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 2025

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

Inhaltsverzeichnis

1. Zusammenfassung – Management Summary

1 Das Jahr 2025 war geprägt von einer weiteren **Intensivierung der datenschutzrechtlichen und informationssicherheitsbezogenen Anforderungen**. Die fortschreitende Digitalisierung, der verstärkte Einsatz künstlicher Intelligenz sowie die Verdichtung regulatorischer Vorgaben haben Unternehmen veranlasst, ihre Prozesse, technischen Systeme und Governance-Strukturen umfassend zu überprüfen und weiterzuentwickeln.

2 Im Mittelpunkt standen insbesondere das nunmehr wirksam angewendete Regelungswerk der **NIS-2-Richtlinie**. NIS-2 erweitert den Kreis verpflichteter Unternehmen erheblich und fordert ein deutlich höheres Niveau an organisatorischen und technischen Maßnahmen zur Gewährleistung von Netz- und Informationssicherheit.

3 Auf nationaler Ebene wurde die **Novellierung des Bundesdatenschutzgesetzes (BDSG)** zwar weiter im parlamentarischen Verfahren beraten, aufgrund des Endes der vorherigen Regierungskoalition ist jedoch offen, ob der vorliegende Gesetzentwurf in seiner bisherigen Form fortgeführt wird. Inhaltlich zielte der Entwurf insbesondere auf die Modernisierung der Aufsichtsstrukturen, die Neuregelung von Scoring-Prozessen sowie die Anpassung an die europäische Rechtsprechung. Ein konkreter Zeitpunkt für eine gesetzliche Neufassung ist derzeit nicht absehbar.

4 Den rechtlichen Rahmen prägten zudem mehrere **richtungsweisende Entscheidungen** des Europäischen Gerichtshofs und der nationalen Gerichte. Zentrale Themen betrafen die Transparenz- und Informationspflichten bei Profiling- und Scoring-Verfahren, die Anforderungen an internationale Datentransfers sowie die datenschutzkonforme Ausgestaltung automatisierter Entscheidungsprozesse. Die Rechtsprechung führte zu einer weiteren Präzisierung der Anforderungen an technische und organisatorische Maßnahmen sowie an Dokumentations- und Nachweispflichten.

5 Die **Europäische Kommission** hat im Rahmen des **Digital-Omnibus** im November 2025 gezielte Änderungen der DSGVO vorgeschlagen, um den europäischen Datenschutzrahmen zu modernisieren und an digitale Geschäftsmodelle anzupassen. Vorgesehen sind insbesondere eine Verlängerung der Meldefrist für Datenschutzverletzungen von 72 auf 96 Stunden, ein einheitliches Meldeportal („Single-Entry-Point“) für Vorfallmeldungen sowie Erleichterungen und Klarstellungen bei Informations- und Transparenzpflichten. Zudem sollen Definitionen und Anforderungen - etwa bei pseudonymisierten Daten oder beim Einsatz von KI - präzisiert werden. Ziel der Reform ist keine Absenkung des Datenschutzniveaus, sondern eine Harmonisierung und Entbürokratisierung, die Unternehmen bei der praktischen Umsetzung entlasten soll.

6 Insgesamt zeigt sich, dass Datenschutz und Informationssicherheit im Jahr 2025 noch deutlicher als integrale Bestandteile einer verantwortungsvollen Unternehmensführung etabliert wurden. Neben der reinen Einhaltung regulatorischer Vorgaben rückt zunehmend die Notwendigkeit in den Vordergrund, die bestehenden Kontroll- und Governance-Strukturen fortlaufend weiterzuentwickeln und das Vertrauen von Kunden, Mitarbeitenden und Geschäftspartnern durch ein konsequent hohes Schutzniveau zu stärken.

7 Im **Datenschutzmanagementsystem (DSMS)** werden wesentliche Anforderungen des Datenschutzrechtes implementiert und umgesetzt. Hierzu zählt 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.

8 Wesentliche Veränderungen mit datenschutzrechtlicher Relevanz sind im Berichtszeitraum nicht eingetreten.

9 Eine Melde- bzw. Informationspflicht an die zuständige Datenschutzaufsichtsbehörde und ggf. Betroffenen aufgrund unrechtmäßiger Kenntniserlangung von Daten Dritter im Sinne der Artikel 33 resp. 34 DSGVO lag im Berichtszeitraum nicht vor.

10 Datenpannen im Sinne der Artikel 33 resp. 34 DSGVO seitens der zum Einsatz kommenden Auftragsverarbeitungsnehmer mit Auswirkungen auf die verantwortliche Stelle sind im Berichtszeitraum nicht vorgekommen.

