ThinPrint®

EU-Datenschutz-Grundverordnung:

Das müssen Sie beim Netzwerkdrucken beachten!

Inhalt

Achtung: Datenschutzrisiko Netzwerkdrucken 3

Drucken im Netzwerk – Hintergrundwissen 5
1. Anwendung 5
2. Druckserver 5
3. Netzwerkdrucker 6

Angriffspunkte beim Netzwerkdruck 6

Druckdatenverschlüsselung 6
1. Anwendung → Druckserver 6
2. Druckserver → Netzwerkdrucker 7
3. Netzwerkdrucker 8

Europäische Datenschutz-Grundverordnung:
So halten Sie sich auch beim Drucken an die Regeln! 9

Anhang 10
Auszüge aus der EU-Datenschutzgrundverordnung 10
Akronyme und Links 13
Hohe Bußgelder 13

Achtung: Datenschutzrisiko Netzwerkdrucken

Die seit Mai 2018 verbindliche Europäische-Datenschutz-Grundverordnung (EU-DSGVO) hat die Regeln für die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht. Doch besonders in kleinen und mittelständischen Unternehmen gibt es immer noch einige Unsicherheiten bezüglich der europäischen Gesetzgebung. Welche Informationen sind den personenbezogenen Daten zuzuordnen? Welche IT-Prozesse sind betroffen? Wo fängt man mit der Umsetzung an? Die gute Nachricht ist, dass die Unternehmen und Behörden in Deutschland mit dem Bundesdatenschutzgesetz schon sehr gut aufgestellt sind. Trotzdem müssen die vorhandenen IT-Prozesse oft weiter optimiert bzw. Sicherheitsmängel behoben werden. Im Zuge dessen sollten auch die Druckprozesse im Unternehmen unter die Lupe genommen werden.

Natürliche Personen haben laut dem EU-DSGVO ein Recht auf Schutz ihrer personenbezogenen Daten (Art. 1 Abs. 2 EU-DSGVO). Durch die Vereinheitlichung wird die Verarbeitung personenbezogener Daten über Landesgrenzen hinweg erleichtert, da eine bis dato möglicherweise abweichende nationale Datenschutzregelung nun keinen Hinderungsgrund mehr darstellt (Art. 1 Abs. 3 EU-DSGVO). Aber wie erkennt man, ob bestimmte Angaben oder Informationen den personenbezogenen Daten zuzuordnen sind oder nicht? Grundsätzlich handelt es sich immer dann um personenbezogene Daten, wenn eine Person direkt oder indirekt identifiziert werden kann – also z.B. mittels des Namens, der Telefonnummer, Kontodaten, Anschrift oder auch der IP-Adresse.

Das Recht auf Schutz personenbezogener Daten wird durch Art. 5 EU-DSGVO (Grundsätze der Verarbeitung personenbezogener Daten) geregelt. Dazu gehören u.a. die Rechtmäßigkeit, Transparenz, Zweckbindung, Richtigkeit, Speicherbegrenzung, Integrität und Rechenschaftspflicht.[1] Für Unternehmen ergibt sich daraus eine umfangreiche Dokumentationspflicht und sie sind dazu verpflichtet, Datenlecks zeitnah zu melden. Bei einem Verstoß gegen die Datenschutzrichtlinien ist mit sehr hohen Bußgeldern zu rechnen.

1 vgl. EU-Datenschutz-Grundverordnung: Das müssen Sie wissen, Dr. Datenschutz, intersoft consulting services, Link: **https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/** (März 2016)

Häufig bleibt jedoch unbeachtet, dass auch beim Druckprozess Sicherheitsrisiken für personenbezogene Daten bestehen:

- Unverschlüsselte Übertragung der personenbezogenen Daten über das Netzwerk
- Unverschlüsselte Speicherung der persönlichen Daten während des Druckprozesses auf Servern oder Festplatten der Drucker
- Ausgabe vertraulicher Dokumente auf falschen Druckern
- Dokumente mit personenbezogenen Daten geraten am Drucker in falsche Hände

Mit ThinPrint können Sie Ihre Druckprozesse ohne Investition in neue Hardware vollständig EU-DSGVO-konform absichern und Schwachstellen einfach ausschalten: Nehmen Sie sich die Zeit und erfahren Sie in diesem White Paper, wie Sie den gesamten Druckprozess gegen Datenschutzrisiken absichern. So machen Sie Ihr IT-Unternehmen DSGVO-konform.

