DS-GVO-konformes Drucken

Drucken, Scannen, Faxen, Kopieren

Leitfaden

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Dr. Roman Bansen | Referent IT-Infrastrukturen
T 030 27576-270 | r.bansen@bitkom.org

Verantwortliches Bitkom-Gremium

AK Printing Solution Services

Autoren

Dr. Roman Bansen | Bitkom e.V.
Robert Duisberg | Insentis GmbH
Bernd Hausmann | ThinPrint GmbH
Sabrina Heidgen | Ricoh Deutschland GmbH
Dennis Klussmann | Lexmark Deutschland GmbH
Christoph Losemann | Canon Deutschland GmbH
Carsten Meerpohl | Kyocera Document Solutions Deutschland GmbH
Jochen Plehnert | Konica Minolta Business Solutions Deutschland GmbH
Stefan Rautenbach | Ricoh Deutschland GmbH
Marc Recktenwald | HP Deutschland GmbH
Dr. Carsten Rückert | Wilhelm Dreusicke GmbH & Co. KG
Daniel Schiwek | HP Deutschland GmbH
Andre Schnibbe | SEAL Systems AG
Hans-Michael Voss | Lexmark Deutschland GmbH
Rebekka Weiß | Bitkom e.V.

Titelbild

© Ana Rivarola – unsplash.com

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Vorwort

1 Vorwort

Die EU-Datenschutzgrundverordnung (DS-GVO) ist seit Jahren der verbindliche Rechtsrahmen für den Schutz personenbezogener Daten. Dabei sieht die DS-GVO hohe Sanktionen vor; bei (schweren) Verstößen wurden bereits mehrfach Bußgelder bis in den achtstelligen Euro-Bereich verhängt.

Daher ist es für Unternehmen unabdingbar, dass auch wirklich alle Mitarbeiter und Abteilungen DS-GVO-konform mit personenbezogenen Daten umgehen. Zu den Systemen, die in Unternehmen oftmals hintangestellt werden, gehören vor allem Drucker und Multifunktionsgeräte, die auch kopieren, faxen und scannen können (im Folgenden kurz »Drucker« bzw. »Drucksysteme« genannt).

Jedoch verarbeiten auch diese Geräte personenbezogene Daten – gleich in doppelter Weise. Zunächst werden während des technischen Druckprozesses zwischen Druckauslösung und Dokumentenerstellung in vielfältiger Weise personenbezogene Daten verarbeitet (z.B. Nutzername); diese Daten werden als Transaktionsdaten bezeichnet. Des Weiteren enthalten die zu druckenden Dokumente in der Regel auch personenbezogene Daten; diese Daten werden als Nutzdaten bezeichnet.

Daher stellt sich die Frage, ob man DS-GVO-konformes Drucken »von der Stange« kaufen kann. Die Erreichung von DS-GVO-Konformität ist in hohem Maße ein individuell zu erarbeitender Prozess, der die Besonderheiten und Spezifika eines jeden Unternehmens in den Mittelpunkt stellen muss. Üblicherweise bedarf es der Zusammenarbeit von Fach- und Technikexperten mit Datenschützern sowie juristischen Experten, damit ein belastbares und nachhaltiges Konzept zur Erreichung von DS-GVO-Konformität entstehen kann.

Zu beachten ist auch, dass man seine Maßnahmen zur DS-GVO-Konformität jederzeit (z.B. gegenüber Behörden oder Wirtschaftsprüfern) nachvollziehbar nachweisen können muss.

Der vorliegende Leitfaden beleuchtet die oben aufgeführten Aspekte, die zur Erreichung von DS-GVO-Konformität betrachtet werden sollten. Bei der Umsetzung kann es hilfreich sein, externe Expertise in Anspruch zu nehmen.

2 Die DS-GVO

2 Die DS-GVO

2.1 DS-GVO – Was ist das überhaupt und warum ist es so wichtig?

Die Datenschutzgrundverordnung (DS-GVO) trat 2016 in Kraft. Sanktionen können bei Verstößen seit 2018 verhängt werden, da die DS-GVO im Mai 2018 EU-weit Geltung erlangte. Sie regelt weltweit für alle Unternehmen und Organisationen die Verarbeitung personenbezogener Daten von natürlichen, in der EU befindlichen Personen.

Die DS-GVO bezieht sich ausschließlich auf personenbezogene Daten. Darunter fallen alle Informationen über die eine Person direkt oder indirekt identifiziert werden kann. Wichtige Punkte der DS-GVO sind dabei auch die Pflicht zur Dokumentation der Maßnahmen sowie eine Meldepflicht bei Verstößen.

2.2 Welche Folgen können Datenschutzpannen haben?

In der Presse liest man gelegentlich über DS-GVO-Verstöße und diesbezügliche Bußgelder. Insofern ist die Verordnung keineswegs als zahnloser Tiger anzusehen. Im ersten Jahr nach Geltungsbeginn haben die Datenschutzbeauftragten der Bundesländer in insgesamt 81 Fällen DS-GVO-Verstöße geahndet. Im direkten Vergleich mit anderen EU-Ländern war Deutschland, insbesondere was die Höhe der Bußgelder anbelangt, zumindest anfänglich noch zurückhaltend. Im November 2019 hat ein Bußgeld jedoch auch hierzulande zum ersten Mal und deutlich die Millionengrenze geknackt. Seitdem schnellen die Bußgelder in die Höhe. Dabei muss berücksichtigt werden, dass mit Bußgeld belegte Unternehmen Vertraulichkeit auch für sich selbst einfordern können. Daher werden nur die wenigsten Fälle publik.

