

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 1/22

Direktive Sicherheitsmaßnahmen Auftragnehmer

Dokumenteneigner: Kahnert

Freigegeben von: Kahnert

Freigabedatum: 09.05.2023

Ziele des Dokumentes

Diese Direktive beschreibt die Anforderungen an die Informationssicherheit der Auftragnehmer bei der ABEKING & RASMUSSEN Schiffs- und Yachtwerft SE.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version	Klassifizierung	Seite
Dokumentnummer	0	02 - intern	2/22

Inhalt

Inhalt	2
1 Einführung und Geltungsbereich	3
1.1 Einleitung.....	3
1.2 Geltungsbereich.....	3
2 Begriffsbestimmung	3
3 Wahrung von Vertraulichkeit von Informationen/Geschäfts-/Betriebsgeheimnissen	5
3.1 Geheimhaltung	5
3.2 Verpflichtung auf Vertraulichkeit (DSGVO, BDSG)	6
3.3 Verpflichtung weiterer Personen	7
4 Formen der Zusammenarbeit	7
5 Anforderungen an den Auftragnehmer zur Aufrechterhaltung der Informationssicherheit	9
5.1 Grundsätzliches.....	9
5.2 Organisation der Informationssicherheit	9
5.3 Privacy by Design (nur relevant bei personenbezogenen Daten)	10
5.4 Privacy by Default (nur relevant bei personenbezogenen Daten)	10
5.5 Zugriffskontrolle.....	10
5.6 Kryptographie und / oder Pseudonymisierung.....	10
5.7 Schutz von Gebäuden.....	11
5.8 Schutz von Betriebsmitteln / Informationswerten.....	11
5.9 Betriebsverfahren und Zuständigkeiten	11
5.10 Datensicherungen	12
5.11 Schutz vor Malware durch Schwachstellen- und Patchmanagement	12
5.12 Protokollierung und Überwachung	12
5.13 Netzwerksicherheitsmanagement	12
5.14 Informationsübertragung	13
5.15 Netztrennung	13
5.16 Anschaffung, Entwicklung und Instandhaltung von Systemen	13
5.17 Auftragnehmerbeziehungen bzw. Auftragsverarbeitung (AV).....	14
5.18 Management von Informationssicherheitsvorfällen.....	14
5.19 Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements	14
5.20 Einhaltung gesetzlicher und vertraglicher Anforderungen.....	14
5.21 Datenschutzerfordernungen und Datenschutzmanagement (nur relevant bei personenbezogenen Daten) ..	15
5.22 Informationssicherheitsüberprüfungen	15
6 Informationspflichten des Auftragnehmers	15
7 Überprüfung der Umsetzung von Sicherheitsmaßnahmen	15
8 Anhang Sicherheitsmaßnahmen in Abhängigkeit der Form Zusammenarbeit	16

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven		
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern Seite 3/22

1 Einführung und Geltungsbereich

1.1 Einleitung

In dieser Direktive werden Regeln für den Umgang mit Informationen und den Einsatz von Informationstechnik definiert, die Lieferanten und Dienstleister (im Folgenden zusammenfassend Auftragnehmer) der ABEKING & RASMUSSEN Schiffs- und Yachtwerft SE (im Folgenden Auftraggeber oder A&R) zu befolgen haben. Zweck dieser Direktive ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Rechte und Interessen des Auftraggebers sowie aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit dem Auftraggeber eingehen und / oder Tätigkeiten für diesen ausführen.

Auftragnehmer und Auftraggeber bilden zusammen die Vertragsparteien (im Folgenden Vertragsparteien).

1.2 Geltungsbereich

Diese Direktive richtet sich an die Geschäftsleitung des Auftragnehmers, deren Beschäftigte, sowie die von dem Auftragnehmer eingesetzten Personen und Unterauftragnehmer zur Erfüllung der Verpflichtungen.

2 Begriffsbestimmung

Dieser Direktive liegen folgende Begriffsbestimmungen zugrunde:

Anwender von IT-Systemen sind solche Personen, welche mit dem A&R-Netzwerk verbunden sind, auf dieses temporär zugreifen oder ein A&R-Endgerät auf stand-alone Basis einsetzen.

Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Bei einem **Auftraggeber** handelt es sich um ein Wirtschaftssubjekt, das dem anderen Vertragspartner einen Auftrag zur Erbringung von Sach- oder Dienstleistungen erteilt.

Bei einem **Auftragnehmer** handelt es sich um ein Wirtschaftssubjekt, das im Rahmen eines Auftrags für den Auftraggeber die Besorgung eines Geschäfts übernimmt. Dieses sind insbesondere Dienstleister und Lieferanten.

Beschäftigte sind Arbeitnehmer, einschließlich der zu ihrer Berufsbildung Beschäftigten und Leiharbeiter im Verhältnis zum Entleiher sowie alle Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten.

Besucher sind Personen, welche einen Aufenthaltsort vorübergehend aufsuchen.

Unter einem **Betroffenen** versteht man jede identifizierte oder identifizierbare natürliche Person, über die personenbezogene Daten verarbeitet werden.

Ein **Datenschutzbeauftragter** ist die zuständige Person für die Thematik des Datenschutzes im Unternehmen. Seine Kernaufgabe liegt in der Überwachung, Beratung und Analyse des Umgangs mit personenbezogenen Daten im Unternehmen.

Dritter (Art. 4 Nr. 10 DS-GVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen,

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version	Klassifizierung	Seite
Dokumentnummer	0	02 - intern	4/22

die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Eigentümer des Informationswertes (Werteeigentümer): Für im Inventar geführte **Werte** muss es Eigentümer geben. Natürliche als auch juristische Personen mit bestätigter Management-Verantwortung für den Lebenszyklus des Wertes können zu Eigentümern der Werte bestimmt werden. Die Eigentümerschaft sollte zugewiesen werden, wenn Werte geschaffen oder auf die Organisation übertragen werden. Der Werteeigentümer sollte für die ordnungsgemäße Verwaltung des Wertes über dessen gesamten Lebenszyklus verantwortlich sein.

