Drucken

D1. Werden Daten auf einem Brother Server gespeichert, wenn ich aus einem Clouddienst, wie Box, Dropbox, Evernote, Google Drive, OneDrive, OneDrive for Business oder OneNote auf mein Brother Gerät drucke?

JPEG: Alle Verbindungen zu diesen Diensten erfolgen direkt ohne Nutzung der Brother Cloud (Standort außerhalb der Europäischen Union).

PDF und Microsoft Office Dateien: Daten können temporär zur Aufbereitung in die Brother Cloud (Standort außerhalb der Europäischen Union) übertragen werden. Nach der Verarbeitung werden sie automatisch gelöscht.

D2. Werden Daten zu einem Brother Server übertragen und dort gespeichert, wenn ich aus Facebook oder Flickr über mein Brother Gerät drucke?

Facebook: Daten werden in der Brother Cloud (Standort außerhalb der Europäischen Union) aufbereitet. Nach der Verarbeitung werden sie automatisch gelöscht.

Flickr: Alle Verbindungen zu Flickr sind direkt, d.h. ohne Einbindung der Brother Cloud (Standort außerhalb der Europäischen Union).

D3. Werden Daten zu einem Brother Server übertragen und gespeichert, wenn ich die Brother iPrint&Scan App zum Drucken verwende?

JPEG: alle Verbindungen zu Clouddiensten sind direkt, d.h. ohne Einbindung der Brother Cloud (Standort außerhalb der Europäischen Union).

PDF und Microsoft Office Dateien: Daten werden in der Brother Cloud (Standort außerhalb der Europäischen Union) aufbereitet. Nach der Verarbeitung werden sie automatisch gelöscht.

D4. Werden alle Druckauftragsdaten nach dem Ausdruck aus dem Gerätespeicher gelöscht?

Teile des Druckauftrags können nach dem Ausdruck temporär im Arbeitsspeicher des Druckers verbleiben, bis diese vom nächsten Druckauftrag oder durch das Trennen des Druckers von der Stromzufuhr überschrieben/gelöscht werden. Brother Geräte unterstützen keine Funktion, auf diese Datenreste zuzugreifen.

D5. Ist es möglich über das Bedienfeld des Druckers einen Druckauftrag noch einmal auszudrucken, nachdem er ausgedruckt wurde?

Nach dem Ausdruck unterstützen die aktuellen Brother Druckgeräte keine Funktion, den Druckauftrag erneut auszudrucken.

D6. Wie arbeitet die Mehrfachsatzdruck-Funktion?

Die Mehrfachsatzdruck-Funktion arbeitet auf die gleiche Weise, wie das normale Drucken. Das Gerät speichert den Druckauftrag, bis er vollständig abgeschlossen wurde. Der Speicherplatz wird dann für das Überschreiben wieder freigegeben. Brother Geräte unterstützen keine Funktion, auf diese Datenreste zuzugreifen.

D7. Werden die Druckdaten verschlüsselt im Gerätespeicher abgelegt?

Die Druckdaten werden aktuell nicht verschlüsselt im Gerätespeicher abgelegt. Teile des Druckauftrags können nach dem Ausdruck temporär im Arbeitsspeicher des Druckers verbleiben, bis diese vom nächsten Druckauftrag oder durch das Trennen des Druckers von der Stromzufuhr überschrieben/gelöscht werden. Brother Geräte unterstützen keine Funktion, auf diese Datenreste zuzugreifen.

D8. Wie werden die Druckaufträge bei der Benutzung der Speicherdruck Funktion aus dem Gerätespeicher gelöscht??

Falls das Modell die Funktion Speicherdruck unterstützt, kann die automatische Löschung der Druckaufträge eingestellt werden. In diesem Fall wird der gesperrte, genutzte Speicherplatz durch das Ausdrucken wieder freigegeben. Teile des Druckauftrags können nach dem Ausdruck temporär im Arbeitsspeicher des Druckers verbleiben, bis diese vom nächsten Druckauftrag oder durch das Trennen des Druckers von der Stromzufuhr überschrieben/gelöscht werden. Brother Geräte unterstützen keine Funktion, auf diese Datenreste zuzugreifen.

