettenabgleich im Auftrag des Verantwortlichen; Personalisierung der Mailings auf den Verantwortlichen; Korrekturfreigabe an den Verantwortlichen; kostenloser Versand des Mailings.

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

Die Datenverarbeitung im Rahmen dieser Auftragsverarbeitung findet grundsätzlich in der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) und in der Schweiz statt. Es ist dem Auftragnehmer gleichwohl gestattet, personenbezogene Daten des Auftraggebers unter Einhaltung der Regelungen dieser Vereinbarung auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber hierüber und über den Ort der Datenverarbeitung rechtzeitig vorab informiert und die besonderen Voraussetzungen der Artt. 44 bis 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSG-VO vorliegt. Die Schweiz bietet nach einem Angemessenheitsbeschluss der Europäischen Kommission ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DSGVO.

2. Dauer des Auftrags

Der Vertrag beginnt mit Unterzeichnung dieser Vereinbarung durch beide Parteien und endet durch Kündigung einer der Parteien. Die Kündigung hat in Textform und mit einer Kündigungsfrist von 4 Wochen zu erfolgen.

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 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):
- Entgegennahme und Speicherung der Kontaktdatensätze (Name, Adresse, E-Mail-Adresse) der zu bewerbenden Kunden und Interessenten des Verantwortlichen
- Dublettenabgleich
- Versand der Werbesendungen der jeweiligen „ThomasLloyd E-Mailing-Aktion“ oder „ThomasLloyd Postmailing-Aktion“

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):
- Kontaktdatensätze (Name, Adresse, E-Mail-Adresse) der zu bewerbenden Kunden und Interessenten des Verantwortlichen

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
- Kunden oder Interessenten des Verantwortlichen

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO 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.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 6 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen gemäß Anlage 1 sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Die Vertragspartner sind einander verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des jeweils anderen Vertragspartners vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

Vorname, Nachname, Organisationseinheit, Telefon

Vorname, Nachname, Organisationseinheit, Telefon

Weisungsempfänger des Auftragnehmers ist der jeweilige Ansprechpartner des Auftraggebers.

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.

6. 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 des Staates, 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 DSGVO).

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.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:
- Einhaltung und Umsetzung der in den Anlagen festgelegten technischen und organisatorischen Maßnahmen.
- Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO 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 DSGVO).

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 DSGVO). 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 – 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 DSGVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nicht gestattet.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO 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 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz
- **Herr Andreas Obrist**, ThomasLloyd Global Asset Management (Schweiz) AG; Uraniastrasse 35, 8001 Zürich; E-Mail: gdpr@thomas-lloyd.com

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

7. 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 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

8. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, hinsichtlich der Auftragsverarbeitung weitere Auftragsverarbeiter (nachfolgend „Subunternehmer“) einzubeziehen, insbesondere verbundene Unternehmen des Auftragnehmers wie die z.B. ThomasLloyd Global Asset Management (Schweiz) AG. Sollten verbundene Unternehmen mit Sitz in einem Drittstatt einbezogen werden, informiert der Auftragnehmer den Auftraggeber gesondert über die getroffenen Maßnahmen zur Sicherung eines angemessenen Datenschutzniveaus gem. Artt. 44 ff. DSGVO.

Der Auftragnehmer wird die vertraglichen Vereinbarungen mit Subunternehmern schriftlich fixieren und die entsprechenden Verträge so gestalten, dass letztlich die vertraglichen Pflichten und ggf. ergänzenden Weisungen, denen der Auftragnehmer nach dieser Vereinbarung unterliegt, auch gegenüber den Subunternehmern gelten. Die Parteien sind sich einig, dass diese Anforderung erfüllt ist, wenn die vertraglichen Vereinbarungen mit dem Subunternehmer ein dieser Vereinbarung entsprechendes Schutzniveau aufweisen bzw. dem Subunternehmer die in Art. 28 Abs. 3 DSGVO vorgeschriebenen Pflichten auferlegt sind.

Nicht als Subunternehmerverhältnisse im Sinne der vorstehenden Regelungen sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Reinigungsleistungen oder unter Umständen auch Prüfleistungen oder Wartungsleistungen, auch wenn dabei ein Zugriff auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann. Der Auftragnehmer wird auch bei solchen fremd vergebenen Nebenleistungen angemessene Regelungen zum Schutz der Vertraulichkeit der Daten des Auftraggebers treffen.

