

BRANDI

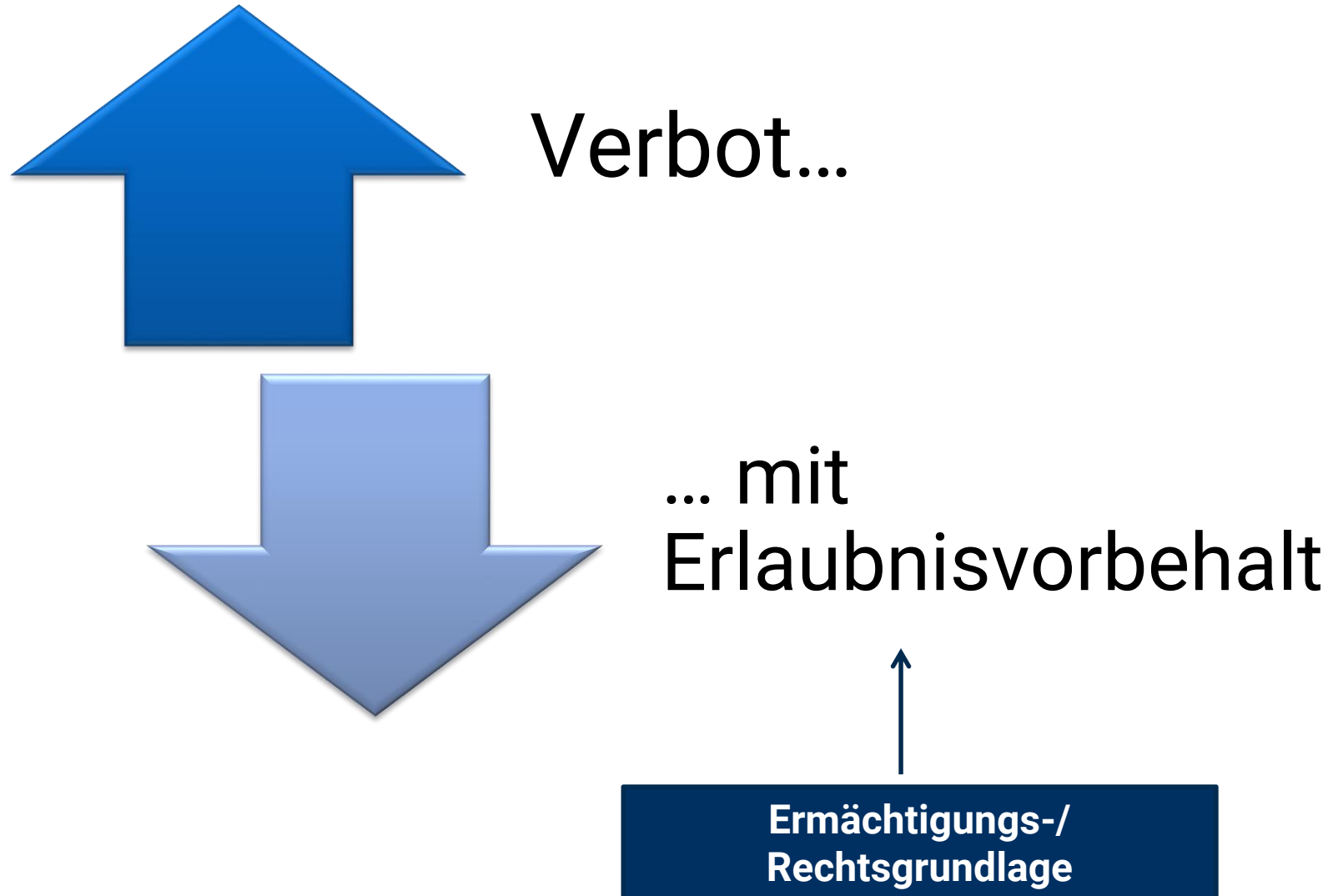
RECHTSANWÄLTE

HERZLICH WILLKOMMEN ZUM

5. BRANDI Datenschutzrechtstag

ZUGRIFF DES ARBEITGEBERS AUF E-MAIL-ACCOUNTS VON ARBEITNEHMERN

Datenschutzrechtliche Anforderungen





§ 26 Abs. 1 S. 1 BDSG

*(1) Personenbezogene Daten von Beschäftigten dürfen für **Zwecke des Beschäftigungsverhältnisses** verarbeitet werden, wenn dies für die **Entscheidung über die Begründung** eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen **Durchführung oder Beendigung** oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden **Rechte und Pflichten der Interessenvertretung der Beschäftigten** erforderlich ist.*