Der Werteeigentümer sollte:

- a) sicherstellen, dass die Werte inventarisiert werden;
- b) sicherstellen, dass die Werte angemessen klassifiziert und geschützt werden;
- c) Zugangsbeschränkungen und Klassifizierungen wichtiger Werte festlegen und regelmäßig überprüfen, unter Berücksichtigung der geltenden Zugangskontrollleitlinien;
- d) einen ordnungsgemäßen Umgang bei der Löschung oder Zerstörung des Wertes sicherstellen.

Der festgestellte Eigentümer verfügt nicht unbedingt im juristischen Sinne über Eigentumsrechte am Wert.

Der **Informationswert/organisationseigene Werte/Asset** (nachfolgend auch **Information** oder **Wert** genannt) besteht nicht nur aus geschriebenen Wörtern, Zahlen und Bildern. Wissen, Konzepte, Ideen und Marken sind Beispiele für immaterielle Informationsformen. Informationen und damit verbundene Prozesse, Systeme, Netzwerke und Personal zu deren Verarbeitung, Handhabung und Schutz stellen in einer vernetzten Welt organisationseigene Werte dar, die genauso wie andere wichtige Unternehmensressourcen für die Geschäftsziele einer Organisation wichtig sind, und damit einen Schutz gegen unterschiedliche Gefährdungen verdienen oder erfordern. **Organisationseigene Werte** unterliegen sowohl vorsätzlichen als auch versehentlichen Bedrohungen, während damit verbundene Prozesse, Systeme, Netzwerke und Menschen ihre innewohnenden Schwächen zeigen. Änderungen von Geschäftsprozessen und Unternehmenssystemen oder andere externe Veränderungen (z. B. neue Gesetze und Verordnungen) können zu neuen Risiken in der Informationssicherheit führen. Angesichts der vielfältigen, potenziellen Bedrohungen, die Schwachstellen zum Schaden der Organisation ausnutzen, bestehen daher immer Risiken in der Informationssicherheit. Eine wirkungsvolle Informationssicherheit verringert diese Risiken durch Schutz der Organisation vor Bedrohungen und Schwachstellen und vermindert dadurch die Auswirkungen auf organisationseigene Werte.

Kunde kann eine Einzelperson, ein Unternehmen oder eine Organisation sein, welche mit einer Gegenpartei ein Geschäft abgeschlossen hat. Bei dem Geschäft kann es sich beispielsweise um einen Kaufvertrag, Leasing, Werkvertrag oder eine Dienstleistung handeln.

Ein **Lieferant** liefert Waren oder Dienstleistungen. Lieferanten stellen für Unternehmen Produkte/Waren oder Dienstleistungen im Rahmen der Geschäftsbeziehung zwischen den beteiligten Parteien (Geschäftspartnern) zur Verfügung. Als **Dienstleister** werden Wirtschaftseinheiten bezeichnet, die eine oder mehrere Dienstleistungen erbringen. Sie sind daher eine unter dem Begriff Lieferant untergeordnete Gruppe von Unternehmen.

Der **Mandant** im Sinne einer technischen Einrichtung in einem Softwaresystem ist die oberste Ordnungsinstanz in dem IT-System und stellt eine datentechnisch und organisatorisch abgeschlossene Einheit im System dar. Der Mandant strukturiert somit die Nutzung des Systems.

Personenbezogene Daten (vgl. Art. 4 Nr. 1 DS-GVO) sind alle Informationen über eine natürliche Person, durch die sie direkt oder indirekt identifiziert wird oder identifizierbar ist. Identifizierbar ist eine Person,

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 5/22

sobald zu ihr eine Verbindung mittels personenbezogener Daten hergestellt werden kann, beispielsweise durch Zuordnung einer Kennung, Standortdaten, oder eines oder mehrerer besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sind. Dies ist auch dann der Fall, wenn ein Rückschluss auf eine natürliche Person durch eine Kombination von Informationen – wenn auch erst mit zufälligem Zusatzwissen verknüpft – möglich ist. Unter personenbezogenen Daten fallen insbesondere der Name, die Adresse, die Telefonnummer, die E-Mail-Adresse, oder Fotos und Videoaufzeichnungen der natürlichen Person sowie Kunden- und Personaldaten. Eine Identifizierung der Person kann mit Hilfe einer Anonymisierung oder Pseudonymisierung ausgeschlossen werden.

Unternehmen (Art. 4 Nr. 18 DS-GVO) ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

Unterauftragnehmer sind vom Auftragnehmer eingesetzte Dienstleister, welche im Auftrag des Auftragnehmers einen Teil der Dienstleistung für den Auftraggeber erbringen.

Verantwortlicher (Art. 4 Nr. 7 DS-GVO) bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

3 Wahrung von Vertraulichkeit von Informationen/Geschäfts-/Betriebsgeheimnissen

3.1 Geheimhaltung

- (1) Die Vertragsparteien sind verpflichtet, sämtliche nicht öffentlich zugänglichen kaufmännischen und technischen Informationen, Kenntnisse, Daten und Unterlagen, Know-how, Berechnungen, Verfahren und Prozesse, die ihnen durch die Geschäftsbeziehungen bekannt werden, als Geschäftsgeheimnis des anderen zu behandeln und stets vertraulich behandeln. Erlangte Informationen dürfen nicht ohne schriftliche Zustimmung der betroffenen Vertragsparteien an Dritte weitergegeben werden. Die Geheimhaltungsverpflichtung hat über die Beendigung der Geschäftsbeziehung hinaus für einen Zeitraum von 5 Jahren Bestand, sofern keine rechtlichen Rahmenbedingungen dem entgegenstehen.
- (2) Dies gilt insbesondere für Geschäfts- und Betriebsgeheimnisse im Sinne des GeschGehG. Diese umfassen die Informationen, die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und bei der ein berechtigtes Interesse an der Geheimhaltung besteht.
Gleiches gilt für sonstige Betriebsangelegenheiten des Auftraggebers und der mit ihm verbundenen Unternehmen sowie seiner Kunden, die ihm aufgrund und/oder im Zusammenhang mit seiner Tätigkeit für den Auftraggeber anvertraut oder zugänglich gemacht worden sind.
- (3) Personenbezogene und betriebsinterne Daten dürfen nicht ohne ausdrückliche Genehmigung des Auftraggebers an Dritte weitergegeben werden. Dies gilt insbesondere auch für: Namen, Anschriften sowie die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse aller Kunden und der persönlichen, rechtlichen und wirtschaftlichen Verhältnisse und aller anderen für den Auftraggeber tätigen Personen.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 6/22

