BRIGHT MINDS,
BRIGHT LIGHTS.

# Informationssicherheitsanforderungen für Lieferanten (Technische und organisatorische Sicherheitsmaßnahmen - TOMs)

## A. EINLEITUNG

### 1. Allgemeines

In diesem Dokument werden technische und organisatorische Maßnahmen für die Verarbeitung von ZKW Informationen und den Einsatz von IT-Systemen bei der Verarbeitung von ZKW Informationen definiert, die Lieferanten bzw. Dienstleister - nachfolgend **„Auftragnehmer"** genannt - der ZKW Group GmbH und/oder den mit ihr im vorstehenden Sinne verbundenen Unternehmen (eine Auflistung aller Gesellschaften finden Sie hier: https://zkw-group.com/home/unternehmen/standorte/), gemeinsam bzw. einzeln "**ZKW**" bzw. **„Auftraggeber"**, zu befolgen haben. Dadurch soll der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von ZKW Informationen sichergestellt werden.

Diese Informationssicherheitsanforderungen richten sich an die Geschäftsleitung der Auftragnehmer, deren Mitarbeiter sowie deren Erfüllungsgehilfen. Der Auftragnehmer hat im Falle von Sub-Auftragnehmer, die Zugriff auf ZKW Informationen erhalten, durch vertragliche Vereinbarungen mit den Sub-Auftragnehmer sicherzustellen, dass die in diesem Dokument geregelten Anforderungen weiterhin uneingeschränkt eingehalten werden.

Sofern diese TOMs eine Anlage zu einem, bspw. die konkrete Leistung regelnden, Vertrag („Hauptvertrag") sind, so gilt Folgendes: Im Hinblick auf das Thema Informationssicherheit haben die gegenständlichen TOMs als speziellere Regelung immer Vorrang vor etwaigen (widersprüchlichen) Regelungen im Hauptvertrag.

Der Auftraggeber hat das Recht, die Einhaltung dieser Informationssicherheitsanforderungen jederzeit nach vorheriger Ankündigung während der üblichen Geschäftszeiten stichprobenartig zu prüfen.

Verstöße gegen diese Informationssicherheitsanforderungen sind als Vertragsverstoß zu werten.

ZKW arbeitet ausschließlich mit Auftragnehmern zusammen, welche sich zur Wahrung von Vertraulichkeit von ZKW Informationen und Betriebsgeheimnissen im Rahmen einer unterzeichneten Geheimhaltungsvereinbarung (Non-Disclosure-Agreement / vertraglich vereinbarte Geheimhaltungsklausel) verpflichtet haben. In Einzelfällen, wenn die übergebenen ZKW Informationen einem gesteigerten Sicherheitsbedürfnis unterfallen, behält sich der Auftraggeber – auch nach Vertragsunterzeichnung / Auftragsvergabe - das Recht vor, darüber hinaus gehende Maßnahmen vom Auftragnehmer zu fordern, um dem gesteigerten Sicherheitsbedürfnis Rechnung zu tragen.

### 2. Dokumentenstruktur und Zielgruppe

Die folgende Tabelle zeigt die Dokumentenstruktur und die Zielgruppe je Kapitel:

| Kapitel | Zielgruppe | Anmerkungen |
|---|---|---|
| A, B und C | Alle Auftragnehmer | Die Anforderungen dieser Kapitel sind von allen Auftragnehmern einzuhalten. |
| D | Auftragnehmer, welche<br>• IT-Geräte des Auftraggebers (z. B. PCs, Arbeitsplätze, Laptops) nutzen und / oder<br>• Zugang zur Infrastruktur (remote / vor Ort) durch IT-Geräte des Auftraggebers oder Geräte des Auftragnehmers erhalten | Die (zusätzlichen) Anforderungen von Kapitel D müssen „nur" von den in der linken Spalte genannten Zielgruppen eingehalten werden.<br><br>Klarstellender Hinweis: Zusätzlich gelten auch für diese Zielgruppen die Kapitel A, B und C. |

### 3. Begriffsdefinitionen

„**Personenbezogene Daten**" sind alle ZKW Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art 4 Z 1 DSGVO). Personenbezogenen Daten – sofern es sich nicht nur um Namen und Kontaktdaten handelt, die als „intern" zu klassifizieren sind, sind als „vertraulich" zu klassifizieren bzw. behandeln, im Falle der „besonderen Kategorie personenbezogener Daten" als „streng vertraulich".

**„ZKW Informationen"** sind physische und digitale Informationen des Auftraggebers, welcher dieser bereitstellt und / oder vom Auftragnehmer im Auftrag des Auftraggebers erstellt werden und aufgrund der Anforderungen aus der Informationssicherheit und des Datenschutzes zu schützen sind, um deren Verfügbarkeit, Integrität und Vertraulichkeit zu gewährleisten, inklusive Personenbezogene Daten.

**„Datenschutz- und Informationssicherheitsvorfall"** ist ein Ereignis oder ein Verdacht, welcher eine negative Auswirkung auf IT-Systeme des Auftraggebers bzw. ZKW Informationen haben kann und damit eine mögliche Verletzung oder drohende Verletzung des Datenschutzes oder/und

der Informationssicherheit zur Folge hat. Dieser umfasst Verstöße gegen das Informationssicherheitsregelwerk und anwendbarer Datenschutzgesetze, welche ZKW Informationen oder IT-Systeme des Auftraggebers betreffen, vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen, der Verdacht auf unberechtigten Zugriff, Änderung und Verlust von vertraulichen oder streng vertraulichen ZKW Informationen des Auftraggebers.

Die **„Verarbeitung von ZKW Informationen"** umfasst die Erhebung, Verarbeitung, Übertragung, Archivierung, Speicherung von ZKW Informationen.

## B. ANFORDERUNGEN ZUR AUFRECHTERHALTUNG DER INFORMATIONSSICHERHEIT

Der Auftragnehmer hat in seinem Verantwortungsbereich die innerbetriebliche Organisation in der Art und Weise auszugestalten, dass sie den Anforderungen der Informationssicherheit und des Datenschutzes gerecht wird.

Der Auftragnehmer wird aufgefordert, ein Informationssicherheits-Managementsystem gemäß den Anforderungen von etablierten Informationssicherheitsstandards (nach ISO 27001/27002, TISAX, BSI) umzusetzen und aufrechtzuerhalten.

Der Auftragnehmer hat technische und organisatorische Sicherheitsmaßnahmen **gemäß dem Stand der Technik** zur angemessenen Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit von ZKW Informationen zu treffen.

In Abhängigkeit der Form der Zusammenarbeit können sich Schwerpunkte bei den Anforderungen der umzusetzenden Sicherheitsmaßnahmen ergeben. Im Laufe der Geschäftsbeziehung kann sich die Form der Zusammenarbeit – und in diesem Zusammenhang auch die umzusetzenden Sicherheitsmaßnahmen - ändern.

