nbs partners audit
GmbH Wirtschaftsprüfungsgesellschaft
Hamburg

B E R I C H T

Direkte Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)

PlusServer GmbH, Hohenzollernring 72, 50672 Köln

Inhaltsverzeichnis

Anlagenverzeichnis

1. Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG
2. Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungs-gesellschaften vom 1. Januar 2017

Abkürzungsverzeichnis

Abs.	Abschnitt
AV	Auftragsverarbeiter
AVV	Auftragsverarbeitungsvertrag
BDSG	Bundesdatenschutzgesetz
BS WP/vBP	Berufssatzung für Wirtschaftsprüfer/vereidigte Buchprüfer
Buchst.	Buchstabe
bzw.	beziehungsweise
DS-Ziel	Datenschutz Kontrollziel
DS-KONTROLLE	Datenschutz-Kontrolle
DS	Datenschutz
DSB	Datenschutzbeauftragte/r
DSFA	Datenschutzfolgeabschätzung
DSMS	Datenschutzmanagementsystem
DSK	Datenschutzkoordinator/in
DS-GVO	EU-Datenschutz-Grundverordnung
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V., Düsseldorf
i. V.	in Verbindung
o. g.	oben genannten
PH	Prüfungshinweis des IDW
PS	Prüfungsstandard des IDW
QS	Qualitätssicherung
sog.	so genannt
TOM	Technisch und organisatorische Maßnahmen
u. a.	unter anderem
VVT	Verzeichnis von Verarbeitungstätigkeiten
VZ	Verarbeitungsverzeichnis
WPO	Wirtschaftsprüferordnung
z. B.	zum Beispiel

1. Prüfungsauftrag

An die Geschäftsführung der

PlusServer GmbH

Köln

- im Folgenden auch kurz "Gesellschaft" genannt -

Wir haben eine Prüfung der Angemessenheit und der Wirksamkeit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG der Gesellschaft für den Zeitraum vom 1. April 2021 bis 31. März 2022 durchgeführt. Zur Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verweisen wir auf nachstehende Anlage 1.

2. Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der Gesellschaft sind für die Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Dokumentation der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG verantwortlich, die in allen wesentlichen Belangen die untengenannten Kriterien zur Angemessenheit und Wirksamkeit erfüllen. Aufgrund bestehender inhärenter Grenzen von Systemen können die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG diese Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen umfassen die im IDW Prüfungshinweis *„Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)“* konkretisierten Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen.

3. Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit über die Angemessenheit und Wirksamkeit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG abzugeben.

Wir haben unsere Prüfung unter Beachtung des IDW Prüfungsstandards „*IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* und des *IDW Prüfungshinweises*: *Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1)“* durchgeführt.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des IDW Qualitätssicherungsstandards *„Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1“)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit die Kriterien zu erfüllen und ob die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen während des Zeitraums vom 1. April 2021 bis 31. März 2022 mit hinreichender Sicherheit implementiert waren und die Kriterien wirksam erfüllt haben.

Eine Prüfung gemäß *IDW PS 860* und *IDW PH 9.860.1* umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Für die Beurteilung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Grundsätze, Verfahren und Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Die Prüfung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbau- und einer Funktionsprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können. Dies schließt die Beurteilung der Risiken des Vorhandenseins von wesentlichen Mängeln ein.

4. Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u. a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt.

Unsere Prüfungshandlungen basieren auf den Auskünften der uns von der Gesellschaft benannten Mitarbeiter (aus Gründen der Lesbarkeit wird das traditionelle generische Maskulinum, z. B. „der Mitarbeiter“, verwendet. Es sind immer alle Geschlechter im Sinne der Gleichbehandlung gemeint), der Einsichtnahme in die zur Verfügung gestellte Dokumentation und dem Einblick in Systemeinstellungen. Wir haben unsere Untersuchung dem Prüfungsrisiko entsprechend auch in Stichproben durchgeführt.

Es wurden die Verarbeitungen und Prozesse mit personenbezogenen Daten bei nachfolgenden Produkten der PlusServer GmbH geprüft:

- Pluscloud open /SCS
- Pluscloud V
- SAP on PlusCloud
- pluscloud open/SCS
- Managed AWS
- Managed Google Cloud
- Managed Azure
- Dedicated Server
- Dedicated Storage
- Application Management Datenbanken
- Shared Firewalling
- Shared Loadbalancing
- Content Delivery Network – CDN
- DDoS Protection
- Schwachstellenscanner
- Veeam Backup
- ESET Antivirus
- Datenvernichtung
- Rechenzentrumsbetrieb

Eine zusammenfassende Beschreibung der durchgeführten Prüfungshandlungen zur Risikobeurteilung, der Aufbau- und Funktionsprüfungen und der weiteren Prüfungshandlungen sowie Prüfungsfeststellungen, Empfehlungen und weitere Erläuterungen sind in der Anlage 1 im Detail beschrieben. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

5. Prüfungsurteil

Nach unserer Beurteilung

- sind die verwendeten Kriterien für den vorgesehenen Anwendungszweck geeignet,
- waren die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG in allen wesentlichen Belangen mit hinreichender Sicherheit
  - geeignet, die o. g. Kriterien zu erfüllen,
  - im geprüften Zeitraum implementiert und
  - im geprüften Zeitraum wirksam.

6. Inhärente Grenzen des geprüften Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt werden.

Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG erstrecken sich auf den Zeitraum vom 1. April 2021 bis 31. März 2022. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

7. Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt Verantwortung der gesetzlichen Vertreter beschriebenen Kriterien, welche für Zwecke der kundenbezogenen Geschäfts- und Verarbeitungsvorgänge konzipiert wurden. Die Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG wurden durch die Gesellschaft abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, welcher aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte. Folglich ist die beigefügte Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG möglicherweise für einen anderen als den vorgenannten Zweck nicht geeignet.

Dementsprechend ist unser Prüfungsbericht an die Gesellschaft gerichtet und darf nicht für einen anderen als den vorgenannten Zweck verwendet werden.

8. Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 1. Januar 2017 zugrunde liegen.