- (4) Technische Dokumentationen (bspw. Zeichnungen, Modelle, Muster etc.) dürfen unbefugten Dritten nicht überlassen oder zugänglich gemacht werden. Die Vervielfältigung oder Reproduktion der Dokumentation ist entsprechend zu dokumentieren und nur im Rahmen betrieblicher Erfordernisse und unter Einhaltung urheberrechtlicher Bestimmungen zulässig. Bei Beendigung der Vertragsbeziehungen sind alle gemäß dieser Vorschrift und in darüberhinausgehenden Geheimhaltungsvereinbarungen/Non Disclosure Agreements bezeichneten Unterlagen zurückzugeben oder auf Verlangen des Auftraggebers zu vernichten.
- (5) Die vorgenannten Verpflichtungen entfallen für solche Informationen oder Teile davon, die zu dem Zeitpunkt, in dem sie bekanntgemacht worden sind, bereits allgemein zugänglich waren.

3.2 Verpflichtung auf Vertraulichkeit (DSGVO, BDSG)

Die einschlägigen gesetzlichen Vorschriften der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet werden. Daher ist es nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der übertragenen Aufgaben erforderlich ist. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Ermächtigungsgrundlage die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

- (1) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- (2) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
- (3) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“),
- (4) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- (5) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist ; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
- (6) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumenttyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 7/22

Es ist untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten, zu erheben, zu nutzen oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder unbefugtem Zugang führt. Dies gilt sowohl für die Tätigkeit innerhalb wie auch außerhalb des Unternehmens.

3.3 Verpflichtung weiterer Personen

Die Geheimhaltungspflicht erstreckt sich auf sämtliche in Betracht kommende Personen der Vertragsparteien. Die Vertragsparteien werden ihre Beschäftigten auf die Geheimhaltungspflicht hinweisen und entsprechend verpflichten. Die Vertragsparteien werden ihre Beschäftigten die unmittelbar oder mittelbar zur Erfüllung des Vertragszweckes herangezogen werden, zu der vorbeschriebenen Verschwiegenheit und Geheimhaltung verpflichten. Sie werden darauf hinwirken, dass diese Personen die gesetzlichen Bestimmungen über den Datenschutz sowie die in dieser Verpflichtung aufgeführten Regelungen beachten und die aus erlangten Informationen nicht an Dritte weitergegeben oder sonst verwertet werden. Zusätzlich werden sie weiterhin angemessene Maßnahmen zur Geheimhaltung durchführen. Gleiches gilt für Unterauftragnehmer.

Der Auftragnehmer und seine Unterauftragnehmer sind verpflichtet, die vom Auftraggeber eingeräumten Zugangs-/Zugriffsrechte (IT-Systeme, Dienste, Daten und Anwendungen) ausschließlich im Rahmen ihrer vertraglich zu erfüllenden Verpflichtungen zu nutzen.

4 Formen der Zusammenarbeit

Der Einsatz von Auftragnehmern zeichnet sich primär dadurch aus, dass sie für die Unterstützung von Arbeits- oder Geschäftsprozessen sowie des Betriebes von Anwendungen und Systemen des Auftraggebers vertraglich beauftragt werden.

Motivationen gibt es viele, Auftragnehmern den Zugriff auf Unternehmensdaten oder -systeme zu geben. Manche Auftragnehmer benötigen z.B. den Zugriff zu Wartungs-, Service- oder Testzwecken. Andere müssen Systeme im Auftrag des Auftraggebers bedienen. Ebenso können komplette Services, z.B. im Rahmen von Outsourcing oder Cloud Computing, an Auftragnehmer vergeben werden.

Mit jedem Zugriff durch Auftragnehmer auf Unternehmensdaten von A&R oder der ausgelagerten Verarbeitung von Daten, ist auch ein potenzielles Risiko missbräuchlicher Nutzung verbunden. Es besteht z.B. das Risiko, dass die Zugriffsrechte des Auftragnehmers dazu verwendet werden, das Umfeld im Unternehmensnetz zu erkunden und auf andere Systeme als die explizit freigegebenen zuzugreifen. Desweiteren besteht das Risiko, dass Informationen aus Anwendungssystemen beschafft werden, die nicht direkt mit dem Auftrag zu tun haben.

Informationen, die verarbeitet werden bzw. auf die zugegriffen wird, sind hierbei wesentliche Vermögenswerte von A&R. Das Informationssicherheitsmanagementsystem von A&R sieht Sicherheitsmaßnahmen zur Gewährleistung eines Grundschutzes für Daten, Informationen und die zugrundeliegende Infrastruktur vor. Zur Erreichung eines durchgängigen Grundschutzes ist es erforderlich, die Sicherheitsstandards auch im Rahmen der Zusammenarbeit mit Auftragnehmern anzuwenden. Je nach Art der Zusammenarbeit können sich unterschiedliche Anforderungen an die umzusetzenden Sicherheitsmaßnahmen beim Auftragnehmer ergeben. Grundsätzlich gelten die definierten Sicherheitsregelungen für Beschäftigte des Auftragnehmers.