Art. 6 Abs. 1 S. 1 lit. b) DSGVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

*b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur **Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen;*

Art. 6 Abs. 1 S. 1 lit. f) DSGVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist

*f) die Verarbeitung ist zur Wahrung **der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern **nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*

§ 26 Abs. 1 S. 2 BDSG

(1) [...] Zur **Aufdeckung von Straftaten** dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn **zu dokumentierende tatsächliche Anhaltspunkte** den Verdacht begründen, dass die betroffene **Person im Beschäftigungsverhältnis eine Straftat begangen hat**, die Verarbeitung zur Aufdeckung **erforderlich** ist und das **schutzwürdige Interesse** der oder des Beschäftigten an dem Ausschluss der Verarbeitung **nicht überwiegt**, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig ist.

Art. 6 Abs. 1 S. 1 lit. a) DSGVO i.V.m. § 26 Abs. 2 BDSG

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist

*a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zweck gegeben;*

*(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die **im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person** sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung hat **schriftlich oder elektronisch** zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht [...] in Textform aufzuklären.*

§ 26 Abs. 4 BDSG

*(4) Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von **Kollektivvereinbarungen** zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.*

Verhältnismäßigkeitsgrundsatz

- Abwägung zwischen Interessen von Arbeitgeber und Arbeitnehmer
- Informationspflichten
- Ergreifen von Maßnahmen zur Absicherung

Grundsatz der Datenminimierung

- Begrenzung des Zugriffs auf das erforderliche Maß
 - inhaltlich
 - zeitlich

(Erlaubte) Privatnutzung des E-Mail-Accounts

ERLAUBTE PRIVATNUTZUNG

- Betriebsmittel
- Grundsatz: ausschließlich dienstliche Nutzung
- Privatnutzung, wenn
 - ausdrückliche Erlaubnis
 - Duldung



Datenschutzaufsichtsbehörden:

- Anwendung im Arbeitsverhältnis, wenn Privatnutzung erlaubt
- Arbeitgeber als Anbieter von Telekommunikationsdiensten
- Zugriff grundsätzlich unzulässig, da Verstoß gegen das Fernmeldegeheimnis

Rechtsprechung:

- keine Anwendbarkeit bei erlaubter Privatnutzung
- Zugriff unter bestimmten Voraussetzungen zulässig
- Zulässigkeit richtet sich nach datenschutzrechtlichen Regelungen
- verschärfte Verhältnismäßigkeitskontrolle



- Gesetzeshistorie
- AN und AG stehen sich als eigenständige Rechtssubjekte gegenüber
- dauerhafte Bereitstellung ist „geschäftsmäßig“
- AG trägt durch „Weitervermittlung“ der Dienste wesentlich zur Kommunikation bei
- Sinn und Zweck: keine Regelung unternehmensinterner Rechtsbeziehungen
- Nutzung unternehmenseigener Kommunikationsnetzwerke ist nicht öffentlich iSd TKG
- AN in der Sphäre des AG
- kein Marktbezug, nicht „geschäftsmäßig“
- AN geht nicht von „Unantastbarkeit“ aus



keine höchstrichterliche Klärung der Thematik

ANWENDBARKEIT DES FERNMELDEGEHEIMNISSES, § 3 TTDSG

- Pro
 - Gesetzeshistorie
 - privater Kommunikation kommt Marktwert zu
- Contra
 - keine Entgeltlichkeit
 - keine Drittgerichtetheit der Dienstleistung
- Zuständigkeit des BfDI
- TTDSG erfasst auch interpersonelle Telekommunikationsdienste

ERLAUBTE PRIVATNUTZUNG

- Verbot der Privatnutzung
- Befreiung von den Beschränkungen des Fernmeldegeheimnisses durch Einwilligung
- Abwägung mit Restrisiko