Drucken im Netzwerk – Hintergrundwissen

1. Anwendung

In jeder Druckumgebung erfolgt das Auslösen des Druckauftrages in der jeweiligen Anwendung. Diese läuft entweder direkt auf der entsprechenden Workstation (Bild 1) oder auf einem Remote-Desktop-Session-Host, einem Citrix-Virtual-Apps-Server oder einem virtuellem Desktop. (Bild 2)

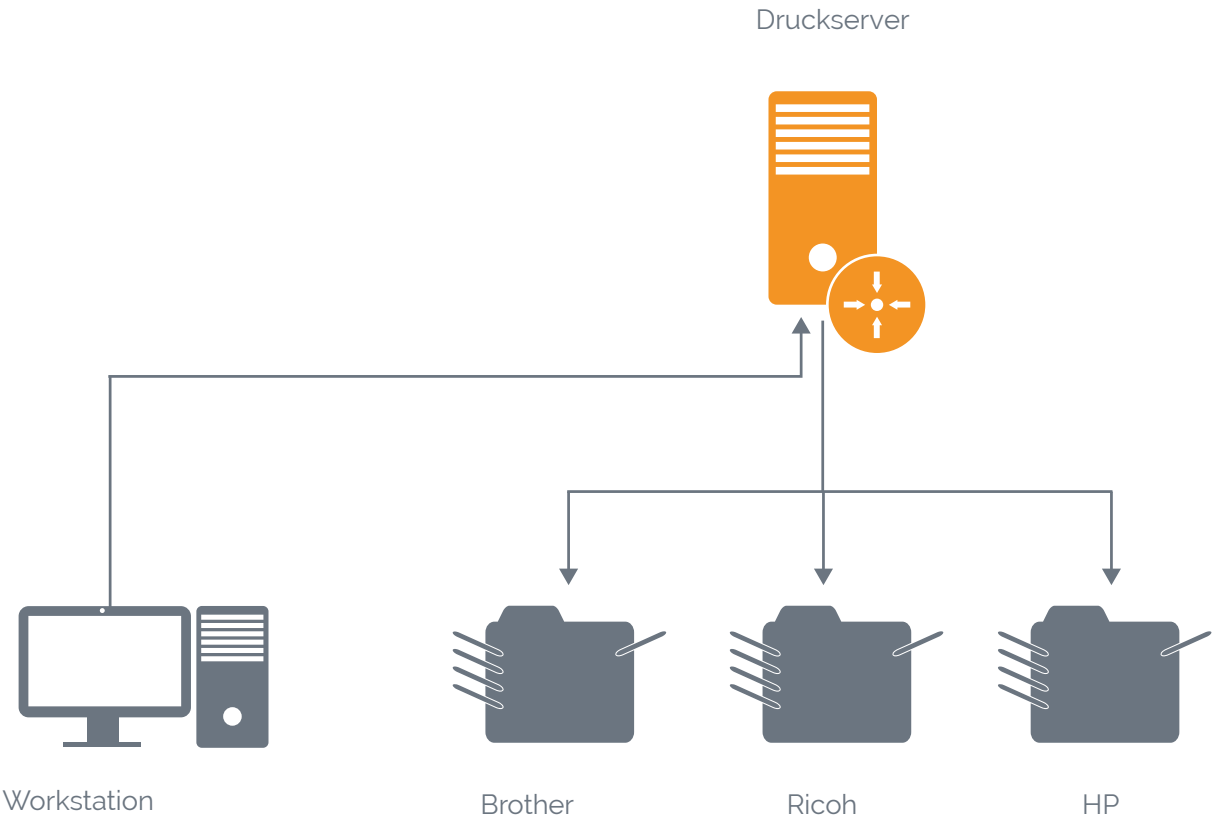

Bild 1: Weg der Druckdaten von der Anwendung via Druckserver zum Netzwerkdrucker

2. Druckserver

In mittleren bis großen Druckumgebungen werden Druckserver zur Zentralisierung der Druckprozesse eingesetzt. Das vereinfacht nicht nur die Administration, sondern es ermöglicht auch, Sicherheitstechniken zu implementieren.