2.3 Welche Grundsätze gelten bei der Datenverarbeitung?

Art und Umfang der personenbezogenen Daten, die ein Unternehmen bzw. eine Organisation DS-GVO-konform verarbeiten darf, hängen vom Zweck ihrer Verarbeitung sowie der beabsichtigten Nutzung ab. Folgende Grundsätze sind dabei zu beachten:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:** Personenbezogene Daten müssen auf rechtmäßige und nachvollziehbare Weise verarbeitet werden. Gegenüber den Personen, deren Daten verarbeitet werden, müssen diesbezügliche Informationen in einfacher Sprache verfasst und leicht zugänglich gemacht werden.

- **Zweckbindung:** Für die Verarbeitung personenbezogener Daten müssen bestimmte Zwecke festgelegt sein und die Personen, deren Daten erhoben bzw. verarbeitet werden, darüber informiert werden. Ein Unternehmen bzw. eine Organisation darf personenbezogene Daten nicht zu unbestimmten Zwecken erheben oder für andere Zwecke nutzen, die mit dem ursprünglichen Zweck der Erhebung unvereinbar sind.

- **Datenminimierung:** Ein Unternehmen bzw. eine Organisation darf ausschließlich jene personenbezogenen Daten erheben und verarbeiten, die zur Erfüllung dieses Zwecks erforderlich sind.

- **Richtigkeit:** Es muss sichergestellt werden, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand hinsichtlich des Zwecks sind, für den sie verarbeitet werden. Wenn dies nicht der Fall ist, sind sie zu berichtigen.

- **Speicherdauer:** Es ist zu gewährleisten, dass personenbezogene Daten nicht länger als erforderlich für den Zweck, für den sie erhoben wurden, bzw. über die Dauer von (gesetzlichen) Aufbewahrungspflichten hinaus gespeichert werden.

- **Integrität und Vertraulichkeit:** Es müssen angemessene technische und organisatorische Maßnahmen getroffen werden, mit denen die Sicherheit der personenbezogenen Daten, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigter Zerstörung, Schädigung oder Verlust gewährleistet wird.

- **Rechenschaftspflicht:** Unternehmen bzw. Organisationen sind in Bezug auf die DS-GVO gegenüber Aufsichtsbehörden rechenschaftspflichtig, d.h. sie müssen die Berücksichtigung bzw. Anwendung der obenstehenden Prinzipien im Zweifel belegen können, z.B. durch den Nachweis geeigneter Verfahren und Prozesse.

- **Auskunftspflicht:** Unternehmen/Organisationen müssen individuell Auskunft über Art und Umfang der Verarbeitung personenbezogener Daten der anfragenden Person geben. Diese Informationen sind grundsätzlich unentgeltlich und unverzüglich, spätestens innerhalb eines Monats zur Verfügung zu stellen. Sie können schriftlich, auf elektronischem Wege oder – auf Verlangen der betroffenen Person – mündlich mitgeteilt werden.

- **Recht auf Löschung:** Personen haben das Recht, die Löschung der sie betreffenden personenbezogenen Daten zu fordern. Sofern dem keine anderen, vorrangigen Regelungen (z.B. gesetzliche Aufbewahrungspflichten) entgegenstehen, ist diese Löschung unverzüglich vorzunehmen.

3 »DS-GVO-konformes Drucken«?

3 »DS-GVO-konformes Drucken«?

Als Schnittstelle zwischen der digitalen und der analogen Welt kommt Druckern bzw. Multifunktionsgeräten in Bezug auf die DS-GVO eine besondere Bedeutung zu. Einerseits können die Dokumente personenbezogene und damit schützenswerte Daten im Sinne der DS-GVO beinhalten. Somit muss die Ausgestaltung diesbezüglicher Prozesse den Prinzipien der DS-GVO folgen. Andererseits fällt bei der Verarbeitung insgesamt eine Vielzahl von Transaktionsdaten an, die ebenfalls personenbezogene Daten enthalten können. Deshalb gilt auch in diesem Zusammenhang, dass personenbezogene Daten mithilfe sogenannter technischer und organisatorische Maßnahmen (TOMs) vor unberechtigtem Zugriff zu schützen sind. Dabei ist immer auch der Entsorgungsvorgang von Altgeräten mitzudenken.

Gleichfalls ist stets auch auf den Kontext bzw. die Verhältnismäßigkeit zu achten. So könnte man annehmen, dass eine mit biometrischen Daten (z.B. Fingerabdruck) abgesicherte Zugriffskontrolle am Drucksystem eine pragmatische und sichere Authentifizierungslösung darstellt. Jedoch zählen insbesondere biometrische Daten zu den besonders schützenswerten personenbezogenen Daten. Der dadurch erforderliche, ungleich umfangreichere Schutz von Biometrie-Daten lässt deren Nutzung zu gewöhnlichen Authentifizierungszwecken nur in Ausnahmefällen verhältnismäßig erscheinen.

Daher sollten alle einem Drucksystem zugrundeliegenden Prozesse, angefangen bei der Beschaffung über den Betrieb bis zu dessen Abbau, entsprechend datenschutzkonform gestaltet sein und in das betriebliche Datenschutzkonzept integriert werden. Aufgrund der Komplexität dieses Themas, den individuellen Bedürfnissen einer Organisation sowie einer Vielzahl an in Frage kommenden Lösungsansätzen, empfiehlt es sich, hierfür spezialisierte Expertise in Anspruch zu nehmen.

