Bericht

des

Externen Datenschutzbeauftragten

der

d.vinci HR-Systems GmbH
Nagelsweg 37-39, 20097 Hamburg

d.vinci Personalmarketing GmbH
Nagelsweg 37-39, 20097 Hamburg

- nachfolgend „d. vinci-Gruppe“ –

über seine Tätigkeit im Geschäftsjahr 2024

GCS – Geno Corporate Services GmbH
Türkenstraße 22 – 24
80333 München

Inhaltsverzeichnis

1. Zusammenfassung – Management Summary ... 3
2. Allgemeine Angaben ... 6
2.1. Auftragsverhältnis ... 6
2.2. Berichtsadressaten ... 6
2.3. Tätigkeitsumfang ... 6
3. Organisation des Datenschutzmanagements ... 7
3.1. Datenschutzbeauftragter ... 7
3.2. Rahmenbedingungen für die Tätigkeit ... 7
3.3. Datenschutz und Informationssicherheit ... 10
3.4. Kontroll- und Überwachungskonzept ... 10
4. Sicherstellung der Ausführung der DSGVO und anderer Vorschriften zum Datenschutz ... 12
4.1. Verantwortlichkeiten und Sensibilisierung ... 12
4.1.1. Regelungen ... 12
4.1.2. Vermittlung maßgeblicher Datenschutzvorschriften - Mitarbeitersensibilisierung ... 12
4.1.3. Datenschutzmanagement im Sinne eines Regelkreislaufes ... 13
4.1.4. Kontrollen durch die Aufsichtsbehörde (Art. 58 DSGVO) ... 14
4.1.5. Prüfung des Datenschutzbeauftragten - Ergebnisse interner und externer Prüfungen zum Datenschutz ... 15
4.2. Umsetzung der Verarbeitungstätigkeiten ... 15
4.2.1. Geplante Datenverarbeitungsvorhaben ... 15
4.2.2. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen - Privacy by Design und Privacy by Default (Art. 25 DSGVO) ... 15
4.2.3. Rechtmäßigkeit der Datenverarbeitung (Art. 6 Abs. 1 DSGVO) ... 16
4.2.4. Datenübermittlung in Drittstaaten (Art. 44 bis 50 DSGVO) ... 16
4.2.5. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) ... 16
4.2.6. Digitales Datenschutzmanagement (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO) ... 16
4.2.7. Datenschutzfolgenabschätzung (Art. 35 DSGVO) ... 17
4.2.8. Besondere Verarbeitungstätigkeiten ... 18
4.2.8.1. Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses (Art. 88 Abs. 1 DSGVO i.V.m. § 26 BDSG) ... 18
4.2.8.2. Prüfung beim Einsatz von optisch-elektronischen Überwachungseinrichtungen (§ 4 Abs. 2 BDSG) ... 18
4.2.8.3. Verarbeitung personenbezogener Daten für Werbung ... 18
4.2.8.4. Scoring-Systeme (Art. 4 Abs. 4 DSGVO, § 31 Abs. 1 Nr. 1 BDSG) ... 18
4.2.8.5. Datenträgerentsorgung bzw. -vernichtung nach DSGVO (DIN 66399) ... 18
4.3. Einbindung Externer ... 19
4.3.1. Auftragsverarbeitung als Auftraggeber (Art. 28 DSGVO) ... 19
4.3.2. Auftragsverarbeitung als Auftragnehmer (Art. 28 DSGVO) ... 19
4.4. Transparenzpflichten und Betroffenenrechte ... 19
4.4.1. Informationspflichten gem. Art. 13, 14 und 21 DSGVO ... 19
4.4.2. Geltendmachung von Betroffenenrechten (Art. 15 bis 21 DSGVO) ... 19
4.4.3. Datenschutzvorfälle (Art. 33 und 34 DSGVO) ... 20
5. Planung 2025 ... 23

1. Zusammenfassung – Management Summary

1 Das Jahr 2024 war von weitreichenden Entwicklungen im Datenschutzrecht geprägt, die sowohl auf nationaler als auch auf europäischer Ebene neue Maßstäbe gesetzt haben. Diese Veränderungen spiegeln die zunehmende Bedeutung des Schutzes personenbezogener Daten in einer digitalisierten und vernetzten Welt wider und erfordern von Unternehmen und Organisationen erhebliche Anpassungen ihrer Prozesse, Technologien und organisatorischen Maßnahmen.

2 Besonders hervorzuheben sind die gesetzlichen Neuerungen, die mit der **NIS-2-Richtlinie** in Kraft getreten sind. Die NIS-2-Richtlinie zielt darauf ab, die Cybersicherheit innerhalb der Europäischen Union zu stärken und den Schutz kritischer Infrastrukturen vor Cyberangriffen und anderen Sicherheitsrisiken zu verbessern. Unternehmen, die als Betreiber wesentlicher Dienste klassifiziert sind, stehen vor der Herausforderung, strenge Vorgaben zur Netz- und Informationssicherheit umzusetzen. Dabei liegt der Fokus nicht nur auf der Absicherung interner Systeme, sondern auch auf der Überwachung von Drittanbietern, die in die digitale Wertschöpfungskette eingebunden sind.

3 Auf nationaler Ebene hat die Bundesregierung zudem mit der **Novellierung des Bundesdatenschutzgesetzes** wichtige Schritte unternommen, um den Datenschutz zu modernisieren. Diese Änderungen betreffen unter anderem die Nutzung von Scoring-Verfahren und die Harmonisierung der Datenschutzaufsicht.

4 Neben diesen regulatorischen Entwicklungen prägten auch **richtungsweisende Gerichtsentscheidungen** das datenschutzrechtliche Umfeld. Der Europäische Gerichtshof hat insbesondere mit seinen Urteilen zur Nutzung von Scoring-Methoden und zum Datentransfer in Drittstaaten für Klarheit, aber auch für neue Herausforderungen gesorgt. Unternehmen müssen sich verstärkt mit den Anforderungen an Datenschutzkonformität bei automatisierten Entscheidungsprozessen und den verschärften Vorgaben für den internationalen Datenaustausch auseinandersetzen.

5 Diese Entwicklungen verdeutlichen, dass der Schutz personenbezogener Daten anspruchsvoller und umfassender geworden ist. Unternehmen stehen vor der Aufgabe, die neuen gesetzlichen und rechtlichen Anforderungen nicht nur zu erfüllen, sondern gleichzeitig das Vertrauen ihrer Kunden, Geschäftspartner und Mitarbeitenden in den Datenschutz zu stärken.

6 Im **Datenschutzmanagementsystem** werden wesentliche Anforderungen des Datenschutzrechtes implementiert. Hierzu zählen neben der Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO auch die risikoorientierte Prüfung datenschutzrelevanter Prozesse und Datenverarbeitungen. Aus den Prüfungshandlungen für das Berichtsjahr ergaben sich keine relevanten Feststellungen.

7 Wesentliche Veränderungen in der d.vinci-Gruppe mit datenschutzrechtlicher Relevanz sind im Berichtszeitraum nicht eingetreten.

8 Eine Informationspflicht durch die d.vinci-Gruppe an die zuständige Datenschutzaufsichtsbehörde und ggf. die betroffenen Personen aufgrund unrechtmäßiger Kenntniserlangung von Daten durch Dritte im Sinne der Artikel 33 resp. 34 DSGVO waren im Berichtszeitraum nicht erforderlich.

9 Datenpannen im Sinne der Artikel 33 resp. 34 DSGVO seitens der zum Einsatz kommenden Auftragsverarbeitungsnehmer mit Auswirkungen auf die verantwortliche Stelle lagen im Berichtszeitraum nicht vor.

10 Die Tätigkeiten des Datenschutzbeauftragten haben ergeben, dass **Datenschutzmaßnahmen** in der d.vinci-Gruppe in angemessenem Umfang vorhanden sind.

11 Gleichwohl konnten einzelne Anregungen zum Datenschutz zur Ergänzung der Maßnahmen in Teilbereichen beitragen. Diese Anregungen wurden jeweils direkt mit der Unternehmensleitung oder den betreffenden Prozessverantwortlichen besprochen.

12 Die d.vinci-Gruppe hat ein den Anforderungen des deutschen Datenschutzrechtes entsprechendes, angemessenes Datenschutzmanagementsystem etabliert.

13 Es besteht zudem ein Informationssicherheitskonzept, welches den Schutzbedarf, das umgesetzte Schutzniveau und die vorhandenen Sicherheitsmaßnahmen dokumentiert. Es gibt Regelvorgehensweisen zum Umgang mit Datenschutz- und Informationssicherheitsvorfällen.

14 Der Einsatz von Microsoft 365 wird von den Datenschutzaufsichtsbehörden weiterhin kritisch bewertet, insbesondere hinsichtlich der Verarbeitung personenbezogener Daten in Drittstaaten (z. B. den USA) und der Einhaltung der DSGVO. Hauptkritikpunkte sind die unzureichende Transparenz bei der Datenverarbeitung durch Microsoft und die Zugriffsmöglichkeit durch US-Behörden gemäß dem Cloud Act. In ihren Bewertungen betonen die Datenschutzbehörden, dass Unternehmen besondere technische, organisatorische und vertragliche Maßnahmen umsetzen müssen, um M365 DSGVO-konform zu nutzen.

Maßnahmen für die datenschutzkonforme Nutzung von M365 sind im Wesentlichen:

- Datenschutz-Folgenabschätzung (DSFA):
  Durchführung einer DSFA gemäß Art. 35 DSGVO, um die potenziellen Risiken für personenbezogene Daten zu analysieren und zu minimieren.
- Einsatz von EU-Standort-Optionen:
  Nutzung der "EU Data Boundary"-Funktion von Microsoft, um sicherzustellen, dass Daten innerhalb des Europäischen Wirtschaftsraums verarbeitet werden.
- Vertragliche Regelungen:
  Abschluss eines Auftragsverarbeitungsvertrags (AVV) mit Microsoft.
  Überprüfung und Anpassung der Standardvertragsklauseln (SCC) an die aktuellen Vorgaben.
- Technische Maßnahmen:
  Verschlüsselung sensibler Daten (end-to-end) durch das Unternehmen, sodass Microsoft keinen Zugriff hat.
  Nutzung von lokalen Verschlüsselungsschlüsseln, die ausschließlich das Unternehmen kontrolliert.
- Minimierung von Datenverarbeitung:
  Anpassung der M365-Einstellungen, um den Umfang der verarbeiteten personen-bezogenen Daten zu reduzieren (z. B. Deaktivierung von Telemetrie-Daten).
  Regelmäßige Audits:
  Überprüfung der Datenschutzmaßnahmen und der Einhaltung der vertraglichen Vereinbarungen durch Microsoft.
- Schulungen und Sensibilisierung:
  Schulung der Mitarbeitenden im Umgang mit M365, insbesondere in Bezug auf Datenschutz und Datensicherheit.

Der Einsatz von Microsoft 365 ist aus datenschutzrechtlicher Sicht eine Herausforderung, kann jedoch durch eine Kombination aus technischen, organisatorischen und vertraglichen Maßnah-

men potenziell konform gestaltet werden. Eine Umsetzung der Maßnahmen sowie deren Auditierung ist im Berichtsjahr erfolgt. Eine Überwachung der risikominimierenden Maßnahmen ist als fortlaufende Tätigkeit Bestandteil des Tätigkeits- und Auditplanes.

15 Die Arbeitspapiere und -unterlagen der Datenschutzbeauftragten werden elektronisch innerhalb des Datenschutzmanagementsystems otris privacy geführt und sind mindestens fünf Jahre aufzubewahren.

16 Den Jahresbericht der Datenschutzbeauftragten haben wir zur Kenntnis genommen.

Nina Rahn

Certified by yousign

Datum	Nina Rahn

Tobias Tiedgen

Certified by yousign

Datum	Tobias Tiedgen

2. Allgemeine Angaben

2.1. Auftragsverhältnis

17 Auf Basis eines Dienstleistungsvertrages hat die d.vinci-Gruppe - im Folgenden auch Gesellschaft genannt - der Geno Corporate Services GmbH - im Folgenden auch GCS genannt - die Stellung eines externen Datenschutzbeauftragten übertragen.

2.2. Berichtsadressaten

18 Adressat dieses Tätigkeitsberichtes ist die Geschäftsführung.

19 Dieser Bericht bezieht sich auf den Zeitraum 1. Januar bis 31. Dezember 2024.

2.3. Tätigkeitsumfang

20 Den Aufgaben als Datenschutzbeauftragter ist Herr Frank Gundlach in der d.vinci-Gruppe sowie darüber hinaus am Dienstsitz nachgekommen. Darüber hinaus stand er dem Unternehmen jederzeit als Ansprechpartner per E-Mail, Telefon oder virtueller Webkonferenzsoftware zur Verfügung.

21 Der Datenschutzbeauftragte konnte im Rahmen seiner Tätigkeit die Prüfungsergebnisse des internen Informationssicherheitsbeauftragten sowie des internen ISO-27001-Audits weitgehend verwerten.

3. Organisation des Datenschutzmanagements

3.1. Datenschutzbeauftragter

22 Auf Basis des bestehenden Dienstleistungsvertrages wurde Herr Frank Gundlach zum Datenschutzbeauftragten der d.vinci-Gruppe benannt. Die Bestellungsurkunde ist bei den Arbeitsunterlagen des Datenschutzbeauftragten abgelegt. Diese dient zur Dokumentation wesentlicher Angaben zum Datenschutzmanagement im Sinne der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO.

23 Die Fachkunde des Datenschutzbeauftragten wird laufend durch Schulungen und Fachliteratur aufrechterhalten. Der aktuelle Fachkundenachweis ist im Datenschutzmanagementsystem otris privacy hinterlegt.

24 Als interner Datenschutzkoordinator für Fragen zu Themen mit Datenschutzrelevanz stand im Berichtsjahr Herr Matthias Blenski zur Verfügung.

25 Die Tätigkeit des Datenschutzbeauftragten bildete 2024 folgende Schwerpunkte:

- Weiterführung und Pflege des Datenschutzmanagementsystems (Erfüllung der Rechenschaftspflichten nach Art. 5 DSGVO
- Tätigkeiten im Rahmen der Anwendung der DSGVO und des BDSG
- Information der Mitarbeiter (Bereitstellung von Newslettern)
- Unterstützung im Rahmen der Umsetzung organisatorischer und technischer Maßnahmen im Sinne des Art. 32 DSGVO
- Prüfung der Unternehmenswebsite unter Einbezug automatisierter Tools
- Beratende Unterstützung bei der Einführung neuer aufsichtsrechtlicher Anforderungen sowie neuer datenschutzrelevanter Verfahren
- Zusammenarbeit mit IT-Dienstleistern sowie Auftragsverarbeitern
- Beratungen zu Sachverhalten mit Bezug zum Datenschutz
- Durchführung von Audit-Tätigkeiten im Rahmen des festgelegten Auditprogramms
- Berichterstattung/Reporting

3.2. Rahmenbedingungen für die Tätigkeit

26 Die Rahmenbedingungen für die Tätigkeit des betrieblichen Datenschutzbeauftragten sowie die datenschutzrechtlichen und innerbetrieblichen organisatorischen Anweisungen ergeben sich aus den nachstehend aufgeführten gesetzlichen Regularien, Verordnungen, Standards und Richtlinien, der organisatorischen Vorgaben und dem im Rahmen des geschlossenen Dienstleistungsvertrages geltenden Schnittstellenplanes. Diese Grundlagen werden seitens des Datenschutzbeauftragten regelmäßig gewürdigt und bei Bedarf aktualisiert.

27 Die Erstellung der darauf beruhenden organisatorischen Regelungen wurde seitens des betrieblichen Datenschutzbeauftragten begleitet.

28 Folgende gesetzliche Regelungen (Auszug) sind im Unternehmen anzuwenden:

- EU-Datenschutzgrundverordnung (DSGVO)
- Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) (BDSG -nationales Auffanggesetz als Ergänzung zur DSGVO) vom 20. September 2019

- Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)
- Bürgerliches Gesetzbuch (BGB), Handelsgesetzbuch (HGB), Abgabenordnung (AO),
- Gesetz gegen den unlauteren Wettbewerb (UWG), Betriebsverfassungsgesetz (BetrVG), Allgemeines Gleichbehandlungsgesetz (AGG), Kunsturheberrechtsgesetz (KunstUrhG), Sozialgesetzbuch SGB IX

29 Verordnungen, Standards und Richtlinien

- Grundsätze ordnungsmäßiger Buchführung, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
- IT-Grundschutz-Kompendium und Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- DIN EN ISO/IEC 270xx Reihe

30 IDW-Standards und –Prüfungshinweise

- PS 330, PS 860, PS 880 und PS 951
- PH 9.330.1 -3
- PH 9.860.1 (Prüfungen nach DSGVO und BDSG)
- Fachausschuss für Informationstechnologie (FAIT) 1 bis 5

31 Interne Regelwerke

- Datenschutzrichtlinie
- IT-Benutzerrichtlinie
- Informationssicherheitskonzept
- Konzept zur Löschung personenbezogener Daten
- Richtlinie zur Nutzung von Internet und E-Mail
- Soll-Berechtigungskonzepte
- weitere relevante aufbau- und ablauforganisatorische Grundlagen der Gesellschaft

32 Folgende aktuelle Veränderungen der aufsichtsrechtlichen sowie gesetzlichen Rahmenbedingungen nehmen Einfluss auf die Umsetzung des Datenschutzkonzeptes in der d.vinci-Gruppe und machen Anpassungen sowie eine Weiterentwicklung notwendig. Es ist aufgrund dessen mit dauerhaft erhöhten Ressourcen in diesem Zusammenhang zu rechnen.

- <u>Novellierung des Bundesdatenschutzgesetzes</u>

  Die Novellierung des Bundesdatenschutzgesetzes (BDSG) befindet sich derzeit im Gesetzgebungsverfahren. Am 15. Mai 2024 wurde der Gesetzentwurf der Bundesregierung in erster Lesung im Bundestag beraten und anschließend an die zuständigen Ausschüsse überwiesen. Zuvor hatte das Bundeskabinett am 7. Februar 2024 den Entwurf zur Änderung des BDSG beschlossen. Dieser Entwurf zielt darauf ab, Vereinbarungen des Koalitionsvertrags umzusetzen und Ergebnisse der Evaluierung des BDSG zu berücksichtigen. Wesentliche Punkte des Entwurfs sind:

  a. Institutionalisierung der Datenschutzkonferenz (DSK): Die DSK soll im BDSG verankert werden, um eine einheitlichere Anwendung des Datenschutzrechts zu fördern.

b. Verbesserte Zusammenarbeit der Aufsichtsbehörden: Unternehmen und Forschungseinrichtungen mit länderübergreifenden Datenverarbeitungsprojekten sollen die Möglichkeit erhalten, nur einer einzigen Aufsichtsbehörde unterstellt zu sein, um Rechtsunsicherheiten zu vermeiden.
c. Neuregelungen zum Scoring: Nach einem Urteil des Europäischen Gerichtshofs vom Dezember 2023 sollen beim Scoring bestimmte Daten, wie ethnische Herkunft oder Gesundheitsdaten, nicht mehr verwendet werden dürfen.

Der Gesetzentwurf befindet sich aktuell in der parlamentarischen Beratung. Ein genauer Zeitpunkt für das Inkrafttreten der Änderungen steht noch nicht fest.

- Beschäftigtendatengesetz (BeschDG)

  Derzeit befindet sich der Entwurf für ein eigenständiges Beschäftigtendatengesetz (BeschDG) in der Abstimmungsphase. Am 8. Oktober 2024 legten das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Innern und für Heimat (BMI) einen Referentenentwurf vor.

  Dieser Entwurf zielt darauf ab, klare Regelungen für den Umgang mit Beschäftigtendaten zu schaffen und die Persönlichkeitsrechte der Beschäftigten in der digitalen Arbeitswelt zu schützen. Er umfasst unter anderem Bestimmungen zur Verarbeitung personenbezogener Daten im Bewerbungsverfahren, während des Arbeitsverhältnisses und nach dessen Beendigung. Zudem werden Regelungen zum Einsatz von Künstlicher Intelligenz (KI) und zur Überwachung am Arbeitsplatz vorgeschlagen.

  Ein konkreter Zeitplan für die Verabschiedung des Gesetzes liegt noch nicht vor.

- Data Act (DA)

  Der europäische Data Act, der am 13. Dezember 2023 verabschiedet wurde, tritt am 12. September 2025 in Kraft. Dieses Gesetz zielt darauf ab, den Zugang zu und die Nutzung von Daten innerhalb der EU zu harmonisieren und zu fördern. Unternehmen sollten sich frühzeitig mit den neuen Verpflichtungen vertraut machen, um eine reibungslose Umsetzung sicherzustellen.

- Umsetzung der NIS-2-Richtlinie i.V.m. Digital Operational Resilience Act (DORA)

  Die NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) wurde am 27. Dezember 2022 im Amtsblatt der Europäischen Union veröffentlicht und trat am 16. Januar 2023 in Kraft. Die EU-Mitgliedstaaten sind verpflichtet, die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen. In Deutschland befindet sich die Umsetzung der NIS-2-Richtlinie derzeit im Gesetzgebungsverfahren. Am 7. Oktober 2024 legte die Bundesregierung einen wiederholt angepassten Gesetzentwurf zur Umsetzung der NIS-2-Richtlinie vor.

  Aktuell ist mit einem Inkrafttreten des entsprechenden Gesetzes vor Juni 2025 nicht zu rechnen.

  NIS-2 stärkt die Cybersicherheit und schützt personenbezogene Daten, indem es Organisationen verpflichtet, ihre IT-Systeme und Netzwerke gegen Cyberbedrohungen abzusichern und Sicherheitsvorfälle zu melden. Es ergänzt damit die Datenschutz-Grundverordnung (DSGVO) durch sektorübergreifende Sicherheitsstandards.

3.3. Datenschutz und Informationssicherheit

33 Der betriebliche Datenschutz ist innerhalb der d.vinci-Gruppe eng mit dem implementierten Informationssicherheitsmanagementsystem verzahnt.

34 Der betriebliche Datenschutzbeauftragte der d.vinci-Gruppe kontrolliert eigenständig die Einhaltung des Datenschutzes, bildet aber auch das Bindeglied zwischen der eigenverantwortlichen Gesetzesanwendung durch die Daten verarbeitende Stelle auf der einen und der staatlichen Kontrolle auf der anderen Seite.

35 Den Wechselwirkungen und Synergien zwischen Datenschutz- und Informationssicherheitsprozess werden innerhalb der d.vinci-Gruppe in besonderem Maße Rechnung getragen.

36 Zur Umsetzung und Einhaltung datenschutzrelevanter Vorgaben wurde ein Datenschutzmanagementsystem implementiert.

37 Die Einhaltung der technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO gewährleisten eine angemessene Sicherheit nach dem Stand der Technik.

38 Durch die Prozessüberwachung im Informationssicherheitsmanagement werden datenschutzrelevante Sachverhalte überprüft bzw. im Rahmen der Datenschutzfolgenabschätzung auf Zulässigkeit und Konformität bewertet.

39 Der Umsetzungsstand des Datenschutzkonzeptes inklusive der Dokumentation der technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO kann dem Datenschutzmanagementsystem otris privacy entnommen werden.

3.4. Kontroll- und Überwachungskonzept

40 Mit der Durchführung von Datenschutz-Audits wird die Zielsetzung verfolgt, dass einerseits die Einhaltung der externen und internen Datenschutzanforderungen überwacht wird und andererseits Verbesserungspotentiale bei der Umsetzung der Datenschutzanforderungen im Rahmen des kontinuierlichen Verbesserungsprozesses identifiziert werden.

41 Die Datenschutzaufbauorganisation bildet die Grundlage für die Umsetzung der Datenschutzvorgaben. Hier erfolgt das Bekenntnis der Unternehmensleitung zum Datenschutz und es werden Verantwortlichkeiten und Zuständigkeiten für die einzelnen Aufgaben zur Umsetzung der Datenschutzvorschriften definiert und in einer Datenschutzrichtlinie festgelegt.

42 Darüber hinaus sind Datenschutzprozesse erforderlich, beispielsweise zur Wahrung der Rechte der Betroffenen oder die Reaktion auf Datenschutzvorfälle.

43 Aufgrund ihres Stellenwertes werden die Datenschutzaufbauorganisation und die Datenschutzprozesse hinsichtlich Angemessenheit und Wirksamkeit regelmäßig geprüft.

44 Da in der Regel eine Vielzahl von Verarbeitungen vorhanden und diese durch unterschiedliche Risiken geprägt sind, erfolgt die Planung von Datenschutz-Audits bei den einzelnen Verarbeitungen wegen begrenzter Prüfungskapazitäten risikoorientiert. Dies dient auch dem Zweck, dass gegenüber Dritten (z. B. der Aufsichtsbehörde) der Planungsprozess dargestellt werden kann und

damit die Entscheidungen bezüglich der Veranlassung von Datenschutz-Audits nachvollziehbar sind.

45 Bei der Planung und Durchführung der Kontroll- und Überwachungstätigkeiten orientieren wir uns grundsätzlich am IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der Datenschutz-Grundverordnung und dem BDSG (IDW PH 9.860.1).

4. Sicherstellung der Ausführung der DSGVO und anderer Vorschriften zum Datenschutz

4.1. Verantwortlichkeiten und Sensibilisierung

4.1.1. Regelungen

46 Eine interne Datenschutzrichtlinie auf Basis der DSGVO sowie dem BDSG wurde im Rahmen der Umsetzung der DSGVO veröffentlicht und wird seitens des Datenschutzbeauftragten regelmäßig auf Aktualität geprüft. Die Kenntnisnahme der Datenschutzrichtlinie wird durch die Beschäftigten schriftlich bestätigt.

47 Der Datenschutzbeauftragte berichtet mindestens einmal jährlich in Form eines Jahresberichtes an die Geschäftsleitung.

48 Örtlich zuständige Aufsichtsbehörde für den nichtöffentlichen Bereich im Datenschutz ist der

Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Thomas Fuchs
Ludwig-Erhard-Str. 22
20459 Hamburg.

49

4.1.2. Vermittlung maßgeblicher Datenschutzvorschriften - Mitarbeitersensibilisierung

50 Alle Mitarbeiter der d.vinci-Gruppe werden bei der Einstellung schriftlich auf die Verschwiegenheit verpflichtet. Die Verpflichtungserklärungen werden nachweislich zu den Personalunterlagen genommen.

51 Es besteht ein Schulungs- und Sensibilisierungskonzept zum Datenschutz und der Informationssicherheit für die Beschäftigten der d.vinci-Gruppe.

52 Sofern sich Vorfälle ereignen sollten, die auf ein mangelndes Bewusstsein für den Datenschutz schließen lassen, sind im Rahmen des Datenschutzmanagementsystems gesonderte Präsenzschulungen für diese betroffenen Bereiche vorgesehen. Schulungsbedarfe dieser Art waren innerhalb des Berichtszeitraumes nicht erforderlich.

53 Dem Datenschutzbeauftragten sind aus seiner Überwachungstätigkeit im Jahr 2024 keine Sachverhalte aufgefallen, die auf Schulungsdefizite der betroffenen Mitarbeiter hätten schließen lassen.

54 Durch den Datenschutzbeauftragten wurden im Jahr 2024 mittels Newsletter bzw. Ad-hoc-Meldung an die d.vinci-Gruppe folgende Informationen zur Verfügung gestellt:

- [2024-12-09] DATENSCHUTZ-INFO | Phishing und Spoofing: So schützen Sie sich im digitalen Alltag
- [2024-12-04] DATENSCHUTZ-INFO | Recht am eigenen Bild einfach erklärt
- [2024-11-22] DATENSCHUTZ-INFO | Zahl der Woche // Gefälschte QR-Codes an Parkautomaten

- [2024-11-04] DATENSCHUTZ-INFO | Passwörter sicher generieren und verwalten mit einem Passwort-Manager
- [2024-10-28] DATENSCHUTZ-INFO | Moderne Authentifizierung: Methoden, Sicherheit und Risiken
- [2024-08-21] DATENSCHUTZ-INFO | Führerscheinkontrolle durch Arbeitgeber: Das ist zu beachten !
- [2024-07-04] Bundeslagebild Cybercrime – wie Cyberkriminelle vorgehen
- [2024-05-22] E-Mail-Postfach: Die Alternativen zur Abwesenheitsnotiz
- [2024-04-02] E-Mail-Disclaimer & -Signaturen: Überflüssig oder Pflicht?
- [2024-03-14] Warum ist Spear-Phishing besonders gefährlich?
- [2024-03-11] - Aufbewahrung von Unterlagen arbeitsmedizinischer Vorsorgen
- [2024-02-15] Effektive Strategien für den Umgang mit E-Mail-Konten abwesender oder ausgeschiedener Mitarbeiter
- [2024-02-07] Online-Vorstellungsgespräch: Datenschutz beim Videointerview
- [2024-01-18] Das Medienprivileg zw. Datenschutz und Meinungsfreiheit
- [2024-01-08] True Crime in Paderborn – Plötzlich stand alles still

4.1.3. Datenschutzmanagement im Sinne eines Regelkreislaufes

55 Mit der Planung, Konzeption und Umsetzung des Datenschutzmanagementsystems wurde unmittelbar zum Inkrafttreten der DSGVO (05.2018) begonnen.

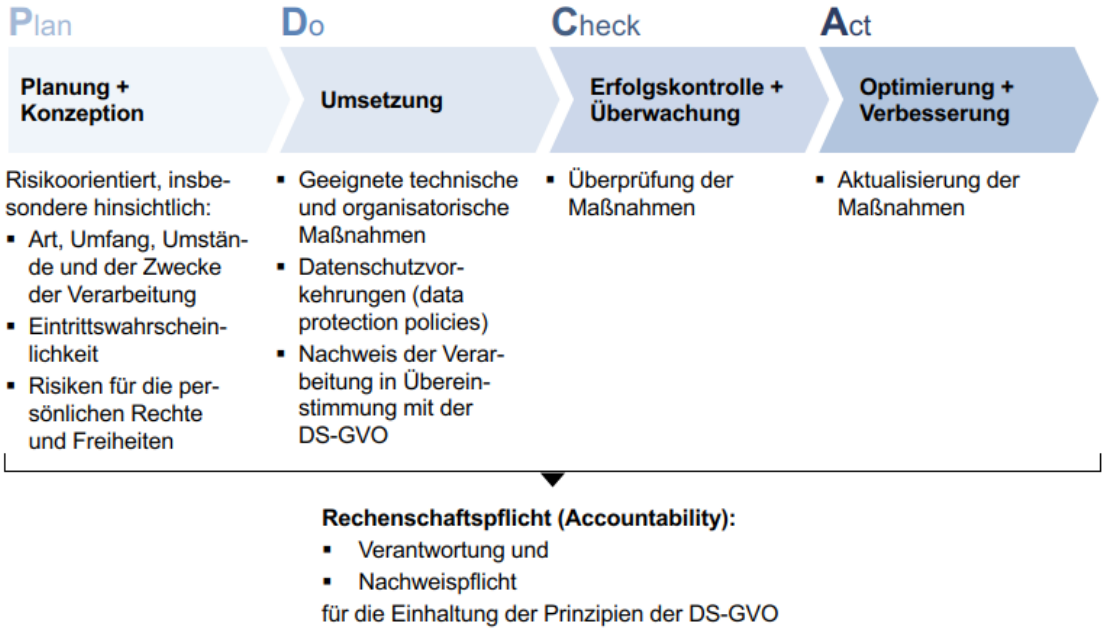
56 Das Datenschutzmanagementsystem befindet sich im PDCA-Zyklus und wird wie folgt umgesetzt bzw. weiterentwickelt:

- Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten
- Verpflichtung / Unterrichtung der Beschäftigten bei der Verarbeitung personenbezogener Daten
- Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten
- Prüfung rechtlicher Rahmenbedingungen und Datenschutzfolgenabschätzung bei der Verarbeitung personenbezogener Daten
- Dokumentation des Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO
- Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten
- Regelungen zur Auftragsverarbeitung bei der Verarbeitung personenbezogener Daten
- Aufrechterhaltung des Datenschutzes im laufenden Betrieb
- Datenschutzaspekte bei der Protokollierung
- Datenschutzgerechte Löschung/Vernichtung/Entsorgung
- Überwachung und Auditierung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

57 Mit dem implementierten Datenschutzmanagementsystem wird sichergestellt, dass

- formale Anforderungen umgesetzt bzw. neue Anforderungen implementiert werden

- relevante Audits auf Basis eine Auditplanes durchgeführt werden
- datenschutzrelevante Prüffelder im risikoorientierten Focus des Datenschutzbeauftragten bleiben



58 Das Datenschutzmanagementsystem dient der Unterstützung des Datenschutzbeauftragten, der Umsetzung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO und ist für das Unternehmen (= Verantwortliche Stelle) in der Anwendung otris privacy abgebildet.

59 Folgende Prüfungshandlungen wurden im Rahmen des Datenschutzmandates durchgeführt:

- Datenschutzrechtliche Betrachtung des Zugriffes auf Mitarbeiterdaten
- Datenschutzrechtliche Prüfung des Internetauftritts
- Datenschutzrechtliche Betrachtung der Personalabteilung
- Datenschutzrechtliche Prüfung Vernichtung von Daten
- Standortbegehungen unter Datenschutz-Aspekten (Verwaltungssitz Nagelsweg als auch externes RZ pop-interactive GmbH, Hamburg)
- DSGVO-Compliance-Check (für Auftragsverarbeiter in Verbindung mit dem GCS-Zertifikat)

60 Über die Auditergebnisse wurden gesonderte Berichte erstellt.

4.1.4. Kontrollen durch die Aufsichtsbehörde (Art. 58 DSGVO)

61 Im Berichtszeitraum sind keine Kontrollen im Sinne des Art. 58 DSGVO durch die zuständige Datenschutzaufstichtsbehörde durchgeführt worden.

4.1.5. Prüfung des Datenschutzbeauftragten - Ergebnisse interner und externer Prüfungen zum Datenschutz

62 Die Tätigkeiten des externen Datenschutzbeauftragten werden regelmäßig einer Qualitätssicherung durch die fachlich verantwortliche Stelle der GCS – Geno Corporate Services GmbH unterzogen. Hinweise oder Feststellungen aus der Qualitätssicherung werden grundsätzlich in einen Maßnahmenplan aufgenommen. Die Bearbeitung von Hinweisen und Feststellungen wird durch die fachlich verantwortliche Stelle der GCS – Geno Corporate Services GmbH überwacht.

63 Inwieweit den Anforderungen der Datenschutzgrundverordnung sowie dem Bundesdatenschutzgesetz prozessual in der d.vinci-Gruppe entsprochen wird, wird zudem regelmäßig durch die interne Revision der GCS – Geno Corporate Services GmbH geprüft. Gegenstand der Prüfungshandlungen ist dabei auch die Tätigkeit des betrieblichen externen Datenschutzbeauftragten.

64 Aus dem Prüffeld „Datenschutz" ergaben sich im Berichtszeitraum keine Feststellungen.

65 Sonderprüfungen durch die Aufsichtsbehörden fanden im Berichtszeitraum nicht statt.

4.2. Umsetzung der Verarbeitungstätigkeiten

4.2.1. Geplante Datenverarbeitungsvorhaben

66 Bevor Software oder Hardware für die Verarbeitung von personenbezogenen Daten eingesetzt wird, erfolgt, je nach vorgesehenem Einsatz, eine Freigabe im Hinblick auf die datenschutzrechtliche Zulässigkeit.

67 Der Datenschutzbeauftragte wird über Veränderungen mit Bezug zum Datenschutz rechtzeitig unterrichtet. Zur Information über geplante Datenverarbeitungsvorhaben dient neben den Anwesenheitszeiten der Datenschutzbeauftragten im Unternehmen der generelle Kontakt über E-Mail, Telefon oder virtuelle Webkonferenzsoftware.

4.2.2. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen - Privacy by Design und Privacy by Default (Art. 25 DSGVO)

68 Datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO finden im Rahmen der Dienstleistungserbringung seitens der eingesetzten Dienstleister grundsätzlich Berücksichtigung.

69 Bei eigenen eingesetzten Verfahren - z.B. die individuelle Formulargestaltung auf den jeweiligen Internetseiten der d.vinci-Gruppe - findet Art. 25 Abs. 2 DSGVO ebenso Beachtung.

70 Es kommt ein Consent-Banner-Tool im Rahmen der Bereitstellung der Webseite zum Einsatz, um den datenschutzrechtlichen Anforderungen ausreichend Rechnung zu tragen.

4.2.3. Rechtmäßigkeit der Datenverarbeitung (Art. 6 Abs. 1 DSGVO)

71 Überwiegend ergibt sich für die d.vinci-Gruppe die Erlaubnis, Daten Betroffener zu verarbeiten, für Zwecke, die sich aus einem mit dem Betroffenen abgeschlossenen Vertrag bzw. einer vorvertraglichen Beziehung ergeben (Art. 6 Abs. 1 lit. b DSGVO).

72 Darüber hinaus werden bedarfsgerecht Einwilligungen Betroffener eingeholt (Art. 6 Abs. 1 lit. a DSGVO) oder die d.vinci-Gruppe unterliegt einer rechtlichen Verpflichtung die Datenverarbeitung durchzuführen (Art. 6 Abs. 1 lit. c DSGVO).

73 In Einzelfällen wird die Datenverarbeitung auf eine Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) gestützt. Diese findet grundsätzlich in Abstimmung mit dem Datenschutzbeauftragten statt und wird innerhalb des Datenschutzmanagementsystems otris privacy nachvollziehbar dokumentiert.

74 Im Berichtsjahr 2024 wurden keine weiteren Verarbeitungstätigkeiten mittels Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) legitimiert.

4.2.4. Datenübermittlung in Drittstaaten (Art. 44 bis 50 DSGVO)

75 Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR) findet nur statt, soweit dies zur Ausführung von Kundenaufträgen erforderlich, gesetzlich vorgeschrieben ist oder der Betroffene seine Einwilligung erteilt hat.

76 Im Rahmen der Prüfungshandlungen der Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO, wird seitens des Datenschutzbeauftragten darauf geachtet, dass eine Datenübermittlung in Drittstaaten nur nach den Voraussetzungen der Art. 44 ff DSGVO erfolgt.

4.2.5. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

77 Eine Aktualisierung des Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO wurde in Abstimmung mit den verantwortlichen Fachbereichen durchgeführt.

78 Die Dokumentation der Verfahren findet innerhalb des Datenschutzmanagementsystems in der Anwendung otris privacy statt.

79 Eine Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO für **Auftragsverarbeiter** wurde ebenso vorgenommen.

4.2.6. Digitales Datenschutzmanagement (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO)

80 Art. 5 Abs. 2 DSGVO regelt ausdrücklich eine „Rechenschaftspflicht“ über die Einhaltung der gesetzlichen Anforderungen an den Datenschutz. Ein Unternehmen kann diese Rechenschaftspflicht durch angemessene Dokumentation seiner Prozesse und Vorkehrungen erfüllen.

81 Mit dem umgesetzten Datenschutzmanagement-Systems werden sämtliche andere Pflichten, die sich unmittelbar aus der DSGVO ergeben, wie bspw. die Koordinierung der Erfüllung von Betroffenenrechten (Auskunftsersuchen, Beschwerde-, Lösch- oder Berichtigungsverlangen), die Inventarisierung von Auftragsverarbeitern und die Dokumentation der zu der jeweiligen Verarbeitungstätigkeit gehörenden technischen und organisatorischen Maßnahmen der Gesellschaft gesteuert.

82 Zur Erfüllung der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) werden zudem Risikobewertungen zu den einzelnen Verarbeitungstätigkeiten vorgenommen und technische und organisatorische Maßnahmen zur entsprechenden Risikominimierung dokumentiert.

4.2.7. Datenschutzfolgenabschätzung (Art. 35 DSGVO)

83 Sind mit einer Datenverarbeitung hohe Risiken für die betroffenen Personen verbunden, hat der Verantwortliche gegebenenfalls eine sog. Datenschutzfolgenabschätzung durchzuführen. Der Verantwortliche muss dabei mögliche Folgen der Datenverarbeitung analysieren und Maßnahmen für den Schutz der betroffenen Personen festlegen, um das Risiko auf ein angemessenes Maß zu reduzieren. Die Datenschutzkonferenz (DSK, Zusammenschluss aller Landesdatenschutzaufsichtsbehörden) hat in diesem Zusammenhang eine Positivliste zur Datenschutz-Folgenabschätzung (DSFA) herausgegeben.

84 Die gesetzlichen Regelbeispiele sind:

- systematische und umfassende Auswertung persönlicher Aspekte,
- umfangreiche Verarbeitung besonderer Daten nach Artikeln 9 und 10 DSGVO,
- weiträumige Überwachung öffentlich zugänglicher Bereiche.

85 Ein hohes Risiko kann sich für den Betroffenen ergeben durch:

- die Verwendung neuer Technologien,
- die Art der Verarbeitung,
- den Umfang der Verarbeitung,
- die Umstände der Verarbeitung,
- die Zwecke der Verarbeitung.

86 Neben verschiedenen Vorgaben für die Durchführung der Datenschutz-Folgenabschätzung sieht sie auch in bestimmten Fällen vor, dass vor Freigabe bzw. Produktivsetzung der Verarbeitung die Aufsichtsbehörde zu konsultieren ist. Auch für diese Konsultation bestehen gesetzliche Vorgaben.

87 Eine nicht legitimierte Verarbeitung von besonders sensiblen Daten gemäß Art. 9 DSGVO wurde im Berichtsjahr nicht festgestellt.

88 Im Berichtszeitraumes wurden seitens der d.vinci-Gruppe folgende Datenschutzfolgenabschätzungen gem. Art. 35 DSGVO im Rahmen der Einführung neuer Verarbeitungsverfahren durchgeführt:

- Nutzung von M365 (Update)

Konsultationen in diesem Bezug mit der Aufsichtsbehörde waren nicht notwendig.

4.2.8. Besondere Verarbeitungstätigkeiten

4.2.8.1. Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses (Art. 88 Abs. 1 DSGVO i.V.m. § 26 BDSG)

89 Die Speicherung von Mitarbeiterdaten ist grundsätzlich auf der Basis des Anstellungs-/Arbeitsvertrages zulässig. Für die Zwecke der Personalverwaltung und Gehaltsbuchhaltung ist davon auszugehen, dass eine Erstellung von Abrechnungen nicht ohne Nutzung einer IT-Verarbeitung erfolgen wird, welche im Rahmen des Personalmanagements durch die d.vinci-Gruppe durchgeführt wird. Für Mitarbeiterdaten liegen Anstellungsverträge zugrunde.

90 Den Informationspflichten gemäß Art. 13, 14 und 21 DSGVO gegenüber Beschäftigten sowie Bewerbern wird gesetzeskonform nachgekommen.

4.2.8.2. Prüfung beim Einsatz von optisch-elektronischen Überwachungseinrichtungen (§ 4 Abs. 2 BDSG)

91 Optisch elektronische Überwachungseinrichtungen (Videoüberwachung) werden durch die d.vinci-Gruppe nicht eingesetzt.

4.2.8.3. Verarbeitung personenbezogener Daten für Werbung

92 Neben der Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO stellt die Interessensabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO eine zentrale Rechtfertigungsgrundlage für werbliche/vertriebliche Kundenansprachen und die dem vorausgehenden Analyse- und Selektionsverfahren dar. Dabei ist insbesondere von Bedeutung, dass der europäische Gesetzgeber in Erwägungsgrund 47 DSGVO das Werbeinteresse grundsätzlich als ein berechtigtes Interesse des Verantwortlichen im Sinne von Art. 6 Abs. 1 lit. f DSGVO anerkennt.

4.2.8.4. Scoring-Systeme (Art. 4 Abs. 4 DSGVO, § 31 Abs. 1 Nr. 1 BDSG)

93 Im Berichtsjahr wurden keine Scoring- bzw. Ratingverfahren eingesetzt, die dem Art. 4 Abs. 4 DSGVO in Verbindung mit § 31 Abs. 1 Nr. 1 BDSG zu Grunde liegen.

4.2.8.5. Datenträgerentsorgung bzw. -vernichtung nach DSGVO (DIN 66399)

94 Eine datenschutzgerechte Entsorgung von papierhaftem Beleggut sowie die fachgerechte Vernichtung von elektronischen Speichermedien, wie z. B. nicht mehr benötigte Datenträger, ist durch zertifizierte Dienstleister nach den vertraglichen Vereinbarungen oder den Vorgaben zur DIN 66399 umgesetzt.

95 Ein Konzept zur Löschung personenbezogener Daten ist eingeführt.

4.3. Einbindung Externer

4.3.1. Auftragsverarbeitung als Auftraggeber (Art. 28 DSGVO)

96 Die d.vinci-Gruppe setzt zur Durchführung der Geschäftsprozesse auch externe Dienstleister im Sinne einer Auftragsverarbeitung gemäß Art. 28 DSGVO ein. Die Einhaltung der gesetzlichen Rahmenbedingungen des Art. 28 DSGVO wurde durch den Datenschutzbeauftragten geprüft und finden im Rahmen der Vertragsgestaltung Berücksichtigung.

97 Darüber hinaus wird die Einhaltung der seitens des externen Dienstleisters getroffenen und vertraglich zugesicherten technischen organisatorischen Maßnahmen in Form von aktuellen Testaten, Berichten oder Berichtsauszügen unabhängiger Instanzen durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) bzw. bei Bedarf durch vor Ort Begehungen seitens des Datenschutzbeauftragten geprüft.

98 Neue Verträge werden dem Datenschutzbeauftragten zur Prüfung vorgelegt.

99 Die aktuell vorliegenden Verträge entsprechen alle den Anforderungen des Art. 28 DSGVO.

4.3.2. Auftragsverarbeitung als Auftragnehmer (Art. 28 DSGVO)

100 Eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO für Dritte wird durch die d.vinci-Gruppe ausgeführt.

101 Es wurde durch die Geno Corporate Services GmbH (GCS) mittels Testat bestätigt, dass die seitens der d.vinci-Gruppe vertraglich zugesicherten technischen und organisatorischen Maßnahmen durch die Gesellschaft umgesetzt werden.

4.4. Transparenzpflichten und Betroffenenrechte

4.4.1. Informationspflichten gem. Art. 13, 14 und 21 DSGVO

102 In Abstimmung mit dem Datenschutzbeauftragten wurde seitens der d.vinci-Gruppe für Betroffene (Interessenten, Kunden sowie Beschäftigte) Hinweise erstellt, um den Informationspflichten gemäß Art. 13, 14 und 21 DSGVO nachzukommen. Die Übermittlung der Hinweise an die Betroffenen wurde in die betreffenden Geschäftsprozesse und Verfahren integriert.

4.4.2. Geltendmachung von Betroffenenrechten (Art. 15 bis 21 DSGVO)

103 Nach den vorliegenden Informationen und Gesprächen lagen innerhalb des Berichtzeitraumes keine Beschwerden zum Datenschutz vor.

104 Durch die d.vinci-Gruppe wurden Prozesse etabliert, um die Betroffenenrechte datenschutzkonform erfüllen zu können. Dies betrifft:

- Recht auf Auskunft gem. Art. 15 DSGVO
- Recht auf Berichtigung gem. Art. 16 DSGVO

- Recht auf Löschung gem. Art. 17 DSGVO
- Recht auf Einschränkung der Verarbeitung (Sperrung) gem. Art. 18 DSGVO
- Recht auf Nachberichtspflicht gem. Art. 19 DSGVO
- Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO
- Recht auf Widerspruch gegen die Verarbeitung gem. Art. 21 DSGVO

105 Im Rahmen der Prüfungshandlungen der Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO wird seitens des Datenschutzbeauftragten darauf geachtet, dass Regelungen zur Einhaltung der Betroffenenrechte in gefordertem Maße enthalten sind.

4.4.3. Datenschutzvorfälle (Art. 33 und 34 DSGVO)

106 Das Vorgehen im Falle einer Verletzung des Schutzes personenbezogener Daten regeln die Artt. 33, 34 DSGVO. Während Art. 33 DSGVO die Meldung an die Aufsichtsbehörde vorschreibt, bezieht sich Art. 34 DSGVO auf die Meldung an die von der Datenschutzverletzung betroffene Person.

107 Eine Informationspflicht durch die d.vinci-Gruppe an die zuständige Datenschutzaufsichtsbehörde und ggf. Betroffenen aufgrund unrechtmäßiger Kenntniserlangung von Daten durch Dritte im Sinne der Artikel 33 resp. 34 DSGVO lag im Berichtszeitraum nicht vor.

108 Datenpannen im Sinne der Artikel 33 resp. 34 DSGVO seitens der zum Einsatz kommenden Auftragsverarbeitungsnehmer mit Auswirkungen auf die verantwortliche Stelle lagen im Berichtszeitraum nicht vor.

109 Übersicht verhängter **Bußgelder in Deutschland 2024** (Auszug maßgeblicher Sachverhalte):

Datum	Summe	Unternehmen	Sachverhalt
04.03.2024	200.000 €	Versicherungsunternehmen	Das Unabhängiges Datenschutzzentrum Saarland verhängte das Bußgeld gegen ein Versicherungsunternehmen, nachdem es aufgrund einer Sicherheitslücke zu einem Vorfall gekommen war. Dabei stellte die Behörde fest, dass die technischen und organisatorischen Maßnahmen, welche das Unternehmen implementiert hatte, kein dem Risiko angemessenes Schutzniveau gewährleistet hatten.
06.06.2024	16.600 €	Unternehmen	Der Landesbeauftragte für Datenschutz Niedersachsen erließ eine Strafe gegen ein Immobilienunternehmen. Dieses hatte keine Vereinbarungen über gemeinsame Datenverantwortlichkeit getroffen und hatte zudem Daten erhoben und verarbeitet, ohne dass es dafür eine rechtliche Grundlage gab. Löschungsanfragen von drei Betroffenen wurde nicht rechtzeitig nachgekommen.
06.06.2024	220.000 €	Kreditinstitut	Der Landesbeauftragte für Datenschutz Niedersachsen verhängte eine Strafe gegen ein Kreditinstitut. Dieses hatte personenbezogene Informationen seiner Kunden verwendet, um Profile von ihnen zu erstellen, auf Basis derer es sie gezielt zu Werbezwecken kontaktierte. Nach Ansicht des Datenschutzbeauftragten stellte dies eine Zweckveränderung dar, die von den Kunden nicht erwartet werden konnte.

22.08.2024	32.000 €	Logistikunternehmen	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verhängte eine Geldstrafe gegen ein Logistikunternehmen. Dieses hatte seine Zustellerlisten nicht ordnungsgemäß entsorgt.
22.08.2024	16.000 €	Hotel	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit erließ ein Bußgeld gegen ein Hotel, weil dieses Personalausweiskopien gespeichert hatte, ohne dass es dafür eine rechtliche Grundlage gab.
22.08.2024	11.500 €	Unternehmen aus der Werbewirtschaft	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verhängte ein Bußgeld gegen ein Unternehmen aus der Werbewirtschaft, weil dieses seinen Löschpflichten nicht nachgekommen war. Zudem stellte die Behörde fest, dass die getroffenen technischen und organisatorischen Maßnahmen nicht zum Schutz der gesammelten Daten ausreichten.
12.11.2024	900.000 €	Dienstleister	Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit untersuchte mehrere in der Stadt ansässige Unternehmen. Bei einem der Dienstleister stellte er dabei fest, dass dieser bis Mitte November 2023 Datensätze im sechsstelligen Bereich gesammelt hatte, die allesamt personenbezogene Informationen enthielten. Diese waren teilweise fünf Jahre über den Ablauf der Aufbewahrungsfrist hinaus gespeichert worden. Hierfür gab es keine Rechtsgrundlage.

Quelle: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php

110 Übersicht verhängter **Bußgelder weltweit 2024** (Auszug maßgeblicher Sachverhalte):

Datum	Summe	Unternehmen	Sachverhalt
23.01.2024	32.000.000 €	AMAZON France Logistique	Übertriebene Mitarbeiterüberwachung und mangelhafte Information über die Verarbeitung personenbezogener Daten.
29.02.2024	79.107.101 €	Enel Energia, Italien	Kein Schutz von Datenbanken vor missbräuchlichem Zugriff für Telefonmarketing.
29.04.2024	74.701.492 €	T-Mobile USA	Die T-Mobile hatte Standortinformationen ihrer Kunden an Dritte weiterverkauft, ohne dafür eine Einwilligung eingeholt zu haben. Diese Dritten hatten die Informationen dann wiederum weiterverkauft, woraufhin die Daten für standortbasierte Dienste verwendet wurden.
29.04.2024	53.419.426 €	AT&T USA	AT&T hatte Standortinformationen seiner Kunden an Dritte weiterverkauft, ohne dafür eine Einwilligung eingeholt zu haben. Diese Dritten hatten die Informationen dann wiederum weiterverkauft, woraufhin die Daten für standortbasierte Dienste verwendet wurden.
26.08.2024	290.000.000 €	Uber Technologies, Uber BV, Niederlande	Die niederländische Datenschutzbehörde ging gegen Uber Technologies und Uber BV (Uber) vor, nachdem sich 172 Fahrer beschwert hatten. Das Unternehmen übermittelte personenbezogene Daten seiner Fahrer in die USA. Die dabei von Uber implementierten Maßnahmen zum Schutz der so verarbeiteten Informationen waren jedoch den Untersuchungsergebnissen zufolge nicht ausreichend, um diesen auch zu gewährleisten.
27.09.2024	91.000.000 €	Meta Platforms Ireland Ltd.	Die irische Datenschutzbehörde ging gegen Meta Platforms Ireland Ltd. (MPIL) vor, nachdem das

			Unternehmen sie im März 2019 darüber informiert hatte, dass in internen Datenbanken unverschlüsselte Passwörter gespeichert waren. Diese konnten intern eingesehen werden, waren jedoch nicht extern zugänglich.
24.10.2024	310.000.000 €	LinkedIn Ireland Unlimited Company	Das Unternehmen hatte selbst und über Drittanbieter gesammelte personenbezogene Daten verwendet, um Verhaltensanalysen ihrer Nutzer durchzuführen und gezielte Werbung zu schalten. Die Nutzenden hatten hierfür keine Einwilligung erteilt und wurden nicht ausreichend über die Sammlung und Verarbeitung informiert. Nach Ansicht der Behörde lag darüber hinaus kein berechtigtes Interesse vor.

Quelle: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php

5. Planung 2025

111 Für das Jahr 2025 wurden nachfolgend aufgeführte Punkte in die Planung aufgenommen, um die datenschutzrechtlichen Anforderungen auch im Hinblick auf die Datenschutzgrundverordnung konform zu erfüllen.

- Fortführung des Datenschutzmanagements
- Durchführung von Audits und Prüfungshandlungen:
  - Prüfung ausgewählter technisch-organisatorischer Maßnahmen nach Art. 32 DSGVO
  - Datenschutzrechtliche Prüfung des Internetauftritts
  - DSGVO-Compliance-Check (Update 2025)
  - Absicherung Active Directory (Microsoft 365)
- Prüfung/Überwachung der Auftragsverarbeitungverhältnisse im Sinne des Art. 28 DSGVO
- Fortschreibung des Verzeichnis von Verarbeitungstätigkeiten gem. Art 30 DSGVO sowie Art 30 Abs. 2 DSGVO (VVT für Auftragsverarbeiter)
- Weiterentwicklung des Löschkonzeptes und Dokumentation in otris privacy
- Sensibilisierungsmaßnahmen zum Datenschutz (koordinierende Rolle)
- Beratende Unterstützung bei der Einführung neuer rechtlicher Anforderungen

22.01.2025

Frank Gundlach

Digital signiert von Frank Gundlach
DN: cn=Frank Gundlach, c=DE, o=Genossenschaftsverband Bayern e.V., ou=OE-ITAC / GCS - Geno Corporate Services GmbH, email=fgundlach@gv-bayern.de
Grund: Ich bin der Autor des Dokuments
Ort: München
Datum: 2025.01.22 15:49:19 +01'00'

Datum

Frank Gundlach
Externer Datenschutzbeauftragter