Scannen/Kopieren

S1. Werden Daten zu einem Brother Server übertragen bzw. gespeichert, wenn ich in einen Clouddienst, wie Box, Dropbox, Evernote, Google Drive, OneDrive, OneDrive for Business oder OneNote von meinem Brother Gerät scanne?

JPEG oder PDF bei Box, Dropbox oder Google Drive: Alle Verbindungen zu diesen Diensten erfolgen direkt ohne Nutzung der Brother Cloud (Standort außerhalb der Europäischen Union).

JPEG und PDF bei Evernote, OneDrive oder OneNote: Daten können temporär zur Aufbereitung in die Brother Cloud (Standort außerhalb der Europäischen Union) übertragen werden. Nach der Verarbeitung werden sie automatisch gelöscht.

Durchsuchbare PDF oder Microsoft Office Dateien: Daten werden temporär zur Aufbereitung in die Brother Cloud (Standort außerhalb der Europäischen Union) übertragen. Nach der Verarbeitung werden sie automatisch gelöscht.

S2. Werden Daten zu einem Brother Server übertragen bzw. gespeichert, wenn ich zu Facebook oder Flickr über mein Brother Gerät scanne?

Alle Verbindungen zu diesen Clouddiensten sind direkt, d.h. keine Daten werden (auch nicht temporär) in die Brother Cloud kopiert.

S3. Werden Daten zu einem Brother Server übertragen bzw. gespeichert, wenn ich die Brother iPrint&Scan App zum Scannen verwende?

Mit der iPrint&Scan App kann nur das scannende Gerät bedient werden. Es werden keine Daten zwischen iPrint&Scan und einem Clouddienst ausgetauscht.

Fax

F1. Wie werden Faxdaten im Gerät gespeichert?

Faxdaten werden getrennt von Druckdaten im Gerätespeicher des Gerätes aufbewahrt. Die Speicherempfangsfunktion ermöglicht es, mehrere empfangene Faxe im Gerätespeicher zu halten, bevor sie ausgedruckt werden. Nach Ausdruck des Faxes wird der belegte Speicherplatz wieder freigegeben, damit das nächste Fax empfangen und dort abgelegt werden kann.

F2. Ist es möglich, ein Fax erneut auszudrucken, nachdem es bereits ausgedruckt wurde?

Bei den aktuellen Brother Modellen ist es nicht möglich, ein Fax erneut auszudrucken, das bereits ausgedruckt worden ist. Teile des Faxes können nach dem Ausdruck temporär im Speicher des Gerätes verbleiben, bis diese vom nächsten empfangenen Fax oder durch das mehrtägige Trennen des Gerätes von der Stromzufuhr bzw. Zurücksetzen überschrieben/gelöscht werden. Bei aktiviertem „Sendebericht mit Andruck der ersten Seite“ verbleibt dieser inklusive des Andrucks der ersten gesendeten Seite temporär im Speicher des Gerätes, bis dieser vom nächsten Sendebericht oder durch das mehrtägige Trennen des Gerätes von der Stromzufuhr bzw. Zurücksetzen überschrieben/gelöscht werden.

F3. Kann die Fax-Schnittstelle eines Multifunktionsgerätes für den Zugriff auf die Netzwerk-Schnittstelle genutzt werden?

Die Faxfunktion der Brother Multifunktionsgeräte ist physisch von den Netzwerk-Schnittstellen getrennt. Daher kann ein mit dem Brother Gerät verbundener Faxanschluss nicht dazu benutzt werden, um Zugriff auf die LAN- oder WLAN-Schnittstelle des Gerätes zu erhalten. Zusammengefasst ausgedrückt: Es ist nicht möglich ein internes Netzwerk über den Faxanschluss zu kompromitieren.

F4. Kann ich die Faxempfangsfunktion deaktivieren?

