Anlage Datenverarbeitungsprozesse

I. Zusatzbedingungen Datenschutz - technische und organisatorische Maßnahmen (ZB/MD)

Die hier beschriebenen technischen und organisatorischen Maßnahmen werden verbindlich festgelegt zwischen _____ (Auftraggeber) und Hubject GmbH (Auftragnehmer). Sie gelten für das Vertragsverhältnis Nutzungsvertrag.

Die Auftragsdatenverarbeitung erfolgt ausschließlich auf und mit Systemen und Hardware, die vom Auftraggeber zur Verfügung gestellt wird:
☐ ja* ☒ nein
*Darf nur angekreuzt werden, wenn keine Daten aus den Systemen des Auftraggebers exportiert werden.
*Bei „ja" sind nur die Fragen mit unterstrichenen Ziffern zu beantworten.

1. Zutrittskontrolle

1.1 Die Gebäude sind mit einer Alarmanlage gesichert:
☒ ja ☐ nein

1.2 Die Eingangstüren des Gebäudes sind mit folgender Schließanlage versehen:
☒ manuelle Schließanlage bei der Hubject GmbH ☒ Chipkartenzugangssystem im Rechenzentrum

1.3 Die Dokumentation der Zutrittsberechtigungen vorgenannter Schließanlage erfolgt namensscharf:
☒ ja ☐ nein

1.4 Der Gebäudezutritt von Firmenfremden/Gästen/Besuchern wird namensscharf dokumentiert:
☒ ja, im Rechenzentrum ☐ nein ☒ nein, Zutritt und Aufenthalt erfolgen nur in Begleitung von Firmenpersonal

1.5 Der Gebäudezutritt von Reinigungs- und Wartungspersonal wird namensscharf dokumentiert:
☒ ja ☐ nein

1.6 Es bestehen Regelungen bzgl. der Entziehung von Gebäudezutrittsberechtigungen und Zugriffsrechten zu Computersystemen inkl. Dokumentation für Mitarbeiter bei Beendigung des Arbeitsverhältnisses:
☒ ja ☐ nein

1.7 Es besteht ein gesondertes Zutrittskonzept für Serverräume inkl. namensscharfer Dokumentation (inkl. Reinigungspersonal, Wachpersonal etc.):
☒ ja, im Rechenzentrum ☐ nein ☐ nein, aber die Reinigung des Serverraums erfolgt nur unter Überwachung

2. Zugangskontrolle

2.1 Das Firmennetzwerk ist gegen das öffentliche Netzwerk durch eine Hardware-Firewall geschützt:
☒ ja, im Rechenzentrum ☐ nein
wenn ja:
Typ: 2 stufig, ASA5520 und ASA5550 sowie Tipping Point 110 IPS
Aktualisierungsverfahren und -häufigkeit: 2x wöchentlich, automatisch

2.2 Es werden regelmäßig Penetrationstests aller zum Internet geöffneten IP-Adressen durchgeführt:
☒ ja, im Rechenzentrum ☐ nein

2.3 Es erfolgt eine netzwerktechnische Separierung der Daten des Auftraggebers innerhalb des Firmennetzwerkes:
☒ ja ☐ nein
wenn ja, durch welche Maßnahmen: eigene virtuelle Einheit (VM-Server) sowie VLAN

2.4 Die Mitarbeiter werden auf folgende Passwortvorgaben verpflichtet:
☒ Individuell geheim zu haltendes Computerkennwort für jeden Mitarbeiter
☒ Keine Sammelkennwörter
☒ Mindestlänge, wenn zutreffend: Anzahl Zeichen/Komplexität: 8 Zeichen mit Sonderzeichen, Großbuchstaben
☒ Wechselrhythmus, wenn zutreffend bitte Zeitintervall angeben: 90 Tage
☒ Automatische Verriegelung des Computers nach Zeitintervall: nach 15 Minuten

2.5 An den folgenden Übergängen zum Firmennetz werden Virenscanner eingesetzt:
☒ E-Mail-Account
☒ FTP
☒ Web

2.6 Einsatz eines Virenscanners auf allen Servern:
☐ ja ☒ nein Ausschließlich Unix Server ohne direkten Datenaustausch mit Windows
wenn ja, Aktualisierungsverfahren und -häufigkeit: Prüfung vor Einbringen der Daten, Linux-Server