Es lässt sich festhalten, dass DS-GVO-konformes Drucken nicht als fertiges Produkt verfügbar ist. Vielmehr ist es das Resultat eines an den Bedürfnissen der betreffenden Organisation ausgerichteten, sauber dokumentierten und implementierten sowie laufend überwachten Datenschutzkonzepts.

Weiterführende Links:

- DS-GVO Gesetzestext: ↗https://eur-lex.europa.eu/eli/reg/2016/679/oj
- FAQ des Bitkom zur Datenschutzgrundverordnung: ↗https://www.bitkom.org/Bitkom/Publikationen/FAQ-zur-Datenschutzgrundverordnung.html
- Bitkom Übersichtsseite zur DS-GVO: ↗https://bitkom.de/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html

4 DS-GVO-relevante Daten im Druckkontext

4 DS-GVO-relevante Daten im Druckkontext

4.1 Übersicht und Schaubild

Nach der Erläuterung der einschlägigen Vorschriften und Regularien der DS-GVO in den vorherigen Kapiteln beschäftigen wir uns im Folgenden mit der Frage, wo überall im Kontext von Drucken, Kopieren, Scannen oder Faxen schützenswerte Daten auftreten können. Dazu betrachten wir die üblichen Prozessabläufe nach Eingabe, Verarbeitung und Ausgabe.

In allen Prozessabläufen fällt eine signifikante Menge von personenbezogenen Daten – sogenannte »Transaktionsdaten« – an. Darüber hinaus können auch personenbezogene Daten im Dokumententext selbst – sogenannte »Nutzdaten« – enthalten sein.

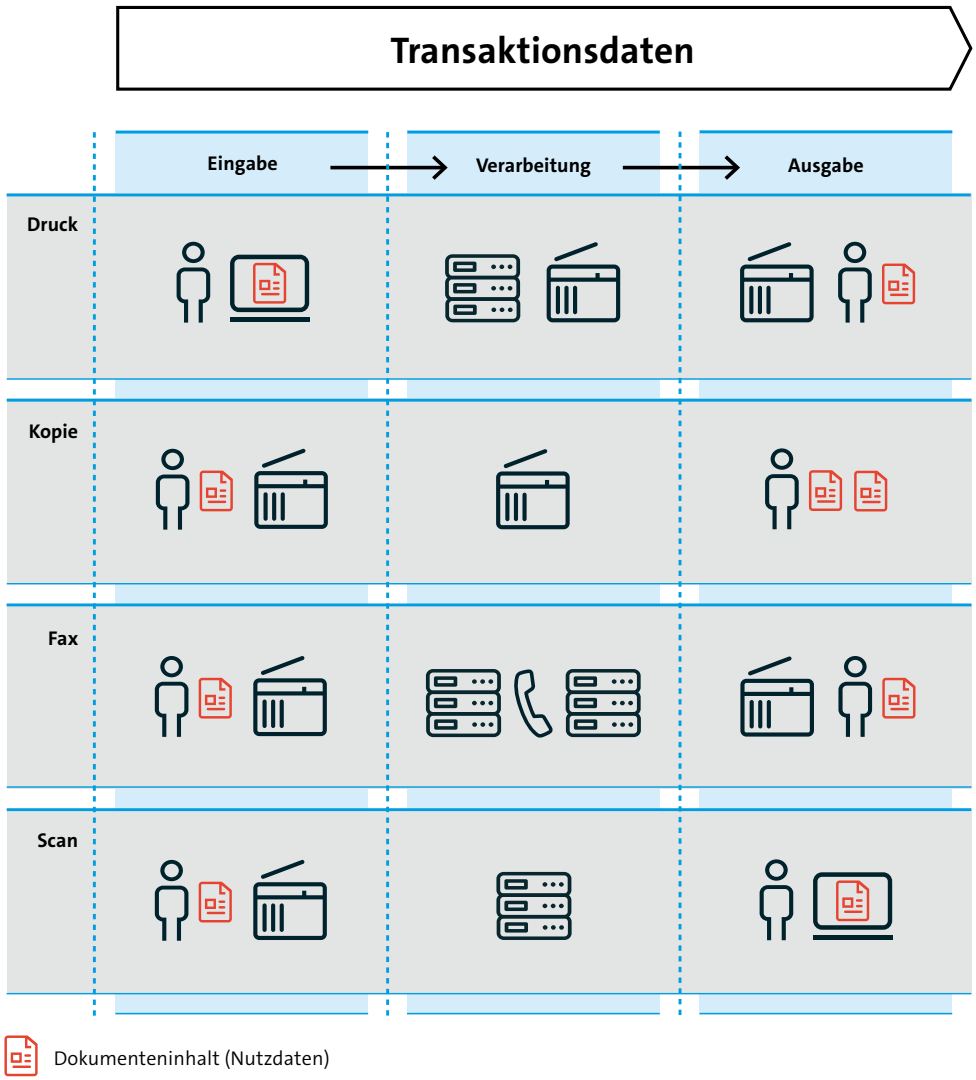

Abbildung 1: Das Schaubild zeigt die grundsätzlichen Unterschiede bei den einzelnen Funktionen

4.2 Welche DSGVO-relevanten Daten treten im Einzelnen auf?

Zur Erinnerung: die DS-GVO bezieht sich ausschließlich auf personenbezogene Daten. Darunter fallen alle Informationen über die eine Person direkt oder indirekt identifiziert werden kann. Dies schließt auch Daten ein, die in papierbasierter Form vorliegen. Im Gegensatz zu anonymisierten Daten fallen pseudonymisierte personenbezogene Daten unter die DS-GVO, weil bei einer Pseudonymisierung die zugehörigen personenbezogenen Daten unter Zuhilfenahme zusätzlicher Daten wiederherstellbar sind.[1]

Im Rahmen des gesamten Eingabe-/Verarbeitungs-/Ausgabeprozesses auf Drucksystemen liegen personenbezogene Transaktionsdaten vor, zum Beispiel Klarname, Benutzername, Login-Daten, Protokolldaten, Personalnummer, IP-Adresse, MAC-Adresse etc.