Hamburg, den 15. April 2022

nbs partners audit
GmbH Wirtschaftsprüfungsgesellschaft

Boris Michels
Wirtschaftsprüfer

Tobias Schreiber
Wirtschaftsprüfer

Anlage 1 - Darstellung der Grundsätze, Verfahren und Maßnahmen nach der DS-GVO und dem BDSG			
Anforderung			
DS-Ziel 1 - Im Unternehmen sind, mit der Einrichtung eines geeigneten Umfelds und einer geeigneten Aufbau- und Ablauforganisation mit hinreichender Sicherheit, die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicherzustellen (Artikel 5 Abs. 1 und 2, Artikel 24 Abs. 1 DS-GVO, Artikel 29 DS-GVO).			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 01-01	Es wurden Datenschutzziele festgelegt, welche sich nachvollziehbar aus der Unternehmensstrategie ableiten. Besondere datenschutzrechtliche Faktoren, welche sich aus dem Geschäftsmodell ergeben, wurden berücksichtigt und dokumentiert. Der angestrebte Zielzustand / Reifegrad der Datenschutzmaßnahmen wurde bestimmt und dokumentiert.	Durchsicht relevanter Dokumente zu den Datenschutzzielen. Prüfung der Datenschutzziele auf Ausrichtung an der Unternehmensstrategie. Einsichtnahme in Berichte / Auswertungen zur Erarbeitung und Anpassung von Datenschutzzielen. Reifegradeinschätzung auf Grundlage des etablierten Business Performance Managements.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-02	Es wurden Maßnahmen ergriffen und dokumentiert, um eine nachhaltige Datenschutz-Kultur im Unternehmen zu etablieren. Diese Maßnahmen ermöglichen, dass sich Mitarbeiter der Relevanz des DS nachhaltig bewusst ist.	Überprüfung des Kommunikationsplan zum DS. Prüfung der jährlichen Nachweisführung zur Vertraulichkeitsverpflichtung der Mitarbeiter und die Sensibilisierung der Mitarbeiter zum datenschutzkonformen Verhalten.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-03	Das in Bezug auf den DS für das Unternehmen relevante rechtliche und regulatorische Umfeld wurde bei der Ausgestaltung der Aufbau- und Ablauforganisation, sowie bei der Festlegung der Datenschutzmaßnahmen berücksichtigt. Es erfolgt eine anlassbezogene sowie regelmäßige Prüfung im Hinblick auf Änderungen des rechtlichen und regulatorischen Umfelds, sowie bei Bedarf die Ableitung von Anpassungsmaßnahmen.	Prüfung des jährlichen Reviews des DSMS, welches die relevante, rechtliche und regulatorische Ausgestaltung der Aufbau- und Ablauforganisation, sowie bei der Festlegung der Datenschutzmaßnahmen berücksichtigt. Einsichtnahme in die Dokumentation über die Durchführung der Prüfung von Änderungen des rechtlichen und regulatorischen Umfelds sowie der daraus abgeleiteten Anpassungs-maßnahmen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 01-04	Ist ein Rahmenwerk (Dokumentenpyramide) vorhanden, welches den Umgang mit dem DS detailliert regelt? Die im Rahmenwerk enthaltenen Regelungen sind durch ein Dokumenten-Management nachvollziehbar dokumentiert und allen Mitarbeitern zugänglich. Sind Richtlinien und Anweisungen zum DS vorhanden, welche die Grundsätze gemäß Artikel 5 DS-GVO berücksichtigen? Die Richtlinien und Anweisungen werden regelmäßig aktualisiert. Die Richtlinien und Anweisungen wurden vom Management freigegeben.	Prüfung des Vorhandenseins eines Rahmenwerkes (Dokumentenpyramide), welches den Umgang mit dem DS detailliert regelt, hinsichtlich Aktualität, Vollständigkeit und Freigabe des Managements.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-05	Die Regelungen des Rahmenwerks zu den Nachweis- und Rechenschaftspflichten umfassen, neben allgemeinen Vorgaben zur nachvollziehbaren Dokumentation der Einhaltung der datenschutzrechtlichen Anforderungen, sowie Vorgaben zur Aufbewahrung der Dokumentation, auch explizite Anforderungen an die Dokumentation von Einzelsachverhalten.	Prüfung der Regelungen im Rahmenwerk.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-06	Existiert eine Datenschutzorganisation mit einer klaren Festlegung von Rollen und Verantwortlichkeiten? Die Zusammenarbeit der verschiedenen Rollen innerhalb der Datenschutzorganisation sowohl untereinander als auch mit der Geschäftsführung (Verantwortlicher) ist festgelegt. Die definierte Datenschutzorganisation ist durch die Geschäftsführung abgenommen, dokumentiert und an alle relevanten Mitarbeiter kommuniziert worden.	Prüfung der Datenschutzorganisation mit Festlegungen zu: - Rollen- und Stellenbeschreibungen, DSK, - Kontaktdaten des DSB, - Rollen und Verantwortlichkeiten, - Ressourcen (DSK), - Berichtswegen, Schnittstellen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-07	Sofern das Unternehmen mit einem anderen Unternehmen für bestimmte Verarbeitungen gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegt (gemeinsam Verantwortliche gemäß Artikel 26 DS-GVO), wird eine Vereinbarung gemäß DS-GVO getroffen	Bewertung der Vereinbarung zu einer bestimmten Verarbeitung mit einer gemeinsamen Verantwortlichkeit auf Vollständigkeit und Aktualität. Prüfung der Einhaltung der wesentlichen Inhalte der Vereinbarung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-08	Es ist ein Schulungskonzept vorhanden, welches die Kommunikation der datenschutzrelevanten Grundsätze, Verfahren und Maßnahmen an die beteiligten Mitarbeiter sicherstellt und dafür sorgt, dass die Mitarbeiter ihre Rolle und Bedeutung im jeweiligen Prozess und deren Abhängigkeiten von vor- und nachgelagerten Prozessschritten bzw. Kontrollen kennen.	Das Schulungskonzept wurde auf Inhalt zu Kommunikation der datenschutzrelevanten Grundsätze, Verfahren und Maßnahmen für alle beteiligten Mitarbeiter geprüft.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 01-09	Das Unternehmen führt geeignete Nachweise zu regelmäßig durchgeführten Schulungen, zur Teilnahme an den Schulungen und zur Überprüfung des Wissensstands der Mitarbeiter. Die beteiligten Mitarbeiter werden zur Teilnahme an Datenschutzschulungen vertraglich verpflichtet. Die vollständige Teilnahme wird nachgehalten. Die Informationsmaterialien werden den Schulungsteilnehmern zur dauerhaften Einsicht zur Verfügung gestellt.	Prüfung der Nachweisführung zu regelmäßig durchgeführten Schulungen, zur Teilnahme an den Schulungen und zur Überprüfung des Wissensstands der Mitarbeiter. Prüfung der Verpflichtung der Mitarbeiter und der Arbeitsvertraglichen Regelungen. Prüfung der Verfügbarkeit der Informationsmaterialien	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-10	Das Unternehmen hat einen Überarbeitungsprozess implementiert, welcher sicherstellt, dass die Schulungsinhalte regelmäßig auf Aktualität und Angemessenheit überprüft und bei Bedarf korrigiert werden.	Prüfung des Überarbeitungsprozesses der Schulungsunterlagen, sowie Implementierung dieser Aktualisierungen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 01-11	Die interne Revision überwacht als prozessunabhängige Institution die Einhaltung der datenschutzrechtlichen Grundsätze, Verfahren und Maßnahmen. Dabei ist die angemessene Kommunikation mit dem DSB sichergestellt.	Die Prüfung dieser Kontrolle entfällt. Im Unternehmen ist keine Interne Revision etabliert. Die Überwachung des IKS erfolgt durch monatliche Self Assessments und externe Prüfungen.	Nicht relevant – siehe Prüfungs-handlung
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 02 - Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass der DSB die Anforderungen an seine Tätigkeit nachweisbar erfüllt.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 02-01	Die Tätigkeiten des DSB sind schriftlich in einer Stellen- bzw. Aufgabenbeschreibung bzw. bei einem externen DSB in dessen Beauftragung festgehalten. Soweit ein Benennungsschreiben bzw. eine Bestellungsurkunde vorliegt, sind die aufgeführten Aufgaben und Tätigkeiten konsistent zur Stellen- bzw. Aufgabenbeschreibung. Die Stellen- bzw. Aufgabenbeschreibung wird mindestens jährlich auf ihre Aktualität überprüft und vom Management bestätigt. Die Stellen- bzw. Aufgabenbeschreibung bzw. die Beauftragung berücksichtigen die Verpflichtung zur Verschwiegenheit gegenüber Dritten und unternehmensintern, sowie folgenden Anforderungen und Aktivitäten: - Unterrichtung und Beratung des Unternehmens und deren Beschäftigten, - Überwachung der Einhaltung der Vorgaben der DS-GVO sowie anderer relevanter Datenschutzvorschriften und Strategien des Unternehmens, - Beratung im Rahmen der Datenschutz-Folgenabschätzung (auf Anfrage), - Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese Beratung und Stellungnahmen gegenüber betroffenen Personen, - Vorgaben zur frühzeitigen Einbindung des DSB in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen, - Durchführung einer eigenen Risikoeinschätzung durch den DSB (auch Gefährdungsanalyse oder Abwägungsentscheidung).	Prüfung der Legitimation und Nachweisführung zu Tätigkeiten des DSB: - Unterrichtung und Beratung des Unternehmens und der Beschäftigten, - Überwachung der Einhaltung der Vorgaben der DS-GVO sowie anderer relevanter Datenschutzvorschriften und Strategien des Unternehmens, - Beratung im Rahmen der Datenschutz-Folgenabschätzung, - Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese, - Beratung und Stellungnahmen gegenüber betroffenen Personen, - Vorgaben zur frühzeitigen Einbindung des DSB in alle mit dem Schutz personenbezogener Daten, - Durchführung einer eigenen Risikoeinschätzung durch den DSB.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-02	Soweit dem Datenschutzbeauftragten neben seinen gesetzlichen Aufgaben weitere Aufgaben gemäß Artikel 38 Abs. 6 DS-GVO in Bezug auf die Datenschutzorganisation (z.B. Führung des VVT, Durchführung von Schulungen, Koordination von Lösch-/Auskunftsersuchen bzw. von Meldeprozessen) übertragen werden, sind auch diese in entsprechenden Stellen-/Aufgabenbeschreibungen bzw. Arbeitsanweisungen festgehalten. Es wird seitens des Unternehmens durch entsprechende Maßnahmen sichergestellt, dass die Unabhängigkeit des DSB aufgrund seiner erweiterten Aufgaben nicht beeinträchtigt wird. Dies kann z.B. durch die externe Überwachung der erweiterten Aufgaben des DSB erfolgen.	Prüfung der Unabhängigkeit des DSB gegenüber dem Management mittels Abgleiches mit der tatsächlichen Organisationsstruktur im Unternehmen. DSB ist extern unter Vertrag mit abgegrenzten Aufgabengebieten. Erweiterte Aufgaben bearbeitet der DSK.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 02-03	Die Verantwortlichkeiten des DSB sind gemäß Artikel 38 DS-GVO klar geregelt. Dies betrifft insbesondere auch die Schnittstellen bzw. die Abgrenzung zur Rechtsabteilung und zum Management bzw. zu soweit vorhanden dezentralen DSK oder anderen DSB in einem Konzern. Dem DSB ist der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen gewährt. Es ist eindeutig festgelegt, dass die Verantwortung für die Einhaltung der datenschutzrechtlichen Anforderungen nicht beim DSB liegt.	Prüfung der Unabhängigkeit des DSB gegenüber dem Management mittels Abgleiches mit der tatsächlichen Organisationsstruktur im Unternehmen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-04	Es ist schriftlich festgehalten, dass der DSB gemäß Artikel 38 Abs. 3 DS-GVO bei der konkreten Ausführung seiner Tätigkeit weisungsfrei agieren kann.	Die Regelungen zu den Verantwortlichkeiten des DSB wurden anhand der Berichtslinien nachvollzogen. Diese sind in den Prozessdarstellungen abgebildet. Dies betrifft insb. auch Schnittstellen bzw. die Abgrenzung zur Rechtsabteilung und zum dezentralen DSK.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-05	Der DSB ist gemäß Artikel 38 Abs. 5 DS-GVO i. V. mit § 6 Abs. 5 Satz 2 BDSG gesetzlich zur Verschwiegenheit verpflichtet. Die Mitarbeiter des DSB sind schriftlich zur Verschwiegenheit verpflichtet worden.	Einsichtnahme in die Verpflichtungserklärung der Mitarbeiter des DSB.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-06	Die Erreichbarkeit als unternehmensinterner Ansprechpartner gemäß Artikel 37 Abs. 2 DS-GVO sowie als Ansprechpartner gegenüber Betroffenen gemäß Artikel 38 Abs. 4 DS-GVO ist gewährleistet. Die Erreichbarkeit berücksichtigt nicht nur eine Stellvertreterregelung, sondern auch die Frage, inwieweit der DSB die relevanten Sprachen für die Korrespondenz mit der Aufsicht oder betroffenen Personen abdecken kann.	Befragung des Datenschutzteams bei PlusServer. Einsichtnahme in die Nachweise der Kommunikation mit Betroffenen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-07	Die Kontaktdaten des DSB sind gemäß Artikel 37 Abs. 7 DS-GVO im Unternehmen bekannt gemacht worden bzw. für Betroffene veröffentlicht (z. B. auf der Homepage des Unternehmens). Die zuständige Aufsichtsbehörde wurde identifiziert und dieser wurden die Kontaktdaten des DSB gemeldet.	Einsichtnahme in die Meldung der Kontaktdaten an die zuständige Aufsichtsbehörde. Einsichtnahme in die Homepage des Unternehmens.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 02-08	Zur Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 DS-GVO dokumentiert der DSB wesentliche Tätigkeiten und zusätzliche Tätigkeiten seiner Person bzw. seiner Mitarbeiter, z. B. in einem zentralen Dokumentation-Tool.	Prüfung der Rechenschaftspflicht des DSB durch Einsichtnahme in den Jahresbericht.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-09	Die operative Ausgestaltung der Aufgaben des DSB ist gemäß Art. 39 Abs. 2 DS-GVO grundsätzlich risikoorientiert geplant. Hierfür hat der DSB ggf. zusammen mit dem Unternehmen und auf Basis des Verzeichnisses von Verarbeitungstätigkeiten eine Risikoeinschätzung (Gefährdungsanalyse oder Abwägungsentscheidung) durchgeführt und das Ergebnis nachvollziehbar dokumentiert. Die Risikoeinschätzung ist regelmäßig bzw. anlassbezogen vom DSB auf ihre Angemessenheit zu überprüfen und ggf. anzupassen.	Prüfung der Risikoeinschätzung des DSB und des DSK. Abgleich der Risikoeinschätzung mit dem vorliegendem VVT und Prüfung der regelmäßigen Aktualisierung auf Basis der Freigabebestätigung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-10	Es erfolgt eine regelmäßige Kommunikation des DSB mit dem Management bzw. der Geschäftsführung. Die Berichtswege, der Rhythmus und die Formate, die Inhalte und der Adressatenkreis der Kommunikation sind klar geregelt. Die Kommunikation umfasst auch die Berichterstattung des DSB über seine Tätigkeit. Hierbei ist gemäß Artikel 38 Abs. 3 DS-GVO die unmittelbare Berichterstattung an die höchste Managementebene des Unternehmens sichergestellt.	Prüfung der Berichterstattung des DSB an das Management bzw. die Geschäftsführung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-11	Für die Tätigkeit des DSB und seiner Mitarbeiter ist eine nachvollziehbare und angemessene Budgetierung erfolgt. Dem DSB werden gemäß Artikel 38 Abs. 2 DS-GVO die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen bzw. die erforderliche Ausstattung zur Verfügung gestellt. Das Budget ermöglicht die Hinzuziehung externer Unterstützung bzw. Beratung oder die Beschaffung von spezifischen Hilfsmitteln.	Abgleich der Budget- und Ressourcenplanung für den DS mit vorhandenen Ressourcen und Ausstattungen. Beurteilung, ob Anhaltspunkte für nicht ausreichende Budgets und Ressourcen vorliegen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 02-12	Der DSB verfügt gemäß Artikel 37 DS-GVO über eine ausreichende Qualifikation bzw. Fachkenntnis. Es sind gemäß Artikel 38 Abs. 2 DS-GVO regelmäßige Schulungs- und Fortbildungsmaßnahmen für den DSB und seine Mitarbeiter vorgesehen. Die jeweilige Teilnahme wird dokumentiert. Notwendige Fachliteratur oder externe Beratung können bei Bedarf in Anspruch genommen werden.	Einsichtnahme in den Prozess zur Auswahl des DSB und Beurteilung der an den DSB gestellten Qualifikationsanforderungen sowie Beurteilung, ob der DSB diese Anforderungen erfüllt. Einsichtnahme in Zertifikate des DSB bzw. Nachweise über die Teilnahme an Schulungen. Befragung des DSB.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-13	Der DSB ist gemäß Artikel 38 Abs. 1 DS-GVO so in Entscheidungs- und Informationsprozesse eingebunden, dass er ordnungsgemäß und frühzeitig bei allen Fragen in Bezug auf den Umgang und den Schutz personenbezogener Daten involviert wird. Der DSB ist in die QS von Arbeitsanweisungen und Arbeitshilfen bzw. Templates mit Bezug zum DS eingebunden.	Durchsicht der Richtlinien und der Dokumentation von Informations- und Kommunikationsprozessen bezogen auf die Einbindung des DSB.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-14	Der DSB unterrichtet und berät gemäß Artikel 39 Abs. 1 DS-GVO das Unternehmen und die Beschäftigten bezogen auf datenschutzrechtliche Anforderungen.	Durchsicht der Stellen- / Aufgabenbeschreibung des DSB. Prüfung der Belegbarkeit der Tätigkeiten.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-15	Die Prozesse zur Datenschutz-Folgenabschätzung stellen gemäß Artikel 39 Abs. 1 Buchst. c) DS-GVO die Konsultation des DSB sicher. Die Beratung zur DSFA erfolgt auf Anfrage des verantwortlichen Fachbereichs und bedarf insb. einer abgestimmten Methodik sowie einer klaren Aufgabenverteilung. Die Beratungsleistung wird vom DSB dokumentiert.	Durchsicht der Prozessdokumentation DSFA. Prüfung ausgewählter VVT in Bezug auf eine DSFA mit der Einbindung des DSB. Einsichtnahme in den Tätigkeitsbericht bzw. andere Nachweise über die Tätigkeit des DSB.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 02-16	Für die allgemeine Zusammenarbeit mit der Aufsichtsbehörde und die Wahrnehmung der Funktion als Anlaufstelle für die Aufsichtsbehörde sind Verhaltensregeln sowie die Verantwortlichkeiten und Kontaktpersonen definiert. Diese werden regelmäßig aktualisiert. Zu den Aufgaben des DSB gemäß Artikel 39 Abs. 1 DS-GVO gehören in diesem Zusammenhang: - Kommunikation mit der Aufsichtsbehörde (Bearbeitung von Anfragen der Aufsichtsbehörde sowie Zugehen auf die Aufsichtsbehörde bei datenschutzrechtlichen Fragestellungen oder Beratungsanliegen); - Konsultation im Rahmen der Datenschutz-Folgenabschätzung; - Anlaufstelle für die Aufsichtsbehörde (u. a. in Bezug auf Rückfragen aus der Konsultation, Anfragen zum VVT, Bearbeitung von Betroffenenbeschwerden). Für diese Fälle sind Regelungen für die interne Kommunikation mit dem Management getroffen.	Prüfung der Aktualisierung der Verhaltensregelungen und Verantwortlichkeiten zur allgemeinen Zusammenarbeit mit der Aufsichtsbehörde und die Wahrnehmung der Funktion als Anlaufstelle für die Aufsichtsbehörde.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-17	Für die Entgegennahme und die Bearbeitung der Anfragen eines Betroffenen gemäß Artikel 38 Abs. 4 DS-GVO sind ein Kommunikationsprozess sowie eine nachweisbare Ablagesystematik (Fallakte) definiert. Bei der Bearbeitung von Beschwerden Betroffener wird bei Bedarf die Rechtsabteilung des Unternehmens eingebunden.	Prüfung des Kommunikationsprozesses zur Entgegennahme und die Bearbeitung der Anfragen eines Betroffenen, sowie eine nachweisbare Ablagesystematik. Prüfung der Bearbeitung von Beschwerden Betroffener auf Einbindung der Rechtsabteilung des Unternehmens.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 02-18	Der DSB überwacht gemäß Artikel 39 Abs. 1 DS-GVO die Einhaltung der Anforderungen der DS-GVO und des BDSG sowie der im Rahmenwerk (Dokumentenpyramide) ggf. ergänzend definierten unternehmensinternen datenschutzrechtlichen Regelungen. Der Überwachung durch den DSB liegt ein Überwachungskonzept mit folgenden Aspekten zugrunde: - Die Planung der Überwachung erfolgt gemäß Artikel 39 Abs. 2 DS-GVO risikoorientiert. Hierzu hat der DSB eine sog. Risikolandkarte erstellt und die Risiken der einzelnen Themen bzw. Verarbeitungstätigkeiten berücksichtigt. Die Risikoeinschätzung wird regelmäßig und anlassbezogen überprüft und in der Änderungs- / Versionshistorie dokumentiert. - Die Überwachungstätigkeit deckt über einen definierten Zeitraum alle datenschutzrechtlichen Aspekte des Unternehmens ab. - Der Berichterstattung über die Ergebnisse der Überwachungstätigkeit liegt ein Berichtsmuster zugrunde. - Beanstandungen werden zeitnah an das Management berichtet und unterliegen einem Follow-up-Prozess. Die Prüfungshandlungen sowie die Ergebnisse werden vom DSB zur Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 DS-GVO dokumentiert.	Prüfung des Überwachungskonzept. Abstimmung der sog. Risikolandkarte mit dem vorliegenden VVT. Abgleich der Ergebnisse der Überwachung durch den DSB mit Ergebnissen der externen Prüfungsberichte. Prüfung der regelmäßigen Aktualisierung des Überwachungskonzepts auf Basis der Freigabebestätigung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 02-19	Die Tätigkeit des DSB wird durch eine unabhängige Stelle überwacht (z. B. durch die Interne Revision oder eine externe Prüfung).	Durchsicht externer Prüfungsberichte.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 3 - Das Unternehmen stellt mit der Einrichtung eines geeigneten datenschutzrechtlichen Risikomanagements die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 03-01	Es ist gemäß Artikel 32, Artikel 35, Artikel 24 Abs. 1 und Artikel 25 Abs. 1 DS-GVO ein geregelter Prozess zum Management von Datenschutzrisiken für die Rechte und Freiheiten von Betroffenen eingerichtet, welcher folgende Aspekte abbildet: - Identifikation potentieller Risiken; - Bewertung der identifizierten Risiken in Bezug auf die Auswirkungen auf Rechte und Freiheiten von Betroffenen; - Festlegung von Maßnahmen zur Risikobehandlung; - Überwachung der Umsetzung der Maßnahmen zur Risikobehandlung; - Kommunikation der Risiken an den Verantwortlichen und alle relevanten Einheiten in der Organisation. Das Risikomanagement berücksichtigt Risiken für die Rechte und Freiheiten von Betroffenen aus Projekten, Risiken aus dem Regelbetrieb, Risiken im Rahmen von Datenschutzvorfällen, Risiken aus Prozessen für datenschutzfreundliche Technik und Voreinstellungen und Risiken aus DSFA. Die Durchführung und die Ergebnisse des Prozesses werden dokumentiert. Der Prozess wird regelmäßig auf seine Aktualität hin geprüft.	Prüfung der Etablierung eines geregelten Prozesses zum Management von Datenschutzrisiken für die Rechte und Freiheiten von Betroffenen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 03-02	Es ist ein geregelter Prozess zur DSFA eingerichtet. Durch ein zweistufiges Prüfungsverfahren ist sichergestellt, dass für Verarbeitungstätigkeiten mit einem hohen Risiko eine DSFA durchgeführt wird. 1. Erforderlichkeitsprüfung 2. Durchführung der DSFA bei voraussichtlich hohem Risiko Die Methode zur Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung erfüllt die formalen Anforderungen gemäß Artikel 35 DS-GVO. Die Ergebnisse der Erforderlichkeitsprüfung und der DSFA werden dokumentiert. Der Prozess wird regelmäßig auf seine Aktualität geprüft.	Prüfung der Aktualität des Prozesses zur DSFA. Nachvollzug, ob ein zweistufiges Prüfungsverfahren sichergestellt ist, dass für Verarbeitungstätigkeiten mit einem hohen Risiko eine DSFA durchgeführt wird.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

DS-KONTROLLE 03-03	Es ist ein geregelter Prozess zur Konsultation mit der relevanten Aufsichtsbehörde gemäß Artikel 36 DS-GVO eingerichtet für den Fall, dass trotz getroffener Maßnahmen nach erfolgter Datenschutz-Folgenabschätzung ein hohes Risiko für die Rechte und Freiheiten von Betroffenen besteht.	Prüfung der Prozessvorgaben zur Konsultation mit der relevanten Aufsichtsbehörde und der abgeleiteten Maßnahmen für den Fall, dass trotz getroffener Maßnahmen nach DFSA ein hohes Risiko für Betroffene besteht .	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 03-04	Die Verantwortlichkeiten im Rahmen des Managements von Datenschutzrisiken und der Datenschutz-Folgenabschätzung sind eindeutig geregelt. Der DSB ist in das Management von Datenschutzrisiken, insbesondere in den Prozess der Datenschutz-Folgenabschätzung eingebunden.	Durchsicht der Prozessdokumentation zum Management von Datenschutzrisiken und zur Datenschutzfolgenabschätzung unter Einbindung des DSB.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 03-05	Es ist ein geregelter Prozess eingerichtet, welcher sicherstellt, dass auf der Grundlage der Risikobewertung angemessene technische und organisatorische Maßnahmen für Verarbeitungstätigkeiten abgeleitet und dokumentiert werden.	Einsichtnahme in die Risikobewertung der Verarbeitungstätigkeiten und die Dokumentation der daraus abgeleiteten technischen und organisatorischen Maßnahmen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 04 - Das Unternehmen hat Maßnahmen ergriffen, die mit hinreichender Sicherheit die Rechtmäßigkeit (Zulässigkeit) der Verarbeitung personenbezogener Daten sicherstellen.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 04-01	Es ist ein geregelter Prozess einschließlich der Festlegung von Rollen und Verantwortlichkeiten zur Klärung der Zulässigkeit bzw. zur Bestimmung des Erlaubnistatbestands jeder Verarbeitungstätigkeit gemäß Artikel 6 DS-GVO eingerichtet. Der Erlaubnistatbestand jeder Verarbeitungstätigkeit wird nachvollziehbar dokumentiert und die fortwährende Zulässigkeit der Verarbeitung wird regelmäßig überprüft.	Die Befragung relevanter Mitarbeiter der Fachbereiche HR und Marketing und Beurteilung einzelner Verfahren aus dem Verzeichnis von Verarbeitungstätigkeiten hinsichtlich der Einhaltung der Vorgaben gemäß Art. 6 DS-GVO. Die nachweisliche Einbindung des DSB wurde in Verarbeitungstätigkeiten stichprobenartig geprüft.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 04-02	In Bezug auf die ggf. erforderliche Einwilligung des Betroffenen zur Herstellung der Rechtmäßigkeit der Verarbeitung gemäß Artikel 7 und 8 DS-GVO sind folgende Aspekte geregelt: Der Text der Einwilligungsformulare entspricht einer internen Mustervorgabe oder es ist ein Prozess eingerichtet, welcher sicherstellt, dass Betroffene transparent über die vorgesehenen Zwecke der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten im Einzelnen informiert werden und somit ihre Einwilligung informiert erteilen. Erteilte Einwilligungen werden nachvollziehbar dokumentiert (Rechenschaftspflicht), dies beinhaltet auch den konkreten Wortlaut bzw. Referenz auf eine versionierte Standardformulierung. Es sind prozessuale Vorgaben zum Umgang mit einem Widerruf einer erteilten Einwilligung definiert. Ein Widerruf wird dokumentiert und ist ebenso einfach gestaltet wie die zugehörige Einwilligung. Auf die Besonderheiten spezifischer Gruppen Betroffener (z. B. Beschäftigte oder Minderjährige) wird in angemessener Weise eingegangen.	Prüfung der Vorgaben zur Herbeiführung von Einwilligungen einschließlich der Bearbeitung von Widerrufen. Kontrolle der erteilten Einwilligungen und der bearbeiteten Widersprüche.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

DS-KONTROLLE 04-03	Es bestehen Vorgaben für die Durchführung und Dokumentation einer Interessenabwägung im Fall der Anwendung des Erlaubnistatbestands des berechtigten Interesses gemäß Artikel 6 Abs. 1 Buchst. f) DS-GVO. Diese beinhalten die bei einer Interessenabwägung anzuwendenden Kriterien und deren Gewichtung (Kriterienkatalog) und sehen die besondere Berücksichtigung der Interessen von Minderjährigen / Kindern vor.	Prüfung der Vorgaben für die Durchführung und Dokumentation einer Interessenabwägung im Fall der Anwendung des Erlaubnistatbestands des berechtigten Interesses gemäß Artikel 6 Abs. 1 Buchst. f) DS-GVO.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 04-04	Es ist ein geregelter Prozess für den Umgang mit einer Zweckänderung der Verarbeitung eingerichtet, welcher folgende Vorgaben enthält: Kriterienkatalog für die Feststellung der Zulässigkeit einer Zweckänderung Berücksichtigung der Anforderungen gemäß Artikel 6 Abs. 4 DS-GVO und Dokumentation der Einhaltung dieser Anforderungen. Anpassung des VVT im Hinblick auf die Zweckänderung.	Prüfung der geregelten Prozessdarstellung für den Umgang mit einer Zweckänderung. Befragung der mit dem Prozess betrauten Mitarbeiter, sowie Beurteilung durchgeführter Zweckänderungen anhand deren Dokumentation.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 05 - Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass gemäß Artikel 30 DS-GVO das VVT im Unternehmen geführt und gepflegt wird und auf Anfrage bereitgestellt werden kann.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 05-01	Das Unternehmen führt ein VVT gemäß Artikel 30 DS-GVO, um seiner Dokumentationspflicht nachzukommen. Das VVT gibt für jede Verarbeitungstätigkeit Auskunft über: - den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen DSB, - die Zwecke der Verarbeitung, - eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, - die Kategorien von Empfängern, welchen personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen, - ggf. 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 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentation geeigneter Garantien, - die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, - eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO. Das Verzeichnis der Verarbeitungstätigkeiten wird gemäß Artikel 30 Abs. 3 DS-GVO in schriftlicher Form oder elektronisch geführt.	Durchsicht der Vorgaben zum Inhalt des Verzeichnisses von Verarbeitungstätigkeiten und Beurteilung, ob diese den Anforderungen von Artikel 30 Abs.1 DS-GVO entsprechen. Einsichtnahme in Verzeichniseinträge hinsichtlich vollständiger Bearbeitung, Nachvollziehbarkeit und Einhaltung von Qualitätskontrollen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 05-02	Soweit das Unternehmen auch als AV tätig ist, führt es gemäß Artikel 30 Abs. 2 DS-GVO ein Verzeichnis zu allen Kategorien von den im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung. Das Verzeichnis gibt Auskunft über: - den Namen und die Kontaktdaten des Verantwortlichen, des / r von ihm beauftragten AV, sowie ggf. der jeweiligen Vertreter; soweit der / die AV einen DSB benannt hat / haben, auch die Daten des DSB, - die Kategorien von Verarbeitungen, welche im Auftrag jedes Verantwortlichen durchgeführt werden, - ggf. 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 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentation geeigneter Garantien - eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO. Mindestens sind die bei der Auftragsvergabe zugrunde gelegten technischen und organisatorischen Maßnahmen zu dokumentieren; - die vorgesehenen Fristen der Löschung der verschiedenen Datenkategorien. Das Verzeichnis zu allen Kategorien von den im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung wird gemäß Artikel 30 Abs. 3 DS-GVO in schriftlicher Form oder elektronisch geführt.	Durchsicht der Vorgaben zum Inhalt des Verzeichnisses von Verarbeitungstätigkeiten und Beurteilung, ob diese den Anforderungen von Artikel 30 Abs. 1 DS-GVO entsprechen. Einsichtnahme in Verzeichniseinträge hinsichtlich vollständiger Bearbeitung, Nachvollziehbarkeit und Einhaltung von Qualitätskontrollen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 05-03	Die Verantwortlichkeiten für die Erfassung und Pflege bzw. die QS der Verzeichniseinträge sind eindeutig definiert.	Prüfung der Vorgaben. Beurteilung, ob die Maßnahmen von den dafür vorgesehenen Mitarbeitern durchgeführt wurden durch Befragung der Mitarbeiter und Abgleich der Vorgaben mit der tatsächlichen Organisations-Struktur und Einsichtnahme in die erfassten Verarbeitungstätigkeiten.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 05-04	Das Unternehmen hat Verfahren und Maßnahmen eingerichtet, welche fortlaufende und ordnungsgemäße Pflege des Verzeichnisses sowie die Erfassung aller relevanten Verarbeitungstätigkeiten sicherstellen.	Prüfung des Verfahrensverzeichnisses auf Vollständigkeit und Beurteilung einzelner Verzeichniseinträge bezogen auf die fortlaufende und ordnungsmäßige Pflege.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 05-05	Die Änderungen im Verzeichnis werden versioniert, so dass die Neuaufnahme, die inhaltliche Veränderung oder das Löschen einer Verarbeitungstätigkeit nachvollziehbar sind.	Prüfung ausgewählter Änderungen und deren Historie. Änderungen im Verzeichnis werden versioniert	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 05-06	Auf Anfrage der Aufsichtsbehörde ist der Verantwortliche bzw. der AV in der Lage, das Verzeichnis gemäß Artikel 30 Abs. 4 DS-GVO zur Verfügung zu stellen. Diesbezüglich ist vom Unternehmen ein Prozess einschließlich klarer Verantwortlichkeiten definiert.	Prüfung der Prozessvorgaben und der Verantwortlichkeiten. Interview mit den Mitarbeitern. Einsichtnahme in das VVT.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 05-07	Es erfolgt eine regelmäßige Überprüfung der Vollständigkeit und Richtigkeit des Verzeichnisses (mindestens einmal jährlich) durch den Verantwortlichen. Das Ergebnis wird dokumentiert (sign-off).	Prüfung der Nachweise für die Überprüfung der Vollständigkeit und Richtigkeit des Verzeichnisses durch den Verantwortlichen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 06 - Das Unternehmen hat gemäß Artikel 25 DS-GVO bereits bei der Programmierung, Konzeption und Entwicklung der Datenverarbeitungsvorgänge und -technik die Datenschutzgrundsätze berücksichtigt (DS durch Technikgestaltung (privacy by design)). Durch datenschutzfreundliche Voreinstellungen unterstützt das Unternehmen, dass grundsätzlich nur personenbezogene Daten verarbeitet werden, welche für den Verarbeitungszweck erforderlich sind (privacy by default).			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 06-01	Es ist ein geregelter Prozess eingerichtet, welcher sicherstellt, dass bei der Konzeption und Entwicklung neuer bzw. bei der Anpassung bestehender Datenverarbeitungsvorgänge und -technik, bei der Beschaffung von Datenverarbeitungstechnik sowie im laufenden Betrieb die Berücksichtigung der Datenschutzgrundsätze erfolgt. Der Prozess enthält Vorgaben, dass sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung unter Berücksichtigung: - des Stands der Technik, - der Implementierungskosten und der Art, des Umfangs, der Umstände, - der Zwecke der Verarbeitung, sowie - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, - geeignete technische und organisatorische Maßnahmen gemäß Artikel 25 Abs. 1 DS-GVO getroffen werden, um die Datenschutzgrundsätze umzusetzen.	Einsichtnahme in die Prozessdarstellung für Datenschutz und Architekturvorgaben. Prüfung der umgesetzten Maßnahmen für Umgebungen in der Verarbeitung von personenbezogenen Daten.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 06-02	Durch geeignete technische und organisatorische Maßnahmen wird sichergestellt, dass gemäß Artikel 25 Abs. 2 DS-GVO durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies betrifft: - die Menge der erhobenen personenbezogenen Daten, - den Umfang der Verarbeitung, - die Speicherfrist, - die Zugänglichkeit, insb. die Sicherstellung, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.	Prüfung des Prinzips Privacy by default bei der Entwicklung neuer Produkte in der Entwicklungsrichtlinie und in der Richtlinie Akzeptable Nutzung von Technologie, welche die Vorgaben der DS-GVO mit einbezieht. Durch die Qualitätssicherung und etablierte ICS Kontrollen werden Schwachstellen identifiziert und nach Lösungen (Updates) gesucht.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 07 - Es sind gemäß Artikel 32 DS-GVO geeignete technische und organisatorische Maßnahmen eingerichtet, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Hierbei wurden der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 07-01	Das Unternehmen hat Maßnahmen eingerichtet, um vollständig alle Systeme und Anwendungen zu erfassen, welche personenbezogene Daten verarbeiten. Dies umfasst auch die unterstützende IT-Infrastruktur.	Prüfung der Richtlinien, Anweisungen, Umsetzung der Erfassung der Systeme und Anwendungen und Beurteilung der angemessenen Ausgestaltung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 07-02	Es sind Richtlinien zur Sicherheit der Verarbeitung gemäß Artikel 32 DS-GVO vorhanden, welche für alle Systeme und Anwendungen gelten, welche personenbezogene Daten verarbeiten. Die Richtlinien umfassen klare Vorgaben, Rollen und Verantwortlichkeiten sowie Dokumentationsanforderungen und werden regelmäßig auf Aktualität geprüft.	Prüfung der Aktualität des Frameworks (Richtlinienpyramide) in Bezug auf Aktualität und Geltungsbereich. Auswertung der Aktualität der Richtlinien und Unterlagen in PSSD bezogen auf die TOMs.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 07-03	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. b) und c) DS-GVO Business Continuity- und IT-Desaster Recovery-Pläne zur Wiederherstellung der Systeme und Anwendungen im Störungs- oder Katastrophenfall definiert, dokumentiert und implementiert. Die Pläne werden gemäß Artikel 32 Abs. 1 Buchst. d) DS-GVO mit einer definierten Häufigkeit auf ihre Wirksamkeit getestet.	Prüfung der Business Continuity- und IT-Desaster Recovery-Pläne zur Wiederherstellung der Systeme und Anwendungen im Störungs- und Katastrophenfall. Einsichtnahme in die Umsetzung der ICS und andere kompensierende Kontrollen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 07-04	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. b) DS-GVO Verfahren und Maßnahmen eingerichtet, um das Zugriffsmanagement sicherzustellen.	Prüfung des Berechtigungsrichtlinie. Einsicht in die Dokumentationen und systemseitig generierte Unterlagen in Bezug auf die Übereinstimmung der definierten Verfahren und Maßnahmen mit den tatsächlichen Abläufen. Überprüfung der Zugriffsrechte für Benutzer und Einsichtnahme in erfasste Logdaten.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 07-05	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. b) DS-GVO geeignete Test- und Freigabeverfahren eingerichtet, welche neben Funktionstrennungen insbesondere die Trennung von Entwicklungs- und Testsystemen von den produktiv genutzten Systemen vorsehen, um sicherzustellen, dass nur freigegebene Systeme und Anwendungen produktiv zum Einsatz kommen.	Prüfung der Change-Management Richtlinie sowie der Test- und Freigabeverfahren, welche neben Funktionstrennungen insbesondere die Trennung von Entwicklungs- und Testsystemen von den produktiv genutzten Systemen vorsehen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 07-06	Das Unternehmen verfügt gemäß Artikel 32 Abs. 1 Buchst. a) DS-GVO über eine Richtlinie für den Umgang mit kryptographischen Maßnahmen zum Schutz von Informationen einschließlich personenbezogener Daten.	Prüfung der Kryptographie Richtlinie hinsichtlich Vollständigkeit und Aktualität in Bezug auf das Schutzniveau, die Schlüsselverwaltung, Rollen und Verantwortlichkeiten, sowie den aktuellen Stand der Technik.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 07-07	Das Unternehmen hat Verfahren und Maßnahmen eingerichtet, um gemäß Artikel 32 Abs. 1 Buchst. b) DS-GVO die Belastbarkeit der Systeme sicherzustellen. Dies betrifft insbesondere den Schutz vor Malware und Viren.	Durchsicht von Richtlinien, Anweisungen und der etablierten ICS Kontrollen hinsichtlich Vollständigkeit und Aktualität in Bezug auf die Berücksichtigung der Systeme und Anwendungen, welche personenbezogene Daten verarbeiten.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt. Wir empfehlen Penetrationstest jährlich durchzuführen.
DS-KONTROLLE 07-08	Das Unternehmen hat Verfahren und Maßnahmen eingerichtet, um gemäß Artikel 32 Abs. 1 Buchst. a) DS-GVO Daten zu pseudonymisieren.	Eine Pseudonymisierung ist im Geltungsbereich der Prüfung nicht anwendbar. Eine Prüfung dieser Anforderung erfolgt nicht.	Nicht relevant – siehe Prüfungshandlung
DS-KONTROLLE 07-09	Das Unternehmen hat gemäß Artikel 32 Abs. 1 Buchst. d) DS-GVO Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Angemessenheit und Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung implementiert. Diese schließen die Evaluierung ein, ob die Maßnahmen dem Stand der Technik entsprechen. Das Ergebnis ist zu dokumentieren.	Einsichtnahme in die Dokumentationen durchgeführter internen und externen Überprüfungen, Bewertungen und Evaluierungen bezogen auf die Einhaltung der Vorgaben und ergriffene Maßnahmen zur Behebung von Schwächen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 08 - Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass personenbezogene Daten gemäß Artikel 17 i. V. mit Artikel 5 DS-GVO regelmäßig nach Zweckbindung (bzw. nach Ablauf der Aufbewahrungsfrist) gelöscht bzw. anderweitig unbrauchbar gemacht werden.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 08-01	Das Unternehmen hat ein schriftlich dokumentiertes Verfahren eingerichtet, welches die folgenden Aspekte beinhaltet: Neben einer übergreifenden Richtlinie zur Löschung und Sperrung personenbezogener Daten sind spezifische Lösch- und Sperrkonzepte je Verarbeitungstätigkeit vorhanden, welche den Grundsätzen der Zweckbindung, Datenminimierung und Speicherbegrenzung gemäß Artikel 5 DS-GVO Rechnung tragen. Die jeweiligen Verantwortlichkeiten sind eindeutig geregelt. Die Erstellung der anwendungsbezogenen Löschkonzepte sieht eine Einbindung der IT-Abteilung und der Fachbereiche vor. Soweit sich Zweckänderungen ergeben, werden die Löschkonzeptionen entsprechend überprüft. Die Einschätzung der Aufbewahrungsfristen sowie der Lösch- und Sperrfristen wird regelmäßig aktualisiert. Eine zentrale QS stellt eine unternehmensübergreifende Umsetzung der Vorgaben sicher. Die produktive Implementierung von technischen Löschroutinen erfolgt durch ein ordnungsgemäßes Test- und Freigabeverfahren. Die Löschverfahren werden auf logische sowie physische Daten (z. B. Akten) angewandt. Hierbei werden auch ausgelagerte Daten, vor- und nachgelagerte Systeme und Datenextrakte berücksichtigt.	Abgleich der in den Lösch- und Sperrkonzepten festgelegten Vorgaben mit Systemeinstellungen und Parametern. Einsichtnahme in Nachweise über die vom Unternehmen durchgeführte regelmäßige Prüfung der Umsetzung der Vorgaben	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 08-02	Für jede Verarbeitungstätigkeit sind automatisierte oder nicht automatisierte Löschmechanismen / -prozesse implementiert, welche eine vollständige Löschung der personenbezogenen Daten ermöglichen. Hierbei werden auch vor- und nachgelagerte Systeme und Datenextrakte berücksichtigt. - Das Intervall der Löschung ist festgelegt. - Die Löschung wird protokolliert. - Die Vorgaben sind konsistent zum VVT.	Prüfung der Richtlinien und Vorgaben zu Löschmechanismen. Abgleich der in den Lösch- und Sperrkonzepten festgelegten Vorgaben mit Systemeinstellungen und Parametern. Einsichtnahme in Nachweise über die vom Unternehmen durchgeführte regelmäßige Prüfung der Umsetzung der Vorgaben.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 08-03	Können personenbezogene Daten aus bestimmten Gründen (bspw. aufgrund von gesetzlichen Aufbewahrungsfristen) trotz Wegfalls der Zweckbindung nicht gelöscht werden (Artikel 17 Abs. 3 DS-GVO), erfolgt eine Sperrung der personenbezogenen Daten bzw. werden andere Schutzmaßnahmen vorgenommen. Die Vorgehensweise wird entsprechend dokumentiert.	Abgleich der Vorgaben mit den Systemeinstellungen und Parametern. Einsichtnahme in die Protokolle über die Durchführung der Löschung. Abgleich der Vorgaben mit den Angaben im VVT oder den Informationsblättern für Betroffene. Prüfung der Einhaltung der Löschvorgaben für ausgewählte Datenbestände.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 08-04	Die fristgerechte und tatsächliche Löschung bzw. Sperrung personenbezogener Daten wird protokolliert und überwacht.	Prüfung der fristgerechten und tatsächlichen Löschung oder Sperrung personenbezogener Daten und die Nachweisführung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 09 - Das Unternehmen stellt mit der Einrichtung von Prozessen für Betroffenenrechte mit hinreichender Sicherheit die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 09-01	Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person gemäß Artikel 13 DS-GVO. Es ist ein Prozess eingerichtet, welcher sicherstellt, dass der betroffenen Person zum Zeitpunkt der Erhebung der Daten die Informationen gemäß Artikel 13 Abs. 1 und 2 DS-GVO mitgeteilt werden und bei einer beabsichtigten Änderung des Zwecks der Verarbeitung die Zweckänderung sowie die Informationen gemäß Artikel 13 Abs. 2 DS-GVO mitgeteilt werden.	Prüfung des Prozesses für die Informationspflicht der betroffenen Personen zum Zeitpunkt der Erhebung der Daten. Überprüfung der Nachweisführung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 09-02	Informationspflicht gemäß Artikel 14 DS-GVO bei der Erhebung von personenbezogenen Daten, welche nicht bei der betroffenen Person selbst erfolgt. Es ist ein Prozess eingerichtet, welcher sicherstellt, dass der betroffenen Person die Informationen gemäß Artikel 14 Abs. 1 und 2 DS-GVO mitgeteilt werden und die in Artikel 14 Abs. 3 DS-GVO genannten Fristen für die Mitteilung der Informationen eingehalten werden. Bei einer beabsichtigten Änderung des Zwecks der Verarbeitung werden die Zweckänderung sowie die Informationen gemäß Artikel 14 Abs. 2 DS-GVO mitgeteilt.	Prüfung des Prozesses für die Informationspflicht, bei der indirekten Datenerhebung von personenbezogenen Daten. Überprüfung der Prozessgestaltung der Nachweisführung der Umsetzung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 09-03	Auskunftsrecht gemäß Artikel 12 und 15 DS-GVO: Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Auskunft eingerichtet. Die Prozesse stellen sicher, dass die Auskunft gemäß Artikel 12 Abs. 1 und 6 DS-GVO nur an den rechtmäßigen Betroffenen gesendet wird bzw. dieser einwandfrei identifiziert wird. Auskünfte entsprechen inhaltlich den Anforderungen von Artikel 15 Abs. 1 DS-GVO. Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten. Es sind Prozesse eingerichtet und technische Voraussetzungen implementiert, welche es ermöglichen, dem Betroffenen auf Anfrage gemäß Artikel 15 Abs. 3 DS-GVO eine Kopie seiner personenbezogenen Daten bereitzustellen, welche Gegenstand der Verarbeitung sind.	Prüfung der Vorgaben zu dem Prozess der Auskunftserteilung. Prüfung auf Vollständigkeit der Informationen im Template für die Beantwortung von Auskunftsersuchen. Prüfung, ob Datenschutzhinweise und Informations-schreiben des Unternehmens in Bezug auf Betroffenenrechte klar verständlich und vollständig sind. Einsichtnahme in Nachweise über erteilte Auskünfte, bezogen auf die Einhaltung der Vorgaben.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 09-04	Recht auf Berichtigung gemäß Artikel 16 DS-GVO: Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Berichtigung eingerichtet. Die Berichtigung erfolgt technisch in allen Systemen bzw. an allen Speicherorten. Die Prozesse stellen sicher, dass die Identität des anfragenden Betroffenen gemäß Artikel 12 Abs. 1 und 6 DS-GVO eindeutig bestimmt werden kann. Prozesse zur Kommunikation einer Berichtigung an weitere Empfänger der relevanten Daten und an Betroffene gemäß Artikel 19 DS-GVO sind definiert und werden konsequent angewendet. Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Vorgaben zu den Prozessen der Berichtigung von personenbezogenen Daten auf Anfrage von Betroffenen. Einsichtnahme in Nachweise über durchgeführte Berichtigungen bezogen auf die Einhaltung der Vorgaben.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 09-05	Recht auf Löschung gemäß Artikel 17 DS-GVO: Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Löschung eingerichtet. Die Prozesse stellen sicher, dass die Identität des anfragenden Betroffenen gemäß Artikel 12 Abs. 1 und 6 DS-GVO eindeutig bestimmt werden kann. Die Prozesse stellen sicher, dass gemäß Artikel 17 Abs. 3 DS-GVO durch die Löschung keine höhergeordneten Rechte eingeschränkt werden, wie z. B. gesetzliche Vorhaltepflichten, vertragliche Grundlagen, Recht der freien Meinungsäußerung. Die Prozesse stellen sicher, dass bei Vorliegen der Voraussetzungen die relevanten personenbezogenen Daten des Betroffenen gelöscht werden. Prozesse zur Kommunikation einer Löschung an weitere Empfänger der relevanten Daten und an Betroffene gemäß Artikel 19 DS-GVO sind eingerichtet und werden konsequent angewendet. Dies gilt ebenso bei einer Offenlegung der Daten gemäß Artikel 17 Abs. 2 DS-GVO. Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Durchsicht der Vorgaben zu den Prozessen der Löschung von personenbezogenen Daten auf Anfrage von Betroffenen. Kontrolle der Bearbeitung von Löschanfragen von Betroffenen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 09-06	Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 DS-GVO: Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Einschränkung der Verarbeitung eingerichtet. Die Prozesse stellen sicher, dass gemäß Artikel 12 Abs. 1 und 6 DS-GVO die Identität des anfragenden Betroffenen eindeutig bestimmt werden kann. Die Prozesse stellen sicher, dass die Einschränkung der Verarbeitung umgesetzt wird. Prozesse zur Kommunikation einer Einschränkung an weitere Empfänger der relevanten Daten und an Betroffene gemäß Artikel 19 DS-GVO sind definiert und werden konsequent angewendet. Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung des Prozesses für die Bearbeitung von Betroffenenanfragen zur Einschränkung der Verarbeitung. Einsichtnahme in Nachweise über durchgeführte Einschränkungen der Verarbeitung bezogen auf die Einhaltung der Vorgaben.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 09-07	Recht auf Datenübertragbarkeit gemäß Artikel 20 DS-GVO: Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zur Datenübertragbarkeit eingerichtet. Diese beinhalten gemäß Artikel 20 Abs. 4 DS-GVO die Überprüfung der Beeinträchtigung der Rechte Dritter vor Übertragung der Daten. Die Prozesse stellen sicher, dass gemäß Artikel 12 Abs. 1 und 6 DS-GVO die Identität des anfragenden Betroffenen eindeutig bestimmt werden kann Prozesse zur Bereitstellung aller personenbezogenen Daten eines Betroffenen sind in einem strukturierten, gängigen, maschinelesbaren Format definiert und werden konsequent angewendet. Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Beantwortung der Betroffenenanfragen sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Prozessvorgaben zur Bearbeitung von Betroffenenanfragen zur Datenübertragbarkeit. Eine Einsichtnahme in Nachweise über die den Betroffenen zur Verfügung gestellten Daten ist auf Grund des Produkt Scope nicht möglich.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 09-08	Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten gemäß Artikel 21 DS-GVO. Es sind Prozesse für die Bearbeitung von Betroffenenanfragen zum Widerspruch gegen die Verarbeitung eingerichtet. Diese stellen sicher, dass bei einem begründeten Widerspruch keine weitere Verarbeitung der personenbezogenen Daten des Betroffenen vorgenommen wird bzw. anderenfalls eine begründete Ablehnung des Widerspruchs erfolgt sowie die Übermittlung der Begründung an den Betroffenen. Betroffene werden gemäß Artikel 21 Abs. 4 DS-GVO rechtzeitig auf das Recht hingewiesen. Die Prozesse stellen sicher, dass gemäß Artikel 12 Abs. 1 und 6 DS-GVO die Identität des anfragenden Betroffenen eindeutig bestimmt werden kann. Die Fristen gemäß Artikel 12 Abs. 3 DS-GVO für die Bearbeitung der Betroffenenanfragen zum Widerspruch sind den Mitarbeitern bekannt und werden eingehalten.	Prüfung der Prozessvorgaben zur Bearbeitung von Betroffenenanfragen zum Widerspruch gegen die Verarbeitung. Einsichtnahme in die Nachweisführung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 09-09	Es ist ein Prozess eingerichtet, welcher sicherstellt, dass gemäß Artikel 22 DS-GVO die betroffene Person nicht einer Entscheidung unterworfen wird, welche ihr gegenüber rechtlicher Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, soweit diese Entscheidung ausschließlich auf einer automatisierten Verarbeitung (einschließlich Profiling) beruht und keine Ausnahme gemäß Artikel 22 Abs. 2 DS-GVO gilt.	Befragung der zuständigen Mitarbeiter und Erläuterungen von Arbeitsabläufen. Einsichtnahme in Nachweise zu Entscheidungsfindungsprozessen und Beurteilung der Entscheidungsgrundlage.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 10 - Die eingerichteten Verfahren und Maßnahmen stellen mit hinreichender Sicherheit sicher, dass gemäß Artikel 33 DS-GVO Datenschutzverletzungen im Unternehmen identifiziert und bewertet werden sowie bei Vorliegen eines Risikos für die Rechte und Freiheiten des Betroffenen eine Meldung an die Aufsichtsbehörde erfolgt und dass darüber hinaus gemäß Artikel 34 DS-GVO bei Vorliegen eines voraussichtlich hohen Risikos für die Rechte und Freiheiten des Betroffenen eine Benachrichtigung des Betroffenen erfolgt.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 10-01	Es ist ein schriftlich dokumentierter Prozess eingerichtet, welcher eindeutige Regelungen zu Verantwortlichkeiten, Kommunikationswegen und Berichtslinien, der Einbindung des DSB sowie zu folgenden Aktivitäten enthält: - Identifikation von Datenschutzverletzungen, dies schließt die unverzügliche Meldung des AVs an den Auftraggeber ein, wenn dem AV eine Datenschutzverletzung bekannt wird; - Bewertung der Risiken (Risiko-Assessment / Risikoanalyse); - Aufarbeitung des Sachverhalts; - Auswahl geeigneter Maßnahmen (ad-hoc Behebung sowie Vermeidung einer Wiederholung); - Entscheidung über eine Meldung und Meldung an die Aufsichtsbehörde (< 72 Stunden); - Unverzügliche Benachrichtigung des Betroffenen bei voraussichtlich hohem Risiko.	Prüfung der Prozessvorgaben und Befragung von Mitarbeitern über identifizierte und bewertete Datenschutzverletzungen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-02	Es sind Kommunikationswege im Unternehmen definiert, über welche Datenschutzverletzungen (auch anonym) gemeldet werden können. Dies beinhaltet, dass die Anlaufstellen im Unternehmen zur Meldung einer Datenschutzverletzung bekannt und für alle Mitarbeiter erreichbar sind. Die Kommunikationswege berücksichtigen auch die Einbindung der Abteilung Unternehmenskommunikation bzw. einer PR-Agentur. Diesbezüglich ist eine Vorabauswahl möglicher Kooperationspartner erfolgt, um die unverzügliche Information sicherzustellen. Alle anderen relevanten Prozesse, bei welchen Datenschutzverletzungen identifiziert oder registriert werden können, sind mit dem datenschutzrechtlichen Meldeprozess des Unternehmens verknüpft.	Befragung von Mitarbeitern zu Kenntnissen über die Kommunikationswege. Durchsicht der jeweiligen Prozessanweisungen und Beurteilung des Vorhandenseins von Absprungpunkten zum datenschutzrechtlichen Meldeprozess. Identifizierung der Möglichkeit zur anonymen Meldung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-03	Die Risikobewertung gemäß Artikel 33 Abs. 1 und Artikel 34 Abs. 1 DS-GVO fokussiert auf die Risiken für die persönlichen Rechte und Freiheiten des Betroffenen. Hierbei werden Eintrittswahrscheinlichkeit und Schwere des Risikos (z. B. im Hinblick auf die Kategorie von betroffenen Daten) berücksichtigt sowie die ergriffenen technischen und organisatorischen Maßnahmen.	Prüfung der Risikobewertung für ausgewählte Datenschutzverletzungen. Hierbei wurden Eintrittswahrscheinlichkeit und Schwere des Risikos, sowie die ergriffenen technischen und organisatorischen Maßnahmen geprüft.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 10-04	Jede identifizierte bzw. gemeldete Datenschutzverletzung wird zur Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 und Artikel 24 Abs. 1 DS-GVO in einem zentralen Verzeichnis dokumentiert.	Prüfung der Vollständigkeit des zentralen Verzeichnisses der Datenschutzverletzungen einschließlich der Inhalte der Meldungen, Risikoabschätzungen und Kommunikation mit den Betroffenen und den Aufsichtsbehörden.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-05	Die Mindestinhalte der Meldung an die Aufsichtsbehörde sind in Form einer Anweisung oder eines Musterschreibens definiert und berücksichtigen die Anforderungen gemäß Artikel 33 Abs. 3 DS-GVO.	Durchsicht der Anweisungen und des Musterschreibens an die Aufsichtsbehörde.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-06	Die Mindestinhalte der Benachrichtigung des Betroffenen sind in Form einer Anweisung oder eines Musterschreibens definiert und berücksichtigen die Anforderungen gemäß Artikel 34 Abs. 2 DS-GVO.	Einsichtnahme in erfolgte Meldungen an die Betroffenen bezogen auf die Einhaltung der Mindestinhalte.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-07	Die Verfahren und Maßnahmen zur Identifikation, Bewertung und Meldung von Datenschutzverletzungen sind so ausgestaltet, dass die gemäß Artikel 33 Abs. 1 DS-GVO vorgegebene Frist von 72 Stunden eingehalten werden kann. Um den Anforderungen an die Reaktionszeit von 72 Stunden bei einer Meldung an die Aufsichtsbehörde gerecht zu werden, sehen die Prozesse auch Kommunikationswege und Eskalationsmaßnahmen vor, welche außerhalb der Geschäftszeiten ergriffen werden.	Durchsicht der entsprechenden Vorgaben für den DSB und erfolgte Meldungen an die Aufsichtsbehörde.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-08	Die Verfahren und Maßnahmen zur Identifikation und Bewertung von Datenschutzverletzungen sowie zur Benachrichtigung des Betroffenen gemäß Artikel 34 Abs. 1 DS-GVO sind so ausgestaltet, dass unter Berücksichtigung der Ausnahmen gemäß Artikel 34 Abs. 3 DS-GVO eine unverzügliche Benachrichtigung des Betroffenen erfolgt. Soweit eine Weisung der Aufsichtsbehörde oder einer Strafverfolgungsbehörde hinsichtlich des Zeitpunkts der Benachrichtigung vorliegt, wird diese berücksichtigt.	Prüfung der Verfahren und Maßnahmen zur Identifizierung und Bewertung von Datenschutzverletzungen sowie der Benachrichtigung der Betroffenen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.

Kontroll-Nr.	Kontrolle	Prüfungshandlung nbs partners	Prüfungsergebnis
DS-KONTROLLE 10-09	Soweit gemäß Artikel 34 Abs. 3 Buchst. c) DS-GVO eine individuelle Benachrichtigung des Betroffenen mit einem unverhältnismäßigen Aufwand verbunden ist, sind Regelungen vorgesehen, welche eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme ermöglichen. Hierfür sind entsprechende Kooperationspartner (z. B. PR-Agenturen) identifiziert, um eine zeitnahe Umsetzung zu ermöglichen.	Durchsicht der entsprechenden Vorgaben im Unternehmen und der definierten Maßnahmen. Im Prüfungszeitraum haben sich keine relevanten Vorfälle ereignet.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-10	Es sind Prozesse, Verantwortlichkeiten und Schnittstellen definiert, welche es dem Unternehmen ermöglichen, auch Datenschutzverletzungen seiner AV zu identifizieren, zu bewerten, nachweisbar zu dokumentieren und ggf. der Aufsichtsbehörde zu melden bzw. den Betroffenen zu benachrichtigen. AV sind vertraglich verpflichtet, regelmäßig zu berichten, auch wenn keine Datenschutzverletzungen vorliegen.	Durchsicht der entsprechenden Vorgaben bzw. Musterverträge, sowie in die regelmäßige Berichterstattung der Auftragsverarbeiter.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 10-11	Die Verantwortlichen der Fachbereiche und Stäbe bestätigen regelmäßig (mindestens jährlich), dass alle Datenschutzverletzungen in den zentralen Prozess gemeldet wurden bzw. keine Datenschutzverletzungen vorlagen.	Durchsicht der entsprechenden Vorgaben und Nachvollzug der Meldungen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 11 - Die eingerichteten Verfahren und Maßnahmen bieten hinreichende Sicherheit dafür, dass die Verarbeitung personenbezogener Daten durch AV nur in Übereinstimmung mit einem entsprechenden Vertrag oder einem anderen rechtlich verbindlichen Dokument (Verarbeitungsvereinbarung) erfolgt und dass die Verarbeitung nur durch die vom Unternehmen zugelassenen AV durchgeführt wird.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 11-01	Das Unternehmen hat vom AV gemäß Artikel 28 Abs. 1 DS-GVO geeignete Garantien erhalten und geprüft, in welchen zugesichert wird, dass die Verfahren, Maßnahmen und Kontrollen den Anforderungen der DS-GVO entsprechen.	Einsichtnahme in die Dokumentation zu den zugesicherten Garantien und die Nachweise für die Überprüfung.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 11-02	Das Unternehmen hat gemäß Artikel 28 i. V. mit Artikel 29 DS-GVO Anweisungen für die Verarbeitung und den Schutz personenbezogener Daten an den AV erteilt, einschließlich der Verarbeitung durch andere AV (Unterbeauftragung). Diese Anweisungen sind Gegenstand eines schriftlichen Vertrags, welcher die Mindestbestandteile gemäß Artikel 28 Abs. 3 DS-GVO enthält.	Einsichtnahme in Verträge bezogen auf die vollständige Berücksichtigung der Anweisungen und Mindestbestandteile.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 11-03	Die Inanspruchnahme weiterer AV durch den AV (Unterbeauftragung) erfordert gemäß Artikel 28 Abs. 2 DS-GVO die vorherige Zustimmung durch das Unternehmen.	Prüfung der Liste der weiteren AV auf Vollständigkeit und Aktualität (z.B. durch Einholung einer schriftlichen Bestätigung vom AV) und Abgleich mit erfolgten Zustimmungen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
DS-KONTROLLE 11-04	Das Unternehmen überwacht regelmäßig die Einhaltung der vertraglichen Regelungen durch den AV und stellt sicher, dass die Verarbeitung und Gewährleistung der Sicherheit der personenbezogenen Daten bei dem AV nach seinen Vorgaben durchgeführt wird.	Befragung der für die Überwachung des AV verantwortlichen Mitarbeiter und Einsichtnahme in die Dokumentation durchgeführter Überwachungsmaßnahmen.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Anforderung			
DS-Ziel 12 - Die eingerichteten Verfahren und Maßnahmen bieten hinreichende Sicherheit dafür, dass die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation in Übereinstimmung mit den Artikeln 44 bis 49 DS-GVO erfolgt und somit das durch die DS-GVO vorgegebene Schutzniveau eingehalten wird.			
Kontroll-Nr.	**Kontrolle**	**Prüfungshandlung nbs partners**	**Prüfungsergebnis**
DS-KONTROLLE 12-01	Es ist ein schriftlich dokumentierter Prozess eingerichtet, welcher sicherstellt, dass die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation durch das Unternehmen oder den AV nur erfolgt, sofern: - die EU-Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet oder - das Unternehmen oder der AV geeignete Garantien gemäß Artikel 46 DS-GVO vorgesehen hat oder - ein Ausnahmetatbestand gemäß Artikel 49 DS-GVO vorliegt.	Durchsicht der Prozessvorgaben und Einsichtnahme in die Nachweisführung der durchgeführten Maßnahmen. Bewertung des Umsetzungsstandes zur Aktualisierung der AVV gemäß den aktuellen Standardvertragsklauseln.	Wir beurteilen die Kontrolle als angemessen und wirksam. Es wurden keine relevanten Ausnahmen festgestellt.
Basierend auf den oben beschriebenen Kontrollen, beurteilen wir die Prozesse und Aktivitäten als angemessen und wirksam, um das Kontrollziel zu erreichen.			

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2017

DokID:

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im Nachstehenden zusammenfassend „Wirtschaftsprüfer" genannt) und ihren Auftraggebern über Prüfungen, Steuerberatung, Beratungen in wirtschaftlichen Angelegenheiten und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Dritte können nur dann Ansprüche aus dem Vertrag zwischen Wirtschaftsprüfer und Auftraggeber herleiten, wenn dies ausdrücklich vereinbart ist oder sich aus zwingenden gesetzlichen Regelungen ergibt. Im Hinblick auf solche Ansprüche gelten diese Auftragsbedingungen auch diesen Dritten gegenüber.

2. Umfang und Ausführung des Auftrags

(1) Gegenstand des Auftrags ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer übernimmt im Zusammenhang mit seinen Leistungen keine Aufgaben der Geschäftsführung. Der Wirtschaftsprüfer ist für die Nutzung oder Umsetzung der Ergebnisse seiner Leistungen nicht verantwortlich. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf – außer bei betriebswirtschaftlichen Prüfungen – der ausdrücklichen schriftlichen Vereinbarung.

(3) Ändert sich die Sach- oder Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Mitwirkungspflichten des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Wirtschaftsprüfer alle für die Ausführung des Auftrags notwendigen Unterlagen und weiteren Informationen rechtzeitig übermittelt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrags von Bedeutung sein können. Dies gilt auch für die Unterlagen und weiteren Informationen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden. Der Auftraggeber wird dem Wirtschaftsprüfer geeignete Auskunftspersonen benennen.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der weiteren Informationen sowie der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

(1) Der Auftraggeber hat alles zu unterlassen, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährdet. Dies gilt für die Dauer des Auftragsverhältnisses insbesondere für Angebote auf Anstellung oder Übernahme von Organfunktionen und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Sollte die Durchführung des Auftrags die Unabhängigkeit des Wirtschaftsprüfers, die der mit ihm verbundenen Unternehmen, seiner Netzwerkunternehmen oder solcher mit ihm assoziierten Unternehmen, auf die die Unabhängigkeitsvorschriften in gleicher Weise Anwendung finden wie auf den Wirtschaftsprüfer, in anderen Auftragsverhältnissen beeinträchtigen, ist der Wirtschaftsprüfer zur außerordentlichen Kündigung des Auftrags berechtigt.

5. Berichterstattung und mündliche Auskünfte

Soweit der Wirtschaftsprüfer Ergebnisse im Rahmen der Bearbeitung des Auftrags schriftlich darzustellen hat, ist alleine diese schriftliche Darstellung maßgebend. Entwürfe schriftlicher Darstellungen sind unverbindlich. Sofern nicht anders vereinbart, sind mündliche Erklärungen und Auskünfte des Wirtschaftsprüfers nur dann verbindlich, wenn sie schriftlich bestätigt werden. Erklärungen und Auskünfte des Wirtschaftsprüfers außerhalb des erteilten Auftrags sind stets unverbindlich.

6. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Arbeitsergebnisse oder Auszüge von Arbeitsergebnissen – sei es im Entwurf oder in der Endfassung) oder die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, es sei denn, der Auftraggeber ist zur Weitergabe oder Information aufgrund eines Gesetzes oder einer behördlichen Anordnung verpflichtet.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers und die Information über das Tätigwerden des Wirtschaftsprüfers für den Auftraggeber zu Werbezwecken durch den Auftraggeber sind unzulässig.

7. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen, Unterlassen bzw. unberechtigter Verweigerung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung kann er die Vergütung mindern oder vom Vertrag zurücktreten; ist der Auftrag nicht von einem Verbraucher erteilt worden, so kann der Auftraggeber wegen eines Mangels nur dann vom Vertrag zurücktreten, wenn die erbrachte Leistung wegen Fehlschlagens, Unterlassung, Unzumutbarkeit oder Unmöglichkeit der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muss vom Auftraggeber unverzüglich in Textform geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z.B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse infrage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

8. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze (§ 323 Abs. 1 HGB, § 43 WPO, § 203 StGB) verpflichtet, über Tatsachen und Umstände, die ihm bei seiner Berufstätigkeit anvertraut oder bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer wird bei der Verarbeitung von personenbezogenen Daten die nationalen und europarechtlichen Regelungen zum Datenschutz beachten.

9. Haftung

(1) Für gesetzlich vorgeschriebene Leistungen des Wirtschaftsprüfers, insbesondere Prüfungen, gelten die jeweils anzuwendenden gesetzlichen Haftungsbeschränkungen, insbesondere die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Sofern weder eine gesetzliche Haftungsbeschränkung Anwendung findet noch eine einzelvertragliche Haftungsbeschränkung besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, sowie von Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen, bei einem fahrlässig verursachten einzelnen Schadensfall gemäß § 54a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt.

(3) Einreden und Einwendungen aus dem Vertragsverhältnis mit dem Auftraggeber stehen dem Wirtschaftsprüfer auch gegenüber Dritten zu.

(4) Leiten mehrere Anspruchsteller aus dem mit dem Wirtschaftsprüfer bestehenden Vertragsverhältnis Ansprüche aus einer fahrlässigen Pflichtverletzung des Wirtschaftsprüfers her, gilt der in Abs. 2 genannte Höchstbetrag für die betreffenden Ansprüche aller Anspruchsteller insgesamt.

(5) Ein einzelner Schadensfall im Sinne von Abs. 2 ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(6) Ein Schadensersatzanspruch erlischt, wenn nicht innerhalb von sechs Monaten nach der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde. Dies gilt nicht für Schadensersatzansprüche, die auf vorsätzliches Verhalten zurückzuführen sind, sowie bei einer schuldhaften Verletzung von Leben, Körper oder Gesundheit sowie bei Schäden, die eine Ersatzpflicht des Herstellers nach § 1 ProdHaftG begründen. Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt.

10. Ergänzende Bestimmungen für Prüfungsaufträge

(1) Ändert der Auftraggeber nachträglich den durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschluss oder Lagebericht, darf er diesen Bestätigungsvermerk nicht weiterverwenden.

Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfasst nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, dass der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Fall hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, dass dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfasst die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 Buchst. d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Sofern der Wirtschaftsprüfer auch Steuerberater ist und die Steuerberatervergütungsverordnung für die Bemessung der Vergütung anzuwenden ist, kann eine höhere oder niedrigere als die gesetzliche Vergütung in Textform vereinbart werden.

(6) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrags. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z.B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen,

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlungen, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen und

d) die Unterstützung bei der Erfüllung von Anzeige- und Dokumentationspflichten.

(7) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzugs wird nicht übernommen.

12. Elektronische Kommunikation

Die Kommunikation zwischen dem Wirtschaftsprüfer und dem Auftraggeber kann auch per E-Mail erfolgen. Soweit der Auftraggeber eine Kommunikation per E-Mail nicht wünscht oder besondere Sicherheitsanforderungen stellt, wie etwa die Verschlüsselung von E-Mails, wird der Auftraggeber den Wirtschaftsprüfer entsprechend in Textform informieren.

13. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Ist der Auftraggeber kein Verbraucher, so ist eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

14. Streitschlichtungen

Der Wirtschaftsprüfer ist nicht bereit, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle im Sinne des § 2 des Verbraucherstreitbeilegungsgesetzes teilzunehmen.

15. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.