Für die Anwendung der A&R Sicherheitsvorgaben wurden unterschiedliche Typen der Zusammenarbeit mit Auftragnehmern definiert.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version 0	Klassifizierung 02 - intern	Seite 8/22
Dokumentnummer			

Formen der Zusammenarbeit	
Typ	Beschreibung der Zusammenarbeit mit den Auftragnehmern
Typ 1: Externe Datenbearbeitung (ohne Netzanbindung und Remote-Zugriff)	<p>Es werden Daten des Auftraggebers auf den Systemen des Auftragnehmers gehalten. Der Auftragnehmer bekommt beispielsweise im Rahmen eines Design-, Entwicklungs- oder Konstruktionsauftrages die Daten des Auftraggebers übermittelt oder wird etwa als Softwareentwickler für den Auftraggeber tätig. Er verarbeitet die Daten selbstständig auf eigenen Systemen. Der Auftragnehmer erhält die Daten vom Auftraggeber via Datenträger (USB-Medien, Tapes, etc.), E-Mail oder auf andere Weise im Rahmen eines Informationsaustausches (Portal, DFÜ-Kommunikation, File-Transfer, Download etc.).</p> <p>Im Fall der Verarbeitung personenbezogener Daten liegt eine Auftragsverarbeitung vor.</p>
Typ 2: Datenverarbeitung auf Systemen des Auftragnehmers (Outsourcing, Cloud, Netzkopplung, etc.)	<p>Der Auftragnehmer nimmt im Auftrag des Auftraggebers die Informationsverarbeitung auf eigener Hard- und Systemsoftware vor. Der Auftragnehmer stellt hierbei beispielsweise die Betriebssysteme, Anwendungssysteme und/oder Kommunikationskomponenten zur Verfügung. Der Auftraggeber ist verantwortlich für die Daten, wobei es sich bei der Verarbeitung der Daten um schutzbedürftige (personenbezogene) Informationen / Daten handelt.</p> <p>Neben der Anbindung des Auftragnehmers auf Basis von Routern/Firewalls, Modem/Kommunikationsservern sowie des Internets, kommt auch die Direkteinbindung des Auftragnehmers in die IT Infrastrukturen des Auftraggebers in Frage, z.B. Cloud Computing, SaaS etc.</p> <ul style="list-style-type: none"> – Der Auftragnehmer greift auf zur Verfügung gestellte Daten des Auftraggebers zu und verarbeitet diese. – Es werden Daten des Auftraggebers auf den Systemen des Auftragnehmers gehalten. – Der Auftraggeber übermittelt Daten an den Auftragnehmer, dieser bearbeitet die Daten auf seinen Systemen und gibt verarbeitete Daten zurück. – Der Datenaustausch kann erfolgen über <ul style="list-style-type: none"> – Austauschplattformen, – Email, – Post und – Datenversand auf Datenträgern. <p>Im Fall der Verarbeitung personenbezogener Daten liegt eine Auftragsverarbeitung vor.</p>
Typ 3: Vor-Ort-Zugriff	<p>Der Auftragnehmer greift am Standort des Auftraggebers auf Daten bzw Informationen zu.</p> <p>Es werden die Infrastrukturen des Auftraggebers vollumfänglich genutzt. Berechtigungen werden nach vordefinierten Rollenprofilen eingerichtet.</p>
Typ 4: Vor-Ort-Präsenz (ohne Systemzugriffe)	<p>Der Auftragnehmer arbeitet mit eigenen Systemen vor Ort beim Auftraggeber ohne einen Zugriff auf die Anwendungen und Systeme des Auftraggebers zu erhalten.</p>

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version	Klassifizierung	Seite
Dokumentnummer	0	02 - intern	9/22

Typ 5: Remote-Zugriff bzw. Direktkopplung	<p>Beim Remote-Zugriff sind zwei Fälle zu unterscheiden:</p> <ul style="list-style-type: none"> – IT-Support – Dienstleistungssupport Fremdfirmen <p>Der Auftraggeber stellt dem Auftragnehmer einen Benutzeraccount zur Verfügung (VPN-Client), um in den Systemen gemäß dem Rollenprofil arbeiten zu können.</p> <p>Der Auftraggeber stellt dem Auftragnehmer einen Benutzeraccount zur Verfügung und gewährt Zugriff über VID (Virtual Infrastructure Desktop, um in den Systemen gemäß dem Rollenprofil arbeiten zu können (Bring your own device)).</p>
Typ 6: Physische Objekte /Informationen	<p>Es werden physisch schützenswerte Informationen, Objekte wie beispielsweise Ordner, Konzepte, Verträge, Muster, Prototypen, Komponenten, Werkzeuge, Vorrichtungen, etc. sowie begleitende Informationen und Daten beim Auftragnehmer bearbeitet, erstellt oder gelagert, die vom Auftraggeber als „vertraulich“ oder „geheim“ klassifiziert wurden.</p>

5 Anforderungen an den Auftragnehmer zur Aufrechterhaltung der Informationssicherheit

5.1 Grundsätzliches

Im Rahmen der Zusammenarbeit sind grundsätzlich die Vorgaben des Informationssicherheits- und Datenschutzmanagementsystems von A&R einzuhalten. Die Auftragnehmer sind grundsätzlich verpflichtet, sich beim Auftraggeber über die aktuell gültigen Direktiven vor Aufnahme der Tätigkeit zu informieren. Zur Einhaltung der Anforderungen der Datenschutzgrundverordnung (DSGVO) kann es erforderlich sein, je nach Art und Umfang der verarbeiteten Daten, Verträge zur Auftragsverarbeitung (Art. 28 DSGVO) oder zur gemeinsamen Verantwortung (Art. 26 DSGVO) abzuschließen. Dies ist im Einzelfall mit dem Auftraggeber abzustimmen.

Der Auftragnehmer wird aufgefordert ein Informationssicherheitsmanagementsystem gemäß den Anforderungen der ISO 27001/27002 umzusetzen und die gesetzlichen Anforderungen zum Datenschutz einzuhalten.

In Abhängigkeit der Form der Zusammenarbeit ergeben sich Schwerpunkte bei den Anforderungen der umzusetzenden Maßnahmen. Diese sind im Kapitel 8 dargestellt. Im Laufe der Geschäftsbeziehung kann sich die Form der Zusammenarbeit ändern. In diesem Zusammenhang ändern sich auch die umzusetzenden Sicherheitsmaßnahmen. Im Folgenden sind die Anforderungen an das Informationssicherheitsmanagementsystem des Auftragnehmers dargestellt.

5.2 Organisation der Informationssicherheit

Es sind Vorgaben, Prozesse und Verantwortlichkeiten zu definieren, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.

Dies beinhaltet unter anderem:

- Die Erstellung einer Informationssicherheits-Leitlinie.
- Richtlinien zur Klassifizierung von und dem Umgang mit Informationswerten.
- Anwenderrichtlinien zur Festlegung von Regeln für den Umgang mit Anwendungen, Systemen und IT-Endgeräten und dem Verhalten bei der Nutzung von Informationstechnologie.
- Die Beschreibung von Prozessen für die Verwaltung von Datenträgern, Dokumenten und Informationen.
- Die Festlegung der Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 10/22

- Die Verpflichtung der Beschäftigten auf Geheimhaltung und Wahrung des Datengeheimnisses.
- Die regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen.

