

Sondervereinbarung im Umgang mit sämtlichem Schriftgut und allen Arten von Datenträgern für den Erweiterungsbau Bundeskanzleramt

Das Merkblatt regelt den Umgang mit sämtlichem Schriftgut und allen Arten von Datenträgern, welche im Projekt „Erweiterungsbau des Bundeskanzleramtes (BKE)“ verwendet werden und Informationen zum Projekt beinhalten. Die Einhaltung der Regelungen dieses Merkblattes sind für alle Projektbeteiligten (Firmen und Behörden) bindend und gegen Unterschrift vor Leistungserbringungen zu bestätigen.

Für Verschlusssachen (VS) gelten zusätzlich die Bestimmungen der Verschlusssachenanweisung (VSA) sowie des Geheimschutzhandbuches (GHB).

I Allgemeines

1 Zugangsberechtigung und Weitergabe

1.1. Schriftgut und Datenträger dürfen nur Personen zugänglich gemacht werden, die im Zusammenhang mit der Auftragsdurchführung oder bei der Auftragsanbahnung Kenntnis erhalten müssen. Den zugangsberechtigten Personen ist dieses Merkblatt vor dem Zugang zu solchem Schriftgut und Datenträgern nachweislich bekannt zu geben; sie werden auf ihre besondere Verantwortung für den Schutz des Schriftgutes und der Datenträger gemäß diesem Merkblatt sowie eventuelle strafrechtliche oder vertragsrechtliche Konsequenzen bei Zuwiderhandlung hingewiesen.

1.2. Über den Inhalt des Schriftgutes und der Datenträger ist Verschwiegenheit gegenüber Nichtbeteiligten zu wahren. Personen, die sich zum Umgang mit solchen Handhabungen als ungeeignet erwiesen oder gegen die Verpflichtung zur Geheimhaltung verstoßen haben, sind von der Bearbeitung solcher Nutzung auszuschließen.

1.3. Die Weitergabe des gesamten Schriftguts oder Datenträger in Bezug auf den Erweiterungsbau des Bundeskanzleramtes darf nur an Auftragnehmer erfolgen, die an diesem Projekt beteiligt sind und die Zugang zu den Informationen im Zusammenhang mit der Bearbeitung des Projekts haben müssen.

2 Bearbeitungsmaßnahmen

2.1 Kennzeichnung und Handhabung bzw. Verwahrung

Schriftgut und Datenträger sind wie folgt zu behandeln und zu verwahren:

2.1.1. Das Schriftgut und die Datenträger sind in verschlossenen Räumen oder Behältern (Schränken, Schreibtischen usw.) zu verwahren. Außerhalb von solchen Räumen oder Behältnissen sind sie stets so aufzubewahren bzw. zu behandeln, dass Unbefugte keinen Zugang zu oder Einblick in die Unterlagen haben. Es sind keine besonderen Kennzeichnungen nötig.

2.1.2. Zwischenmaterial (z. B. Vorentwürfe) ist gegen Einsichtnahme Unbefugter in derselben Weise zu schützen wie das Bezugsdokument.

2.1.3. Für den Umgang mit Schriftgut mit einem Geheimhaltungsgrad VS-Vertraulich oder höher, gelten die Regelungen der VSA (vgl. VSA §23) sowie des GHB.

2.2 Weitergabe

2.2.1. Die Weitergabe in Deutschland erfolgt durch Boten oder Versand durch Zustelldienste in einem einfachen verschlossenen Umschlag bzw. Behältnis. Der Umschlag bzw. das Behältnis erhalten keine besondere Kennzeichnung.

2.2.2. Schriftgut und Datenträger können durch private Zustelldienste als gewöhnlicher Brief bzw. Paket oder auch als Luft- oder Seefracht nach Zustimmung des Bundeskanzleramtes in das Ausland versendet werden.

2.2.3. Bei der elektronischen Übermittlung (z. B. per E-Mail und über das vom Auftraggeber vorgegebene Projektkommunikationsmanagementsystem) von nicht VS-eingestuftem Schriftgut kann auf eine Verschlüsselung der Informationen verzichtet werden.

Bei einer elektronischen Übermittlung von Schriftgut mit einem Geheimhaltungsgrad von VS-Nur für den Dienstgebrauch (NfD) oder höher, gelten die Regelungen der VSA (vgl. VSA §55) sowie des GHB.

2.2.4. Die Vervielfältigung von VS-eingestuften Dokumenten außerhalb der Räume des Auftragnehmers ist nur über den vom Auftraggeber (Bundesamt für Bauwesen und Raumordnung – BBR) vorgegebenen Dienstleister zulässig. Es gelten die Regelungen der VSA sowie des GHB.

2.3 Vernichtung

2.3.1. Nicht mehr benötigtes Schriftgut und externe Datenträger (z.B. CD-ROM, USB-Sticks, SD-Speicherkarten) mit Projektbezug, auch Zwischenmaterial, sind so zu vernichten, dass der Inhalt nicht mehr erkennbar ist und nicht wiederhergestellt werden kann. Unterschieden wird zwischen der Vernichtung von Schriftgut und externen Datenträgern mit und ohne VS-eingestuftem Inhalt. Die nachfolgenden Vorgaben sind uneingeschränkt umzusetzen und ein wesentlicher Bestandteil des Geheimschutzes.

2.3.2. Schriftgut und externe Datenträger ohne VS-eingestuften Inhalt sind nach Sicherheitsstufe 5 gemäß DIN 66399 zu vernichten. Für die Materialkategorie P (u. a. Papier) ist dazu z. B. ein handelsüblicher Aktenvernichter der Sicherheitsstufe P5 nach DIN 66399 zu verwenden. Eine Vernichtung außerhalb der Räume des Auftragnehmers ist nur durch einen Dienstleister zulässig, welcher für Vernichtungen nach Sicherheitsstufe 5 gemäß DIN 66399 zertifiziert ist. Die Sicherheitsstufe ist mit dem Dienstleister vertraglich festzuhalten.

2.3.3. Schriftgut und externe Datenträger mit VS-eingestuften Inhalt sind nach Sicherheitsstufe 6 gemäß DIN 66399 zu vernichten. Die Vernichtung ist nur über den vom Auftraggeber (BBR) vorgegebenen Dienstleister zulässig. Die Aufbewahrung des zu vernichtenden Schriftgutes und der externen Datenträger hat in abschließbaren Behältern im Bereich des Auftragnehmers zu erfolgen.

2.4 Verlust, unbefugte Weitergabe, Auffinden von Schriftgut/Datenträgern oder Nichtbeachtung des Merkblatts

Der Verlust, die unbefugte Weitergabe sowie das Auffinden von Schriftgut/Datenträgern oder die Nichtbeachtung dieses Merkblattes ist unverzüglich dem Auftraggeber zu melden, um einen eventuell entstandenen Schaden zu begrenzen und den Vorfall aufzuklären.

2.5 Aufträge

2.5.1. Alle Auftragnehmer/-Unterauftragnehmer sind vom Auftraggeber vertraglich zu verpflichten, die Regelungen dieses Merkblattes zu beachten. Dabei ist darauf hinzuweisen, dass eine Nichtbeachtung die Auflösung des Vertrages bzw. von Teilen des Vertrages zur Folge haben kann und Schadenersatzforderungen gestellt werden können.

2.5.2. Schriftgut und Datenträger, welche im Rahmen von Vergabeverfahren an mögliche Auftragnehmer versandt werden, sind bei Nichtzustandekommen eines Vertrages zeitnah zu vernichten.

II Nutzung von Informationstechnik (IT)

1 Bearbeitung und Speicherung

1.1. Wird IT für die Bearbeitung von Schriftgut/Datenträgern mit Projektbezug genutzt, sind zum Schutz der Unterlagen (entsprechend Teil I 1.1 und 1.2) geeignete informationstechnische Maßnahmen und / oder materielle und organisatorische Maßnahmen zu treffen.

1.2. Vor der Bearbeitung oder Speicherung von Schriftgut und Datenträgern ist sicherzustellen, dass das Gerät oder das interne Netzwerk nicht unmittelbar (z.B. ohne Schutz durch eine Firewall) mit dem Internet verbunden ist.

1.3. Bei der Bearbeitung von Schriftgut/Datenträgern kommen insbesondere folgende technisch-organisatorische Maßnahmen in Betracht:

- Übersicht und Einschränkungen über den berechtigten Personenkreis und die entsprechenden Zugriffsberechtigungen herstellen.
- Nutzung von Identifizierungs- und Authentisierungsmechanismen (z. B. Passwortschutz, Fingerprint, Zwei-Faktor-Login).
- Geeignete IT-Sicherheitsanweisung (einzelplatz- oder unternehmensbezogen) erstellen.

1.4. Werden für die Bearbeitung oder Speicherung von VS-NfD eingestuften Daten tragbare IT-Systeme (z.B. Datenträger, Notebooks oder Handhelds) eingesetzt, sind die verwendeten Speichermedien durch vom BSI zugelassene Produkte zu verschlüsseln (z.B. „GnuPG VS-Desktop“ der Firma g10 Code). Bei nicht VS-ingestuften Daten kann auf eine Verschlüsselung verzichtet werden, ein Passwortschutz mit mindestens einer vierteljährlichen Änderung des Passwortes ist jedoch auf jeden Fall erforderlich.

Passwörter sollen mindestens acht Zeichen lang sein, sowie aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

1.5. Externe Datenträger mit Projektbezug (z.B. CD-ROMs, USB-Sticks, SD-Speicherkarten) sind ausschließlich für dieses Projekt zu verwenden. Nach Abschluss der Arbeiten sind die Datenträger (entsprechend Teil I 2.3) zu vernichten.

1.6. Fest installierte Datenträger (z.B. Festplatten) sowie externe Festplatten mit Projektbezug sind ausschließlich für dieses Projekt zu verwenden. Nach Abschluss der Arbeiten sind sie sicher und nicht wiederherstellbar, gemäß den Empfehlungen des BSI, zu löschen.

1.7. Auf fest installierten Datenträgern, die Schriftgut dieses Projekts enthalten, sind die Daten sicher und nicht-wiederherstellbar zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten an IT-Systemkomponenten den Bereich der zugriffsberechtigten Personen verlassen. Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzubehalten bzw. ist die Wartungs-/Reparaturfirma vertraglich auf die Einhaltung der Regeln dieses Merkblattes zu verpflichten.

1.8. Informationstechnik und Datenträger sind auf Virenbefall (insbesondere Trojanische Pferde oder Würmer) zu überprüfen bevor das Schriftgut und die Datenträger damit bearbeitet werden. Diese Prüfung ist in regelmäßigen Zeitabständen zu wiederholen.

1.9. Werden IT-Systeme (PCs, Notebooks, etc.) zur Parametrierung oder Programmierung von technischen Anlagen auf der Baustelle eingesetzt (z.B. Anlagen der Gebäudeautomation, Elektrotechnik, Sicherheitstechnik), sind die Endgeräte fertig installiert vor dem ersten Einsatz an diesen Anlagen und danach vierteljährlich an das Sicherungspersonal des BKAmtes zur technischen Kontrolle im Eingangsbereich der Baustelle zu übergeben. Die Kontrollmaßnahmen beinhalten u.a. einen Virenskan und können einen zeitlichen Umfang von bis zu 30 Minuten in Anspruch nehmen. Die Möglichkeit für diese Kontrollmaßnahmen besteht zu den regulären Baustellenöffnungszeiten. Eine Terminvereinbarung ist erforderlich.

Ab der Inbetriebnahme-Phase des Gebäudes (geplant Q4/2027) ist ein Einsatz von firmeneigenen IT-Systemen an den technischen Anlagen aus Sicherheitsgründen nicht mehr gestattet. Ab diesem Zeitpunkt werden die benötigten IT-Systeme vom BKAmt dann kostenfrei zur Verfügung gestellt.

1.10. Private Informationstechnik (z.B. Laptops), Software oder Datenträger dürfen nicht für die Bearbeitung eingesetzt werden. In für Schriftgut und Datenträger dieses Projekts genutzten Informationssystemen dürfen keine private Software oder private Datenträger verwendet werden.

2 Maßnahmen zum Schutz der Vertraulichkeit

Die im Folgenden empfohlenen Maßnahmen sollen die Vertraulichkeit der elektronisch gespeicherten Daten sicherstellen. Sie dienen nicht in erster Linie dazu, die Integrität und die Verfügbarkeit der Daten zu gewährleisten.

Absicherung IT – Systeme:

- Aktuelle Betriebssystem- und Firmwareversionen müssen eingesetzt werden.
- Betriebssysteme und Anwendungssoftware sollten nur mit aktuellen Updates und Patchen genutzt werden.
- Auf stationären und mobilen Geräten muss eine aktuelle Virenschutzsoftware eingesetzt werden.
- Das Betriebssystem muss ein differenziertes Benutzerprofil und Zugriffsschutz bis auf Dateiebene gewährleisten.
- Es muss ein Login und ein Passwort vorhanden sein. Das Passwort muss mindestens 8 alphanumerische Stellen, Sonderzeichen; Groß- und Kleinbuchstaben enthalten.
- Das BIOS muss ebenfalls durch ein Passwort geschützt sein.
- Ein Booten des IT-Systems darf grundsätzlich nur von der Festplatte aus möglich sein.
- Bei Netzwerken sollte eine eigene Partition zum Speichern der Daten auf dem Server installiert werden, die dadurch gegebenen Schutzmechanismen sind entsprechend anzuwenden.
- Es müssen verbindliche Anwenderregelungen innerhalb des Unternehmens festgelegt und geschult werden. Die neuesten Sicherheitsupdates der genutzten Software sind nach Verfügbarkeit insbesondere auch an der Firewall einzubinden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt auf seiner Homepage **www.bsi-fuer-buerger.de** alle wichtigen Informationen zum Thema IT - Sicherheit zur Verfügung und informiert stets über neue Themeninhalte.