3. Netzwerkdrucker

Aus Administrations- und Kostengründen wurden in den letzten Jahrzehnten viele Arbeitsplatzdrucker durch Netzwerkdrucker ersetzt. Dadurch werden sensible Daten oftmals offen über das Firmennetz gesendet.

Angriffspunkte beim Netzwerkdruck

IT-Administratoren sichern Anwendungen und Daten durch Zugriffsschutz[2] sowie durch verschlüsselte Verbindungen zu Servern und Workstations. Dagegen werden Druckdaten oft ungesichert zu Druckservern und von dort zu Netzwerkdruckern gesendet. Dadurch ergeben sich folgende Angriffspunkte:

- die Netzwerkkarten aller Geräte, über die der Druckdatenstrom geleitet wird: Workstation, Desktop, Hub, Router, Server und Netzwerkdrucker
- die auf dem Druckserver freigegebenen Drucker
- die Festplatten der Netzwerkdrucker

Art. 4** + **9 EU-DSGVO:
Verarbeitung besonderer Kategorien personenbezogener Daten

Art. 30 EU-DSGVO:
Grundsätze der Verarbeitung

Druckdatenverschlüsselung

Es gibt mehrere Stellen, an denen der Druckprozess optimiert werden muss, um eine umfassende, sichere Druckdatenverschlüsselung, entsprechend der EU-DSGVO, zu erreichen.

1. Anwendung → Druckserver

Ab SMB 3.0 können Druckdaten von der Anwendung zur Druckerfreigabe auf dem Druckserver mit Windows-Bordmitteln verschlüsselt werden (Bild 2).[3] Dadurch ist der Zugriff auf die auf dem Druckserver freigegebenen Drucker nur noch über verschlüsselte Verbindungen möglich.

Art. 5 EU-DSGVO:
Vertraulichkeit und Integrität

Art. 32 Ia EU-DSGVO:
Verschlüsselung

2 sowohl für Anwendungsserver und Workstations, aber auch für Dateiserver und Datenbanken
3 Voraussetzung: mind. Windows Server 2012 resp. Windows 8

2. Druckserver → Netzwerkdrucker

Für die Verbindungen vom Druckserver zu Netzwerkdruckern kann nur auf Drittanbieterlösungen zurückgegriffen werden. Dabei stellen die Lösungen der einzelnen Druckerhersteller einen erhöhten Administrationsaufwand dar, weil sie pro Druckerhersteller auf dem Druckserver installiert und verwaltet werden müssen. Eine universelle, herstellerunabhängige Lösung, die auch mit unterschiedlichsten Active-Directory-Strukturen kompatibel ist, stellt ThinPrint bereit (Bild 2).

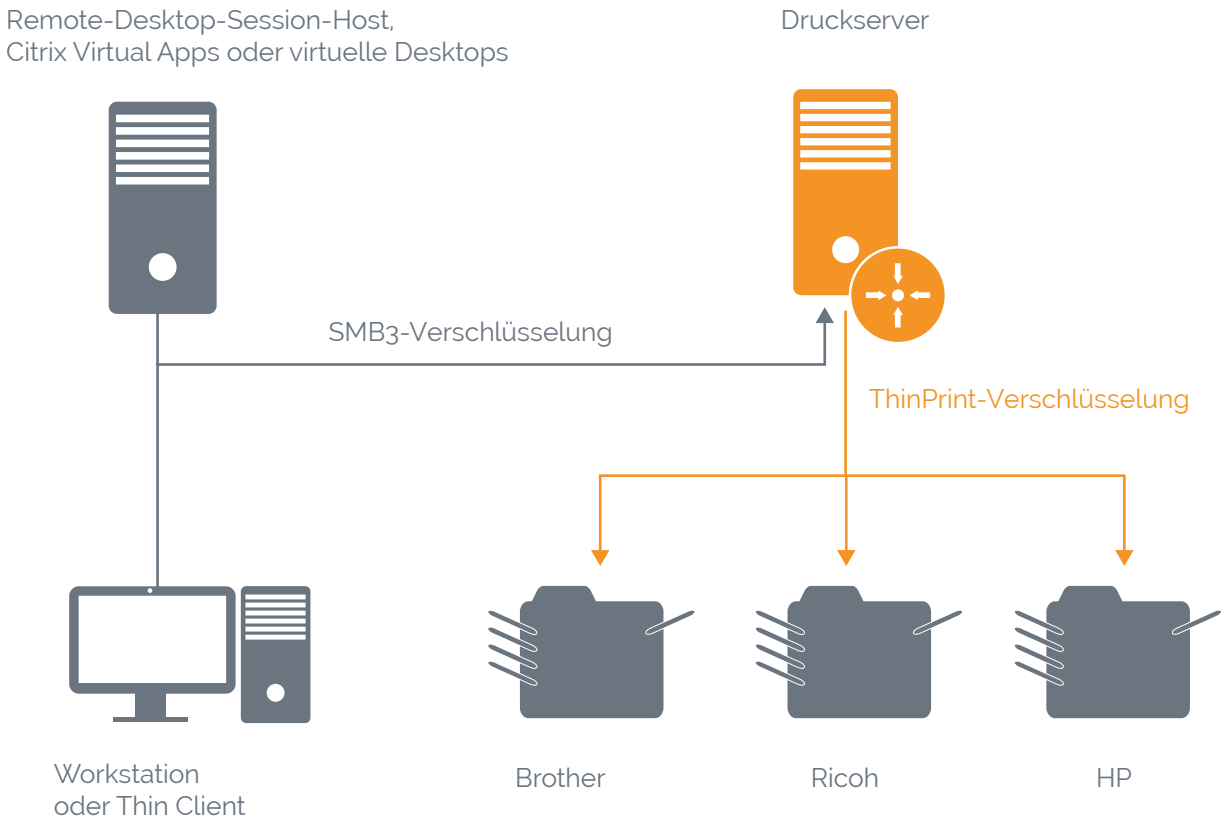

Bild 2: Verschlüsselung der Druckdaten von der Anwendung zum Druckserver und von dort zu den Netzwerkdruckern

Für Druckermodelle, die von ThinPrint (noch) nicht unterstützt werden, kann der **ThinPrint Hub** verwendet werden, der die Druckdaten über USB zum Netzwerkdrucker weiterleitet (Bild 3).