Unter Einhaltung der Anforderungen gemäß Ziff. 1 dieser Vereinbarung gelten die Regelungen in dieser Ziff. 8 auch, wenn ein Subunternehmer in einem Drittstaat einbezogen wird. Der Auftraggeber erklärt sich bereit, an der Erfüllung der besonderen Voraussetzungen der Artt. 44 ff. DSGVO mitzuwirken.

9. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

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 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbar-

keit 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.

Die in der Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit beim Auftragnehmer stellen 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.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen nach der Anlage 1 zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Sollte sich ein Nachbesserungs- bzw. Anpassungsbedarf hinsichtlich der technischen oder organisatorischen Maßnahmen ergeben, wird der Auftragnehmer den Auftraggeber hierüber unverzüglich informieren. Der Auftragnehmer unterstützt den Auftraggeber ferner bei der Dokumentation der Einhaltung der gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Soweit eine Prüfung durch den Auftraggeber vor Beginn oder während der Auftragsverarbeitung einen Nachbesserungs- bzw. Anpassungsbedarf hinsichtlich der technischen oder organisatorischen Maßnahmen ergibt oder soweit ein solcher aus anderen Gründen erforderlich ist, wird dieser im gegenseitigen Einvernehmen vom Auftragnehmer erfüllt und dokumentiert. Die Dokumentation ist dem Auftraggeber zu übergeben; die dokumentierten Maßnahmen werden Bestandteil und Grundlage dieses Vertrags.

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 Auftragnehmer 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.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Beendigung dieser Vereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder auf dessen Verlagen 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.

11. Haftung

Auf Art. 82 Abs. 1 DSGVO wird verwiesen. Im Übrigen wird folgendes vereinbart:
Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Vertragspartner im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall einen Vertragspartner ganz oder über dem Verantwortungsanteil des betreffenden Vertragspartners liegend auf Schadenersatz in Anspruch, kann dieser Vertragspartner von der jeweils anderen Vertragspartner Freistellung oder Schadloshaltung verlangen, soweit der Schadenersatz über ihrem Anteil an der Verantwortung liegt.

12. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften:

_____	_____
Auftraggeber	Auftragnehmer

Anlage 1: Technische und organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit beim Auftragnehmer

ANLAGE 1
ZUM AUFTRAGSVERARBEITUNGSVERTRAG NACH ART. 28 ABS. 3 DSGVO

Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit bei ThomasLloyd

Nach Art. 28 Abs. 3 DSGVO sind die nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Datenschutzmaßnahmen schriftlich festzulegen.

Die Umsetzung und Einhaltung der nachstehenden technischen und organisatorischen Maßnahmen wird durch regelmäßige Kontrollen des Datenschutzbeauftragten bei ThomasLloyd überprüft.

1. Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsunterlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:
- Eingangstür zum Büro ist ständig verschlossen (während und außerhalb der Geschäftszeiten).
- Es existiert eine chipgestützte elektronische Zutrittskontrolle mit Protokollierung.
- Die Chip- und Schlüsselvergabe wird dokumentiert.
- Eingangsbereich befindet sich im Sichtbereich des Sekretariats- und Empfangspersonals.
- Externe dürfen und können sich nur unter ständiger Begleitung im Büro bewegen.
- Besucher werden in ein Besucherbuch eingetragen.
- Alarmanlage außerhalb der Bürozeiten aktiv; zusätzliche Sperrung der chip-gestützten elektronischen Zutrittssperre.
- Zutritt zu Server- und Netzwerkbetriebsräumen nur für IT-Leiter und Stellvertreter möglich.