2.7 Einsatz eines Virenscanners auf allen Einzelarbeitsplatzcomputern:
☒ ja ☐ nein
wenn ja, Aktualisierungsverfahren und -häufigkeit: stündliche Prüfung auf aktuelle Signaturen, automatische Verteilung,

2.8 Sicherheitsrelevante Softwareupdates werden regelmäßig und automatisiert in die vorhandene Software eingespielt:
☒ ja ☐ nein

2.9 Mitarbeiter haben lokale Administrationsrechte:
☐ ja ☒ nein

2.10 Mitarbeiter haben Internetzugangsberechtigung:
☒ ja ☐ nein
wenn ja: restriktive, von Mitarbeitern nicht änderbare Browserkonfiguration eingerichtet:

☐ ja ☒ nein

3. Zugriffskontrolle

3.1 Berechtigungskonzepte sind vorhanden und werden dokumentiert:
☒ ja ☐ nein

3.2 Die Organisation der Berechtigungsvergabe wird namensscharf dokumentiert (insb. wer darf welche Rechte vergeben):
☒ ja ☐ nein

3.3 Die vergebenen Berechtigungen werden namensscharf aktualisiert und dokumentiert:
☒ ja ☐ nein

3.4 Anzahl der Administratoren mit der Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren: 2, Verpflichtungserklärungen nach BDSG liegen vor

3.5 Anzahl Mitarbeiter (keine Administratoren!) mit der Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren: keiner

3.6 Folgende Komponenten der Arbeitsplatzcomputer wurden verriegelt/deaktiviert, damit keine Datenexporte aus dem Rechenzentrum extern gespeichert werden können:
☐ USB-Ports
☐ CD-/DVD-Brenner
☐ Speicherkartenslots
☐ andere mobile Datenträger, wenn zutreffend welche: _____

3.7 Fernwartungs-/Fernzugriffszugänge sind vorhanden für:
☒ weitere Dienstleister
☒ Mitarbeiter
wenn Fernwartungs-/Fernzugriffszugänge vorhanden sind, bitte folgende Angaben ergänzen:
Art der Authentisierung: Benutzername und Passwort
Verwendete Protokolle (z.B.: SSH): SSL zertifikatsbasiert und IP Whitelisting

4. Weitergabekontrolle

4.1 Eingesetzte Verschlüsselungsart für Datenaustausch zwischen Auftraggeber und Auftragnehmer:
☐ SFTP
☒ S/Mime: Dokumentenaustausch erfolgt mit BSI über den Sharepoint, der mittels Credentials eine Zugangsteuerung zu diesen Dokumenten ermöglicht.
☒ Sonstige, Verfahren bitte erläutern: SSL zertifikatsbasiert und IP Whitelisting

4.2 Die per Datenträger versendeten Daten werden verschlüsselt:
☐ ja ☐ nein
wenn ja, Verfahren bitte erläutern: kein Versand per Datenträger

4.3 Erläuterung des Rückmeldeverfahrens an den Auftraggeber bei erhaltenem Datenträger oder vermutetem Datenträgerverlust:
kein Versand per Datenträger

4.4 Erläuterung der Entsorgung des vom Auftraggeber erhaltenen Datenträgers inkl. Dokumentation:
kein Versand per Datenträger

4.5 Daten des Auftraggebers werden zusätzlich verschlüsselt gespeichert:
☒ ja ☐ nein
wenn ja, Erläuterung des Verfahrens: FIPS 140-2 Level 1FSS

4.6 Werden Backups durchgeführt:
☒ ja, verschlüsselt ☐ ja, unverschlüsselt ☐ nein

4.7 Gesicherte Aufbewahrung der Backupmedien:
☒ ja ☐ nein

4.8 Wie und wann werden die Daten des Auftraggebers nach Auftragsende gelöscht (elektronische Datenträger/Papierdokumente):
Nach Beendigung des Vertrags werden dem Kunden alle seine gespeicherten Daten auf Wunsch maschinenlesbar zur Verfügung gestellt und nach Bestätigung der Lesbarkeit oder einer angemessenen Frist die Administrator und Benutzerkonten sowie jegliche Anwendungen und Daten von Colt gelöscht