Darüber hinaus können im Gesamtprozess weitere personenbezogene Daten erforderlich sein, die oftmals über den Verzeichnisdienst im Netzwerk bezogen werden – dies geht bis zu Login-Daten zur Anmeldung bei Drittdiensten (z.B. cloudbasierten Diensten).

Eine weitere, nicht unbedingt offensichtliche Datenquelle sind Adressbücher auf dem Drucksystem, in denen beispielsweise interne oder externe Rufnummern, persönliche Mailadressen etc. gespeichert sind.

Eine große Menge an personenbezogenen Daten kann sich auch in den Nutzdaten befinden. Beispiele sind Rechnungen, Personalunterlagen oder Gesundheitsdaten, aber auch Serienbriefe können DS-GVO-relevante Daten enthalten.

Neben der Möglichkeit, diese Dokumente auf den Systemen zu speichern, sind die Daten auch Bestandteil der Druck- oder Scandaten. Gerade ein Massen- oder Transaktionsdruck (z. B. Rechnungen, Mahnungen) wird oftmals im Rahmen einer Stapelverarbeitung gestartet und durchgeführt. Auch wenn die zu erstellenden Einzeldokumente einen hohen Schutzbedarf haben, hat der Anwender während des maschinellen Druck- und Versandprozesses (der Stapelverarbeitung) in der Regel keine direkten Eingriffsmöglichkeiten mehr. Dieser Umstand erfordert für den Gesamtprozess eine zuverlässige Qualitätskontrolle zur Erkennung von potentiellen Datenschutzverstößen.

1 Siehe zur Unterscheidung zwischen Pseudonymisierung und Anonymisierung ab Seite 31 hier: ↗**https://www.bitkom.org/Bitkom/Publikationen/Machine-Learning-und-die-Transparenzanforderungen-der-DS-GVO.html**

4.3 Die Funktionen im Detail

4.3.1 Funktion Druck

- Bei dieser Funktion muss zunächst ein Druckauftrag für das zu druckende Dokument generiert werden. Dieser kann durch einen Anwender an einem Endgerät (PC, Tablet etc.) ausgelöst werden.
- In der Verarbeitung wird dieser Auftrag anschließend in einen für den Drucker verständlichen Druckjob umgewandelt. Dieser wird im Anschluss für gewöhnlich an eine vorher definierte Drucker-Warteschlange weitergeleitet.
- Im Rahmen der Ausgabe kann eine Authentifizierung des Anwenders am Drucksystem erforderlich sein (z.B. mit seiner Zugangskarte). Daraufhin wird der ausgewählte Druckauftrag ausgelöst und der Ausdruck im Ausgabefach zur Entnahme durch den Benutzer ausgegeben.

	Eingabe	Verarbeitung	Ausgabe	
Druck	▪ Initiator, angemeldeter Benutzer ▪ Klarname ▪ E-Mail-Adresse ▪ Personalnummer **IT-Infrastruktur & Netzwerksicherheit:** ▪ Benutzerkennung, Nutzerkonto ▪ IP-Adresse, MAC-Adresse ▪ Subnetzmaske/Standorterfassung	▪ Datenbank (z.B. Serienbrief, kundenspezifische Nutzerdaten) ▪ Gerätespezifische Protokolldaten ▪ Druckdaten **IT-Infrastruktur & Netzwerksicherheit:** ▪ Verzeichnisdienst ▪ System-Protokolldaten	▪ Authentifizierungsdaten (PIN, Chipkarte, Fingerabdruck,...) ▪ Drucker-Kennung	**Dokumenteninhalt (Nutzdaten)**
	Dokumenteninhalt (Nutzdaten)			

Tabelle 1: DS-GVO-relevante Daten bei der Funktion Druck

Bei den folgenden Funktionen authentifiziert sich der Anwender am Drucksystem seiner Wahl bevor er eine Funktion starten kann; im Einzelnen sind dies:

4.3.2 Funktion Kopie

- Authentifizierung siehe oben
- Einlegen des Originals und Vornehmen der Kopiereinstellungen (Anzahl, Simplex/Duplex, ggf. Nachverarbeitung etc.)
- Verarbeitung des Kopierauftrags
- Ausgabe der Kopien

	Eingabe	Verarbeitung	Ausgabe	
Kopie	▪ Authentifizierungsdaten (PIN, Chipkarte, Fingerabdruck,...) ▪ Initiator, angemeldeter Benutzer ▪ Klarname ▪ E-Mail-Adresse ▪ Personalnummer **IT-Infrastruktur & Netzwerksicherheit:** ▪ Benutzerkennung, Nutzerkonto ▪ IP-Adresse, MAC-Adresse ▪ Subnetzmaske/Standorterfassung	▪ Datenbank (z.B. Serienbrief, kundenspezifische Nutzerdaten) ▪ Gerätespezifische Protokolldaten ▪ Druckdaten **IT-Infrastruktur & Netzwerksicherheit:** ▪ Verzeichnisdienst ▪ System-Protokolldaten	▪ Nicht zutreffend	**Dokumen-teninhalt (Nutzdaten)**
	Dokumenteninhalt (Nutzdaten)			