5.3 Privacy by Design (nur relevant bei personenbezogenen Daten)

Privacy by Design beinhaltet den Gedanken, dass Systeme so konzipiert und beschaffen sein sollten, dass der Umfang der verarbeiteten personenbezogenen Daten auf das für den Verarbeitungszweck erforderliche begrenzt wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein.

Dies beinhaltet unter anderem:

- Es werden nicht mehr personenbezogene Daten erhoben als für den Zweck erforderlich sind.
- DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ist sichergestellt.
- Bei Änderung und Einführung von Systemen und Anwendungen wird Privacy by Design berücksichtigt.

5.4 Privacy by Default (nur relevant bei personenbezogenen Daten)

Die Systeme und Anwendungen müssen so eingestellt werden, dass datenschutzfreundliche Voreinstellungen/Standardeinstellungen vorliegen und möglichst wenig personenbezogene Daten erfasst werden.

Dies beinhaltet unter anderem:

- Im Falle von einwilligungsbedürftigen Datenverarbeitungen, die einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen.
- Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert.
- Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins).

5.5 Zugriffskontrolle

Umsetzung von Maßnahmen, die gewährleisten, dass die zur Benutzung der Informationsverarbeitungsverfahren Beschäftigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können

Dies beinhaltet unter anderem:

- Die Erstellung von Berechtigungskonzepten für den Zugriff auf schützenswerte Informationen, Systeme und Applikationen.
- Die Umsetzung von Zugriffsbeschränkungen.
- Die Vermeidung der Konzentration von Funktionen und Etablieren einer Funktionstrennung.
- Die Umsetzung eines Prozesses zur Berechtigungsvergabe.
- Die regelmäßige Überprüfung der Berechtigungen.
- Die Protokollierung der Berechtigungsvergabe und des Datenzugriffs.

5.6 Kryptographie und / oder Pseudonymisierung

Der Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes von personenbezogenen Daten bzw. schutzbedürftigen Informationen hinsichtlich der

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumenttyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 11/22

Vertraulichkeit, Authentizität oder Integrität. Maßnahmen bei der Verarbeitung von personenbezogenen Daten, die geeignet sind, eine Identifikation des Betroffenen zu erschweren.

Dies beinhaltet unter anderem:

- Die Verschlüsselung von Datenträgern und Festplatten von PC, Laptops, mobilen Endgeräten und Verzeichnissen.
- Die gesicherte Speicherung von Daten auf mobilen Datenträgern. Als vertrauliche oder geheim klassifizierte Daten sind auf mobilen Datenträgern zu verschlüsseln.
- Organisatorische Anweisung für die Verschlüsselung von Daten.
- Verschlüsselte Ablage von personenbezogenen Daten.
- Verschlüsselung von Datensicherungsmedien (z.B. Bänder, Festplatten etc.).
- Verschlüsselung von Zugängen zum Netzwerkzugängen und -verbindungen.
- Einsatz von Pseudonymen, Verfahren zur Pseudonymisierung von Daten.
- Einsatz Verfahren zur Anonymisierung von Daten.

5.7 Schutz von Gebäuden

Umsetzung von Maßnahmen, die den unautorisierten physischen Zugriff auf die Informationen und informationsverarbeitenden Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung verhindern.

Dies beinhaltet unter anderem:

- Die Festlegung von Sicherheitsbereichen.
- Die Realisierung des Zutrittsschutzes.
- Die Festlegung zutrittsberechtigter Personen.
- Die Verwaltung von personengebundenen Zutrittsberechtigungen.
- Die Regelungen zur Begleitung von Dritten.
- Die Überwachung der Räume außerhalb der Schließzeiten.
- Die Protokollierung des Zutritts.

5.8 Schutz von Betriebsmitteln / Informationswerten

Es sind geeignete Schutzmaßnahmen zur Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Betriebsmitteln / Informationswerten und zur Vermeidung von Unterbrechungen der Betriebstätigkeit der Organisation zu implementieren.

Dies beinhaltet unter anderem:

- Regelungen zur sicheren Platzierung von Betriebsmitteln.
- Schutz der Betriebsmittel vor Überspannung, Stromausfall, Wasser und Feuer.
- Schutz vor Diebstahl.
- Regelungen zur regelmäßigen Wartung von Betriebsmitteln.
- Die Implementierung eines Prozesses zur sicheren Löschung, Entsorgung und Vernichtung von Betriebsmitteln.

5.9 Betriebsverfahren und Zuständigkeiten

Es ist der ordnungsgemäße und sichere Betrieb von Systemen und Verfahren zur Verarbeitung von Informationen sicherzustellen.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 12/22

Dies beinhaltet unter anderem:

- Die Dokumentation der Betriebsverfahren.
- Die Härtung der Backend Systeme.
- Die getrennte Verarbeitung von Produktiv- und Testdaten.
- Sicherstellung der Mandantentrennung / Mandantenfähigkeit.
- Die Anforderungen an eine Funktionstrennung sind umzusetzen. Es ist festzulegen, zu dokumentieren und zu begründen, welche Funktionen nicht miteinander vereinbar sind, also nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar.

5.10 Datensicherungen

Es sind Maßnahmen umzusetzen, die gewährleisten, dass schutzbedürftige Informationen und Daten / personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Dies beinhaltet unter anderem:

- Die Erstellung eines Datensicherungskonzeptes.
- Regelmäßige Datensicherungen.
- Getrennte Aufbewahrung von Datensicherungsmedien.

5.11 Schutz vor Malware durch Schwachstellen- und Patchmanagement

Eine Ausnutzung technischer Schwachstellen sind durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines Patchmanagements zu verhindern. Es wird empfohlen, regelmäßige Überprüfungen zur Erkennung von Schwachstellen durchzuführen.

Dies beinhaltet unter anderem:

- Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen.
- Einsatz von Anti-Malware-Software.
- Regelmäßiges Einspielen von Sicherheitspatches und Updates.