Die Faxfunktion kann nicht über die Administrationsoberfläche deaktiviert werden. Sie müssen das Anschlusskabel für Fax vom Multifunktionsgerät abstecken.

Auf Anfrage ist die komplette Deaktivierung der Faxfunktion für Projekte möglich. Wenden Sie sich diesbezüglich an Ihren Fachhändler oder direkt an Brother.

Lösungen

L1. Wie kann ich verhindern, dass unbefugte Personen Zugriff auf Dokumente bekommen, die bereits zum Drucker gesendet wurden?

Viele Brother Geräte bieten Funktionen wie „Sicherer Druck“ und Benutzersperre. Jeder Nutzer kann dabei mit einem persönlichen Passwort, einer PIN oder einer NFC-Karte ausgestattet werden, die zum Entsperren des Gerätes nutzbar sind. Erst nach dieser Authentifizierung am Gerät können die Druckaufträge ausgedruckt werden. Bitte prüfen Sie, ob Ihr Modell mit diesen Funktionen ausgestattet ist.

L2. Wie kann ich sicherstellen, dass ein Brother Gerät vor unauthorisierter Benutzung gesichert ist?

Brother bietet je nach Modell Funktionen um die Sicherheit des Gerätes und der Daten sicherzustellen. Diese beinhalten:

Benutzersperre: verhindert den Zugriff auf einige Funktionen und die Geräteeinstellungen. Diese Funktion ermöglicht dem Administrator zu entscheiden, wer welche Funktion des Gerätes nutzen kann. Beispiele dafür ist die Nutzung der Fax- und Scanfunktion oder die Vergabe monatlicher Druckkontingente. Dies wird über persönliche PIN-Codes oder NFC-Karten ermöglicht.

Sicherer Druck: besonders geeignet für Nutzer, die nur gelegentlich vertrauliche Dokumente ausdrucken. Der Druckauftrag wird erst ausgedruckt, wenn der Benutzer sich direkt am Gerät per PIN-Code authentifiziert hat. Der PIN-Code wird zuvor vom Benutzer direkt im Treiber für diesen Druckauftrag festgelegt.

Secure Print+: besonders geeignet für Nutzer, die vertrauliche Dokumente ausdrucken möchten. Der Druckauftrag wird erst ausgedruckt, wenn der Benutzer sich direkt am Gerät per optionaler, vorkonfigurierter NFC Zugangskarte authentifiziert hat. Beim Drucken eines vertraulichen Dokuments, weist der Nutzer die NFC Zugangskarte einfach dem Druckauftrag im Druckertreiber zu. Im Anschluss muss der o.g. Authentifizierungsvorgang am Gerät durchgeführt werden, um den Druckauftrag abzuholen.

Active Directory Secure Print: Diese Funktion verhindert den Zugriff auf das Gerät durch das grundsätzliche Sprerren für Unbefugte. Um das Gerät zu entsperren und den Druckauftrag abzuholen, müssen sich Benutzer erst mit ihrer bestehenden Windows® Active Directory Benutzername-/Passwort-Kombination authentifizieren. Der Druckauftrag verbleibt so lange im Gerätespeicher, bis er abgeholt wurde oder durch Stromunterbrechung/Ausschalten oder Rücksetzung des Geräts gelöscht wird.

Brother bietet zudem das sichere Drucken über LDAP-unterstützende Datenbank-Server. Dies funktioniert wie das Active Directory Secure Print, aber mittels Kommunikation zu einem LDAP Server.

Für einen zusätzlichen Schutz bei beiden Methoden kann der Administrator ein Zeitlimit einrichten, wie lange nicht abgeholte Druckjobs im Gerätespeicher abgelegt werden können.