**Im Folgenden ist eine nicht abschließende Auflistung von (Mindest-)Anforderungen an das Informationssicherheits-Managementsystem des Auftragnehmers dargestellt. Es liegt in der Verantwortung des Auftragnehmers, je nach Risikosituation, notwendige zusätzliche Maßnahmen zu definieren und umzusetzen.**

## C. ALLGEMEINE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN BEI DER VERARBEITUNG VON ZKW INFORMATIONEN

### 1. Management von organisationseigenen Werten des Auftraggebers

#### 1.1. Vertraulichkeit

ZKW Informationen dürfen nur einer berechtigten Gruppe von Personen zum Zwecke der vereinbarten Tätigkeiten und unter Einhaltung der entsprechenden Regelungen zugänglich gemacht werden. ZKW Informationen müssen während des gesamten Lebenszyklus entsprechend ihrer aktuellen Vertraulichkeitseinstufung geschützt werden. Die aktuelle und jeweilige Vertraulichkeitseinstufung wird vom Auftraggeber deklariert. **Nicht gekennzeichnete Dokumente / ZKW Informationen sind zumindest als „vertraulich" einzustufen.**

Es gelten folgende Kategorien und Regelungen für die Klassifikation von ZKW Informationen:

| Klassifikation | Definition | Kennzeichnung | Anforderungen |
|---|---|---|---|
| **Öffentlich** | ZKW Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung, aufgrund der öffentlichen Einsehbarkeit keinen Einfluss auf das Erreichen von Produkt- und Projektzielen haben kann und daher keinem besonderen Schutzbedarf unterliegen.<br><br>Öffentlich einsehbare personenbezogene Daten | Angabe der Vertraulichkeitsstufe „öffentlich" auf der ersten Seite eines Dokuments oder im Impressum | „Öffentlich" klassifizierte ZKW Informationen unterliegen keinen Einschränkungen und infolgedessen sind keine Maßnahmen zu beachten. |
| **Intern** | ZKW Informationen, deren Kenntnis durch Unbefugte oder deren missbräuchliche Weitergabe oder Verwendung nur geringen Einfluss auf das Erreichen von Produkt- und Projektzielen haben kann und daher einem | Angabe der Vertraulichkeitsstufe „intern" auf der ersten Seite eines Dokumentes durch den | Zusätzlich zu den Maßnahmen aus Kapiteln A bis D sind im Kapitel D die Maßnahmen für die |

| | | | |
|---|---|---|---|
| | berechtigten Personenkreis zugänglich gemacht werden dürfen. Vertraulichkeitsverstöße können zu geringen negativen Folgen führen wie z.B. geringer Reputationsschaden, geringe finanzielle Auswirkungen.<br><br>Personenbezogene Daten, die nur geschäftliche Kommunikationsdaten einer natürlichen Person enthalten (Name, Telefon-nummer, E-Mail-Adresse) | Auftraggeber | Klassifizierung „intern" sind zu beachten. |
| **Vertraulich** | ZKW Informationen, deren Bekanntgabe oder Offenlegung an unbefugte Personen das Erreichen von Produkt- und Projektzielen gefährden kann und die daher ausschließlich einer begrenzten Gruppe von Berechtigten zugänglich gemacht werden dürfen. Vertraulichkeitsverstöße können zu messbaren negativen Folgen führen wie z.B. Verlust des Kunden, starker Rückgang von Umsatzzahlen, Schadenersatzforderungen.<br><br>Personenbezogene Daten, die über geschäftliche Kommunikationsdaten hinausgehen und nicht personenbezogenen Daten besonderer Kategorie zuzuordnen sind (z.B. Gehaltsdaten, Bankdaten, etc.) | Angabe der Vertraulichkeitsstufe „vertraulich" auf jeder Seite des Dokuments in elektronischer und gedruckter Form durch den Auftraggeber | Zusätzlich zu den Maßnahmen aus Kapiteln A bis D sind im Kapitel D die Maßnahmen für die Klassifizierung „vertraulich" zu beachten. |
| **Streng Vertraulich** | ZKW Informationen, deren Bekanntgabe oder Offenlegung an unbefugte Personen das Erreichen von Unternehmenszielen in hohem Maße gefährden kann. Vertraulichkeitsverstöße haben massive Auswirkungen auf das Image bzw. Erscheinungsbild des Unternehmens sowie wirtschaftliche Folgen wie z.B. erheblicher Verlust von Kunden, sehr starker Rückgang von Umsatzzahlen, sehr hohe Schadensersatz-Forderungen, Ausschluss aus bestimmten Marktgebieten.<br><br>Personenbezogene Daten besonderer Kategorie (Art. 9 und 10 DSGVO) sind:<br>A. strafrechtlich relevante Daten<br>B. Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,<br>C. genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. | Angabe der Vertraulichkeitsstufe „streng vertraulich" auf jeder Seite des Dokuments in elektronischer und gedruckter Form durch den Auftraggeber | Zusätzlich zu den Maßnahmen aus Kapiteln A bis D sind im Kapitel D die Maßnahmen für die Klassifizierung „streng vertraulich" zu beachten. |

### 1.2. Integrität

Der Schutz vor unbefugten Änderungen an ZKW Informationen muss sichergestellt werden. Die Maßnahmen aus den Kapiteln A bis D sind zu beachten.

### 1.3. Verfügbarkeit

Die Verfügbarkeit von ZKW Informationen muss sichergestellt werden. Die Maßnahmen aus den Kapiteln A bis D sind zu beachten.

## 2. Management von Datenschutz- und Informationssicherheitsvorfällen

Der Auftragnehmer hat Maßnahmen, für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.), umzusetzen.

Technische und organisatorische Maßnahmen

- Etablierung von Prozessen zur Erkennung, Behandlung, Reaktion und zur Verhinderung / Wiederholung von Datenschutz- und Informationssicherheitsvorfällen
- Protokollierung von Datenschutz- und Informationssicherheitsvorfällen
- Die unverzügliche Meldung von Informationssicherheitsvorfällen an den Auftraggeber

Bei Verdacht auf einen Datenschutz- und Informationssicherheitsvorfall, welche ZKW Informationen und/oder IT-Systeme des Auftraggebers betreffen, ist eine unverzügliche Reaktion von entscheidender Bedeutung, um Auswirkungen auf die Geschäftsprozesse des Auftraggebers zu vermeiden.
Datenschutz- und Informationssicherheitsvorfälle sind unverzüglich an folgende Stelle zu melden:

**ZKW Group GmbH – ZKW Global IT Services & Support Center (GISSC)**
**E-Mail: gissc@zkw-group.com**

## 3. Löschung von ZKW Informationen nach Vertragsende

Der Auftragnehmer ist verpflichtet, die ZKW Informationen, wie im Hauptvertrag definiert, zu löschen und / oder zurückzugeben. Mangels Definition im Hauptvertrag sind die ZKW Informationen unverzüglich nach Erbringung der vereinbarten Leistung, spätestens nach Beendigung der Vertragsbeziehung, nachweislich an den Auftraggeber zu retournieren und anschließend zu löschen. Rechtliche Anforderungen (z.B. gesetzliche Aufbewahrungspflichten) sind zu beachten.