5.12 Protokollierung und Überwachung

Es sind Maßnahmen zu implementieren, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem sensible oder personenbezogene Daten in IT-Systemen in unrechtmäßiger Weise geändert wurden.

Dies beinhaltet unter anderem:

- Die Protokollierung der Berechtigungsvergabe und des Datenzugriffs.
- Die Überprüfung von Benutzerberechtigungen.
- Die Protokollierung der Aktivitäten und regelmäßige Überwachung der Benutzer- und Systemaktivitäten.

5.13 Netzwerksicherheitsmanagement

Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden.

Dies beinhaltet unter anderem:

- Die Implementierung eines Netzwerkmanagements.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 13/22

- Die Umsetzung einer Benutzerauthentifizierung für externe Verbindungen und Verbindungen zwischen einzelnen Systemen.
- Die Gewährleistung eines Schutzes der Diagnose- und Konfigurationsports.
- Sicherheitsgateways an den Übergabepunkten / Netzgrenzen.
- Die Isolation sensibler Systeme.

5.14 Informationsübertragung

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und 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 bzw. schutzbedürftiger Informationen und Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. (Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Dies beinhaltet unter anderem:

- Den sicheren Transport und den Versand von Daten / Dokumenten in Abhängigkeit vom Schutzbedarf der Daten.
- Die Protokollierung der Datenübertragungen.
- Die Beschreibung von Schnittstellen zwischen Systemen und der externen Datenverbindungen.
- Angemessener Schutz von Emails, die sensible Informationen / Daten beinhalten.
- Den Abschluss von Verträgen zum Schutz von Geschäftsgeheimnissen mit Dritten und Unterauftragnehmern.

5.15 Netztrennung

Gruppen von Informationsdiensten, Mandanten, Anwendern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.

Dies beinhaltet unter anderem:

- Gruppen von Informationsdiensten, Mandanten, Anwendern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.
- Um das Risiko zu mindern, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten, die zwischen IT-Systemen weitergegeben werden, auf dem Netz mitgelesen werden, sind diese zu segmentieren.
- Direkte Verbindungen des Clients zum Internet sind bei remote Zugriffen (z.B. über VPN oder RAS) auf das Unternehmensnetz durch geeignete Maßnahmen zu unterbinden.

5.16 Anschaffung, Entwicklung und Instandhaltung von Systemen

Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil von Informationssystemen ist. Dieses gilt für die Anforderungsdefinition, der Entwicklung, der Beschaffung, der Nutzung und die Außerbetriebnahme dieser Systeme.

Dies beinhaltet unter anderem:

- Die Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 14/22

- Die Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen.
- Entwicklung von Leitlinien zur sicheren Systementwicklung.
- Die Überwachung von ausgelagerten Systementwicklungstätigkeiten.
- Den Schutz von Testdaten.

5.17 Auftragnehmerbeziehungen bzw. Auftragsverarbeitung (AV)

Maßnahmen an die Informationssicherheit, zur Verringerung von Risiken, im Zusammenhang mit dem Zugriff von Auftragnehmern auf die Werte des Auftraggebers, sollten mit Unterauftragnehmern vereinbart und dokumentiert werden.

Dies beinhaltet unter anderem:

- Die schriftliche Adressierung von Sicherheitsthemen in Verträgen mit Unterauftragnehmern.
- Die Überprüfung der Sicherheit bei den Unterauftragnehmern.
- Die Festlegung von technisch-organisatorischen Maßnahmen (TOMs) bei Verarbeitung personenbezogener Daten.
- Die laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.

5.18 Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) zu implementieren.

Dies beinhaltet unter anderem:

- Die unverzügliche Meldung von Informationssicherheitsvorfällen an den Auftraggeber.
- Die Protokollierung von Sicherheitsvorfällen.
- Die Implementierung von Prozessen zur Behandlung und Vermeidung von Informationssicherheitsvorfällen.

5.19 Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements

Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen wie Krisen- oder Schadensfällen muss aufrechterhalten werden. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Dies beinhaltet unter anderem:

- Die Schaffung von Redundanzen.
- Risikoabschätzung und Planung von Maßnahmen zur Sicherstellung des Geschäftsbetriebes.
- Erstellung von Notfallplänen.
- Regelmäßige Tests bzgl. der Wirksamkeit der Notfallmaßnahmen.
- Frühzeitige Information des Auftraggebers bei Notfällen.

5.20 Einhaltung gesetzlicher und vertraglicher Anforderungen

Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen.

Dies beinhaltet unter anderem:

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer			 ABEKING & RASMUSSEN
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer Dokumentnummer	Version 0	Klassifizierung 02 - intern	Seite 15/22

- Geheimhaltungsverpflichtungen mit Beschäftigten sowie Auftragnehmern.
- Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit.
- Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende.

5.21 Datenschutzerfordernungen und Datenschutzmanagement (nur relevant bei personenbezogenen Daten)

Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollten entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmungen sichergestellt werden.

Dies beinhaltet unter anderem:

- Die Bestellung eines Datenschutzbeauftragten wenn gesetzlich erforderlich.
- Den Aufbau eines Datenschutzmanagements.
- Die Erstellung von Verfahrensverzeichnissen.
- Den Aufbau eines Datenschutznotfallmanagements.
- Die Durchführung regelmäßiger Überprüfungen / Audits zur Bestimmung des Datenschutzniveaus.
- Die Einhaltung der gesetzlichen Anforderungen im Rahmen der Auftragsverarbeitung.

5.22 Informationssicherheitsüberprüfungen

Es muss regelmäßig vom Auftragnehmer überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Prüfungen beim Auftragnehmer durchzuführen.

6 Informationspflichten des Auftragnehmers

Der Auftragnehmer muss den Auftraggeber unverzüglich über Informationssicherheitsvorfälle, bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers; insbesondere solche Vorfälle, die einen Zugriff durch unbefugte Dritte möglich machen, informieren.

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

Die Meldungen sind an die zentrale E-Mail Adresse: ISMS@ABEKING.com zu richten.

7 Überprüfung der Umsetzung von Sicherheitsmaßnahmen

A&R behält sich das Recht vor, die Umsetzung der in Kapitel 5 dargestellten Sicherheits-Anforderungen zu überprüfen.

Für die Überprüfung kommt die jeweils gültige Version der ISO 27001, des VDA Fragebogens und/oder ein individuelles Assessment zum Einsatz. Alternativ kann die Einhaltung der Informationssicherheit auch über ein gültiges ISO 27001 Zertifikat oder durch eine andere gleichwertige Überprüfung nachgewiesen werden.

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version 0	Klassifizierung 02 - intern	Seite 16/22
Dokumentnummer			

8 Anhang Sicherheitsmaßnahmen in Abhängigkeit der Form Zusammenarbeit

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrag verarbeitet werden)			Formen der Zusammenarbeit					
Nr	Referenz ISO 27001/ DSGVO	Technisch-organisatorische Maßnahme	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4- Vor-Ort-Präsenz (ohne Systemzugriffe)	Typ 5: Remote-Zugriff bzw. Direktkopplung	6. Physische Objekte /Informationen
01	A.05 A.06 A.07 A.08	Organisation der Informationssicherheit Festlegungen von Richtlinien, Prozessen und Verantwortlichkeiten mit denen die Informationssicherheit implementiert und kontrolliert werden kann. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Informationssicherheits-Leitlinie. - Richtlinien zur Klassifizierung von und dem Umgang mit Informationswerten. - Anwenderrichtlinien für den Umgang mit Geräten und dem Verhalten bei der Nutzung von Informationstechnologie. - Prozesse für die Verwaltung von Datenträgern. - Festlegung der Rollen und Verantwortlichkeiten. - Verpflichtung der Beschäftigten auf Geheimhaltung und Wahrung des Datengeheimnisses. - Regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen. 	x	x	x	x	x	x
02	A.06 A.14 A.18 Art 25 (1)	Privacy by Design Systeme und Anwendungen sollen so konzipiert und beschaffen sein, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Es werden nicht mehr personenbezogene Daten erhoben als für den Zweck erforderlich sind. - DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ist sichergestellt. - Bei Änderung und Einführung von Systemen und Anwendungen wird Privacy by Design berücksichtigt. 	AV	AV		AV	AV	AV

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version 0	Klassifizierung 02 - intern	Seite 17/22
Dokumentnummer			

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrag verarbeitet werden)			Formen der Zusammenarbeit					
Nr	Referenz ISO 27001/ DSGVO	Technisch-organisatorische Maßnahme	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Vor-Ort-Präsenz (ohne Systemzugriffe)	Typ 5: Remote-Zugriff bzw. Direktkopplung	6. Physische Objekte /Informationen
03	A.06 A.14 A.18 Art 25 (2)	Privacy by Default Die Systeme und Anwendungen müssen so eingestellt werden, dass datenschutzfreundlichen Voreinstellungen/Standardeinstellungen vorliegen und möglichst wenig personenbezogene Daten erfasst werden. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen. - Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert. - Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins). 	AV	AV		AV	AV	
04	A.09 Art 32 (1) b	Zugriffskontrolle Umsetzung von Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Beschäftigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Erstellen eines Berechtigungskonzeptes. - Umsetzungen von Zugriffsbeschränkungen. - Vermeidung der Konzentration von Funktionen und Etablieren einer Funktionstrennung. - Umsetzen eines Prozesses zur Berechtigungsvergabe. - Regelmäßige Überprüfung der Berechtigungen. - Protokollierung der Berechtigungsvergabe und des Datenzugriffs. 	x	x		x	x	
05	A.10 Art 32 (1) a	Kryptographie und / oder Pseudonymisierung Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Verschlüsselung von Datenträgern und Festplatten von PC, Laptops, mobilen Endgeräten und Verzeichnissen. - Gesicherte Speicherung von Daten auf mobilen Datenträgern. - Organisatorische Anweisung für die Verschlüsselung von Daten - Verschlüsselte Ablage von personenbezogenen Daten. - Verschlüsselung von Datensicherungsmedien. 	x	x		x	x	

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version 0	Klassifizierung 02 - intern	Seite 18/22
Dokumentnummer			

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrag verarbeitet werden)			Formen der Zusammenarbeit					
Nr	Referenz ISO 27001/ DSGVO	Technisch-organisatorische Maßnahme	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4- Vor-Ort-Präsenz (ohne Systemzugriffe)	Typ 5: Remote-Zugriff bzw. Direktkopplung	6. Physische Objekte /Informationen
		<ul style="list-style-type: none"> - Verschlüsselung von Zugängen zum Netzwerk und zu Netzverbindungen - Einsatz von Pseudonymen, Verfahren zur Pseudonymisierung von Daten. - Einsatz Verfahren zur Anonymisierung von Daten. 						
06	A.11 Art 32 (1) b	Schutz von Gebäuden Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Festlegung von Sicherheitsbereichen. - Realisierung des Zutrittschutzes. - Festlegung zutrittsberechtigter Personen. - Verwaltung von personengebundenen Zutrittsberechtigungen. - Regelung zur Begleitung von Dritten. - Überwachung der Räume außerhalb der Schließzeiten. - Protokollierung des Zutritts. 	x	x				x
07	A.11 Art 32 (1) b Art 32 (1) c	Schutz von Betriebsmitteln / Informationswerten Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Sichere Platzierung von Betriebsmitteln. - Schutz vor Überspannung, Stromausfall, Wasser und Feuer. - Schutz vor Diebstahl. - Regelmäßige Wartung. - Prozess zur sicheren Löschung, Entsorgung und Vernichtung von Betriebsmitteln. 	x	x		x		x
08	A.12 Art 32 (1) b	Betriebsverfahren und Zuständigkeiten Sicherstellung des ordnungsgemäßen und sicheren Betriebes von Systemen und Verfahren zur Verarbeitung von Informationen. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Dokumentation der Betriebsverfahren. - Härtung der Backend Systeme. - Getrennte Verarbeitung von Produktiv- und Testdaten. - Mandantenfähigkeit - Aufgabenverteilung und Funktionstrennung von Funktionen, die nicht miteinander vereinbar sind. 	x	x		x		

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumententyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version 0	Klassifizierung 02 - intern	Seite 19/22
Dokumentnummer			