Cloud Secure Print: ermöglicht es einem Nutzer ein Dokument per E-Mail oder per Webbrowser (in Verbindung mit HTTPS) zum zukünftigen Abruf am Drucker zu versenden. Dazu bekommt er als Antwort ein einmalig nutzbares Passwort zugesendet, mit dem der Druckauftrag am Gerät gestartet werden muss. Die Daten werden temporär zur Aufbereitung in die Brother Cloud (Standort außerhalb der Europäischen Union) per HTTPS übertragen und nach der Verarbeitung automatisch gelöscht. Bitte beachten Sie: sollte der Druckauftrag am Gerät nicht innerhalb von 24 Stunden ausgedruckt werden, wird er automatisch gelöscht.

Geschützte PDF: Gescannte Dokumente können im Format „geschützte PDF“ abgelegt werden. Brother Scanner und Multifunktionsmodelle können sofort jede PDF Datei mit einem vierstelligen PIN-Code versehen, um den Zugriff Unbefugter auf die Informationen zu vermeiden.

Scan-to-SFTP: Das Secure File Transfer Protokoll (SFTP) verwendet einen geschützten Datenstrom. Durch die Kontrolle des Zugangs zu SFTP-Servern können Unternehmen/Organisationen helfen, dass komplette Netzwerk sicherer zu gestalten.

IP Filter: verhindert den Gerätezugang über das Netzwerk. Das Gerät akzeptiert nur Verbindungen von zugelassenen/hinterlegten IP Adressen.

Protokoll Kontrolle: ermöglicht es Administratoren, nicht benötigte Protokolle zu sperren.

L3. Ist es bei der Benutzung von Funktionen wie Sicherer Druck möglich, dass der Druckerspeicher ausgelesen wird und Druckdaten sichtbar werden?

Der Zugriff auf temporär im Gerätespeicher abgelegte Druckdaten ist nicht möglich. Nachdem ein Druckauftrag ausgedruckt wurde, können Teile des Druckauftrags nach dem Ausdruck temporär im Arbeitsspeicher des Druckers verbleiben, bis diese vom nächsten Druckauftrag oder durch das Trennen des Druckers von der Stromzufuhr überschrieben/gelöscht werden. Brother Geräte unterstützen keine Funktion, auf diese Datenreste zuzugreifen.

L4. Werden bei der Nutzung von Brother Apps über die Benutzeroberfläche der Geräte Daten zu einem Brother Server übertragen oder gespeichert?

Die Dokumente werden zur Aufbereitung in die Brother Cloud (Standort außerhalb der Europäischen Union) gesendet. Nach der Verarbeitung werden sie automatisch gelöscht.

L5. Kann ich die Papierzufuhren sichern, um den unbefugtem Zugriff auf die enthaltenen Papiere/Formulare zu vermeiden?

Brother bietet bei einigen Modellen Lösungen, um die Papierfächer zu verschließen. Wenden Sie sich diesbezüglich an Ihren Fachhändler oder direkt an Brother.

L6. Kann ich das Benutzerpanel vor unbefugtem Zugriff schützen?

Viele Brother Geräte bieten Schutz vor unbefugtem Zugriff:

Einstellsperre: schränkt den Zugriff der Geräteeinstellungen über das Gerätebedienfeld ein. Das ist ideal für Unternehmen, die nicht den Zugang zu Funktionalitäten, aber die Änderung von Einstellungen durch Unbefugte sperren möchten.

Benutzersperre: verhindert den Zugriff auf einige Funktionen und die Geräteeinstellungen. Diese Funktion ermöglicht es dem Administrator zu entscheiden, wer welche Funktion des Gerätes nutzen kann. Beispiele dafür ist die Nutzung der Fax- und Scanfunktion oder die Vergabe monatlicher Druckkontingente. Dies wird über persönliche PIN-Codes oder NFC-Karten ermöglicht.

L7. Wie kann ich physische Schnittstellen, wie WLAN oder USB, deaktivieren?

Je nach Produktkategorie und Geräteserie können physische Schnittstellen, wie USB, Fax oder WLAN auf Anfrage deaktiviert werden. Wenden sie sich an Ihren Brother Fachhandelspartner oder an Brother direkt.