2. Zugangskontrolle

Maßnahmen zur Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
- Alle DV-Systeme sind nur mit Username und Passwort nutzbar.
- Username und Passwort werden individuell vergeben.
- Passwörter sind vertraulich und müssen eine Mindestlänge haben.
- Passwörter müssen regelmäßig geändert werden.
- Das gleiche Passwort kann nicht mehrmals verwendet werden.
- Arbeitsstationssperre nach 20 Minuten Inaktivität, Sperre kann nur durch angemeldeten Benutzer oder Administrator aufgehoben werden.
- Serversysteme sind nur an der Konsole oder über verschlüsselte Verbindung administrierbar.
- Serversysteme sind durch unterschiedliche Passwörter geschützt.
- Zugang zu den Daten und Prozessen der Serversysteme ist nur innerhalb des internen Netzes möglich; es sind keine externen Clients vorhanden; Abschottung nach außen durch zweistufiges Firewall-Konzept inkl. Intrusion Detection System (IDS) mit Software unterschiedlicher Hersteller.
- Zweifaches Viren-Scanning durch Software unterschiedlicher Hersteller mit mindestens täglicher Aktualisierung der Signaturen.
- Es existiert ein regelbasierter Viren-Komplettscan.

3. Zugriffskontrolle

Maßnahmen zur Gewährleistung, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
- Einrichtung von persönlichen Mitarbeiteraccounts.
- Vergabe von Zugriffsberechtigungen nur für die unmittelbar involvierten Mitarbeiter auf ausschließlich die Daten, die entsprechend der zu erledigenden Aufgaben benötigt werden (rollenbasiertes Zugriffsrechtesystem).
- Rechtevergabe erfolgt zentral durch den Systemadministrator, getrennt nach Dateiabfrage, Erstellen, Schreiben, Modifizieren, Löschen, Lesen und Zugriffsteuerung.
- Zugriffsrechte werden nach Gruppenrichtlinien, in Ausnahmefällen individuell, vergeben.
- Rechte können kurzfristig vergeben und wieder entzogen werden.
- Überprüfung der Zugriffsrechte bei jeder Authentifizierung gegenüber den Arbeitsstationen und Servern.

- Freigabeverfügung nur Geschäftsführung bzw. Verantwortliche des Datenbereiches .
- Zugriffsberechtigungen werden protokolliert.
- Eindeutige Identifizierung der Rechner durch den Server über IP-Adress-Prüfung.
- Schutz der Arbeitsstationen gegen unbefugte Veränderungen der Hard- oder Software.
- Ständig aktualisierter Schutz der Arbeitsstationen und Server gegen Virenbefall und Schadsoftware.
- Abschottung des internen Netzwerks durch ein permanent gepflegtes und überwachtes mehrstufiges Firewall- und Intrusion Detection System.
- Eingeschränkter Zugriff auf das Internet (regelbasiert)

4. Weitergabekontrolle

Maßnahmen zur Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
- Elektronische Datenübertragung erfolgt entsprechend den konkreten Vereinbarungen mit autorisierten Empfängern.
- Personenbezogene Daten werden bevorzugt über einen SSL-gesicherten Internetserver („Dokumentenschließfach“) übertragen (https, hochgradig verschlüsselt, RSA 2048 Bit, durch Verisign signiert).
- Zugriff auf Dokumentenschließfach ist nur über personenbezogene Accounts möglich.
- Daten werden nicht auf Arbeitsstationen gespeichert.
- Daten werden ausschließlich über das interne Netzwerk auf gesicherten Datenträgern (Server) im Rechnerraum gespeichert.
- Es werden auf mobilen Datenträgern (Disketten, CDs, USB-Sticks etc.) keine personenbezogenen Daten gespeichert.
- Unabhängig davon werden sonstige Daten (z. B. Präsentationen) nur durch autorisierte Mitarbeiter auf mobilen Datenträgern (Disketten, CDs, USB-Sticks etc.) gespeichert.
- Wiederbeschreibbare mobile Datenträger (USB-Sticks) werden nach Verwendung in der Grafikabteilung abgegeben und die darauf befindlichen Daten gelöscht.
- Nach der Verwendung werden mobile Datenträger durch einen externen zertifizierten Dienstleister (documentus GmbH Berlin & Co. Betriebs KG) vernichtet.
- Verbot der Nutzung eigener Notebooks, USB-Sticks, Festplatten im Firmennetzwerk.
- Sperrung entsprechender Schnittstellen an den Arbeitsstationen (z.B. USB-Controller, Diskettenlaufwerke, optische Schreibgeräte).
- Nutzung entsprechender Schnittstellen nur an ausgewählten und kontrollierten Arbeitsstationen.
- Permanente Überwachung und Protokollierung der Zugriffe und Prozesse auf allen beim Auftragnehmer zur elektronischen Datenübertragung genutzten Servern und Netzwerkeinrichtungen (Firewalls, Router).
- Aufbewahrung der Sicherungsbänder in feuerfestem Tresor, Zugriff nur durch die IT-Abteilung.
- Datenübertragung zwischen den Standorten erfolgt über VPN.