Zugriff

Vorübergehende Abwesenheit

- bei planbaren Abwesenheiten: vorab allgemeine Regeln festlegen
 - vorherige automatische Abwesenheitsnotiz
 - vorherige Einrichtung einer Weiterleitung
- nicht planbare Abwesenheiten: Zugriff nach Erforderlichkeit
- Weiterbearbeitung offener Aufgaben ausschließlich über eigenes Postfach

Ausscheiden des Mitarbeiters

- Vereinbarung im Vorfeld
 - Zugriff oder Weiterleitung durch Arbeitgeber nach Ausscheiden
 - Verpflichtung zur Übergabe offener Aufgaben oder Hinterlegung von geschäftlichen Dokumenten und Korrespondenz an bestimmten Speicherort
- Information externer Kommunikationspartner, um das Erfordernis des Zugriffs zu minimieren

ZUGRIFF BEI MISSBRÄUCLICHEM VERHALTEN

- Bei Verdacht der Begehung einer Straftat: § 26 Abs. 1 S. 2 BDSG
 - Verdacht in Bezug auf eine Straftat im Beschäftigungsverhältnis
 - tatsächliche Anhaltspunkte
 - Erforderlichkeit des Zugriffs zur Aufdeckung
 - Bei Verletzung arbeitsvertraglicher Pflichten: § 26 Abs. 1 S. 1 BDSG
 - zum Zwecke des Beschäftigungsverhältnisses
 - problematisch: Arbeitgeber geht bereits von Verletzung aus, mögliche Beeinflussung der Interessenabwägung
- ➔ Prüfung durch Datenschutzbeauftragten empfehlenswert

VORGEHEN

- maßgeblich: einschlägige Rechtsgrundlage und Umstände des Einzelfalls
- Grundsätzlich:
 - Bewertung durch Datenschutzbeauftragten
 - „Mehr-Augen-Prinzip“
 - Auswahl sensibilisierter Mitarbeiter
 - Beteiligung des Betriebsrats (falls vorhanden)
 - Zugriff selektiv und zeitlich eingegrenzt
 - Protokollierung des Zugriffs inkl. Dokumentierung der Interessenabwägung
- kein Zugriff auf private Kommunikation (ggf. Abbruch des Zugriffs)
- EGMR: Anlass und Ausmaß der Überwachung des elektronischen Schriftverkehrs am Arbeitsplatz müssen durch Arbeitgeber transparent gemacht werden



Christina Prowald
Wissenschaftliche Mitarbeiterin
T +49 521 96535 - 980
F +49 521 96535 - 113
E christina.prowald@brandi.net

Gesche Kracht
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 984
F +49 521 96535 - 113
E gesche.kracht@brandi.net



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

**BGH ZUM RECHT AUF EINE DATENKOPIE
NACH ART. 15 III DSGVO**

DIE THEMEN DIESES VORTRAGS

1 SACHVERHALT

2 VERFAHRENSGANG

3 ENTSCHEIDUNG DES BGH

4 BEDEUTUNG

1. VERFAHRENSGANG

- Die Klägerin erweiterte ihre bereits anhängige Klage um den Antrag:
 - „Die Beklagten zu verurteilen, **Kopien aller personenbezogenen Daten [...] auszuhändigen**, die sich in ihrem Besitz befinden“.
- Das Landgericht verurteile die Beklagten zur Aushändigung der Kopien.
- Inhalt und Reichweite des Auskunftsanspruchs sind nach Auffassung des Gerichts weit auszulegen:
 - d.h. von den Beklagten könne nicht nur verlangt werden, einzelne Stammdaten, sondern **generell die relevante Kommunikation** mit der Klägerin **vorzulegen**.

1. VERFAHRENSGANG

- Im Ergebnis schloss sich das Berufungsgericht der Auffassung des erstinstanzlichen Gerichts an.
- OLG führte aus:
 - Berechtigte aus Art. 15 III DSGVO habe einen eigenständigen **Anspruch auf Überlassung der Informationen in der Form, wie sie dem Verpflichteten vorliegen.**
 - Es reiche also gerade keine Auskunftserteilung hinsichtlich der vorhandenen Daten, sondern es sei eine **Reproduktion** der entsprechenden Unterlagen **erforderlich.**

