Anlage 1 Konkretisierung der Auftragsverarbeitung

Erbringung von Wartungsleistungen an Drucksystemen und Multifunktionsgeräten

A. ART UND ZWECK DER AUFTRAGSVERARBEITUNG

teamXbingen GmbH (nachfolgend als **„Auftragnehmer“** bezeichnet) führt im Auftrag des Kunden (nachfolgend als „**Auftraggeber**“ bezeichnet) Wartungs- und/oder Pflegearbeiten an Drucksystemen und Multifunktionsgeräten durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogenen Daten bekommt bzw. Kenntnis erlangt. Die Vertragsparteien sind sich daher darüber einig, dass es sich bei dieser Teilleistung im Rahmen der Abwicklung des jeweiligen Wartungsvertrages um eine Auftragsverarbeitung i.S.d. Art. 28 DS-GVO handelt.

B. ARTEN VON DATEN UND KATEGORIEN BETROFFENER PERSONEN

In Abhängigkeit der durch den Auftraggeber / Kunden auf den Drucksystemen und Multifunktionsgeräten verarbeiteten Daten können folgenden Daten/ Kategorien betroffener Personen Bestandteil der Datenverarbeitung sein:

Art der Daten:
Personenstammdaten
Kommunikationsdaten z.B. Telefon, E-Mail)
Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
Kundenhistorie
Vertragsabrechnungs- und Zahlungsdaten
Planungs- und Steuerungsdaten
Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

Kategorien betroffener Personen:
Kunden
Interessenten
Beschäftigte
Lieferanten
Ansprechpartner

Dabei kann es sich um folgende Kategorien personenbezogener Daten handeln: (Diese Angaben betreffen nicht alle Kunden.):
Name, Anschrift, Kontaktdaten, Telefon, E-Mail, Kontaktperson, Kundennummer, Rechnungs- und Lieferanschrift, Steuer-ID, Umsatzsteueridentifikationsnummer, Bankverbindungen, Vertragsdaten und -historie (z.B. Laufzeit, Konditionen, Sicherheiten, Regulierer, Wartungs-, Kauf- und Mietgegenstände mit Produktbezeichnung, Standort, Seriennummer, Vertragsnummer, Installations- und Abbaudaten, technischen Daten/Gerätekonfiguration, Zählerstände, Nutzungsgrad, IP-Adresse, Problem-/Fehlercode), Rechnungsdaten und Rechnungshistorie, Daten aus der Erfüllung vertraglicher Verpflichtungen (Liefer- und Zahlungsverkehrsdaten, Lastschriftdaten), Korrespondenzen (z.B. telefonische, elektronische oder schriftliche Kontakte mit Informationen über Kontaktkanal, Zeitpunkt, Anlass, Ergebnis und Kopien des Schriftverkehrs), Art und Dauer der gewerblichen oder beruflichen Tätigkeit, Name, Anschrift, Handelsregisterdaten, betriebswirtschaftliche Kennzahlen (z.B. Einnahmen-/Überschussrechnungen, Bilanzen, betriebswirtschaftliche Auswertungen, private Vermögen- und Schuldenübersichten, Mitarbeiteranzahl), Bonitätsmerkmale (z.B. Zahlungsverhalten, interne und externe Ratings, externe Zahlungsweise, Creditreform-Nummer und -Auskünfte, Risi-

koklassenvergleich mit anderen Rating-Agenturen, Bonitätsindex, Ausfallwahrscheinlichkeit, Kreditlinie), politische Exponiertheit i.S.d § 1 Abs. 12 bis 14 des Geldwäschegesetzes, Anfragezähler, Identifikationsdaten (z.B. Personalausweis- oder Passangaben).