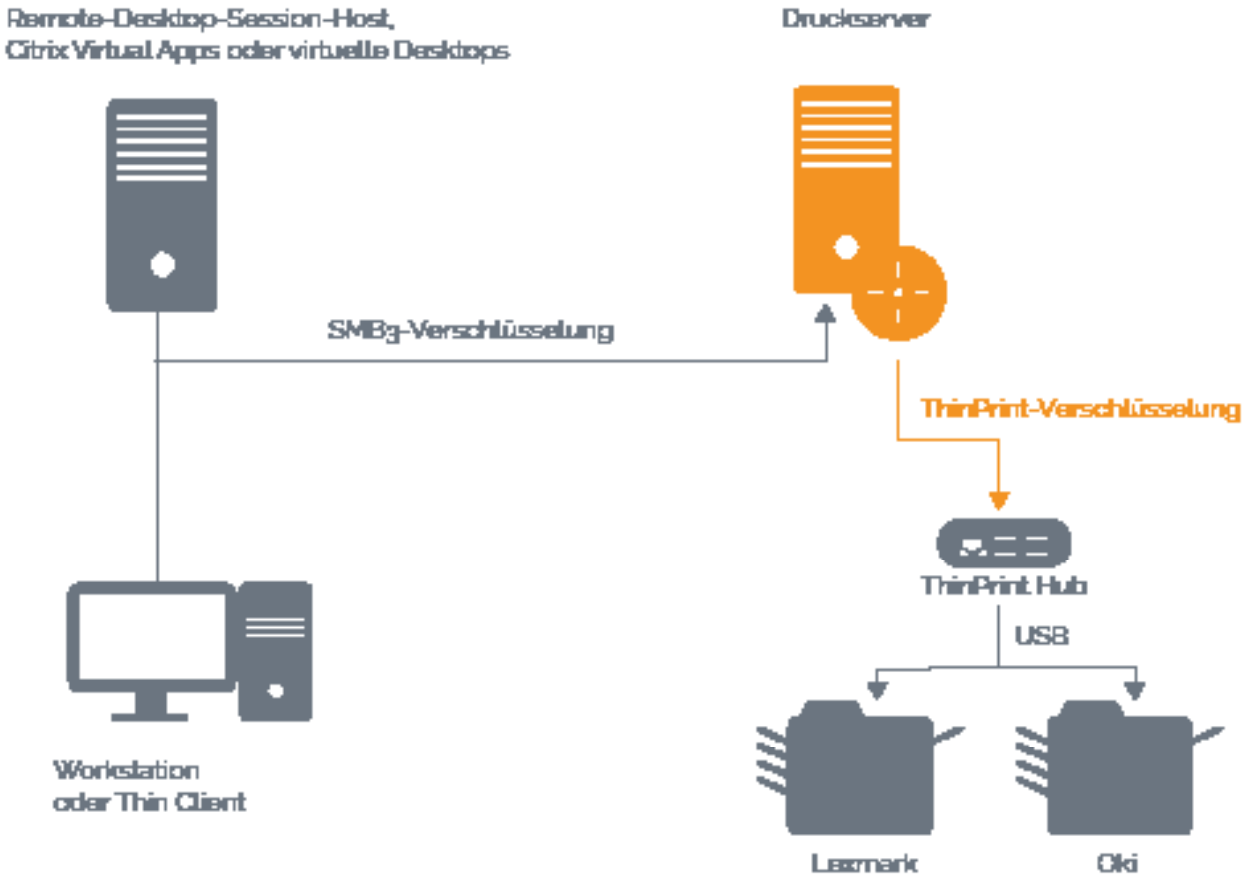

Bild 3: Verschlüsselung der Druckdaten von der Anwendung zum Druckserver und von dort zum ThinPrint Hub

3. Netzwerkdrucker

Am Netzwerkdrucker selbst ist sicherzustellen, dass Unbefugte sich nicht in das Interface des Druckers einloggen können; hierzu sollten Zertifikate einer Authentifizierung mit Benutzername und Passwort vorgezogen werden. Wird die interne Festplatte des Druckers verwendet, muss diese (hardwareseitig) verschlüsselt werden.

Der Diebstahl von fertigen Ausdrucken aus dem Ausgabefach kann durch eine Authentifizierung am Drucker verhindert werden. ThinPrint bietet mit Personal Printing diverse Authentifizierungsoptionen: per Chipkarte oder Smartphone sowie zusätzlich per PIN.

Art. 32 EU-DSGVO:
Sicherheit der Verarbeitung

Europäische Datenschutz-Grundverordnung: So halten Sie sich auch beim Drucken an die Regeln!

Es ist es unerlässlich, dass Unternehmen bei einer Überprüfung der datenschutzrelevanten Abläufe auch dem kompletten Druckprozess Beachtung schenken. Wie in diesem White Paper dargestellt, durchläuft ein Druckjob vom Zeitpunkt des Auslösens bis hin zum fertigen Ausdruck verschiedene Stationen. Die einzelnen Etappen wurden in diesem Dokument veranschaulicht. Dabei haben Sie auch die vorhandenen Sicherheitsrisiken und Schwachstellen kennengelernt.