5. Eingabekontrolle

Maßnahmen zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
- Automatische Protokollierung von Anmelde- und Systemaktivitäten auf allen Arbeitsstationen und Servern.
- Kein Zugriff auf komplette Datensätze oder mehr als einen Datensatz gleichzeitig während der Datenerhebung bzw. -erfassung.
- Nachvollziehbare Zeitpunkt- und Benutzerinformationen für alle Dateien.
- Automatische Protokollierung aller Änderungen im Datenerhebungssystem mit Zeit und User.
- Tägliche Datensicherung aller Daten und Protokolle mit entsprechenden Informationen zur Erstellung, Änderung oder Löschung von Daten.
- Aufbewahrung der Sicherungsdatenträger im Tresor.

6. Auftragskontrolle

Maßnahmen zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Die Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer wird auftragsbezogen durch den jeweiligen Vertrag geregelt.
- Die im jeweiligen auftragsbezogenen Vertrag genannten ThomasLloyd-Ansprechpartner („Projektleiter“) sind gegenüber anderen ThomasLloyd Mitarbeitern hinsichtlich der Nutzung und der Verarbeitung der personenbezogenen Daten weisungsberechtigt.
- Belehrung und vertragliche Verpflichtung aller für ThomasLloyd tätigen Mitarbeiter zur Einhaltung der Datenschutzbestimmungen.
- Vergabe von Tätigkeiten der Datenverarbeitung nach außen nur nach vorheriger Zustimmung des jeweiligen Auftraggebers, sofern Daten des Auftraggebers betroffen sind (hier ausgeschlossen); Abschluss von AVV-Verträgen.
- Abstimmung des Fragebogens mit dem Auftraggeber und Freigabe durch diesen.
- Programmierung entsprechend des freigegebenen Fragebogens.
- Stichprobenweise Kontrolle der Übereinstimmung durch den/die Projektleiter/in und die/den Datenschutzbeauftragte/n.

7. Verfügbarkeitskontrolle

Maßnahmen zur Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
- Schutz gegen Viren und Schadsoftware sowie Netzwerkabschottung.
- Schutz aller Arbeitsstationen und Server gegen Ausfall.
- Ausfalltolerante Plattensysteme (RAID).
- Synchrone Duplizierung auf Fallback-Systeme.
- Gewährleistung schneller Wiederherstellung inkl. der Benutzerprofile.
- Tägliche Komplettsicherung aller Datenbestände und E-Mail-Kommunikation.
- Tägliches Backup für alle wichtigen Server inkl. Systemeinstellungen und Protokollierung.
- Gegen Diebstahl, Missbrauch und Feuer geschützte Lagerung der Sicherungsdatenträger im Tresor innerhalb des Büros und außerhalb (anderer Gebäudeteil).
- USV-Pufferung ist vorhanden.
- Abschottung nach außen durch zweistufiges Firewall-Konzept inkl. Intrusion Detection System (IDS) mit Software unterschiedlicher Hersteller.
- Zweifaches Viren-Scanning durch Software unterschiedlicher Hersteller mit mehrfach täglicher Aktualisierung der Signaturen.

8. Trennungsgebot

Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:
- Datenschutzgerechte Mandantentrennung der Daten nach Auftraggebern und Aufträgen.
- Organisatorische Trennung zwischen Programmentwicklung, -realisierung, Datenerhebung und -verarbeitung sowie den anderen Unternehmensbereichen.
- Abbildung der Organisationskontrolle in Gruppenrichtlinien und Zugriffsrechten.
- Physisch getrennte Aufbewahrung von Befragungsdaten und personenbezogenen Daten.
- Zugriff entsprechend des Berechtigungskonzeptes.
- Löschung personenbezogener Daten nach Abschluss des Auftrages entsprechend der Vorgaben der jeweiligen Auftraggeber.