4.9 Maßnahmen zum Schutz von Daten des Auftraggebers (auch temporären) auf mobilen Arbeitsplatzrechnern:
nicht anwendbar

4.10 Maßnahmen zum Schutz von Daten des Auftraggebers (auch temporären) auf mobilen Datenträgern:
nicht anwendbar

5. Eingabekontrolle

5.1 Es werden Log-Files für die Nachvollziehbarkeit der Löschung/Änderung von Daten des Auftraggebers namensscharf je Mitarbeiter angelegt:
☒ ja ☐ nein

5.2 Es besteht ein restriktives Zugriffskonzept für vorgenannte Log-Files:
☒ ja ☐ nein

6. Auftragskontrolle

6.1 Die Mitarbeiter werden schriftlich auf das Datengeheimnis gem. § 5 BDSG [vgl. Artikel 16 RiLi 95/46/EG] verpflichtet
☒ ja ☐ nein

6.2 Die Mitarbeiter werden schriftlich auf das Fernmeldegeheimnis gem. § 88 TKG [Artikel 5 RiLi 2002/58/EG] verpflichtet

☐ ja ☒ nein

6.3 Folgende schriftliche Zusatzerklärungen (im Zusammenhang mit Datenschutz und Datensicherheit) holt der Auftragnehmer von seinen Mitarbeitern ein:

6.4 Es werden/wurden Subauftragnehmer beauftragt, die Zugriff auf Daten des Auftraggebers haben:
☒ ja ☐ nein

6.5 Mit Subauftragnehmern, die Daten des Auftraggebers verarbeiten, bestehen Verträge zur Auftragsdatenverarbeitung gem. § 11 BDSG [Artikel 17 Abs. 3 RiLi 95/46/EG i.V.m. Artikel 17 Abs. 1 RiLi 95/46/EG sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG]:
☒ ja ☐ nein

6.6 Es gibt Subauftragnehmer außerhalb der EU, die Zugriff auf Daten des Auftraggebers haben:
☐ ja ☒ nein

6.7 Subauftragnehmer, die Zugriff auf Daten des Auftraggebers erhalten, halten die in dieser Checkliste vereinbarten technischen und organisatorischen Maßnahmen genau so wie der Auftragnehmer selbst ein und haben deren Einhaltung vertraglich zugesichert:
☒ ja ☐ nein

6.8 Es erfolgen Schulungen der Mitarbeiter zum Datenschutz inkl. namensscharfer Dokumentation:
☒ ja ☐ nein

6.9 Für das Unternehmen des Auftragnehmers bestehen zurzeit folgende Zertifikate/Datenschutzkonzepte, die auf Verlangen beim Auftragnehmer im Hause eingesehen werden können:
Hubject: Datenschutzkonzept vom 2./3. Mai 2013

7. Verfügbarkeitskontrolle

7.1 Häufigkeit und Anzahl Generationen der Datensicherungsmaßnahmen: Vollsicherung wöchentlich, inkrementell täglich

7.2 Aufbewahrungsort von Sicherungsdatenträgern:
☐ Safe ☒ Externe Auslagerung ≥3km (Luftlinie) Entfernung

7.3 Wiederanlaufzeit nach vollständiger Zerstörung des Rechenzentrums in Tagen: ---

7.4 Es bestehen Verträge für die Wartung von IT-Systemen durch Externe:
☒ ja ☐ nein

8. Trennungskontrolle

8.1 Daten des Auftraggebers werden in einem eigenen, extra für den Auftrag vorgesehenen Mandanten vorgehalten:
☒ ja ☐ nein

8.2 Es besteht ein Berechtigungskonzept für vorgenannte Mandanten, dass den Datenzugriff von Mitarbeitern ausschließt, die nicht für den Auftraggeber tätig sind:
☒ ja ☐ nein

8.3 Mitarbeiter, die Daten des Auftraggebers verarbeiten, sitzen räumlich getrennt von Mitarbeitern, die für andere Auftraggeber arbeiten:
☐ ja ☒ nein

8.4 Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen:
☒ ja ☐ nein

9. Unterschrift

Wir versichern, dass die hier getätigten Angaben dem aktuellen Stand der bei uns umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten Angaben sind unmittelbar an den Auftraggeber des Nutzungsvertrages gem. Satz 1 dieses Teils I. Zusatzbedingungen Datenschutz - technische und organisatorische Maßnahmen (ZB/MD) zu melden.