Tabelle 2: DS-GVO-relevante Daten bei der Funktion Kopie

4.3.3 Funktion Fax

- Authentifizierung siehe oben
- Einlegen des Originals und Eingabe des Faxziels
- Verarbeitung des Faxauftrags
- Eingang des Faxes am Ziel; i.d.R. mit direkter Möglichkeit der Ausgabe

	Eingabe	Verarbeitung	Ausgabe	
Fax	▪ Authentifizierungsdaten (PIN, Chipkarte, Fingerabdruck,...) ▪ Initiator, angemeldeter Benutzer ▪ Klarname ▪ E-Mail-Adresse ▪ Personalnummer **IT-Infrastruktur & Netzwerksicherheit:** ▪ Benutzerkennung, Nutzerkonto ▪ IP-Adresse, MAC-Adresse ▪ Subnetzmaske/Standorterfassung	▪ Empfänger-Nummer ▪ Sende-Nummer ▪ Datenbank (z.B. Serienbrief, kundenspezifische Nutzerdaten) ▪ Gerätespezifische Protokolldaten ▪ Druckdaten **IT-Infrastruktur & Netzwerksicherheit:** ▪ Verzeichnisdienst ▪ System-Protokolldaten	▪ Fax-Kennung	**Dokumen-teninhalt (Nutzdaten)**
	Dokumenteninhalt (Nutzdaten)			

Tabelle 3: DS-GVO-relevante Daten bei der Funktion Fax

4.3.4 Funktion Scan

- Authentifizierung siehe oben
- Einlegen des Originals und Eingabe des Scanziels (Hinweis: ggf. ist eine Sicherheitsüberprüfung des Scanziels hilfreich bzw. eine Einschränkung der anwählbaren Ziele sinnvoll
- Verarbeitung durch Übertragung des Scans und Übermittlung an das Ziel

	Eingabe	Verarbeitung	Ausgabe	
Scan	▪ Authentifizierungsdaten (PIN, Chipkarte, Fingerabdruck,...) ▪ Initiator, angemeldeter Benutzer ▪ Klarname ▪ E-Mail-Adresse ▪ Personalnummer **IT-Infrastruktur & Netzwerksicherheit:** ▪ Benutzerkennung, Nutzerkonto ▪ IP-Adresse, MAC-Adresse ▪ Subnetzmaske/Standorterfassung	▪ PDF-Eigenschaften ▪ Datei-Attribute, Metadaten ▪ Index-Datei ▪ Datenbank (z.B. Serienbrief, kundenspezifische Nutzerdaten) ▪ Gerätespezifische Protokolldaten ▪ Druckdaten **IT-Infrastruktur & Netzwerksicherheit:** ▪ Verzeichnisdienst ▪ System-Protokolldaten	▪ Ablageort Ziel ▪ Empfänger E-Mail	**Dokumenteninhalt (Nutzdaten)**
	Dokumenteninhalt (Nutzdaten)			

Tabelle 4: DS-GVO-relevante Daten bei der Funktion Scan

In folgender Grafik finden Sie alle oben genannten Bereiche und Daten noch einmal übersichtlich zusammengefasst wieder:

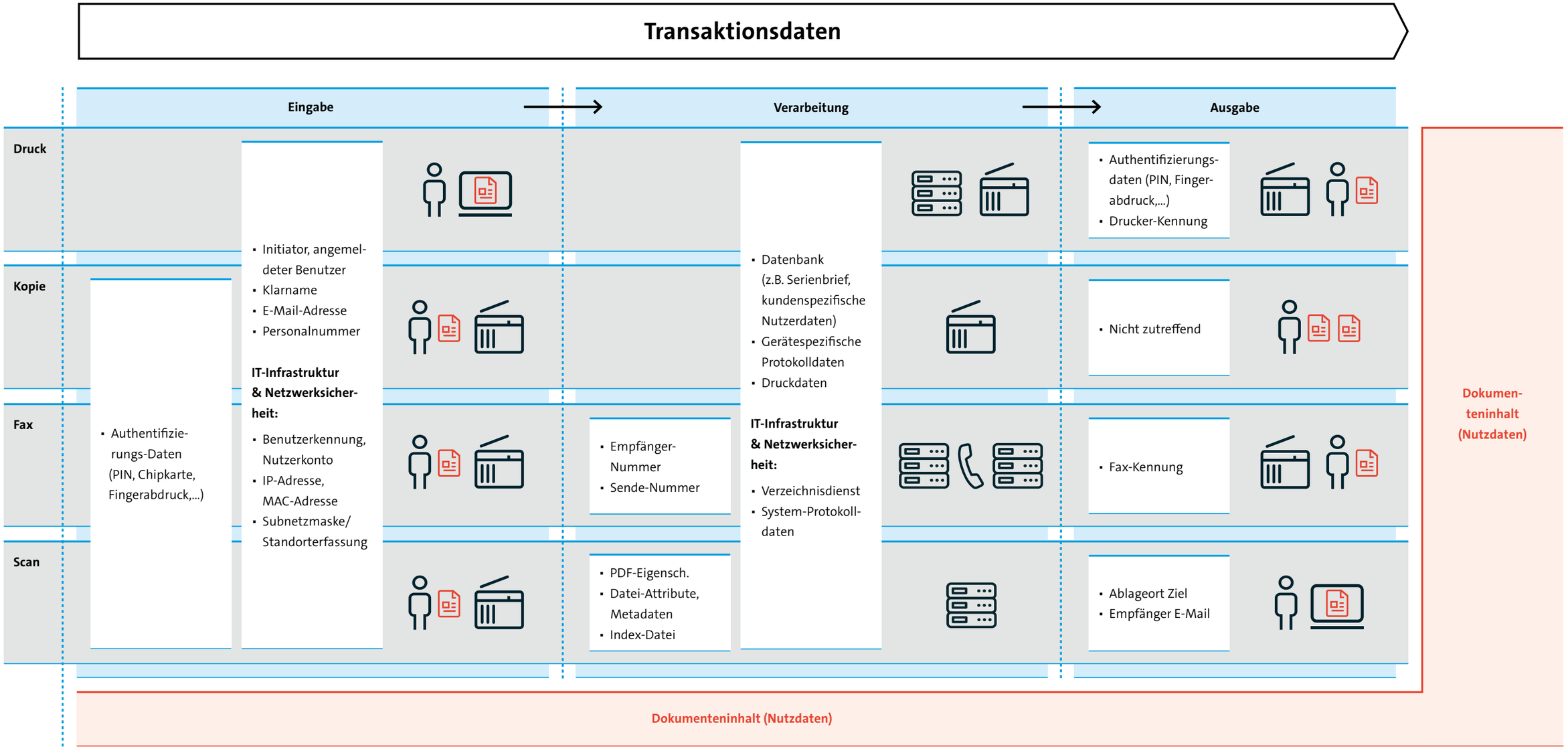

Tabelle 5: Funktionales Schaubild: Eingabe – Verarbeitung – Ausgabe

5 Wie erreicht man DS-GVO-Konformität?

5 Wie erreicht man DS-GVO-Konformität?

5.1 Individuelles Konzept

Weil es »DS-GVO-konformes Drucken« nicht von der Stange gibt, ist ein ganzheitliches und unternehmensindividuelles Konzept erforderlich, das auch die Vorortmaßnahmen einschließt (z.B. Zugangs- und Zugriffskontrollen auf Druckererzeugnisse). Die technischen und organisatorischen Maßnahmen müssen vor allem folgende Kriterien erfüllen:

- Die Lösung muss dem Stand der Technik entsprechen. Diese Anforderung ist kontextabhängig und von daher individuell zu beurteilen. Grundsätzlich ist ein praxiserprobter Stand gemeint, der über Rechtsvorschriften oder technische Normen hinausgehen kann.

- Die Verarbeitung von personenbezogenen Daten ist nur erlaubt, wenn ein entsprechender Erlaubnistatbestand aus der DS-GVO oder aus einem Spezialgesetz erfüllt ist. Jedes Unternehmen darf diejenigen personenbezogenen Daten verarbeiten, die zur Erfüllung seines Geschäftszwecks erforderlich sind. Unabdingbar sind dabei die genaue Prozessbeschreibung und die expliziten Maßnahmen gegen Datenmissbrauch jedweder Art. Dabei ist zu beachten, dass in Geschäftsprozessen u.U. personenbezogene Daten auch in Papierform anfallen bzw. entstehen können, die natürlich ebenfalls vollumfänglich geschützt werden müssen.

- Der Aufwand für die technisch-organisatorischen Maßnahmen muss in einem angemessenen Verhältnis zum erforderlichen Schutzniveau stehen (Grundsatz der Verhältnismäßigkeit).

- Ganz zentrale Punkte sind die vollständige Implementierung und kontinuierliche Überwachung des DS-GVO-Konzepts verbunden mit einer angemessenen Dokumentation. Zur nachhaltigen Umsetzung gehören beispielsweise auch regelmäßig zu wiederholende Mitarbeiterschulungen und eine für alle Mitarbeiter verpflichtende Richtlinie. Die Dokumentation ist aus zwei Gründen wichtig:

  1. Um identifizierte Datenschutzverstöße ad hoc protokollieren zu können, damit die gesetzlich vorgeschriebene Frist zur Meldung der Datenpanne von 72 Stunden auch eingehalten werden kann.[2]

  2. Um jederzeit bei spontanen Kontrollen aussage- und beweisfähig zu sein. Bei DS-GVO-Verstößen steht erfahrungsgemäß eine Frage im Mittelpunkt der rechtlichen Beurteilung: »Wie intensiv bemüht sich das Unternehmen, personenbezogene Daten effektiv vor Missbrauch zu schützen?«

2 Ob die Datenpanne verpflichtend bei der Aufsichtsbehörde zu melden ist ergibt sich im Detail aus Art. 33 DS-GVO

5.2 Beispielhaft folgen einige Anregungen, wie Sie Daten schützen können

5.2.1 Authentifizierung – zum Schutz vor unbefugtem Zugriff auf personenbezogene Daten

Schützen Sie Ihr System durch eine Authentifizierung vor unbefugtem Zugriff. DS-GVO-relevante Daten lassen sich schützen, indem ein Dokument erst dann gedruckt wird, nachdem ein berechtigter Nutzer sich z.B. per ID-Karte oder PIN-Code am Gerät angemeldet hat (»Vertraulicher Druck«).