C. SUBUNTERNEHMER

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgendes Subunternehmers durchgeführt:

Xerox GmbH, Hammer Landstraße 91, 41460 Neuss

Die Xerox GmbH vergibt wiederum die Einsätze für Techniker an folgende Subunternehmen:

Top Service Logistic GmbH
Wendenstrasse 294, 20537 Hamburg

LPR GmbH, Heerdterbuschstr. 2, 41460 Neuss

Anhang
Technische und organisatorische Maßnahmen i.S.d. Artikel 32 DS-GVO zur Erbringung von Wartungsleistungen von Drucksystemen und Multifunktionsgeräten

A - Zutrittskontrolle

Zielsetzung:
Es sollen nur Befugte zu den Räumen mit Datenverarbeitungsanlagen Zutritt haben, mittels derer personenbezogene Daten verarbeitet oder genutzt werden.

Geltungsbereich:
Die Vertragsparteien sind für die zu treffenden Maßnahmen in ihrem jeweiligen Herrschaftsbereich grundsätzlich selbst verantwortlich. Dies gilt auch bei der Auftragsdatenverarbeitung. In Fällen der ADV ist der Auftraggeber dafür verantwortlich, dass die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen eine zum Schutz der verarbeiteten Daten angemessene Sicherheit bieten. Aus diesem Grund sind sie im Folgenden zu spezifizieren.

Umgesetzte Maßnahmen:
Die zu wartenden Drucksysteme und Multifunktionsgeräte (nachfolgend als „**Produkte**“ bezeichnet“) sind in den Produktions- oder Geschäftsräumen des Auftraggebers / Kunden installiert. Die Zutrittskontrolle zum Herrschaftsbereich unterliegt der Verantwortung des Auftraggebers / Kunden und ist nicht durch den Auftragnehmer zu gewährleisten. Daher ist der Auftraggeber dafür verantwortlich, entsprechende Sicherheitsmaßnahmen zu treffen, damit der Zutritt von Unbefugten zu den Räumen in denen die Produkte installiert sind unterbunden wird.

Umgesetzte Maßnahmen in den eigenen Räumen:
Die Büroräume der teamXbingen – Andreas Walloch GmbH befinden sich in einem Bürohaus in Bingen Kempten. Die Zugänge zum Bürohaus sind tagsüber frei zugänglich. Jeder Zugang zu den Büro´s ist von den Mitarbeitern einsehbar und somit für Fremde nicht frei zugänglich. Alle Bürozugänge und auch der Zugang zu dem Bürohaus sind von abends bis morgens verschlossen.
Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.
Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten beauftragt wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich anmeldet. Jeder Besucher wird von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet oder wird gebeten am Empfang auf seinen Ansprechpartner zu warten. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.
Die Eingänge und Fenster des Bürohauses und auch der Büroräume der team X bingen – Andreas Walloch GmbH sind mit einer Alarmanlage gesichert. Diese kann manuell aktiviert und deaktiviert werden. Unabhängig davon wird die Alarmanlage jeden Abend durch den Hausmeister aktiviert.

B - Zugangskontrolle

Zielsetzung:
Mit den Maßnahmen der Zugangskontrolle sollen nur Befugte Zugang zu den Datenverarbeitungseinrichtungen haben. Hier geht es nicht um die körperliche Zutrittskontrolle nach (A), sondern um den technischen / organisatorischen Zugang zu Datenverarbeitungssystemen bzw. deren Nutzungsmöglichkeit.

Geltungsbereich:
Es sind alle Personen einzubeziehen, die Datenverarbeitungsanlagen nutzen.