Technische Informationen

T1. Wo befinden sich die Server der Brother Cloud?

Die Brother Cloud nutzt Cloud Computing Dienste von Amazon Web Services mit derzeitigem Standort außerhalb der Europäischen Union (→ in den Vereinigten Staaten von Amerika).

T2. Welche Versionen des SMB (Server Message Block) Protokolls unterstützen Brother Geräte?

Je nach Produktreihe werden die SMB Versionen 1.0, 2.0, 2.1 und 3.x unterstützt.

T3. Welche Clouddienste werden unterstützt?

Brother unterstützt Box, Dropbox, Evernote, Google Drive, OneDrive, OneDrive for business und OneNote.

T4. Wie schützt Brother seine Geräte vor Denial of Service (DoS) oder Ransomware Attacken, wie z.B. „WannaCry“?

Brother bietet Funktionen wie IP Filter (d.h. das Gerät akzeptiert nur Verbindungen von zugelassenen/hinterlegten IP Adressen) und andere Industriestandard-Schutzmethoden. Bitte beachten Sie, dass eine ordnungsgemäß konfigurierte Firewall immer der erste Verteidigungspunkt ist. Netzwerk-Administratoren sollten sicherstellen, dass Geräte nur zu benötigten Services oder IP Ports Zugang haben.

T5. Wie kann ich die Geräteadministration und -konfiguration mit einem Passwort sichern?

Alle Brother Lasermodelle und die unten aufgeführten Tintenstrahlmodelle ermöglichen die Passwort-Sicherung der Embedded Web Server (EWS) Schnittstelle. Bei der L5000er/L6000er Monolaser-Serie (s.u.) wird zudem der Zugriff auf die Weboberfläche der Geräte nach fünfminütiger Inaktivität des Administrators beendet. Brother empfiehlt ausdrücklich, ggf. ein Administrator-Passwort bei der initialen Einrichtung festzulegen. Zusätzlich können Nutzer von den integrierten Brother Sicherheitsfeatures profitieren. Dies beispielsweise über das Zulassen nur von Port 443 in den Servereinstellungen der Web-Oberfläche. Am besten sichern Sie die EWS-Schnittstelle direkt bei der Ersteinrichtung des Gerätes.

Netzwerk-Administratoren sollten sicherstellen, dass Geräte nur zu benötigten Protokollen und IP-Adressen Zugang haben.

Tintenstrahlmodelle

- MFC-J6520DW
- MFC-J6720DW
- MFC-J6920DW
- DCP-J4110DW
- MFC-J4410DW
- MFC-J4510DW
- MFC-J4610DW
- MFC-J4710DW
- DCP-J4120DW
- MFC-J4420DW
- MFC-J4620DW
- MFC-J4625DW
- MFC-J5320DW
- MFC-J5620DW
- MFC-J5625DW
- MFC-J5720DW

- DCP-J772DW
- DCP-J774DW
- MFC-J890DW
- MFC-J895DW

L5000er/L6000er Monolaserserie

- HL-L5100DN
- HL-L5100DNT

- HL-L5100DNTT
- HL-L5200DW
- HL-L6250DN
- HL-L6300DW
- HL-L6400DW
- HL-L6400DWTT
- DCP-L5500DN
- DCP-L6600DW
- MFC-L5700DN
- MFC-L5750DW
- MFC-L6800DW
- MFC-L6800DWT
- MFC-L6900DW

T6. Unterstützt Brother eine sichere Kommunikation?

Brother unterstützt Kommunikationsprotokolle und -verschlüsselungen nach Industriestandard. Dazu gehört:

802.1x: Alle Brother Geräte für den professionellen Einsatz sind konform mit dem extrem sicheren IEEE 802.1x Standard, egal ob sie an ein kabelgebundenes oder kabellosen Unternehmensnetzwerk angebunden sind.

IPsec: Zahlreiche Brother Modelle können über IPsec direkt mit internen oder externen Umgebungen verbunden werden. IPsec ist in den Geräten bereits integriert. Es muss keine Middleware- oder Drittanbieter-Hardware genutzt werden.