Berlin, 13. Oktober 2015

(Thomas Daiber) (Christian Hahn)

II. Zusatzbedingungen Datenschutz - Auftragsdatenverarbeitung (ZB/D)

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt im Rahmen einer Auftragsdatenverarbeitung (ADV) im Sinne des § 11 Bundesdatenschutzgesetz (BDSG). Erfolgt die ADV außerhalb des Gebietes der Bundesrepublik Deutschland aber in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum gilt die entsprechende EU-Gesetzgebung [Artikel 17 Absatz 3 RiLi 95/46/EG], welche nachfolgend jeweils in Klammern genannt wird. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG [Artikel 25 und 26 RiLi 95/46/EG] erfüllt sind.

1. Gegenstand, Umfang und Dauer des Auftrags

1.1. Gegenstand und Umfang des Auftrags
Der Gegenstand des Auftrags ergibt sich aus dem Nutzungsvertrag, zu dem diese Zusatzbedingungen Anlage sind und auf den hier verwiesen wird (im Folgenden: Vereinbarung).

1.2. Dauer des Auftrags
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Vereinbarung.
Eine vorzeitige Beendigung der Laufzeit durch fristlose Kündigung ist im Falle einer Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen zulässig. Gleiches gilt, wenn der Auftragnehmer eine berechtigte Weisung des Auftraggebers nicht ausführen will oder kann.

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten
Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Vereinbarung in § 8 i.V.m. § 15 (Vertragsbedingungen Nutzungsvertrag EMP) sowie in § 10 i.V.m. § 17 (Vertragsbedingungen Nutzungsvertrag CPO) konkret beschrieben.

2.2. Art der Daten
Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten:

- ☐ Name, Titel, akademischer Grad
- ☐ Berufs-, Branchen- oder Geschäftsbezeichnung
- ☐ Anschrift
- ☐ Geburtsdatum/-jahr/-tag
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ TKG-Daten (Verkehrs-, Standort,- und Nutzungsdaten, Einzelverbindungsdaten i.S. des Telekommunikationsgesetzes, TKG, [Artikel 3 RiLi 2002/58/EG]
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Sensitive Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben)
- ☐ Daten, die einem Berufsgeheimnis unterliegen
- ☐ Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen
- ☐ Daten zu Bank- und Kreditkartenkonten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☒ Contract-ID, Charge-Detail-Record (vgl. Anlage OICP)

2.3. Kreis der Betroffenen
Der Kreis der Betroffenen, deren Daten im Rahmen dieses Auftrags verwendet werden, umfasst:

- ☐ Mitarbeiter
- ☐ Angehörige von Mitarbeitern
- ☐ Pensionäre/Hinterbliebene
- ☐ Bewerber
- ☒ Kunden der Vertragspartner von Hubject (EM-User)
- ☐ Mitarbeiter von Fremdfirmen
- ☐ Interessenten
- ☐ Mieter/Vermieter, Pächter/Verpächter
- ☐ Lieferanten
- ☐ Ansprechpartner

3. Technische und organisatorische Maßnahmen nach § 9 BDSG [Artikel 17 Abs. 1 RiLi 95/46/EG]

Der Auftragnehmer hat die Umsetzung der dargelegten technischen und organisatorischen Maßnahmen gem. § 9 BDSG [Artikel 17 Abs. 1 RiLi 95/46/EG sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG] vor der Auftragserteilung und vor Beginn der Verarbeitung zu dokumentieren und das Dokument dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

Er verpflichtet sich zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen gem. § 9 BDSG und Anlage [Artikel 17 Abs. 1 RiLi 95/46/EG sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG]:

☒ Die als Anlage beigefügten Zusatzbedingungen Datenschutz - technische und organisatorische Maßnahmen (ZB/MD) werden für den Auftragnehmer als verbindlich festgelegt.

☐ Anstelle der ZB/MD kann der Auftragnehmer in Ausnahmefällen nach Abstimmung mit dem Auftraggeber eine auftragsbezogene Dokumentation der technischen und organisatorischen Maßnahmen vornehmen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind schriftlich zu vereinbaren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG [Artikel 18 RiLi 95/46/EG] dem Auftraggeber zur Verfügung zu stellen.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat, mit Ausnahme der Regelungen unter Punkt 11 dieser Zusatzbedingungen, nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Falls eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG [Artikel 17 Abs. 3 RiLi 95/46/EG] folgende Pflichten:

- Wahrung des Datengeheimnisses entsprechend § 5 BDSG [Artikel 16 RiLi 95/46/EG) und/oder des Fernmeldegeheimnisses § 88 TKG [Artikel 5 RiLi 2002/58/EG i.V.m. 2009/136/EG]. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden. Die sich daraus ergebende Geheimhaltungspflicht gilt über das Vertragsende auf unbefristete Zeit hinaus, unabhängig von der Regelung über sonstige Geheimhaltungspflichten. Gleiches gilt für Daten, die dem Fernmeldegeheimnis unterliegen.
- Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage [Artikel 17 Abs. 1 RiLi 95/46/EG sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG].
- Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG [Artikel 28 RiLi 95/46/EG].
  Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG [Artikel 22 ff. RiLi 95/46/EG] beim Auftragnehmer ermittelt.
- Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweis der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit vorheriger schriftlicher Zustimmung des Auftraggebers gestattet. Derzeit sind nachfolgend aufgeführte Subunternehmer mit der Verarbeitung von personenbezogenen Daten beauftragt, mit der sich der Auftraggeber einverstanden erklärt:

  Betrieb Plattform inkl. IT-Service
  - Bosch Software Innovations GmbH; Stuttgarter Str. 130; 71332 Waiblingen
  - Colt Technology Services GmbH, Herriotstraße 4, 60528 Frankfurt
  - Datenvernichtung
  - Auslagerung Datenträger

- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG [Artikel 17 Abs. 3 RiLi 95/46/EG i.V.m. Artikel 17 Abs. 1 RiLi 95/46/EG sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG] beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den Vertragsinhalt hinsichtlich datenschutzrechtlicher Vereinbarungen und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

7. Zuständige Personenkreise

Beim Auftragnehmer:

Der Auftragnehmer wird dem Auftraggeber den zuständigen Datenschutzbeauftragten oder – sofern kein Datenschutzbeauftragter erforderlich ist – einen Ansprechpartner für den Datenschutz benennen.
Der bestellte Datenschutzbeauftragte des Auftragnehmers ist:
Herr Stefan Drost, mailto: datenschutz@hubject.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

Beim Auftraggeber:
Sofern sensitive Daten vom Auftragnehmer für den Auftraggeber verarbeitet werden, benennt der Auftraggeber folgende weisungsberechtigte Personen:

_____
Name, Vorname, Tel.

8. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Kontrolleure durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung im Geschäftsbetrieb des Auftragnehmers zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.
Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG [Artikel 17 Abs. 2 RiLi 95/46/EG] bzw. entsprechender nationaler Gesetzgebung weist der Auftragnehmer dem Auftraggeber vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage [Artikel 17 Abs. 1 RiLi 95/46/EG sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG] nach.
Der Auftragnehmer kann dem Auftraggeber zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschafsprüfer, Revision, IT-

Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz) vorlegen.

9. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet dem Auftraggeber unverzüglich eine Meldung, wenn durch ihn oder durch die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.
Es ist bekannt, dass nach § 42a BDSG sowie § 93 Abs. 3 TKG wie auch § 15a TMG [Artikel 4 RiLi 2002/58/EG] Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs (z.B. verschwundene Daten, zerstörte oder gelöschte Dateien, Infektionen mit Computerviren, Ausfall wesentlicher Hardwarekomponenten, softwarebedingte Störungen als Folge von Programmfehlern oder fehlerhafter Konfiguration), bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

10. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG [Artikel 17 Abs. 3 RiLi 95/46/EG]. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind zwischen Auftraggeber und Auftragnehmer abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen, es sei denn, die Leistungsbeschreibung sieht dies ausdrücklich vor.
Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden nur mit Zustimmung des Auftraggebers erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG [Artikel 17 Abs. 3 RiLi 95/46/EG] zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Vereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung/Vernichtung ist dem Auftraggeber vorzulegen.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.