## 4. Organisationskontrolle

Der Auftragnehmer hat Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes und der Informationssicherheit gerecht wird, umzusetzen.

Technische und organisatorische Maßnahmen

- Etablierung eines Standards zur Informationssicherheit bzw. eines Informationssicherheitsmanagement-Systems (ISMS)
- Informationssicherheitsrichtlinien und -prozesse (z.B. Informationssicherheitsleitlinie, Passwortrichtlinie, Clean-Desk and Clear-Screen Richtlinie, Teleworking-Richtlinie, etc.)
- Etablierung eines Informationssicherheits-Risikomanagementprozesses
- Dokumentation der gesetzten technischen und organisatorischen Maßnahmen
- Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Überprüfung des Informationssicherheits-Managementsystems durch regelmäßige Audits (jährlich) auf Ordnungsmäßigkeit und Effizienz
- Festlegung der Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit und Datenschutz (Bestellung eines Datenschutzbeauftragten/-koordinators und Informationssicherheitsbeauftragter mit notwendigen Fachkenntnissen)
- Definition der Aufgabenverteilung zwischen Organisationseinheiten und zwischen Mitarbeitern bezüglich Datenverwendung
- Etablierung von Vertretungs- und Abwesenheitsregelungen für Mitarbeiter
- Etablierung eines Datenschutz-Management-Systems (Datenschutzrichtlinie, Prozesse für Betroffenenrechte, Datenschutzerklärungen, Verarbeitungsverzeichnis, etc.)
- Regelmäßige Durchführung von Awareness-Schulungen zu Informationssicherheit und Datenschutz für Mitabeiter (bei Neuanstellung und danach jährlich)

## 5. Auftragskontrolle

Der Auftragnehmer hat Maßnahmen, die gewährleisten, dass ZKW Informationen nur entsprechend den Weisungen durch den Auftraggeber verarbeitet werden, umzusetzen und entsprechende Regelungen mit seinen Sub-Auftragnehmern zu treffen. Der Auftragnehmer muss die ihn treffenden Datenschutz- und Informationssicherheitsanforderungen, auch mit seinen Sub-Auftragnehmern entsprechend vereinbaren und deren Einhaltung überprüfen.

Technische und organisatorische Maßnahmen

- Abgeschlossene Geheimhaltungsvereinbarungen bzw. Verträge zum Schutz von Geschäftsgeheimnissen (Non-Disclosure-Agreements) mit Firmenpersonal, Dritten und Sub-Auftragnehmern, die Zugriff auf ZKW Informationen erhalten

- Abgeschlossene Verträge zur Auftragsverarbeitung (Data Processing Agreement - DPA) mit Dritten und Sub-Auftragnehmern im Falle der Verarbeitung von personenbezogenen Daten Technische und organisatorische Maßnahmen sind einzuhalten
- Der Auftragnehmer muss Subunternehmer zur Einhaltung dieser Informationssicherheitsanforderungen schulen bzw. unterweisen (jährlich).
- Inhalte der Verträge zur Auftragsverarbeitung unterliegen der Einhaltung der gesetzlichen Regelungen der EU-DSGVO
- Es sind klare Vertragsgestaltungen und -ausführungen zu definieren.
- Es ist ein Personenkreis definiert, der Aufträge erteilen darf.
- Aufträge werden auch nur schriftlich bzw. in elektronischer Form erteilt und entgegengenommen.
- In den Servicebeschreibungen und den Service-Level-Agreements werden die Leistungen, die Kompetenzen und Pflichten des Auftragnehmers bzw. des Sub-Auftragnehmern klar beschrieben.
- Die Verwendung von ZKW Informationen ist an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden.
- Verträge zur Auftragsverarbeitung sind einer regelmäßigen Prüfung zur Validierung der Anforderungen aus Datenschutz und Informationssicherheit zu unterziehen

## 6. Benutzerkontrolle

Der Auftragnehmer stellt sicher, dass jene IT-Systeme und Applikationen, die er verwendet, um ZKW Informationen zu verarbeiten, nicht durch Unbefugte benutzt werden können. Er hat Maßnahmen, die verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können, umzusetzen.

Technische und organisatorische Maßnahmen

- Verwendung von Benutzererkennung mit Passwort
- Regelung der Weitergabe von Identifikationsmitteln (z. B. Hardwaretoken für 2 Faktor Authentifizierung)
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern
- Keine Verwendung von Gruppenkonten und Passwörtern ohne zusätzliche Maßnahmen
- Limitierung der Rechte privilegierter Benutzerkonten (Administratoren) nach Umfang und Zeit
- Separierung von Rechten privilegierte Benutzerkonten (Administratoren) nach Aktivitäten
- Überwachung von Aktivitäten privilegierter Benutzerkonten
- Etablierte Passwortrichtlinie, die insb. folgende Kriterien erfüllt:
    - Generierung von Passwörtern mit entsprechender Komplexität, Länge (mind. 8 Stellen, Klein- und Großbuchstaben, mind. 1 Sonderzeichen und eine numerische Ziffer)
    - Mind. 20 Zeichen für Servicekonten und Unterbindung des interaktiven Logins
    - Erzwungene Änderungsintervalle (min. 90 Tage)
    - Begrenzung der Passwort-Fehlversuche bei der Anmeldung (5 fehlgeschlagene Versuche)
    - Keine Wiederverwendung der letzten 10 Passwörter
    - Änderung von Initialpasswörtern bei Erstverwendung (z.B. für neue Benutzerkonten)

## 7. Datenintegrität

Der Auftragnehmer hat Maßnahmen, die gewährleisten, dass gespeicherte ZKW Informationen nicht durch Fehlfunktionen der IT-Systeme und Applikationen beschädigt werden können, umzusetzen. Es muss gewährleistet werden, dass Ausfällen oder Fehlfunktionen erkannt werden können und es keine Beeinträchtigung an den zu schützenden ZKW Informationen gibt.

Technische und organisatorische Maßnahmen

- Etablierung einer mehrere Schichten umfassende Sicherheitsstrategie zum Schutz vor unautorisierten Änderungen
- Etablierung und Dokumentation eines Datensicherungs- und Wiederherstellungskonzepts (tägliche Erstellung von Datensicherungen)
- Die Datenzulieferungen werden ausschließlich durch getestete und abgenommene Input-Programme durchgeführt
- Bei Datenveränderungen werden Integritätsprüfungen durchgeführt. Im Fehlerfall werden die ZKW Informationen, mit entsprechender Protokollierung, nicht übernommen.
- Firewalls und Antimalware-Schutz (z.B. für unterschiedliche Systeme wie Firewall, E-Mail, Server, Clients)
- Erkennung und Alarmierung von Sicherheitsereignissen (Security-Monitoring)
- Hochverfügbare IT-Systeme (Sicherstellung der Redundanz), sofern nicht abweichend mit dem Auftraggeber schriftlich vereinbart
- Regelmäßige, von der IT freigegebenen Updates von Betriebssystemen und installierten Applikationen
- Regelmäßige technische Überprüfungen (Penetration Tests)
- Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Auditoren

## 8. Dateneingabekontrolle

Der Auftragnehmer hat technische und organisatorische Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem ZKW Informationen in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, umgesetzt.