Sie wissen nun, dass die Verbindung vom Druckserver zu Netzwerkdruckern nur durch Drittanbieterlösungen abgesichert werden kann. Dabei entsteht ein hoher Administrationsaufwand, da die Druckerherstellerlösungen einzeln auf dem Druckserver installiert und verwaltet werden müssen. Auch der Netzwerkdrucker stellt ein Sicherheitsrisiko dar. Wenn der Druckjob am Netzwerkdrucker ankommt, ist nicht garantiert, dass er auch in die richtigen Hände gerät.

ThinPrint ist eine professionelle, herstellerunabhängige Drucklösung, mit der Sie die hier dokumentierten Schwachstellen einfach beseitigen. Mit ThinPrint gestalten Sie Ihre Druckumgebung DSGVO-konform – ohne zusätzlichen Administrationsaufwand.

Anhang

Auszüge aus der EU-Datenschutzgrundverordnung

Art. 4 EU-DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck: „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Art. 5 EU-DSGVO

(1) Personenbezogene Daten müssen

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verar-beitung nach Treu und Glauben, Transparenz“);
b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverar-beitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der perso-nenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 9 EU-DSGVO

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen: ...

Art. 30 EU-DSGVO

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b. die Zwecke der Verarbeitung;
c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Art. 32 EU-DSGVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risi-ken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 83 IVa EU-DSGVO

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a. die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

Art. 83 Va EU-DSGVO

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a. die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

Akronyme und Links

BDSG	Bundesdatenschutzgesetz
EU-DSGVO	Europäische Datenschutzgrundverordnung
EU	Europäische Union
GDPR	General Data Protection Regulation (Datenschutzgrundverordnung)

Für weitere Informationen zur ThinPrint-Verschlüsselung inklusive einer Übersicht über Netzwerkdrucker mit integriertem ThinPrint Client siehe:

blog.thinprint.com/end-to-end-encryption-hp-printers

Hohe Bußgelder

Verstoß gegen ...	Bußgeldvorschrift
Art. 5 EU-DSGVO	bis zu 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes gemäß Art. **Art. 83 Va EU-DSGVO**
Art. 9 EU-DSGVO	bis zu 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes gemäß **Art. 83 Va EU-DSGVO**
Art. 30 EU-DSGVO	bis zu 10 Mio. EUR oder 2% des weltweiten Jahresumsatzes gemäß **Art. 83 IVa EU-DSGVO**
Art. 32 EU-DSGVO	bis zu 10 Mio. EUR oder 2% des weltweiten Jahresumsatzes gemäß **Art. 83 IVa EU-DSGVO**

Weitere White Paper:
Das vorliegende und viele andere White Paper zu interessanten IT-Themen finden Sie auf unserer Webseite als kostenlosen Download:
www.thinprint.com/whitepaper

Haben Sie Fragen?
Das ThinPrint-Team hilft Ihnen gerne weiter. Wir stehen Ihnen unter der folgenden Telefonnummer zur Verfügung: **+49-(0)30-39 49 31-0** oder senden Sie uns einfach eine E-Mail an **info@thinprint.com.**

Hauptniederlassung

ThinPrint GmbH
Alt-Moabit 91 b
10559 Berlin, Germany
Tel.: +49 (0)30-39 49 31-0
Fax: +49 (0)30-39 49 31-99
E-Mail: info@thinprint.com
www.thinprint.com

Australien

ThinPrint by Cortado Pty Ltd.
Level 10 I 20 Martin Place
Sydney, NSW 2000
Australia
Tel.: +61 2 9639 6643

USA (Colorado)

ThinPrint, Inc.
3827 Lafayett St #130
Denver, CO 80205
Tel.: +1-303-487-1302
E-mail: info@thinprint.com
www.thinprint.com

Japan

ThinPrint Japan
6F Shinmakicho Building
1-8-17 Yaesu
Chuo-ku Tokyo
Post Code 103-0028
Japan
E-Mail: info@thinprint.com
Telefon: +81 3 5542 1551

ThinPrint®

Alle genannten Marken und Produktnamen sind Warenzeichen bzw. eingetragene Warenzeichen der jeweiligen Hersteller und Unternehmen.

Folgen Sie ThinPrint auf: facebook twitter youtube linkedin