SNMPv3: Brother Modelle unterstützen die mit SNMP Version 1, 2 und 3 (MD5 und SHA1) verschlüsselte Kommunikation, sogar bei Remote-Setup und Routinewartungen.

T7. Sind die Daten bei der Netzwerkkommunikation von/zu meinem Brother Modell verschlüsselt?

Je nach Modell sind Brother Geräte mit Transport Layer Security (TLS) und Secure Socket Layer (SSL) Verschlüsselung ausgestattet. Diese Technologie wird auch im Onlinehandel zum Schutz von Bank- und Kreditkarteninformationen genutzt. Dokumente werden bei der Übertragung durch das Netzwerk so mit bis zu 256-bit verschlüsselt.

T8. Ist das WLAN meines Brother Geräts vor WPA2-KRACK-Angriffen geschützt?

Die Key Reinstallation Attacke (KRACK) zielt auf den Vier-Wege-Handshake des WPA2-Protokolls ab und täuscht ein Gerät so, dass es einen bereits genutzten Key noch einmal benutzt. Die Schwachstelle liegt hier beim WiFi-Standard selbst und nicht bei Produkten oder Umsetzungen. Daher können selbst korrekt eingerichtete WPA2-Umsetzungen betroffen sein.

Die potenziellen Angreifer müssen sich in der lokalen Reichweite des WiFi Routers-befinden, den sie angreifen möchten. Zudem sind Daten, die bereits durch HTTPS, TLS etc. verschlüsselt wurden, weiterhin geschützt. Selbst bei WPA2-Angriffen können Datenverluste durch das Einschalten verschlüsselter Datenströme (je nach Gerät z.B. SSL/TLS, SSH usw.) vermieden werden.

Updates für die aktuellen Mono- und Farblasermodelle sind seit Januar 2018 verfügbar. Wenden Sie Sich an Brother für weitere Informationen.

T9. Werden Zugangsdaten für Clouddienste, wie Google Drive auf einem Brother Gerät oder in der Brother Cloud (Standort außerhalb der Europäischen Union) gespeichert?

Zugangsdaten werden verschlüsselt, getrennt und in zwei Teilen gespeichert. Der erste Teil befindet sich im Gerät, der zweite Teil in der Brother Cloud.

T10. Welche Protokolle werden von Brother Modellen unterstützt und können diese konfiguriert oder deaktiviert werden?

Je nach Modell finden Sie eine vollständige Liste der unterstützten Protokolle inkl. Port hier. Manche Protokolle können optional deaktiviert werden.

Protokol	**Default TCP/UDP Port**
Web Based Management (Web Server)	80, 443, 631
Telnet	23
SNMP	161, 162
Remote Setup	-
LPD	515
Raw Port	9100
IPP	631
AirPrint	-
Mopria	-
Web Services	80, 443, 631
Google Cloud Print	5222
Proxy	8080
Network Scan	445
POP3/IMAP4/SMTP	25, 110, 143, 465, 587
FTP Server	21
FTP Client	21
SFTP	22
TFTP	69
WebDAV	445
CIFS	137, 138, 139, 445
LDAP	389

mDNS	5353
LLMNR	5355
SNTP	123

T11. Wie funktioniert Cloud Secure Print? Werden dabei Daten auf einem Brother Server, auch temporär, gespeichert?

Cloud Secure Print ermöglicht es einem Nutzer ein Dokument per E-Mail oder per Webbrowser (in Verbindung mit HTTPS) zum zukünftigen Abruf am Drucker zu versenden. Dazu bekommt er als Antwort ein einmalig nutzbares Passwort zugesendet, mit dem der Druckauftrag am Gerät gestartet werden muss. Die Daten werden temporär zur Aufbereitung in die Brother Cloud (Standort außerhalb der Europäischen Union) per HTTPS übertragen und nach der Verarbeitung automatisch gelöscht. Bitte beachten Sie: sollte der Druckauftrag am Gerät nicht innerhalb von 24 Stunden ausgedruckt werden, wird er automatisch gelöscht.