1. ENTSCHEIDUNG DES BGH

- prozessuale Frage: entsprechen die Anträge der Klägerin den Bestimmtheitsanforderungen des § 253 II Nr. 2 ZPO
 - „Die Beklagten zu verurteilen, **Kopien aller personenbezogenen Daten** - insbesondere in Form von Telefonnotizen, Aktenvermerken, Protokollen, E-Mails, Briefen und Zeichnungsunterlagen für Kapitalanlagen - **auszuhändigen, die sich in ihrem Besitz befinden**“
 - „Die Beklagten zu verurteilen, der Klägerin **Kopien der** von den Beklagten verarbeiteten **personenbezogenen Daten der Klägerin betreffend die Datenkategorien** Telefonnotizen, Aktenvermerke, Gesprächsprotokolle, E-Mails, Briefe und Zeichnungsunterlagen für Kapitalanlagen im Zeitraum vom 1. Januar 1997 bis 31. März 2018 zu überlassen“

1. ENTSCHEIDUNG DES BGH

- BGH bestätigte Ergebnis und Begründung des Berufungsgerichts diesbezüglich und führte aus:
 - Für Anspruchsteller **bei Geltendmachung des Anspruchs nicht ersichtlich, welche Unterlagen sich bei dem Auskunftspflichteten befinden**
 - Berechtigter will mit Antrag in der Regel gerade **erst in Erfahrung bringen, in welchen, bei dem Verpflichteten vorhandenen Dokumenten, welche Daten** enthalten sind.
 - **Weitere Konkretisierung** für den Berechtigten daher **nicht möglich**.

1. ENTSCHEIDUNG DES BGH

- Hinsichtlich der Reichweite des Anspruchs aus Art. 15 III DSGVO führt der BGH sein eigene Rechtsprechung fort und entspricht damit auch der des EuGH:
 - **EuGH:** *Betroffene haben einen Anspruch auf eine originalgetreue und verständliche Reproduktion, soweit dies zur wirksamen Ausübung der Betroffenenrechte erforderlich ist (EuGH 4.5.2023, C-487/21, EuZW 2023, 575)*
 - **BGH:** *Vollständige Vorlage von Unterlagen kann nur dann verlangt werden, wenn alleine auf diese Weise eine Bewertung durch den Betroffenen möglich ist (BGH 6.2.2024, VI ZR 15/23).*

1. ENTSCHEIDUNG DES BGH

- BGH stellt noch einmal klar:
 - Schreiben der berechtigten Person an den Verantwortlichen sind ihrem gesamten Inhalt nach als personenbezogene Daten einzustufen.
 - Es besteht daher ein Anspruch auf Überlassung einer **Kopie des gesamten Dokuments**.
 - Hinsichtlich Unterlagen, die nicht von der berechtigten Person selbst stammen, sind nur die darin wirklich enthaltenen personenbezogenen Daten vom Auskunftsrecht des Art. 15 III DSGVO umfasst.
 - Es besteht grds. nur Anspruch auf Überlassung einer **Kopie der enthaltenen Daten**.

1. ENTSCHEIDUNG DES BGH

■ **Urteil:**

Der Klägerin steht der vom Berufungsgericht zuerkannte Anspruch auf Überlassung von Kopien von Unterlagen nur insoweit zu, als es sich um von der Klägerin verfasste Briefe und E-Mails, die den Beklagten aus dem beantragten Zeitraum vorliegen, handelt.

- In Revisionsverhandlung gestellte Hilfsantrag wird als unzulässige Klageänderung in der Revisionsinstanz zurückgewiesen
- In dem Antrag der Klägerin, auf Überlassung der Kopien der Dokumente, ist nicht als Minus ein Antrag auf Überlassung der Kopien personenbezogenen Daten enthalten.

1. BEDEUTUNG

- Trotz vorangehender Klarstellung des EuGH immer noch erhebliche Unsicherheiten, unter welchen Voraussetzungen ein Datenauszug genügt und wann ganze Unterlagen vorzulegen sind.
- Konkretisierung des BGH dahingehend:
 - Das Recht auf eine Datenkopie nach Art. 15 III DSGVO **bezieht sich auf eine Kopie der personenbezogenen Daten** und nicht grds. auf eine Kopie des Dokuments, das diese Daten enthält.
 - Eine Kopie des vollständigen Dokuments kann notwendig sein, wenn
 - eine **Kontextualisierung** der Daten erforderlich ist.
 - das Dokument **an sich einen Personenbezug** aufweist.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