11 Die Tätigkeiten des Datenschutzbeauftragten haben ergeben, dass **Datenschutzmaßnahmen** in angemessenen Umfang vorhanden sind. 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. Es gibt Regelvorgehensweisen zum Umgang mit Datenschutz- und Informationssicherheitsvorfällen.

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

14 Der Jahresbericht des Datenschutzbeauftragten wurde zur Kenntnis genommen.

Datum

Nina Rahn

Nina Rahn

Zertifiziert von yousign

Datum

Sebastian Thuma

Sebastian Thuma

Zertifiziert von yousign

Datum

Tobias Tiedgen

Tobias Tiedgen

Zertifiziert von yousign

2. Allgemeine Angaben

2.1. Auftragsverhältnis

15 Im Rahmen 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

16 Adressat dieses Tätigkeitsberichtes ist die Geschäftsführung der Gesellschaft.

17 Dieser Bericht bezieht sich auf den Zeitraum 1. Januar bis 31. Dezember 2025.

2.3. Tätigkeitsumfang

18 Den Aufgaben als Datenschutzbeauftragter ist Herr Frank Gundlach in der Gesellschaft vor Ort sowie darüber hinaus an seinem Dienstsitz nachgekommen.

19 Zudem stand er dem Unternehmen jederzeit als Ansprechpartner per E-Mail, Telefon oder virtueller Webkonferenzsoftware zur Verfügung.

3. Organisation des Datenschutzmanagements

3.1. Datenschutzbeauftragter

20 Auf Basis des bestehenden Dienstleistungsvertrages wurde Herr Frank Gundlach zum Datenschutzbeauftragten benannt. Die Bestellungsurkunde ist bei den Arbeitsunterlagen des Datenschutzbeauftragten abgelegt.

21 Die Fachkunde des Datenschutzbeauftragten wird laufend durch Schulungen und Fachliteratur aufrechterhalten. Die entsprechenden Nachweise sind im Datenschutzmanagementsystem otris privacy hinterlegt

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

23 Die Tätigkeit des Datenschutzbeauftragten bildete 2025 folgende Schwerpunkte:

- Weiterführung des Datenschutzmanagements
- Tätigkeiten im Rahmen der Anwendung der DSGVO und des BDSG
- Information der Beschäftigten (regelmäßige Newsletter)
- 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 den festgelegten Auditprogramms
- Berichterstattung/Reporting

3.2. Rahmenbedingungen für die Tätigkeit

24 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.

25 Die Erstellung der darauf beruhenden organisatorischen Regelungen wurde seitens des betrieblichen Datenschutzbeauftragten unterstützt.

26 Folgende Rahmenwerke (Auszug) ergänzen diese:

27 Gesetzliche Regelungen

- 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

28 Verordnungen, Standards und Richtlinien

- Grundsätze ordnungsmäßiger Buchführung, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
- RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
- IT-Grundschutz-Kompendium und Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- DIN EN ISO/IEC 27001:2022

29 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

30 Interne Regelwerke

- Datenschutzrichtlinie
- IT-Benutzerrichtlinie
- Konzept zur Löschung personenbezogener Daten
- Richtlinie zur Nutzung von Internet und E-Mail
- IT-Sicherheitskonzept (Regularien aus dem ISMS)
- Soll-Berechtigungskonzepte
- weitere relevante aufbau- und ablauforganisatorische Grundlagen der Gesellschaft

31 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.

- Novellierung des Bundesdatenschutzgesetzes

  Die Novellierung des Bundesdatenschutzgesetzes (BDSG) befindet sich weiterhin im parlamentarischen Verfahren. Der Gesetzentwurf der Bundesregierung wurde am 15. Mai 2024 in erster Lesung im Bundestag beraten und anschließend an die zuständigen Ausschüsse überwiesen, nachdem das Bundeskabinett den Entwurf bereits am 7. Februar 2024 beschlossen hatte. Ziel des Entwurfs war es, Vereinbarungen aus dem Koalitionsvertrag der damaligen Regierungskoalition umzusetzen und Ergebnisse der Evaluierung des BDSG aufzugreifen.

  Der Entwurf umfasste insbesondere folgende Kernpunkte:

  Institutionalisierung der Datenschutzkonferenz (DSK)
  Die DSK sollte im BDSG gesetzlich verankert werden, um eine kohärentere und einheitlichere Aufsichtspraxis in Deutschland zu gewährleisten.

  Verbesserte Zusammenarbeit der Aufsichtsbehörden
  Für Unternehmen und Forschungseinrichtungen mit länderübergreifenden Verarbeitungsvorgängen war vorgesehen, eine eindeutige Zuordnung zu einer einzigen zuständigen Aufsichtsbehörde zu ermöglichen, um Rechtsunsicherheiten zu reduzieren.

  Neuregelungen zum Scoring
  Auf Grundlage der Rechtsprechung des Europäischen Gerichtshofs vom Dezember 2023 sollten Vorgaben für den Einsatz bestimmter Kategorien personenbezogener Daten (z. B. ethnische Herkunft oder Gesundheitsdaten) im Scoring präzisiert und eingeschränkt werden.

  Mit dem Ende der früheren Regierungskoalition ist jedoch offen, ob der bestehende Gesetzentwurf in der vorliegenden Fassung weiterverfolgt wird. Zwar ist der Entwurf formal nicht obsolet, Änderungen oder eine vollständige Neuausrichtung im weiteren parlamentarischen Verfahren sind jedoch möglich. Ein konkreter Zeitpunkt für die Verabschiedung oder das Inkrafttreten der Änderungen ist derzeit nicht absehbar.

- Beschäftigtendatengesetz (BeschDG)

  Ein Referentenentwurf des Gesetzentwurfs wurde von Bundesministerium für Arbeit und Soziales (BMAS) gemeinsam mit dem Bundesministerium des Innern und für Heimat (BMI) am 8. Oktober 2024 vorgelegt. Der Entwurf sieht einen eigenständigen Rechtsrahmen für den Beschäftigtendatenschutz vor und soll den bisher geltenden § 26 Bundesdatenschutzgesetz (BDSG) ersetzen bzw. substanzielle Ergänzungen bringen.

  Vorgesehene Eckpunkte sind u. a. striktere Erforderlichkeitsprüfungen der Datenverarbeitung im Beschäftigungsverhältnis, umfangreiche Informations- und Auskunftsrechte bei Einsatz von KI, stärkere Mitbestimmungsrechte von Betriebsräten, besondere Regelungen zur Überwachung von Beschäftigten. Ursprünglich war im Entwurf mit einem Inkrafttreten des Gesetzes im September 2025 gerechnet worden. Allerdings bestehen erhebliche Unsicherheiten. Aufgrund des Regierungswechsels ist nicht gesichert, ob das Gesetz in der vorliegenden Form verabschiedet wird.

  Auch wenn das BeschDG noch nicht verabschiedet ist, verlangt der Entwurf bereits, dass Unternehmen auf eine erhöhte Transparenz-, Dokumentations- und Abwägungspflicht für Beschäftigtendaten vorbereitet sind. Da viele der geplanten Regelungen (z. B. bei KI-Einsatz, Überwachung, Profiling) in Zukunft gelten könnten, empfiehlt es sich, jetzt bereits proaktiv Prozesse zu überprüfen, insbesondere im HR- und IT-Kontext. Aus Sicht des Outsourcing- und IT-Dienstleisters-Managements (z. B. bei Dritt- oder Sub-Auftragnehmern im Beschäftigungsverhältnis) ist es ratsam, mögliche Änderungen im Mitbestimmungs-, Dokumentations- und Prüfungs-Rahmen frühzeitig zu antizipieren.

- Umsetzung der NIS-2-Richtlinie

  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. In Deutschland hätte die Umsetzung bis zum 17. Oktober 2024 erfolgen müssen, wurde jedoch verzögert – infolgedessen verfuhr das Bundesministerium des Innern und für Heimat in einem mehrstufigen Gesetzgebungsverfahren. Am 13. November 2025 beschloss der Deutscher Bundestag den Gesetzentwurf zur Umsetzung („Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“). Der Bundesrat hat am 21. November 2025 beschlossen, keinen Antrag auf Anrufung des Vermittlungsausschusses zu stellen. Damit war das parlamentarische Verfahren abgeschlossen und das Gesetz ist am 6.Dezember 2025 in Kraft getreten.

- Bestrebungen auf EU-Ebene zur Vereinfachung und Entlastung im Rahmen der DSGVO

  Auf EU-Ebene wurden im Berichtsjahr verschiedene Initiativen zur Vereinfachung und Entlastung im Anwendungsbereich der DSGVO vorangetrieben. Ziel dieser Maßnahmen ist es, die administrativen Anforderungen für Unternehmen mit geringem Datenschutzrisiko zu reduzieren, ohne das Schutzniveau der Verordnung abzusenken. Im Mittelpunkt steht eine stärkere Harmonisierung und Standardisierung der Auslegung durch die europäischen Aufsichtsbehörden, insbesondere durch einheitlichere Vorgaben zu Verzeichnissen, Risikoanalysen und Datenschutzfolgenabschätzungen.

  Zudem prüft die Europäische Kommission, wie der risikobasierte Ansatz der DSGVO operativ geschärft werden kann, um vor allem kleinere Unternehmen und Organisationen mit einfachen Verarbeitungsszenarien zu entlasten. Für die Gesellschaft ergeben sich

dadurch zwar keine unmittelbaren gesetzlichen Änderungen, jedoch eine perspektivisch erhöhte Rechtssicherheit und eine Entlastung bei Dokumentation und Abstimmung mit unterschiedlichen Aufsichtsbehörden. Die Entwicklungen werden fortlaufend beobachtet und in die Compliance-Planung integriert.