Technische und organisatorische Maßnahmen

- Protokollierung sämtlicher Sicherheits-Events (Benutzeranlage, Fehlerhafte Logins), sowie Datenzugriffe (z.B. Änderungen/Neuanlagen/Löschungen) und Event-Protokolle für IT-Systeme und Applikationen
- Protokollierung und Archivierung unter Berücksichtigung der firmeninternen Aufbewahrungsfristen
- Eingeschränkter Zugriff auf Protokolldaten
- Regelmäßige Überprüfung und Analyse der Protokolldaten (mind. alle 30 Tage)

## 9. Datenträgerkontrolle

Der Auftragnehmer hat sicherzustellen, dass Datenträger nicht von Unbefugten verwendet werden können, mobile Datenträger verschlüsselt werden und nicht mehr benötigte elektronische Datenträger vernichtet werden.

Technische und organisatorische Maßnahmen

- Regelungen betr. Schutz und Umgang mit Datenträgern in den Informationssicherheitsregeln des Auftragnehmers
- Ordnungsgemäße Vernichtung (Datenschutztonne, Schredder)
- Sichere Aufbewahrung von Datenträgern
- Regelmäßige Mitarbeiter-Schulung und Etablierung verbindlicher IT-Nutzungsregelungen

Zusätzliche Maßnahmen ab Klassifizierung „vertraulich“:

- Verschlüsselung von mobilen Datenträgern (Laptop, USB)
- Kontrolle und Protokollierung der Weitergabe von ZKW Informationen auf Datenträgern
- Sicheres, mehrmaliges Überschreiben von Datenträgern (7-Zyklen)
- Sichere, ordnungsgemäße Entsorgung nach Sicherheitsstufe 4 laut ISO 21964

Zusätzliche Maßnahmen ab Klassifizierung „streng vertraulich“:

- Sichere, ordnungsgemäße Entsorgung nach Sicherheitsstufe 5 nach ISO 21964 (ausschließlich Schredder)

## 10. Datenlöschung- und Vernichtungskontrolle

Der Auftragnehmer hat technische und organisatorische Maßnahmen, die gewährleisten, dass ZKW Informationen nach Ende der Aufbewahrungsfristen - bzw. wenn diese nicht mehr benötigt werden - gelöscht werden (insbesondere unter Einhaltung der Datenschutzvorschriften), umgesetzt.

Technische und organisatorische Maßnahmen

- Regelwerk für die Löschung von ZKW Informationen (Löschkonzept)
- Löschung von ZKW Informationen aus IT-Systemen, Datenbanken und Datensicherungen, Log-Informationen
- Ordnungsgemäße Entsorgung (Datenschutztonne, Schredder)

Zusätzliche Maßnahmen ab Klassifizierung „vertraulich“:

- Sichere, ordnungsgemäße Entsorgung nach Sicherheitsstufe 4 laut ISO 21964

Zusätzliche Maßnahmen ab Klassifizierung „streng vertraulich“:

- Sichere, ordnungsgemäße Entsorgung nach Sicherheitsstufe 5 nach ISO 21964 (ausschließlich Schredder)

## 11. Speicher- und Aufbewahrungskontrolle

Der Auftragnehmer stellt sicher, dass nur befugte Personen entsprechenden Zugriffsrechte auf ZKW Informationen besitzen. Der Auftragnehmer setzt Maßnahmen um, die die unbefugte Eingabe sowie die unbefugte Kenntnisnahme, Veränderung, Aufbewahrung oder Löschung gespeicherter ZKW Informationen verhindern.

Technische und organisatorische Maßnahmen

- Zugangs-/Zugriffsberechtigungssystem (Genehmigung von Zugängen durch Vorgesetzte)
- Berechtigungs- und Rollenkonzept mit Zugriffsberechtigungen nach dem "Need-to-Know"- und „Least-Privilege"-Prinzip
- Internes Kontrollsystem („IKS") zur Sicherstellung der definierten Abläufe (Rechtevergabe-, Änderung und Entzug)
- Sicherstellung der Verfolgbarkeit von Datenbankaktivitäten (Tracking)
- Sichere Authentifizierung mit Benutzerkennung und starkem Passwort (siehe Kapitel „Benutzerkontrolle")
- Protokollierung von Datenzugriffen
- ZKW Informationen sind nicht einsehbar aufzubewahren

Zusätzliche Maßnahmen ab Klassifizierung „vertraulich":

- Verschlüsselung von gespeicherten ZKW Informationen
- Vertrauliche Dokumente müssen in versperrten Schränken und/oder Räumen aufbewahrt werden, welche durch einen definierten, berechtigten Personenkreis geöffnet werden kann.

Zusätzliche Maßnahmen ab Klassifizierung „streng vertraulich":

- Streng vertrauliche Dokumente müssen in versperrten, einbruchssicheren Stahlschränken und/oder Räumen aufbewahrt werden, welche durch einen definierten, stark eingeschränkten, berechtigten Personenkreis geöffnet werden kann.

## 12. Datenübertragungs- und Transportkontrolle

Der Auftragnehmer hat Maßnahmen, die verhindern, dass bei der elektronischen Übertragung von ZKW Informationen, sowie beim Transport von Datenträgern ZKW Informationen unbefugt gelesen, kopiert, verändert oder gelöscht werden können, umgesetzt. Es muss sichergestellt werden, dass ZKW Informationen auf mobilen Datenträgern (Laptop, USB-Sticks) nur verschlüsselt gespeichert werden und nur beim berechtigten Empfänger ankommen. Es muss auch gewährleistet sein, dass ZKW Informationen bei elektronischer Übertragung oder Transport nicht gelöscht, verändert oder kopiert werden und, dass diese Übertragungen protokolliert werden.

Technische und organisatorische Maßnahmen

- Sicherer Transport und Versand von ZKW Informationen in Abhängigkeit derer Klassifizierung
- Festlegung von Übermittelungswegen (Beschreibung von Schnittstellen zwischen Systemen und der externen Datenverbindung)
- Anbindung von Sub-Auftragnehmer bzw. sonstigen Dritten (sofern eine Anbindung im konkreten Fall zulässig ist), mit denen ZKW Informationen ausgetauscht werden, ausschließlich über gesicherte Verbindungen (z.B. VPN)
- Zertifikatsausstellung durch eine vertrauenswürdige/anerkannte Zertifizierungsstelle
- Einsatz von sicheren Authentifizierungsverfahren (Benutzererkennungen mit starken Passwörtern – siehe Kapitel „Benutzerkontrolle")
- Firewalls mit aktivierten Sicherheitsfunktionen (z.B. IDS/IPS, Webfilter)
- Antimalware-Schutz in den Firewall- und E-Mail-Systemen
- Sicherstellung von sicheren Transporten von Datenträgern (zuverlässige Unternehmen oder Personen)
- In den Informationssicherheitsregeln des Auftragnehmers ist der Umgang mit Datenträgern geregelt. Z.B. ist dort festgelegt, dass ZKW Informationen auf physischen Datenträgern während eines Transportes außerhalb des Firmengeländes, sofern technisch und wirtschaftlich vertretbar, zu verschlüsseln sind.
- Nutzung von verschlossenen Transportbehältern und autorisierten Kurierdiensten
- Etablierte Prozesse für die sichere Löschung/Vernichtung von ZKW Informationen, sofern diese nicht mehr benötigt werden
- Protokollierung von Datenübertragungen

Zusätzliche Maßnahnahmen ab Klassifizierung „vertraulich"

- Verschlüsselung bei Übertragung und Austausch von ZKW Informationen (z.B. Nutzung von VPNs, https, E-Mail-Verschlüsselung bzw. verschlüsselter Austausch von Dateien unter Verwendung der vom Auftraggeber vorgegebenen Plattform, Verschlüsselung beim Schreiben auf mobile Datenträger, etc.) nach Stand der Technik muss sichergestellt werden.
- Vertrauliche Dokumente und mobile Datenträger müssen als doppeltes Kuvert und eingeschrieben bzw. in verschlossenen Behältern transportiert werden.

Zusätzliche Maßnahnahmen ab Klassifizierung „streng vertraulich"

- Streng vertrauliche Dokumente müssen in doppelten Kuverts bzw. verschlossenen Behältern transportiert werden. Der Transport muss persönlich erfolgen.
- Der Transport von streng vertraulichen Informationen auf mobilen Datenträgern ist nicht gestattet.

## 13. Weitergabe- und Vervielfältigungskontrolle

Der Auftragnehmer hat Maßnahmen umgesetzt, die verhindern, dass ZKW Informationen nur unter bestimmten Voraussetzungen vervielfältigt und nur an berechtigte Personen weitergegeben werden.

Technische und organisatorische Maßnahmen

- ZKW Informationen werden nur an einen eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen) weitergegeben
- ZKW Informationen unterliegen keinen Einschränkungen bei der Vervielfältigung

Zusätzliche Maßnahnahmen ab Klassifizierung „vertraulich"

- ZKW Informationen werden nur an einen eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen) weitergegeben

Zusätzliche Maßnahnahmen ab Klassifizierung „streng vertraulich"

- ZKW Informationen werden nur an stark eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen) weitergegeben und **nur nach vorheriger Genehmigung durch den Auftraggeber.**
- Eine Vervielfältigung von ZKW Informationen ist **nur nach vorheriger Genehmigung durch den Auftraggeber.**

## 14. Cloud-Kontrolle

Der Auftragnehmer hat Maßnahmen, die verhindern, dass ZKW Informationen in der Cloud nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können, umgesetzt.

Technische und organisatorische Maßnahmen

- Verschlüsselung von Daten zwischen jeder Anwendungsebene und zwischen Applikationsschnittstellen
- Mandantentrennung für die Verwendung von kryptografischen Schlüsseln

Zusätzliche Maßnahnahmen ab Klassifizierung „streng vertraulich"

- Kryptografische Schlüssel werden durch den Auftraggeber verwaltet (z.B. Generierung, Wechsel, Entzug)

## 15. Trennungskontrolle

Der Auftragnehmer hat Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene ZKW Informationen getrennt verarbeitet werden, umgesetzt.

Technische und organisatorische Maßnahmen

- Strikte Mandantentrennung als oberstes Prinzip in allen technischen und organisatorischen Überlegungen, insbesondere auch Mandantentrennung innerhalb von ZKW Informationen nach betroffener Gesellschaft / juristischer Person des Auftraggebers
- Trennung der Verarbeitung von ZKW Informationen und Datenhaltung (logische und/oder physische Ebene)
- Trennung von Produktiv- und Testsystemen
- Sicherstellung, dass das Testsystem dieselben technischen und organisatorischen Maßnahmen wir das Produktivsystem erfüllt
- Durchführung von Tests seitens Auftragnehmer nur mit anonymisierten Daten (keine Tests mit ZKW Informationen durch Auftragnehmer)

## 16. Verfügbarkeitskontrolle und Wiederherstellbarkeit

Der Auftragnehmer hat Maßnahmen umgesetzt, die gewährleisten, dass ZKW Informationen gegen zufällige Zerstörung oder Verlust geschützt sind. Es muss gewährleistet werden, dass im Falle einer Störung (z.B.: Diebstahl, Zerstörung, Verlust), ZKW Informationen wiederhergestellt werden

können.

Technische und organisatorische Maßnahmen

- Vollständiges Datensicherungs- und Archivierungskonzept für kritische und wesentliche IT-Systeme (tägliche Datensicherung)
- Datenspeicherung auf Servern des Auftragnehmers
- Zentrale Speicherung von ZKW Informationen in Systemen, welche in die regelmäßige Datensicherung integriert werden
- Die vom Auftragnehmer verwendete Hardware für IT-Systeme wird gemäß dem aktuellen Stand der Technik regelmäßig geprüft, gewartet und ersetzt
- Redundante Datenhaltung durch Betrieb von zwei Rechenzentren (Einsatz von Clustersysteme zur Datenspeicherung und Einsatz von Festplattenspiegelung durch RAID-Verfahren), sofern nicht abweichend mit dem Auftraggeber schriftlich vereinbart
- Redundantes/Zusätzliches Rechenzentrum in separatem Brandabschnitt
- Einsatz von unterbrechungsfreien Stromversorgung-Systemen (USV, Generatoren usw.) und regelmäßige Durchführung von Wartungen und Tests
- Brandschutzmaßnahmen (Brandschutzmeldeanlage, Löschanlage, Widerstandsklassen bei Türen, etc.)
- Datensicherungs-Systeme sind in gesicherten Sicherheitszonen und in separatem Brandabschnitt untergebracht
- Sachkundiger Einsatz von Sicherheitsfunktionen (Firewall, IDS/IPS Systeme, Antimalware-Schutz, SPAM-Filter, etc.)
- Etablierung eines Business-Continuity-Managements (BCM) und eines Desaster-Recovery-Prozesses (DR) wodurch gewährleistet wird, dass Notfallpläne zur Verfügung stehen und laufend überprüft werden.
- Regelmäßige Tests der BCM & DR Prozesse (Regelmäßige Simulation von Informationssicherheitsvorfällen und Tests zur Wiederherstellung von Daten und IT-Systemen)

## 17. Zutrittskontrolle

Der Auftragnehmer hat Maßnahmen, die sicherstellen, dass der Zutritt zu Datenverarbeitungsanlagen, mit denen schützenswerte ZKW Informationen verarbeitet oder genutzt werden, nur für berechtigte Personen möglich ist, umgesetzt.

Technische und organisatorische Maßnahmen

- Zutritt nur für berechtigtes, internes Personal des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- Festlegen von Sicherheitsbereichen/-zonen
- Sicherung der Gebäudeaußenhaut (Zäune, Tore, Portier)
- Kontrollierter Empfangsbereich in allen Betriebsgebäuden
- (Elektronisches) Zutrittssystem (z.B. Zutritt per Chipkarte)
- Versperrte Türen und geschlossene Fenster außerhalb der Betriebszeiten
- Videoüberwachung, Einbruchmeldeanlage, und/oder und Sicherheitsdienst außerhalb der Betriebszeiten
- Für alle Rechenzentren gelten strenge Sicherheitsmaßnahmen, die u. a. durch einen Sicherheitsdienst, Überwachungskameras, Bewegungsmelder und 2-Faktor-Authentifizierung unterstützt werden, um Anlagen und Einrichtungen von Rechenzentren vor dem Zugriff Unbefugter zu schützen. Zu den Systemen und zur Infrastruktur der Rechenzentren haben nur autorisierte Personen Zugang.
- Sicherheitsschlösser mit Schlüsselregelung für besonders schützenswerte Bereiche (z.B. Büros der HR-Abteilung)
- Besuchermanagement (Anmeldung/Registrierung des Besuchers, Beaufsichtigung/Begleitung des Besuchers durch firmeneigenes Personal, Tragen von Besucherausweisen oder/und Mitarbeiterausweisen)
- Berechtigungskonzept für die Zutrittskontrolle (Berechtigungsmatrix) und Berechtigungsvergabe nach dem „Need-to-Know Prinzip"
- Prozesse für die Vergabe, Änderung und Entzug von Zutrittsberechtigungen
- Protokollierung der Zutritte
- Dokumentierte und regelmäßige Berechtigungskontrollen und Kontrolle der Zutritte

Zusätzliche Maßnahnahmen ab Klassifizierung „vertraulich"

- Zutritt nur für eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- Abhängig von der Sicherheitseinstufung werden Gebäude, einzelne Bereiche und das umliegende Gelände ggf. durch weitere Maßnahmen geschützt

Zusätzliche Maßnahnahmen ab Klassifizierung „streng vertraulich"

- Zutritt nur für stark eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- Abhängig von der Sicherheitseinstufung werden Gebäude, einzelne Bereiche und das umliegende Gelände ggf. durch weitere Maßnahmen geschützt

## 18. Zugangskontrolle

Der Auftragnehmer stellt sicher, dass die Nutzung der IT-Systeme bzw. System-Komponenten und Netze, sowie der Zugang zu analogen und digitalen ZKW Informationen nur mit einer Zugangsberechtigung möglich ist. Diese Zugangsberechtigung wird aufgrund der ausgeübten Funktion im Einzelnen festgelegt und nur nach Freigabe durch den Vorgesetzten vergeben.

Technische und organisatorische Maßnahmen

- Zugang nur für berechtigtes, internes Personal des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- Sichere Verfahren zur Benutzerauthentifizierung (Benutzer und Passwort)
- Einhaltung der Vorgaben und der Passwortrichtlinie des Kapitels „Benutzerkontrolle“
- Berechtigungskonzept für die Zugangskontrolle
- Berechtigungsvergabe nach dem „Need-to-Know Prinzip“ und „Least Privilege Prinzip“
- Prozesse für die Vergabe, Änderung und Entzug von Zugangsberechtigungen
- Protokollierung von Zugängen (z.B. berechtigte und unberechtigte Anmeldungen)
- Regelmäßige Prüfung der Zugangsberechtigungen
- Automatische Aktivierung eines Bildschirmschoners mit Passwortschutz
- Schutz des Unternehmensnetzwerkes vor dem öffentlichen Netzwerk (Firewall mit aktivierten Sicherheitsfunktionen)
- Perimeter-Firewall an externen Eintrittspunkten (Internet, Partner-Netzwerk, etc.)
- Gesicherte Netzsegmente und Isolation kritischer Systeme (Interne Netzwerksegmentierung)
- Terminierung externer Verbindungen in einer Demilitarized Zone (DMZ)
- Aktivierte Security-Services auf allen Firewalls (IDS/IPS, Webfilter, Applikationskontrolle, etc.)
- Netzwerkzugangskontrolle
- Anti-Malwareschutz auf allen relevanten IT-Systemen (Firewall, E-Mail Gateway, Datenserver, Clients, etc.) und regelmäßige Updates der Virendefinitions- und Signaturdaten
- Etabliertes Patch- und Schwachstellenmanagement (z.B. regelmäßige Updates aller IT-System)
- Härtung der IT-Systeme (z.B. Deaktivierung von nicht benötigten Diensten, Firewall-Regelwerk, etc.)
- Richtlinien für Clean-Desk und Clear-Screen und Zugang zu Druckern

Zusätzliche Maßnahnahmen ab Klassifizierung „vertraulich“

- Zugang nur für eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- 2-Faktor-Authentifizierung mindestens für Remote-Zugänge und Administratorenzugänge

Zusätzliche Maßnahnahmen ab Klassifizierung „streng vertraulich“

- Zugang nur für stark eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen) und nur nach vorheriger Genehmigung durch den Auftraggeber
- Ausschließlich 2-Faktor-Authentifizierung

## 19. Zugriffskontrolle

Der Auftragnehmer hat Maßnahmen umgesetzt, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können sowie Maßnahmen, die sicherstellen, dass ZKW Informationen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können.

Technische und organisatorische Maßnahmen

- Zugriff nur für berechtigtes, internes Personal des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- Schutz vor unbefugtem Zugriff (Passwortschutz)
- Berechtigungskonzept für die Zugriffskontrolle

- Berechtigungsvergabe nach dem „Need-to-Know Prinzip“ und „Least Privilege Prinzip“ für die Zugriffsrechte (z.B. Lesen, Schreiben, Ändern, Löschen)
- Prozesse für die Vergabe, Änderung und Entzug von Zugriffsberechtigungen
- Protokollierung der Berechtigungsvergabe, -änderung und -entzug
- Protokollierung des Datenzugriffs (z.B. Zugriff, Lesen, Schreiben, Ändern, Löschen)
- Regelmäßige Prüfung der Zugriffsberechtigungen

Zusätzliche Maßnahnahmen ab Klassifizierung „vertraulich“

- Zugriff nur für eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen)
- Schloss für versperrte Schränke.

Zusätzliche Maßnahnahmen ab Klassifizierung „streng vertraulich“

- Zugriff nur für stark eingeschränkten Personenkreis des Auftragnehmers und berechtigte Dritte im Rahmen der Tätigkeiten bzw. des Anwendungsbereiches (Auftragsbezogen) und nur nach vorheriger Genehmigung durch den Auftraggeber
- Stahlschloss für versperrte Schränke

## 20. Kryptografische Kontrolle

Der Auftragnehmer hat Maßnahmen umgesetzt, die gewährleisten, dass Verfahren für ein sicheren Umgang mit kryptographischen Schlüsseln gewährleistet ist.

Maßnahmen ab Klassifizierung „vertraulich“:

- Verfahren für kryptographisches Schlüsselmanagement
- Generierung von Schlüsseln mit freigegebenen Schlüssellängen
- Sichere Verteilung, Aktivierung, Speicherung, Wiederherstellung, Austausch und Update von kryptografischen Schlüsseln
- Sicherung und Archivierung von kryptografischen Schlüsseln einschließlich der Pflege der kryptografischen Schlüsselhistorie
- Sofortige oder Deaktivierung von kryptografischen Schlüsseln bei Kompromittierung
- Wiederherstellung von kryptografischen Schlüsseln bei Kompromittierung, Verlust und Verfall
- Zuordnung eines definierten Datums bei Aktivierungs- und Deaktivierung von kryptografischen Schlüsseln
- Eingeschränkter Zugriff auf kryptografische Schlüssel ausschließlich durch autorisiertes Personal

## D. ZUSÄTZLICHE INFORMATIONSSICHERHEITSANFORDERUNGEN BEI NUTZUNG VON IT-GERÄTEN / ZUGANG ZUR INFRASTRUKTUR DES AUFTRAGGEBERS

In diesem Abschnitt werden zusätzliche Bestimmungen definiert, die von Auftragnehmern nur dann einzuhalten sind, wenn der Auftragnehmer auf Anweisung von ZKW

- IT-Geräte des Auftraggebers (z. B. PCs, Arbeitsplätze, Laptops) nutzt und / oder
- Zugang zur Infrastruktur (remote / vor Ort) durch IT-Geräte des Auftraggebers oder Geräte des Auftragnehmers erhält

### 1. Allgemeine Anforderungen und Verhaltensregeln

Um Datendiebstahl, Spionage und Cyber-Security-Angriffe zu vermeiden, sind insbesondere folgende Anforderungen einzuhalten:

- Das Mitbringen von IT-Geräten des Auftragnehmers auf das Firmengelände des Auftraggebers ist nur unter Einhaltung der Anweisungen des Personals der jeweiligen Konzerngesellschaft des Auftraggebers zulässig.
- Eine Einbindung von (IT-)Geräten in die Netzwerkinfrastruktur des Auftraggebers, ohne Freigabe durch das Personal des Auftraggebers, ist nicht gestattet.
- Der Einsatz von Software zur Verarbeitung von ZKW Informationen, die weder vom Auftraggeber noch vom Auftragnehmer bereitgestellt oder freigegeben ist, ist nicht zulässig.
- Für die Verarbeitung von ZKW Informationen auf anderen als vom Auftraggeber, oder im Eigentum des Auftragnehmers oder dessen Subauftragnehmer zur Verfügung gestellten Plattformen, ist vorab eine schriftliche Freigabe durch die Informationssicherheitsstelle des Auftraggebers (Einsteuerung über das ZKW Global IT Services & Support Center (GISSC) erforderlich. Darunter sind u.a. Outsourcing und jegliche Art von Cloud-Plattformen zu verstehen.
- Der Auftragnehmer darf die ZKW Informationen nur in jenen IT-Systemen/mit jenen IT-Diensten verarbeiten, die der Auftraggeber bereitstellt, oder die im Rechenzentrum des Auftragnehmers betrieben werden. Eine darüberhinausgehende Verarbeitung von ZKW Informationen in von nicht vom Auftragnehmer betriebenen IT-Diensten (Outsourcing, Cloud-Dienste), bedarf einer schriftlichen Freigabe durch die Informationssicherheitsstelle des Auftraggebers (Einsteuerung über das ZKW Global IT Services & Support Center (GISSC).
- Hinsichtlich der Weitergabe von ZKW Informationen an Dritte gelten die vertraglichen Vereinbarungen.
- Regelungen des Auftraggebers zur Erhebung, Verarbeitung und Nutzung von ZKW Informationen müssen eingehalten werden.
- Mitarbeiter des Auftragnehmers müssen von ihrer Geschäftsleitung auf die Geheimhaltung im Sinne der bestehenden Vertraulichkeitsvereinbarung zwischen Auftraggeber und Auftragnehmer verpflichtet werden. Dem Auftraggeber ist jederzeit Einsicht in diese Vereinbarungen zu gewähren. Falls ZKW Informationen auf mobilen Systemen oder IT-Geräten gespeichert werden, sind diese mit dem aktuellen Stand der Technik entsprechender Hardware oder Software zu verschlüsseln.
- Vor Auslandsreisen sind die länderspezifischen Regelungen zum Einsatz von Sicherheitstechniken (z. B. Verschlüsselung) zu beachten.
- Als „vertraulich“ und „streng vertraulich“ klassifizierte Dokumente dürfen niemals unbeaufsichtigt liegen gelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.
- Es dürfen nur sichere Internetverbindungen verwendet werden, wenn keine Verbindung zum Netzwerk des Auftraggebers besteht.
- „Anonymes Surfen“ hat zu erfolgen, um die lokale Speicherung der besuchten Websites zu vermeiden (auch wenn, der Internet Anbieter noch immer Zugang zu diesen Daten hat)
- Sichere HTTPS-Verbindungen (statt http) sind zu verwenden.
- Es dürfen keine ZKW Informationen in sozialen Medien veröffentlicht werden.
- E-Mails mit ungewöhnlichen Texten oder Links sind sofort zu löschen.
- Externe Datenträger wie Festplatten und USB-Sticks sind zu verschlüsseln.
- IT-Geräte des Auftraggebers bzw. auf denen ZKW Informationen verarbeitet werden dürfen nicht an Dritte geliehen bzw. von Dritten benutzt werden.
- IT-Geräte sind beim Transport zu verpacken und versiegeln (Abgabe am Zoll, o.ä.), um eine Überprüfung/Manipulation nachvollziehen zu können.
- Updates sind zeitnahe zu installieren.
- Auf "Schultersurfer" (jeden, der die Nutzung des IT-Geräts physisch überwacht) ist besonders Acht zu geben. Ein hochwertiger Sichtschutz am Laptop ist einzusetzen.
- Ein Passwort-Manager ist zur sicheren Speicherung von Passwörtern einzusetzen. Passwörter dürfen nicht in Browsern oder als Klartext in Dateien gespeichert werden.
- Nicht benötigte Netzwerkprotokolle (wie z. B. WiFi, Bluetooth oder Infrarot) sind zu deaktivieren.
- Da integrierte Kameras und Mikrofone in jedem IT-Gerät per Fernzugriff aktiviert werden können, sind integrierte Kameras zu verdecken oder verschließen bzw. in geschützten Räumen zu verwenden.
- Die Aufzeichnungsfunktion von IT-Geräten darf nur mit Zustimmung des Auftraggebers und unter Einhaltung der anwendbaren Datenschutzbestimmungen genutzt werden. Der heimliche Mitschnitt von online sowie offline Besprechungen (etwa durch Aktivieren der Diktierfunktion am Smartphone) ist strengstens untersagt.
- Es dürfen keine Fotos / Videos auf dem Firmengelände des Auftraggebers oder Fotos / Videos von ZKW Informationen ohne Zustimmung des Auftraggebers (und unter Einhaltung der anwendbaren Datenschutz- und Geheimhaltungsbestimmungen) angefertigt werden.

## 2. Verwendung von Passwörtern

- Für die Generierung und Verwendung von Passwörtern sind die Anforderungen aus *„Allgemeine Technische und organisatorische Maßnahmen bei der Verarbeitung von ZKW Informationen"* zu befolgen
- Keine Verwendung von trivialen Passwörtern, oder Passwörtern mit persönlichem Bezug
- Wenn Passwörter sicher aufbewahrt werden sollen ist dafür ein Passwortmanager zu verwenden
- Es ist nicht gestattet, für den Zugriff auf IT-Systeme/-Applikationen des Auftraggebers, ein identisches Passwort für berufliche und private Zwecke zu verwenden.
- Die Verwendung der Benutzerkennung oder des Kontos einer anderen Person ist nicht gestattet.
- Passwörter oder PINs einer Benutzerkennung, die zur persönlichen Verwendung bestimmt ist (bezeichnet als „persönliche Benutzerkennung"), sind geheim zu halten und dürfen nicht weitergegeben werden.
- Wenn das Passwort oder ein PIN unautorisierten Personen bekannt geworden ist oder der Verdacht besteht, ist sofort ein Passwortwechsel durchzuführen und das ZKW Global IT Services & Support Center (GISSC) zu informieren.

## 3. Remote-Verbindungen

Remote Verbindungen in die Netzwerkinfrastruktur des Auftraggebers müssen über eine 2-Faktor-Authentifizierung hergestellt werden (Bereitstellung durch den Auftraggeber).

Bei Remote-Verbindungen, bei denen aus Gründen der Architektur keine 2-Faktor-Authentifizierung möglich ist (z.B. Site-to-Site VPN), sind folgende Mindestanforderungen des Auftraggebers einzuhalten:

- Freigabe der Remote-Verbindung durch den Auftraggeber
- Starke Verschlüsselung nach Stand der Technik
- Zugriffseinschränkung zu Netzsegmenten
- Initiierter Verbindungsaufbau durch den Auftraggeber

Wird die Verbindung nicht mehr benötigt, ist diese zu trennen.

## 4. Datensicherungen

Sofern der Auftragnehmer ZKW Informationen auf IT-Geräten des Auftraggebers verarbeitet, so sind ZKW Informationen auf den zugeordneten Netzlaufwerken zu speichern und nicht auf der lokalen Festplatte der IT-Geräte.

Für die Sicherung der Daten, die nicht auf zentralen Netzlaufwerken gespeichert sind (z.B. lokale Festplatte, mobile Datenträger) oder Systemen mit vergleichbarer Funktionalität, ist der Auftraggeber nicht verantwortlich. Backupdaten und Medien zur Sicherung sind so zu behandeln, wie die Produktivdaten.

## 5. Austausch von ZKW Informationen

- Bei Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen) ist sicherzustellen, dass diese nicht unberechtigt mitgehört werden können.
- Beruflichen Kontaktdaten (zB E-Mail-Adressen) sind aktuellen Verzeichnissen zu entnehmen oder beim Empfänger zu erfragen, um fehlerhafte Übertragungen zu vermeiden.

## 6. Verwendung und Rückgabe von IT-Geräten des Auftraggebers

- Änderungen an der Hardware, am System (z.B. Änderung einer fixen IP-Adresse) und an Sicherheitseinstellungen (z.B. Browsereinstellungen) sind immer mit der Ansprechperson des Auftraggebers abzustimmen.
- Auf den zur Verfügung gestellten IT-Geräten dürfen keine Daten von anderen Kunden, die nicht zur Gruppe des Auftraggebers gehören, verarbeitet werden.
- Das Verwenden von IT-Geräten des Auftraggebers durch Mitarbeiter des Auftragnehmers erfordert die ausdrückliche Zustimmung des Auftraggebers.
- Der Auftraggeber ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z.B. bei Missbrauch).
- IT-Geräte des Auftraggebers sind so zu verwenden, dass keine Unbefugten diese Daten einsehen oder darauf zugreifen können. Klarstellend wird darauf hingewiesen, dass dies auch bei mobilen IT-Geräten des Auftraggebers gilt.
- Die zur Verfügung gestellten IT-Geräte des Auftraggebers sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen. Durch den Auftraggeber zur Verfügung gestellte Geräte (z.B. Laptops) dürfen nur nach erfolgter Genehmigung vom Werksgelände des Auftraggebers mitgenommen werden. Der Auftragnehmer ist dafür verantwortlich, das Gerät gegen Verlust oder Diebstahl zu schützen.
- Überlassene Geräte (z. B. Laptops) und Datenträger bzw. Speichermedien müssen nach Ablauf des Vertrags, oder wenn diese nicht mehr benötigt werden, an den Auftraggeber zurückgegeben werden. Der Verlust von an den Benutzer übergebenen IT-Geräten sowie von Medien zum Zwecke der Authentifizierung sind durch den Benutzer umgehend dem ZKW Global IT Services & Support Center (GISSC)

zu melden.

**7. Entzug von Berechtigungen**

- Der Auftragnehmer muss sicherstellen, dass seinen Mitarbeitern unverzüglich die Zugangs- und Zugriffsrechte entzogen werden, wenn diese nicht mehr benötigt werden (z.B. bei Projektende, Austritt des Mitarbeiters).
- Wird eine Benutzerkennung oder ein Zugriffsrecht auf ZKW Informationen des Auftraggebers nicht mehr benötigt und/oder ist Zugang zum Netzwerk bzw. Applikationen des Auftraggebers vor Beendigung des Auftragsverhältnisses nicht mehr notwendig, ist dies von dem jeweiligen Mitarbeiter des Auftragnehmers unverzüglich bei den jeweiligen auftraggebenden Stellen (z.B. zuständiger Benutzeradministrator des Auftraggebers, ZKW Global IT Services & Support Center (GISSC), interne Ansprechperson im Projekt) zu melden.

Auftragnehmer:

_____

Name: _____

Datum: _____

## E. ÄNDERUNGSVERZEICHNIS

| Version | Änderungsdatum | Änderungen |
|---|---|---|
| 01 | 2022-06-07 | Erstversion |
| 02 | 2023-09-22 | Änderung Bezeichnung ZKW Service Desk -> ZKW Global IT Services & Support Center (GISSC)<br>Änderung Kapitel 2, Kontaktdaten ZKW Global IT Services & Support Center (GISSC) |