DIE NUTZUNG VON MICROSOFT 365 IM UNTERNEHMEN

- Vielzahl von Office- und Kollaborationsanwendungen (Word, Excel, Teams, SharePoint etc.)
- Beherrschender Marktanteil v. 85%
- In der Regel cloudbasiert, aber auch Nutzung „on premise“ möglich

VERTRAGLICHE SITUATION

- Nutzungsumfang von Microsoft 365 hängt vom Umfang der Lizenzvereinbarung ab
- Zusätzlich zur Lizenzvereinbarung ist jedenfalls eine Vereinbarung zur Auftragsverarbeitung (bei Microsoft: „DPA“) abzuschließen
- Aufgrund der Marktmacht des Anbieters lediglich Standardverträge
- Für besonders sensible Informationen können uU auch gesonderte Vereinbarungen abgeschlossen werden (bspw. Berufsgeheimnisträger)

- Teilweise starke Kritik an der Nutzung seitens von Aufsichtsbehörden
- Häufige Kritikpunkte
 - Intransparente Datenverarbeitungen
 - Abhängigkeit der Kunden aufgrund des Abo-Modells
 - Datenübermittlungen in die USA
- Exemplarisch: Festlegung der Datenschutzkonferenz v. November 2022
 - Der Nachweis von Verantwortlichen, Microsoft 365 datenschutzkonform zu betreiben, kann auf Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden.

- Erfüllung der Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO
 - Unternehmen müssen Einhaltung des Datenschutzes nachweisen können
 - Hier werden gerade die intransparenten Informationen von Microsoft bemängelt

ABER

- Interpretationsspielraum dahingehend, wie umfassend der Nachweis tatsächlich erbracht werden muss
- Modell der Auftragsverarbeitung: Auftraggeber muss eben nicht vollständige Kontrolle haben
- MS argumentiert mit Schutz von Geschäftsgeheimnissen und der Sicherheit der technischen Systeme

- Nutzung der Daten durch Microsoft & unzureichende Abgrenzung der Verantwortlichkeiten
 - Microsoft verarbeitet einige Daten zu eigenen Zwecken (etwa Diagnose- oder Telemetriedaten)
 - Kritisch, wenn in der Praxis sicherlich auch häufig vorkommend, insbesondere bei großen Anbietern
 - Es gibt technische Möglichkeiten, den Abfluss der Diagnose- und Telemetriedaten zu unterbinden bzw. zu minimieren
 - Nutzer sollten jedenfalls über die Verwendung der Daten durch MS transparent informiert werden

- Unzureichende Ausgestaltung des DPA
 - Unspezifische Informationen hinsichtlich der verarbeiteten Datenarten und der Kategorien betroffener Personen
 - Welche Daten anfallen, hängt von Nutzung des Unternehmens ab
 - Fehlende Weisungs- und Kontrollmöglichkeiten
 - Leider üblich bei großen Anbietern
 - Trotz Einschränkungen bleibt Unternehmen Herr der Daten

- Drittstaatenübermittlung in die USA

Übermittlung v. Daten in die USA und damit verbundenen Zugriffsmöglichkeit v. Behörden

- Microsoft: Data Boundary

- Angemessenheitsbeschluss „EU-US Data Privacy Framework“

- Entwicklungen jedoch weiter beobachten

- Aktuelle Version des DPA
 - DPA wird ständig modifiziert
- Technische Konfigurationsmöglichkeiten datenschutzfreundlich nutzen
 - Den Datenabfluss an Microsoft bestmöglich einschränken
- Organisatorische Maßnahmen
 - Vorgaben zur Nutzung der IT-Systeme, Mobile Device Management etc.
- Datenschutz-Folgenabschätzung/Dokumentation
 - DSFA abhängig davon, welche Risiken bei der Nutzung tatsächlich anfallen. Jedenfalls aber eine umfassende Dokumentation.
- Einsatz von Verschlüsselungstechnologien
 - Idealerweise Hold-Your-Own-Key-Methode
- Incident-Response-Management
 - Auf Änderungen der Rechtslage oder der Praktiken Microsofts schnell reagieren können

1 0 1 0 1 1 0



Hendrik Verst
Wissenschaftlicher Mitarbeiter

T +49 521 96535 - 891
F +49 521 96535 - 113
E hendrik.verst@brandi.net

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT