**Checkliste Multifunktionsgeräte**

*Multifunktionsgeräte – eierlegende Wollmichsau und*

*nicht unerhebliches Sicherheitsrisiko*

Multifunktionsgeräte – eierlegende Wollmichsau und nicht unerhebliches Sicherheitsrisiko. Heutzutage sind diese Geräte aus fast keinem Büro mehr wegzudenken. Egal ob kleinere Geräte direkt am Arbeitsplatz oder wuchtige Standgeräte an zentralen Stellen im Haus. Es wird fleißig gedruckt, gescannt, gefaxt und kopiert. Doch bei all dem Komfort sollten die Sicherheitsaspekte nicht außer Acht gelassen werden. Große Druckaufträge, die noch eine Weile bis zum Abholen im Druckausgang verbleiben; Fehlausdrucke, die im Papierkorb neben dem Gerät entsorgt werden; Faxe, zentral eingegangen und durch verschiedene Hände gegangen, bevor sie den eigentlichen Empfänger erreichen. Das sind nur einige Probleme und Risiken, denen aus Sicht des Datenschutzes und der Informationssicherheit mit geeigneten technischen und organisatorischen Mitteln begegnet werden muss.

Unsere Checkliste soll helfen, vorhandene Schwachstellen zu identifizieren und möglichst zeitnah zu schließen. Auch wenn hier hauptsächlich von Multifunktionsgeräten die Rede ist, so können die Schwachstellen auf bei Einzelfunktionsgeräten vorhanden sein. Prüfen Sie bitte penibel.

Grundlage der Checkliste: [BSI IT-Grundschutz 200-2 Baustein SYS 4.1](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_1_Drucker,_Kopierer_und_Multifunktionsgeräte.html) sowie [Orientierungshilfe Fotokopierer der Landesdatenschutzbehörde Freie Hansestadt Bremen](https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen_und_handlungshilfen/fotokopierer__die_angreifbare_datenstation-3904).

Wir empfehlen, die Checkliste von dem Fachbereich (oder den Fachbereichen) ausfüllen zu lassen, der oder die für Beschaffung, Konfiguration, Inbetriebnahme und Betreuung während des Betriebs sowie die Außerbetriebnahme zuständig ist bzw. sind. Im Anschluss sollten die Ergebnisse vom Datenschutzbeauftragten (DSB) und / oder Informationssicherheitsbeauftragten (ISB) aufgegriffen werden, um durch Nachjustierung oder Ergänzung geeigneter technischer und organisatorischer Maßnahmen das Risiko für Datenpannen zu mindern bzw. deren Konsequenzen zu begrenzen.

Je nach Ernsthaftigkeit der Bearbeitung dieser Checkliste kann diese durchaus als ein Nachweis (von vielen) über Prüfung der Wirksamkeit von technischen und organisatorischen Maßnahmen in Ihrer Organisation dienen.

Viel Erfolg bei der Umsetzung wünscht das

Team von a.s.k. Datenschutz

**Checkliste Multifunktionsgeräte / Drucker / Kopierer / Faxe**

Ausgefüllt durch (für Rückfragen):

Fachbereich(e)

Ansprechpartner

Rufnummer(n)

Email

Die Bearbeitung dieser Checkliste fand statt im Zeitraum vom       bis      .

| **Prüfpunkt** | **Beschreibung** | **Status / Kommentar** |
| --- | --- | --- |
| **Aufstellort** | Dem Komfortmerkmal „zentraler Aufstellort“ fallen schnell notwendige Sicherheitsanforderungen zum Opfer.  Einige Risiken:   * Unberechtigte Einsichtnahme in Ausdrucke / Faxe / Kopien durch Außenstehende * Verlust von Unterlagen * Unbefugte Bedienung * Zugriff auf Netzwerkfunktionen   Von daher sollten MFG nicht öffentlich oder in frei zugänglichen bzw. unverschlossenen Räumen aufgestellt werden. Wenn doch sind zwingend weitere Schutzmaßnahmen notwendig.  BSI SYS.4.1.A1, BSI SYS.4.1.A2 | Alle Geräte stehen  nicht in frei zugänglichen Räumen  und sind zusätzlich mit weiteren Maßnahmen geschützt wie  in verschlossenen Räumen, Zutrittsberechtigung nur interne Mitarbeiter  und zusätzlich mit weiteren Maßnahmen geschützt wie  teilweise frei zugänglich oder unverschlossen und sind  durch weitere Maßnahmen geschützt  nicht geschützt  Kommentar / Handlungsbedarf |
| **Voreingestellte Passwörter / Codes** | Sofern die im Auslieferungszustand des Geräts vorgegebenen Passwörter bzw. Codes für die Geräteverwaltung und Konfiguration nicht geändert wurden, besteht ein nicht unerhebliches Risiko, Zugriff auf Funktionen und zwischengespeicherte Daten des Geräts zu nehmen. Die Änderung dieser Passwörter sollte in einem festen Prozeß der Inbetriebnahme vorgeschrieben bzw. sichergestellt und die erfolgte Umsetzung protokolliert werden.  BSI SYS.4.1.A2, BSI SYS.4.1.A18 | Passwörter / Codes sind auf allen Geräten geändert  Status unbekannt, alle Geräte müssen geprüft werden (wer bis wann?)  Es existiert ein verbindlicher Prozeß zur Änderung von voreingestellten Passwörtern (Achtung: nicht alle Geräte werden durch die IT beschafft und in Betrieb genommen – berücksichtigen Sie bitte alle Fachbereiche)  Kommentar / Handlungsbedarf |
| **Regelungen für die Nutzung / Einweisung der Mitarbeiter** | Existieren klare (leicht verständliche) Regelungen für die Nutzung der MFG? Aufgrund der enormen Druckleistung der Geräte sind Mitarbeiter schnell versucht, Druckaufträge abzusenden und erst geraume Zeit später abzuholen („geht ja sonst so viel wertvolle Arbeitszeit verloren“). Dies sollte a) organisatorisch durch eine Anweisung und b) technisch z.B. durch Freigabe des Druckauftrags am Gerät mittels PIN / Chipkarte vermieden werden.  Datenpannen sind oft die Folge von Unkenntnis und Unwissenheit. Daher ist es mehr als angeraten, die Mitarbeiter in die Gerätenutzung einzuweisen.  BSI SYS.4.1.A5 | Es liegen schriftliche Regelungen zur Nutzung von MFG vor  Diese Regelungen wurden den Mitarbeitern in geeigneter Form bekanntgegeben (in welcher?)  Alle Mitarbeiter sind in die Bedienung der MFG eingewiesen  Die Einweisung wird auch für neue Mitarbeiter sichergestellt  Kommentar / Handlungsbedarf |
| **Umgang mit Fehlausdrucken bzw. nicht abgeholten Druckaufträgen / Faxen** | Klassiker schlechthin: Der Papierkorb neben einem MFG. Eine sehr gute Gelegenheit, sich über Internas der Organisation zu informieren. Auch schon gesehen als Steigerung – 2 Papierkörbe. Beschriftung Korb 1 „Altpapier“, Korb 2 „Vertraulich“  Wenn eine Entsorgungsmöglichkeit angeboten werden soll, so bietet sich ausschließlich ein Schredder mit geeigneter Sicherheitsstufe an ([siehe DIN 66399](https://www.datenschutzbeauftragter-info.de/die-neue-datentraegervernichter-din-66399/))  BSI SYS.4.1.A5 | Es stehen keine Papierkörbe neben den MFG  Direkt bei den MFG oder im näheren Umfeld sind Schredder mit geeigneter Sicherheitsstufe vorhanden  Statt bzw. ergänzend zu Schreddern stehen Entsorgungsboxen (verschlossen) zur Verfügung  Kommentar / Handlungsbedarf |
| **Freigabe von Druckaufträgen** | MFG sind aufgrund der enormen Druckleistung sehr komfortabel. Da bietet es sich geradezu an, große Druckaufträge vom Arbeitsplatz zum Drucker zu schicken und nach Ablauf einer gewissen Zeit, die fertigen Ausdrucke am MFG abzuholen. Wenn sie denn dann noch da sind ☺  Mechanismen zur Vermeidung direkter Ausdrucke sind daher unabdingbar. Der Ausdruck am MFG darf erst nach Freigabe durch den Nutzer am MFG selbst erfolgen. Bis zur Beendigung des Ausdrucks muss der Mitarbeiter am Gerät verbleiben und den eigenen Ausdruck be- / überwachen. Letzteres werden Sie organisatorisch regeln müssen. | Druckaufträge können erst am MFG durch den jeweiligen Mitarbeiter gestartet werden  Die Druckfreigabe erfolgt mittels  fester PIN, die jedem Mitarbeiter zugeordnet ist  frei wählbare einmalige PIN, die für jeden Druckauftrag durch den Mitarbeiter vergeben werden kann  Chipkarte / Coin / Token  andere:  Es existiert eine verbindliche Regelung, dass Druckaufträge am MFG freigegeben und der Ausdruck bewacht werden muss  Kommentar / Handlungsbedarf |
| **Fehlversand von Faxen / Rufnummernverteiler** | Gerade der aktuelle Stand der Technik erlaubt die Annahme von Faxen unter jeder beliebigen Rufnummer, selbst wenn auf der Gegenseite physikalisch kein Faxgerät an dem Anschluss installiert ist.  Von daher sollte vor dem Versand von Faxen stets eine Überprüfung der anzuwählenden Rufnummer durch den Nutzer erfolgen, um Fehlversand und damit schnell einhergehend eine Datenpanne nach Art. 33, 34 DSGVO zu vermeiden. | Mitarbeiter sind gehalten (z.B. durch Anweisung / Regelung) Faxnummern vor Versand auf Aktualität und korrekte Eingaben zu prüfen  Rufnummern-Verteiler in den MFG werden regelmäßig auf Aktualität überprüft und bearbeitet (wer und wann?)  An exponierter Stelle auf dem MFG ist ein entsprechender Warnhinweis angebracht „Faxnummer korrekt?“  Kommentar / Handlungsbedarf |
| **Zurücksetzen nach Bedienung** | Sofern das MFG das automatische Rücksetzen aller durch den letzten Nutzer vorgenommenen Einstellungen nicht beherrscht, sollten Mitarbeiter angehalten sein, diese Einstellungen (z.B. durch den „C“ Button“) vor Verlassen des MFG selbst zurückzusetzen.  Weiterhin sollte sichergestellt sein, dass z.B. für die Druckfreigabe benötigte Coins / Tokens / Kopierkarten nicht am Gerät verbleiben.  BSI SYS.4.1.A5, BSI SYS.4.1.A18 | Die MFG setzen sich nach einem Zeitraum von       automatisch zurück  Mitarbeiter sind per Anweisung / Regelung zum Zurücksetzen des Geräts angehalten  Die Einhaltung wird regelmäßig am MFG geprüft (wer wann wie?)  Kommentar / Handlungsbedarf |
| **Umgang mit eingebauten Zwischenspeichern** | Die Leistungsfähigkeit von MFG ist vom Vorhandensein großer Zwischenspeicher abhängig. Jeder Auftrag rein oder raus wird auf den eingebauten Zwischenspeichern (HDD / SSD) abgelegt. Von dort sind diese durchaus auch sehr sensiblen Informationen mit wenigen Handgriffen auslesbar bzw. wiederherstellbar. Aus diesem Grund ist auf diese Zwischenspeicher bei Konfiguration, Betrieb aber auch Außerbetriebnahme des Geräts besonderes Augenmerk zu legen.  Wenn möglich, sollte der Datenträger verschlüsselt sein. Wirkungsvoll ist hier ausschließlich die Option, das Verschlüsselungspasswort selbst zu setzen und dies nicht dem externen Dienstleister bei Service / Wartung zu überlassen.  Für die Außerbetriebnahme sollten klare Regelungen zum Umgang mit den Zwischenspeichern getroffen sein. Vernichtung samt Nachweis durch den Dienstleister bzw. Ausbau und datenschutzkonforme Entsorgung im eigenen Haus sind probate Lösungswege.  Hinweis: Die Leistungen im Rahmen von Wartung und Support eines MFG durch einen externen Dienstleister können die Regelung einer Auftragsverarbeitung nach Art. 28 DSGVO erforderlich machen. Fragen Sie Ihren Datenschutzbeauftragten.  BSI SYS.4.1.A12, BSI SYS.4.1.A15, BSI SYS.4.1.A19 | Der Zwischenspeicher ist verschlüsselt  Das Verschlüsselungspasswort wurde von uns selbst gesetzt und ist dem Dienstleister nicht bekannt  Für die Entsorgung des Zwischenspeichers sind geeignete Verfahrensweisen vorhanden  durch den Dienstleister, Beschreibung:  interne Verfahrensweise, Beschreibung:  Die Notwendigkeit der Regelung einer Auftragsverarbeitung wurde geprüft und bei positiver Prüfung sind TOM des Dienstleisters geprüft und eine aktuelle Vereinbarung zu Art. 28 DSGVO Auftragsverarbeitung vorhanden  Kommentar / Handlungsbedarf |
| **Sicherheitsupdates** | Sofern der Hersteller des MFG Sicherheitsupdates anbietet, sind diese im Rahmen des normalen Patch- und Fix-Managements zu berücksichtigen und zeitnah einzuspielen. Gerade bei Netzwerkfunktionalitäten der Geräte ist dies zwingend erforderlich, um mögliche Sicherheitslücken zeitnah zu schließen.  BSI SYS.4.1.A3 | Sicherheitsupdates werden regelmäßig nach Erscheinen im Rahmen des Patch-Managements eingespielt  Kommentar / Handlungsbedarf |
| **Abschalten nicht benötigter (Netz-) Dienste** | Die Funktionsvielfalt von MFG wird nicht immer voll ausgeschöpft. Es empfiehlt sich daher, nicht benötigte Funktionen bzw. (Netz-) Dienste zu deaktivieren, um Schwachstellen zu beseitigen oder auch Fehlbedienungen durch Ausprobieren zu vermeiden.  BSI SYS.4.1.A18 | Nicht benötigte Dienste sind auf den MFG abgeschaltet.  Bei Neugeräten werden diese nicht benötigten Dienste im Rahmen der Inbetriebnahme abgeschaltet  Kommentar / Handlungsbedarf |
| **Zugriff auf Protokolle / Metadaten** | Fax- und Druckprotokolle enthalten zwar nicht unbedingt die konkreten Angaben zum Dokumenteninhalt, verraten dennoch einiges an personenbezogenen Daten. Der Zugriff auf diese Protokolle bzw. Angaben sollte daher sehr restriktiv gehandhabt werden ebenso wie die Speicherdauer. Ein Abruf am Gerät mit normalen Nutzerrechten sollte unterbunden sein.  BSI SYS.4.1.A17 | Metadaten bzw. Protokolle (Druck, Empfang, Versand) sind ausschließlich mit Administrationsrechten am MFG einsehbar bzw. abrufbar  Die Speicherdauer wurde begrenzt auf       Tage  Kommentar / Handlungsbedarf |
| **Sperre vorhandener Anschlüsse** | Vorhandene USB- oder Speicherkarten-Schnittstellen können für Digitalisierung und unbemerkte Mitnahme von großen analogen Datenmengen genutzt werden. Sofern nicht zwingend benötigt, sind diese und weitere Schnittstellen zu sperren (Geräteeinstellungen, mechanische Blockade etc.) | Nicht zwingend benötigte Schnittstellen sind an allen MFG gesperrt  Kommentar / Handlungsbedarf |
| **Netztrennung** | Es ist empfehlenswert, MFG in einem separaten Netz (VLAN) zu betreiben und eine Trennung zum „Arbeitsnetz“ einzurichten. Dies erschwert den Übergriff auf das Produktivnetz durch den Netzwerkanschluß des MFG. | MFG werden in einem separaten VLAN betrieben  Kommentar / Handlungsbedarf |
| **Absichern des Bootmenüs** | Jedes MFG verfügt über Bootmenüs bzw. Zugänge zur erleichterten Wartung. Der Zugriff auf diese Funktionen sollte stets passwortgeschützt sein. Sinnvollerweise verwendet man keine einheitlichen Passwörter für alle MFG. | Das Bootmenü bzw. der Wartungszugang ist bei allen MFG mittels eines neuen Passworts abweichend vom Initialpasswort gesperrt  Auf identische Passwörter für alle MFG wurde verzichtet  Kommentar / Handlungsbedarf |