Allgemein

A1. Ist der Einsatz von Kensington Locks mit Brother Geräten möglich?

Verschiedene Brother Modelle besitzen eine mit Schlössern, z.B. von Kensington oder Belkin kompatible physische Sicherheitsvorrichtung.

A2. Sind Brother Modelle konform mit den IEC 60950 und IEC 60601-1 Standards für die Verbindung mit medizinischen Geräten?

Brother Modelle sind konform mit dem IEC 60950 Standard. Aktuell sind sie nicht konform mit dem IEC 60601-1 Standard.

A3. Welche Analyse-Daten werden über meine Nutzung von Brother Hardware, Software oder Services gesammelt? Ermöglichen die Daten eine persönliche Identifizierung?

Informationen zur Nutzung von Brother Hardware, Software oder Services werden nur gesammelt, wenn das a) vertraglich bei einem MPS (Managed Print Services) Programm oder b) im Rahmen eines Wartungs-/Verbrauchsmaterial-Programms vereinbart worden ist. Diese Daten sind nicht personen-, sondern produkt-/servicenutzungsbezogen und unterstützen das Geräte-Feedback. Diese Informationen werden genutzt, um die Brother Dienste und Services zu verbessern und zukünftige Anforderungen zu erkennen.

Wenn Sie die Brother Software auf Ihrem PC installieren, können Sie zustimmen, am BPRSP (Brother Product Research and Support Program) teilzunehmen. In diesem Rahmen

sammelt Brother anonymisierte Nutzungsdaten von Ihrem Drucker zu Zwecken der Verbesserung unserer Produkte und Services. Sie können sich jederzeit von diesem Programm wieder abmelden. Die gesammelten Informationen lassen keine persönliche Identifizierung zu und werden nur zur Planungsoptimierung unserer Produkte und Services genutzt,

A4. Wo und wie werden meine Daten gespeichert, wenn ich mein Brother Gerät registriere?

Die Registrierungsdaten werden im Europäischen Brother Daten Center und der Brother Cloud konform mit der aktuellen EU Datenschutzverordnung (EU-DSGVO) für alle Individuen innerhalb der Europäischen Union (EU) gespeichert.

Videokonferenzen/OmniJoin

V1. Wie kann ich erkennen, dass das Meeting, an dem ich teilnehme, aufgezeichnet wird?

Wenn die Aufzeichnung des Meetings gestartet wird, erscheint dazu ein zweiseküdiger Pop-Up Hinweis. Zudem wird über die gesamte Aufnahmedauer ein roter Punkt in der linken unteren Ecke des Meetingbildschirms angezeigt.

V2. Wo befindet sich die Server der OmniJoin Public Cloud?

Die Server stehen in Deutschland, Skandinavien, Großbritanien, Vereinigten Staaten von Amerika und Japan. Es ist möglich eine der oben aufgeführten Serverregionen auszuwählen, so dass nur diese genutzt wird.

V3. Wie werden meine Daten in der OmniJoin Public Cloud geschützt?

Alle OmniJoin Konferenzen, OmniJoin IM und Portalseiten-Sitzungen werden mit TLS 1.0, TLS 1.2 Protokollen verschlüsselt. Wenn eine sichere Verbindung nicht hergestellt werden kann, schlägt die Verbindung fehl. OmniJoin setzt eine Public-Key-Infrastruktur (PKI) und Drittanbieter-Zertifikate und Zertifizierungsstellen ein. Zudem werden weder intern Schlüsselpaare verwaltet noch proprietäre Verschlüsselungsmethoden verwendet. Zusätzlich sind die Verbindungen für alle Kontrollprotokolle und für den Medien-Payload per RSA 256bit AE-Verschlüsselung gesichert.

V4. Muss ich für eine OmniJoin Videokonferenz bestimmte Ports freigeben?

OmniJoin wurde für Multisite-Netzwerke und NAT, sowie Firewall- und Proxy-Traversale entwickelt. OmniJoin nutzt TLS-Verbindungen auf den Ports 80, 443, 22, 23, 1270 und 37000 (sog. „legacy ports“). OmniJoin nutzt TCP und stellt keine UDP oder andere broadcastorientierte Verbindungen her. Alle Verbindungen werden vom Client außerhalb der Firewall aufgebaut – es gibt keine sog. „Inbound Connections“. OmniJoin unterstützt Proxy-Authentifizierung-Standards inklusive WPAD, NTLM, Proxy-Autokonfiguration, Socks5 und manuelle Proxykonfigurationseinstellungen. OmniJoin Software beinhaltet herstellerspezifische Proxy-Optimierungen für z.B. Squid Web Proxy, Microsoft® Threat Management Gateway/ISA Server. OmniJoin bietet außerdem Ausweichmechanismen für Proxy-Server ohne installierten Proxy-Client.

V5. Kann ich meinen eigenen Server als Speicherort meiner Videokonferenzinhalte nutzen?

Mit der OmniJoin Hybrid Cloud Version werden Ihre Meetinginhalte und Video/Audio-Daten auf dem Server Ihrer Wahl gehostet. Eine Verbindung zur Public Cloud besteht nur zu Administrationszwecken, z.B. für Updates und zur Accountauthentifizierung.

In der OmniJoin Private Cloud werden alle Inhalte (auch administrative) exklusiv auf dem Server Ihrer Wahl gehostet.

V6. Kann ich den Zutritt zu meiner Videokonferenz mit einem Passwort schützen?

Ja, Sie können Ihre Videokonferenz mit einem Passwort versehen. Nur mit diesem Passwort gelangt man in Ihren Videokonferenzraum.

Managed Print Service (MPS)

Unsere Datenschutzrichtlinie finden Sie unter
https://www.brother.de/unternehmen/datenschutzrichtlinie

M1. Entsprechen die Brother Managed Print Services den Anforderungen der Datenschutz-Grundverordnung (DSGVO)?

Die von Brother erbrachten Dienstleistungen der Brother Managed Print Services, d. h. Geräteüberwachung, Wartung und Reparatur, verbrauchsabhängige Abrechnung und Verbrauchsmateriallieferung werden konform zu den Anforderungen der DSGVO angeboten.

Bitte beachten Sie: Jeder Managed Print Service Vertrag kann auf individuelle Bedürfnisse zugeschnitten werden; unsere Partner können zusätzliche Dienstleistungen anbieten, die in das jeweilige Angebot aufgenommen werden können. Für spezielle Informationen über die

Einhaltung der DSGVO-Richtlinien für Ihr individualisiertes Angebot wenden Sie sich bitte an den für Sie zuständigen Vertriebsmitarbeiter.

M2. Haben die Brother Managed Print Services Zugriff auf gedruckte Daten?

Die Kerndienste von Brother Managed Print Services, also Geräteüberwachung, Wartung und Reparatur, verbrauchsabhängige Abrechnung und Verbrauchsmateriallieferung verarbeiten keine gedruckten Daten.

Bitte beachten Sie: Jeder Managed Print Service Vertrag kann auf individuelle Bedürfnisse zugeschnitten werden; unsere Partner können zusätzliche Dienstleistungen anbieten, die in Ihr Angebot aufgenommen werden können. Für Informationen über die Einhaltung der DSGVO-Richtlinien für Ihr spezielles Angebot wenden Sie sich bitte an den für Sie zuständigen Vertriebsmitarbeiter.

M3. Welche Daten werden bei Nutzung der Brother Managed Print Services erfasst?

Brother nutzt Kundenkontakt- und Adressdaten, Geräteservice-, Gerätestandort- und Gerätenutzungsdaten, Rechnungsdaten und andere Informationen, die für den Geschäftszweck der Erfüllung oder Verbesserung Ihres Brother Managed Print Service Vertrages erforderlich sind.