Umgesetzte Maßnahmen:

Bei Produkten, die über einen internen Druckercontroller verfügen, obliegt es dem Auftraggeber / Kunden den Zugang zum Produkt mittels Vergabe eines Benutzernamens und der Setzung eines Passworts sicherzustellen.
Bei Produkten, die über einen externen Druckercontroller verfügen und bei denen der Auftraggeber oder ein vom Auftraggeber beauftragter Dienstleister die Installation/Einbindung ins Netzwerk vornimmt, wird der Zugang standardmäßig bei der Installation durch den Auftraggeber / beauftragten Dienstleister mit einem Benutzernamen und Passwort gemäß Vorgabe des Auftraggebers / dessen Kunden zugriffsgeschützt.
Die Pflege und ggf. Änderung der Passwörter obliegt dem Auftraggeber / Kunden. Wurde das Passwort abweichend vom Standard durch den Auftraggeber geändert, muss dem Techniker der Zugriff auf das zu wartende Produkt aktive eingeräumt werden.
Die Zugriffs- und Rechtevergabe im Netzwerk des Auftraggebers / Kunden (z.B. im Active Directory) obliegt dem Auftraggeber / Kunden.

Umgesetzte Maßnahmen im eigenen Netzwerk:
Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag kann auch über die Personalabteilung gestellt werden.
Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 6 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.
Passwörter werden unregelmäßig gewechselt. Fehlerhafte Anmeldeversuche werden protokolliert. Bei 6-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts. Remote-Zugriffe auf IT-Systeme der team X bingen – Andreas Walloch GmbH erfolgen stets über verschlüsselte Verbindungen. Auf den Servern der team X bingen – Andreas Walloch GmbH ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.
Alle Server und Clients sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.
Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt. Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter werden grundsätzlich verschlüsselt gespeichert.

C - Zugriffskontrolle
Zielsetzung:
Ziel der Zugriffskontrolle ist es, mithilfe geeigneter Maßnahmen sicherzustellen, dass im Rahmen der Datenverarbeitung durch die Mitarbeiter nur auf die personenbezogenen Daten zugegriffen werden kann, für die sie eine Zugriffsberechtigung besitzen. Dritte dürfen keinen unbefugten Zugriff auf die Daten hinsichtlich Verarbeitung, Nutzung und Speicherung haben und auch eine unbefugte Entfernung der Daten darf nicht möglich sein.
Geltungsbereich:
Die Zugriffskontrolle ist bei jeglicher EDV-Anwendung durchzuführen; somit auch für den PC-Bereich.
Umgesetzte Maßnahmen:
Die Zugriffskontrolle ist grundsätzlich durch den Auftraggeber / Kunden sicherzustellen. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte sind vom Kunden / Auftraggeber zu erstellen / zu vergeben.
Im Rahmen der Erbringung von Wartungsleistungen kann der Techniker mit dem eingesetzten Diagnose-PCs eigenständig keinen Zugang zum Netzwerk des Auftraggebers / Kunden herstellen.

In Abhängigkeit der vom Auftraggeber / Kunden vorgenommenen Konfiguration des Produktes kann nicht ausgeschlossen werden, dass Xerox Techniker bzw. der durch Xerox beauftragte Subunternehmer mittels Diagnose-PC bzw. manuell Einsicht und/oder Zugriff auf die auf dem Produkt gespoolten oder gespeicherten Druckdaten erhält.
Es obliegt dem Auftraggeber /Auftraggeber, sicherzustellen, dass Jobprotokolllisten und Druckjobs regelmäßig gelöscht werden.

Ergänzende Regelungen zur Fernwartung:
teamXbingen führt grundsätzlich keine Fernwartung an Produkten durch.

Soweit durch teamXbingen zum Zwecke der Fernwartung ein Remote-Zugriff auf das Produkt erfolgt, gilt Folgendes:

- der Auftraggeber / Kunde muss teamXbingen bei jedem Remote-Zugriff/Sitzung eine Berechtigung erteilen
- jeder Remote-Zugriff/Sitzung wird telefonisch durch den Auftraggeber/ Kunden begleitet
- der Auftraggeber / Kunde bestimmt selbst die Art des Zugriffslevels (Fernsteuerung / nur Desktopansicht / Dateiübertragung / Abruf von Systeminformationen / Neustart)
- die Remote-Zugriff/Sitzung wird protokolliert und jeder Schritt ist ausschließlich für die beiden Parteien einsehbar/zugänglich. Weitere Einsicht in die zwischen den Computern übertragenen Daten ist ausgeschlossen
- die Datenübertragung nutzt das Verschlüsselungsprotokoll 2048 Bit RSA Public-/Private Key Exchange und ist mit 256 Bit AES verschlüsselt
- die zweistufige Verifizierung bei der Anmeldung ist sichergestellt

Interne umgesetzte Maßnahmen:
Berechtigungen für IT-Systeme und Applikationen der team X bingen – Andreas Walloch GmbH werden ausschließlich von Administratoren eingerichtet.
Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen.
Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden.
Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
Die Vernichtung von Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. Datenträger wie Festplatten, CD´s oder USB-Sticks werden vor der Entsorgung durch die Administratoren unbrauchbar und unlesbar gemacht.
Alle Mitarbeiter bei team X bingen – Andreas Walloch GmbH sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.
Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

D - Weitergabekontrolle
Zielsetzung:
Ziel der Weitergabekontrolle ist es, durch geeignete Maßnahmen zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung und beim Transport per Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Der Gesetzgeber empfiehlt hierzu insbesondere die Maßnahme der Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Der Einsatz eines

Verschlüsselungsverfahrens ist jedoch dann nicht zwingend notwendig, wenn durch die getroffenen Schutzmaßnahmen eine der Verschlüsselung vergleichbare Sicherheit erreicht wird. Sofern die getroffenen Schutzmaßnahmen diese Sicherheit nicht erreichen, wird die Verwendung der dem Stand der Technik entsprechenden Verschlüsselungsverfahren empfohlen.

Geltungsbereich:

Die Weitergabekontrolle gilt sowohl für die Datenweitergabe an Dritte als auch für den innerbetrieblichen Datentransfer und zwischen Auftraggeber und Auftragnehmer bei der Auftragsdatenverarbeitung.

Umgesetzte Maßnahmen:

Die Weitergabekontrolle obliegt der Verantwortung des Auftraggebers / Kunden, mit folgenden Ausnahmen:

- Dateien mit personenbezogenen Daten, die der Auftraggeber dem Auftragnehmer zu Test-/Analysezwecken zur Verfügung stellt
- Fernwartung

Die an den Auftragnehmer zu Test-/Analysezwecken übermittelten Dateien werden innerhalb des Netzwerkes ausschließlich verschlüsselt übermittelt. Nach Beendigung der Arbeiten werden die Dateien sowie alle erstellten Testdrucke durch den Auftragnehmer unverzüglich datenschutzgerecht vernichtet bzw. gelöscht. Zur Fernwartung siehe oben unter C.

Intern umgesetzte Maßnahmen:

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von team X bingen – Andreas Walloch GmbH erfolgt, darf jeweils nur in dem Umfang, erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.
Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.
Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.Die Nutzung von privaten Datenträgern ist den Beschäftigten im Zusammenhang mit Kundenprojekten untersagt.Mitarbeiter werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

E - Eingabekontrolle

Zielsetzung:

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass die näheren Umstände der Dateneingabe nachträglich überprüft und festgestellt werden können.

Geltungsbereich:

Es sind die Personen einzubeziehen, die Datenverarbeitungssysteme des Unternehmens nutzen.

Umgesetzte Maßnahmen:

Es findet durch den Auftragnehmer keine Eingabekontrolle oder Protokollierung der Zugriffe auf den Multifunktionsgeräten und externen Druckcontrollern statt.
Es obliegt dem Auftraggeber / Kunden, die Eingabe mittels Berechtigungskonzepten und bedarfsgerechter Zugriffsrechte zu überwachen.

F - Auftragskontrolle

Zielsetzung:

Ziel der Auftragskontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass personenbezogene Daten, die von einem externen Dienstleister im Auftrag verarbeitet werden (z.B. durch ein Rechenzentrum, IT-Dienstleister oder Call-Center), nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen.

Geltungsbereich:

Die Gewährleistung der erforderlichen Kontrollmaßnahmen obliegt sowohl dem Auftraggeber als auch dem Auftragnehmer.

Umgesetzte Maßnahmen:

Zwischen dem Auftragnehmer und den mit der Erbringung von Wartungsleistungen beauftragten Subdienstleitern bestehen Vereinbarungen zur Auftragsvereinbarung nach Maßgabe des Art. 28 DS-GVO. Die zur Leistungserbringung eingesetzten Subdienstleister wurden sorgfältig ausgewählt und werden regelmäßig hinsichtlich der Einhaltung der technisch-organisatorischen Maßnahmen geprüft und auditiert.

Die mit der Umsetzung des Auftrages befassten Mitarbeiter sind über den Leistungsumfang des Vertrages, die Regelungen der Vereinbarung der Auftragsverarbeitung sowie die einzuhaltenden/umgesetzten technisch-organisatorischen Maßnahmen unterrichtet.

Alle mit der Erfüllung des Auftrages beschäftigten Mitarbeiter des Auftragnehmers oder deren Subunternehmen sind auf das Datengeheimnis gem. § 5 BDSG a.F. / Vertraulichkeit verpflichtet worden.

G - Verfügbarkeitskontrolle

Zielsetzung:

Ziel der Verfügbarkeitskontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass geschützte Daten nicht durch Zufälligkeiten zerstört werden oder verloren gehen.

Geltungsbereich:

Es ist die Gesamtheit des Datenverarbeitungssystems einzubeziehen - sowohl Menschen als auch Programme und Materialien.

Umgesetzte Maßnahmen:

Die Verfügbarkeitskontrolle obliegt dem Auftraggeber/ Kunde. Datenschutzbezogene Maßnahmen wie bspw. Datensicherung, Datenauslagerung, unterbrechungsfreie Stromversorgung und andere Belange der Verfügbarkeitskontrolle sind grundsätzlich durch den Auftraggeber / Kunden zu ergreifen.

Intern umgesetzte Maßnahmen:

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von team X bingen – Andreas Walloch GmbH im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

H - Trennungsgebot

Zielsetzung:

Mit dieser Anforderung soll gewährleistet werden, dass Daten nur zu dem Zweck, zu dem sie bei der Erfassung erhoben wurden, verarbeitet werden dürfen. Der Zweck für den die Daten erhoben wurden, darf nicht geändert werden.

Aus diesem Grund ist es wichtig, dass Daten, die zu unterschiedliche Zwecken erhoben wurden, vollständig getrennt voneinander gespeichert werden.

(Zweckbindungsgrundsatz)

Geltungsbereich:

Diese Vorschrift gilt sowohl für Daten, die von der verantwortlichen Stelle selbst als auch für die, die durch Dritte im Auftrag erhoben wurden.

Umgesetzte Maßnahmen:

Alle von team X bingen – Andreas Walloch GmbH für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet**.**

I - Pseudonymisierung & Verschlüsselung:

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

J - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Zielsetzung

In regelmäßigen Abständen, jedoch mind. jährlich, soll durch eine geregeltes Verfahren sichergestellt und überprüft werden, ob die getroffenen technischen und organisatorischen Maßnahmen noch wirksam sind.
Hierdurch soll das Datenschutz-Risiko minimiert werden, indem Angriffsstellen lokalisiert und behoben werden. Dies ist auch aufgrund der ständigen technologischen Weiterentwicklung unbedingt erforderlich.

Geltungsbereich

Die Vertragsparteien sind für die zu Umsetzung des Verfahrens in ihrem jeweiligen Herrschaftsbereich grundsätzlich selbst verantwortlich. Dies gilt auch bei der Auftragsdatenverarbeitung.

Umgesetzte Maßnahmen:

Datenschutzmanagement

Datenschutz durch Technikgestaltung (Privacy by Design)

Einhaltung aller in diesen TOM definierten und aufgeführten Maßnahmen.