**Vom DSB / ISB auszufüllen**

Rückmeldungen geprüft am       von

Weitere Aktivitäten notwendig  Ja  Nein

Konkrete notwendige Aktivitäten (neue oder anzupassende technische und organisatorische Maßnahmen benennen)

|  |  |  |  |
| --- | --- | --- | --- |
| **Wer** | **Was** | **Bis wann** | **Umsetzung geprüft** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Alternative Dokumentation und Nachbearbeitung notwendiger Maßnahmen mittels (konkret beschreiben):

**Hinweis**

Sie sind herzlich eingeladen, diese Vorlage für Ihre Organisation zu nutzen und auch weiterzugeben. Prinzip der Fairness: Keine Nutzung im Rahmen kommerzieller Angebote wie Bücher, CD/DVD, Bezahlportale ohne Rücksprache mit uns.

Zentralruf 09155-263 99 70 oder Email [info@ask-datenschutz.de](mailto:info@ask-datenschutz.de)

Verbesserungsvorschläge? Dann immer her damit.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Titel des Dokuments** | | | | **Vertraulichkeitsstatus** | |
| Checkliste Sicherheit Datenschutz Multifunktionsgeräte | | | | Intern | |
| **Version** | **Datum** | **Änderungen** | **Autor** | **Status** | **Freigabe** |
| 1.0 | 30.04.2019 | Erstellung des Dokuments | Sascha Kuhrau | Final | 01.05.2019 / SK |