Eine Authentifizierung durch Biometriedaten ist prinzipiell ebenfalls möglich. Allerdings müssen dazu Biometriedaten der Nutzer dauerhaft gespeichert werden. Bitte beachten Sie, dass dies laut DS-GVO besonders schützenswerte Daten sind. Ob die Authentifizierung mittels Biometriedaten erfolgen kann, ist im Einzelfall angesichts der Zwecke, der spezifischen Geschäftsprozesse und der zu implementierenden Schutzmaßnahmen zu prüfen.

Unter Umständen kann auch die Einrichtung einer Nutzerzugangskontrolle sinnvoll sein.

5.2.2 Systemverwaltung – zum Schutz vor nicht autorisierten Nutzern

Beschränken Sie die Administratorenrechte für alle am Druck beteiligten Systeme auf möglichst wenige Nutzer. Alternativ können Sie spezifische Administratorenrechte auf verschiedene Rollen verteilen. Auch Funktionen sollten nur jenen Benutzern zugänglich sein, die sie für ihre Arbeit brauchen.

Darüber hinaus sollten Sie regelmäßig Software- und Firmware-Updates durchführen, um eventuelle Sicherheitslücken zu schließen. Ist eine größere/dezentrale Druckerflotte im Einsatz, können Sie auf Hilfsmittel wie Remote-Services oder Druckflottenmanagementsysteme zurückgreifen.

5.2.3 Einschränkung der Sendefunktion – zum Schutz vor unkontrolliertem Versand an Empfangsadressen außerhalb der Organisation

Vor allem die Sendefunktion sollte grundsätzlich nur solchen Nutzern zugänglich gemacht werden, die diese auch tatsächlich benötigen. Dabei ist es ratsam, den Versand von Dokumenten auf jene Empfänger zu beschränken, die im Adressbuch oder LDAP-Server verzeichnet sind. Alternativ können Sendeziele auch auf die angemeldete Nutzeradresse oder auf bestimmte Domänen beschränkt werden. So kann z.B. das Missbrauchspotenzial der Sendefunktionen (Scan to Mail, Scan to Fax) auf ein Minimum reduziert werden.

5.2.4 Verschlüsselung von Druckdaten, Dokumenten und Transportwegen – zum Schutz vor Zugriff von unautorisierten Personen

Generell sollte beim Drucken, Scannen oder Faxen von personenbezogenen Daten das Dokument selbst verschlüsselt werden. Darüber hinaus sollte auch der Transport der Daten verschlüsselt erfolgen.

Unabhängig davon muss sichergestellt werden, dass die Übertragungswege vor Zugriff geschützt sind. Detaillierte Informationen dazu finden technisch versierte Anwender im IT-Grundschutz-Kompendium des BSI.[3]

5.2.5 Minimierung der Menge und Dauer (zwischen)gespeicherter Daten – zum Schutz vor unautorisiertem Zugriff

Vor allem personenbezogene Daten sollten unmittelbar nach der Verarbeitung vom System – sowohl dem Drucksystem als auch ggf. dem verarbeitenden Gesamtsystem – gelöscht werden. Dazu empfiehlt sich das regelbasierte Löschen der Speichermedien nach internationalen Standards (z.B. vom BSI). Neben der regelbasierten Datenlöschung temporärer Dateien im laufenden Betrieb lässt sich das Speichermedium am Ende der Nutzungsdauer (herstellerspezifisch) auf verschiedene Arten sicher löschen – im Zweifelsfall durch Zerstörung.

5.3 Zusätzlich sind folgende Punkte zu berücksichtigen bzw. deren Relevanz zu prüfen

5.3.1 Aufklärung

Stellen Sie sicher, dass alle mit personenbezogenen Daten befassten Personen die Anforderungen der DS-GVO in ihrer täglichen Arbeit berücksichtigen.

5.3.2 Datensätze

Um für ein mögliches Auskunftsersuchen der Datenschutzbehörde gewappnet zu sein, dokumentieren Sie Herkunft, Zweck und Dauer der Speicherung von personenbezogenen Daten. Das Verarbeitungsverzeichnis ist ein wichtiger Baustein für die Nachvollziehbarkeit der Datenverarbeitungen.[4]

3 ↗https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html

4 Detaillierte Hinweise zum Verzeichnis finden sich im folgenden Bitkom-Leitfaden:
↗https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html

5.3.3 Datenschutzerklärung

Halten Sie Ihre Datenschutzerklärung stets aktuell, indem Sie diese regelmäßig mit den jeweils aktuellen Verarbeitungsaktivitäten abgleichen und deren Rechtsgrundlage berücksichtigen.[5]

5.3.4 Persönlichkeitsrechte

Prüfen Sie Ihre Geschäftsprozesse periodisch, um sicherzustellen, dass alle individuellen Rechte in Bezug auf Datenschutz gewahrt werden. Wenn die Verarbeitung durch externe Dienstleister erfolgt, muss die Wahrung dieser Rechte ggf. im Rahmen eines Auftragsverarbeitungsvertrags geregelt werden. Außerdem ist darauf zu achten, dass das betroffene Individuum über eine solche Auslagerung von Dienstleistungen zu informieren ist.

5.3.5 Auskunftsersuchen

Jede natürliche Person hat ein Auskunftsrecht. Bringen Sie Ihre Prozesse auf den (ver)ordnungsgemäßen Stand und stellen Sie die Beantwortung von Anfragen zu den erhobenen Daten und deren Verwendungszweck innerhalb der gesetzlichen Fristen sicher.