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrag verarbeitet werden)			Formen der Zusammenarbeit					
Nr	Referenz ISO 27001/ DSGVO	Technisch-organisatorische Maßnahme	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4- Vor-Ort-Präsenz (ohne Systemzugriffe)	Typ 5: Remote-Zugriff bzw. Direktkopplung	6. Physische Objekte /Informationen
09	A.12 Art 32 (1) c	Datensicherungen: Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten gegen zufällige Zerstörung oder Verlust geschützt sind. <u>Allgemeine Anforderungen:</u> - Erstellen eines Datensicherungskonzeptes. - Durchführung regelmäßiger Datensicherungen. - Getrennte Aufbewahrung der Datensicherungsmedien.	x	x		x		
10	A.12 Art 32 (1) b	Schutz vor Malware und Patchmanagement Verhinderung einer Ausnutzung technischer Schwachstellen durch Einsatz von aktueller Virenschutzsoftware und Implementierung eines Patchmanagements. Regelmäßiges Durchführen von Überprüfungen zur Erkennung von Schwachstellen. <u>Allgemeine Anforderungen:</u> - Regelmäßige Überwachung des Status von Sicherheitsupdates und System Schwachstellen. - Einsatz von Anti-Malware-Software. - Regelmäßige Einspielen von Sicherheitspatches und Updates.	x	x		x	x	
11	A.12 Art 32 (1) d	Protokollierung und Überwachung Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem (personenbezogene) Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind. (Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.) <u>Allgemeine Anforderungen:</u> - Protokollierung der Berechtigungsvergabe und des Datenzugriffs. - Überprüfung von Benutzerberechtigungen. - Protokollierung der Aktivitäten und regelmäßige Auswertung der Benutzer- und Systemaktivitäten.	x	x		x	x	
12	A.13 Art 32 (1) b	Netzwerksicherheitsmanagement Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden. <u>Allgemeine Anforderungen:</u> - Implementierung eines Netzwerkmanagements. - Benutzerauthentifizierung für externe Verbindungen und Verbindungen zwischen einzelnen Systeme. - Schutz der Diagnose- und Konfigurationsports. - Sicherheitsgateways an den Übergabepunkten / Netzgrenzen. - Isolation sensibler Systeme.	x	x			x	

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumenttyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version	Klassifizierung	Seite
Dokumentnummer	0	02 - intern	20/22

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrag verarbeitet werden)			Formen der Zusammenarbeit					
Nr	Referenz ISO 27001/ DSGVO	Technisch-organisatorische Maßnahme	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4- Vor-Ort-Präsenz (ohne Systemzugriffe)	Typ 5: Remote-Zugriff bzw. Direktkopplung	6. Physische Objekte /Informationen
13	A.13 Art 32 (1) b	Informationsübertragung Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und 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 welchen Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen und Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. (Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.) <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Sicherer Transport und Versand von Daten / Dokumenten in Abhängigkeit vom Schutzbedarf der Daten. - Protokollierung der Datenübertragungen. - Beschreibung von Schnittstellen zwischen Systemen und der externen Datenverbindungen. - Angemessener Schutz von Emails, die sensible Informationen / Daten beeinhalteten. - Abschluss von Verträgen zum Schutz von Geschäftsgeheimnissen mit Dritten und Unterauftragnehmern. 	x	x		x		
14	A.13 Art 32 (1) b	Netztrennung Gruppen von Informationsdiensten, Mandanten, Anwendern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Logische Mandantentrennung). - Datentrennung durch Segmentierung von Netzwerken unterschiedlicher Mandanten - Trennung der Netze bei Remote Zugriffen. 	x	x			x	
15	A.14 Art 25 (1) Art 25 (2)	Ansaffung, Entwicklung und Instandhaltung von Systemen Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme. - Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen. - Leitlinien zur sicheren Systementwicklung. 	x	x		x	x	

Dokument Name Direktive Sicherheitsmaßnahmen Auftragnehmer		 ABEKING & RASMUSSEN	
Dokumenttyp Management System 03 Richtlinien / Direktiven			
Dokument Nummer	Version 0	Klassifizierung 02 - intern	Seite 21/22
Dokumentnummer			

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrag verarbeitet werden)			Formen der Zusammenarbeit					
Nr	Referenz ISO 27001/ DSGVO	Technisch-organisatorische Maßnahme	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4- Vor-Ort-Präsenz (ohne Systemzugriffe)	Typ 5: Remote-Zugriff bzw. Direktkopplung	6. Physische Objekte /Informationen
		<ul style="list-style-type: none"> - Überwachung von ausgelagerten Systementwicklungstätigkeiten. - Schutz von Testdaten. 						
16	A.15 Art 28)	Auftragnehmerbeziehungen bzw. Auftragsverarbeitung Maßnahmen an die Informationssicherheit, zur Verringerung von Risiken, im Zusammenhang mit dem Zugriff von Auftragnehmern auf die Werte des Auftraggebers, sollten mit Unterauftragnehmern und dokumentiert werden. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Schriftliche Adressierung von Sicherheitsthemen in Verträgen mit Unterauftragnehmern. - Festlegung von technisch organisatorischen Maßnahmen (TOMs) bei Verarbeitung personenbezogener Daten. - Überprüfung der Sicherheit bei Unterauftragnehmern. - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten. 	x	x	x	x	x	x
17	A.16	Management von Informationssicherheitsvorfällen Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) zu implementieren. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Prozesse zur unverzüglichen Information des Auftraggebers. - Protokollierung von Sicherheitsvorfällen. - Prozesse zur Behandlung und Vermeidung von Informationssicherheitsvorfällen. 	x	x	x	x	x	x
18	A.17 Art 32 (1) c	Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen wie Krisen- oder Schadensfällen muss aufrechterhalten werden. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden. <u>Allgemeine Anforderungen:</u> <ul style="list-style-type: none"> - Schaffung von Redundanzen. - Risikoabschätzung und Planung von Maßnahmen zur Sicherstellung des Geschäftsbetriebes. - Notfallpläne. - Regelmäßige Testes bzgl. der Wirksamkeit der Notfallmaßnahmen. - Frühzeitige Information des Auftraggebers bei Notfällen. 		x				