5.3.6 Zustimmung

Prüfen Sie Ihre Vorgehensweise zur Erlangung, Verwaltung und Handhabung von personenbezogenen Daten. Erneuern Sie bestehende Zustimmungen, die nicht mehr konform sind.

5.3.7 Datenschutzverletzungen

Stellen Sie sicher, dass Sie Ihre Geschäftsprozesse überwachen, um mögliche Datenschutzverletzungen frühzeitig aufdecken zu können und ggf. an die Aufsichtsbehörde melden zu können. Der Meldepflicht muss unverzüglich und möglichst innerhalb von 72 Stunden, nachdem die Verletzung bekannt wurde, nachgekommen werden.

5.3.8 Datenschutzbeauftragte

Prüfen Sie, ob Ihr Unternehmen zur Bestellung eines Datenschutzbeauftragten rechtlich verpflichtet ist. Ermöglichen Sie ihm die ordnungsgemäße Durchführung seiner Aufgaben. Auch die Beauftragung eines externen Datenschutzbeauftragten ist möglich.

5 Anleitungen zur Erstellung der Datenschutzerklärung finden sich im Bitkom-Leitfaden zu den Informationspflichten: ↗**https://www.bitkom.org/Bitkom/Publikationen/Informationspflichten-nach-der-DS-GVO**

6 Schlusswort

6 Schlusswort

Die Etablierung von DS-GVO-konformem Drucken ist ein unternehmensindividueller Prozess und kann nicht »von der Stange« erworben werden.

Von herausragender Bedeutung ist die fachliche Analyse des Geschäftszwecks. Hieraus bemisst sich, welche personenbezogenen Nutzdaten überhaupt verarbeitet werden dürfen. Zu berücksichtigen sind ebenso die bei den technischen Prozessen anfallenden Transaktionsdaten. Daraus kann dann ein Konzept mit angemessenen IT-technischen und organisatorischen Maßnahmen entwickelt werden, das sicherstellt, dass die Daten technologisch DS-GVO konform verarbeitet werden.

An dieser Stelle konnten nur einige Anregungen für die dafür sinnvolle IT-Technik gegeben werden. Wer sich darüber hinaus über den sicheren Betrieb von Drucksystemen informieren möchte, dem sei der ↗Bitkom-Leitfaden »Sicherheit von Drucksystemen«[6] empfohlen.

Wichtig ist aber auch, dass dem umfangreichen Konstrukt DS-GVO das Prinzip der Verhältnismäßigkeit zugrunde liegt. Es ist also keinesfalls gefordert, mit »Kanonen auf Spatzen« zu schießen. Ganz grundsätzlich ist zu beachten, dass DS-GVO-Konformität ein dynamischer Prozess ist, der sich im Zeitverlauf immer wieder ändern kann, beispielsweise bei der Erschließung neuer Geschäftsfelder.

6 ↗https://www.bitkom.org/Bitkom/Publikationen/Sicherheit-von-Drucksystemen

7 Anhang – Zugrunde liegende Begriffsklärungen

7 Anhang – Zugrunde liegende Begriffsklärungen

7.1 Personenbezogene Daten – sind was genau?

Gemäß DS-GVO Artikel 4, Absatz 1 sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Verschiedene Teilinformationen, die gemeinsam zur Identifizierung einer bestimmten Person führen können, stellen ebenfalls personenbezogene Daten dar. Personenbezogene Daten, die verschlüsselt oder pseudonymisiert wurden, aber zur erneuten Identifizierung einer Person genutzt werden können, bleiben personenbezogene Daten und fallen in den Anwendungsbereich der EU-DS-GVO. Personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, gelten nicht mehr als personenbezogene Daten. Damit die Daten wirklich anonymisiert sind, muss die Anonymisierung unumkehrbar sein.

Die Datenschutz-Grundverordnung schützt personenbezogene Daten unabhängig von der zur Datenverarbeitung verwendeten Technik – sie ist technologieneutral und gilt für die automatisierte wie die manuelle Verarbeitung, sofern die Daten nach vorherbestimmten Kriterien (z.B. alphabetische Reihenfolge) geordnet sind. Es ist ebenfalls nicht entscheidend, wie die Daten gespeichert werden – in einem IT-System, mittels Videoüberwachung oder auf Papier. In all diesen Fällen fallen die personenbezogenen Daten unter die in der Datenschutz-Grundverordnung dargelegten Datenschutzklauseln.

Beispiele für personenbezogene Daten:

- Name und Vorname
- eine Privatanschrift
- eine E-Mail-Adresse wie vorname.nachname@unternehmen.com
- eine Ausweisnummer
- Standortdaten (z.B. die Standortfunktion bei Mobiltelefonen)
- eine IP-Adresse
- eine Cookie-Kennung
- pseudonymisierte Daten (Personenbezug rekonstruierbar)

Beispiele für nicht personenbezogene Daten:

- Handelsregisternummer
- eine E-Mail-Adresse wie info@unternehmen.com
- anonymisierte Daten (Personenbezug nicht rekonstruierbar)

Beispiele für besonders schützenswerte personenbezogene Daten:

- Biometrische Daten
- Politische Überzeugungen
- Sexuelle Orientierung
- Religionszugehörigkeit
- Gesundheitsdaten

7.2 Verarbeitung von Daten – Was genau heißt denn das?

Gemäß DS-GVO Artikel 4, Absatz 2 schließt die »Verarbeitung« eine Vielzahl unterschiedlicher mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgänge im Zusammenhang mit personenbezogenen Daten ein. Sie umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org