3.3. Datenschutz und Informationssicherheit

32 Der betriebliche Datenschutzbeauftragte 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.

33 Den Wechselwirkungen und Synergien zwischen Datenschutz- und Informationssicherheitsprozess werden in besonderem Maße Rechnung getragen.

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

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

36 Es werden datenschutzrelevante Sachverhalte bewertet bzw. im Rahmen der Datenschutzfolgenabschätzung auf Zulässigkeit und Konformität geprüft.

37 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

38 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.

39 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.

40 Darüber hinaus sind besondere Datenschutzprozesse erforderlich, beispielsweise zur Wahrung der Rechte der Betroffenen oder die Reaktion auf Datenschutzvorfälle. Aufgrund ihres Stellenwertes werden die Datenschutzaufbauorganisation und die Datenschutzprozesse hinsichtlich Angemessenheit und Wirksamkeit regelmäßig geprüft.

41 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.

42 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).

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

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

4.1. Verantwortlichkeiten und Sensibilisierung

4.1.1. Regelungen

44 Eine 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.

45 Der Datenschutzbeauftragte berichtet mindestens einmal jährlich an die Geschäftsleitung.

46 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
Telefon: 040 42854-4040
E-Mail: mailbox@datenschutz.hamburg.de
Homepage: https://www.datenschutz-hamburg.de

4.1.2. Vermittlung maßgeblicher Datenschutzvorschriften - Mitarbeitersensibilisierung

47 Alle Beschäftigten werden bei der Einstellung schriftlich auf die Verschwiegenheit verpflichtet. Die Verpflichtungserklärungen werden nachweislich zu den Personalunterlagen genommen.

48 Es besteht ein Schulungs- und Sensibilisierungskonzept zum Datenschutz und der Informationssicherheit für die Beschäftigten der Gesellschaft.

49 Um eine aussagekräftige Bewertung der bislang durchgeführten Sensibilisierungsmaßnahmen hinsichtlich des Datenschutzes durchführen zu können und eine nachhaltige Steigerung des Sensibilisierungsgrades der Mitarbeiter zu erreichen, wurde aufbauend zur Kampagne in den Vorjahren im 4. Quartal 2025 erneut eine Security Awareness Kampagne mit „realitätsnaher Phishing-

Simulation“ durchgeführt. Die Kampagne wurde im Rahmen des Datenschutzmandates durch einen von der GCS beauftragten Dienstleister durchgeführt.

50 Über die Ergebnisse der Awareness-Kampagne wurde gesondert berichtet.

51 Sofern sich Vorfälle ereignen sollten, die auf ein mangelndes Bewusstsein für den Datenschutz schließen lassen, sind im Rahmen des Datenschutzmanagements Präsenzschulungen für diese betroffenen Bereiche vorgesehen. Dies war innerhalb des Berichtszeitraumes nachweislich nicht der Fall.

52 Dem Datenschutzbeauftragten sind aus seiner Überwachungstätigkeit im Jahr 2025 keine Sachverhalte aufgefallen, die auf Schulungsdefizite der betroffenen Mitarbeiter hätten schließen lassen.

53 Der Datenschutzbeauftragte informiert die Gesellschaft auch unterjährig regelmäßig über datenschutzrelevante Themen, insbesondere durch Newsletter sowie anlassbezogene Ad-hoc-Mitteilungen.

54 Folgende Informationen wurde im Jahr 2025 zur Verfügung gestellt:

- [01-2025] DATENSCHUTZ-INFO | Spam, Phishing & Co
- Alert: Großflächige Brute-Force-Angriffe auf M365 – vorsichtshalber Log-ins checken (23.01.2025)
- [02-2025] DATENSCHUTZ-INFO | DeepSeek: Große Sicherheitsbedenken gegen chinesische KI
- [02.01-2025] DATENSCHUTZ-INFO | KI-Kompetenz ist Pflicht ab 2025
- [02.02-2025] DATENSCHUTZ-INFO | Einsichtnahme in Steuerakten: Eine Frage der DSGVO?
- [03-2025] DATENSCHUTZ-INFO |E-Mail-Konto gehackt ? - Ein Notfallplan für Betroffene
- [03.01-2025] DATENSCHUTZ-INFO |Ende-zu-Ende-Verschlüsselung für E-Mail-Rechnungen erforderlich
- [04-2025] DATENSCHUTZ-INFO | BEG IV: Weniger Bürokratie dank neuer Aufbewahrungsfristen
- [05-2025] DATENSCHUTZ-INFO | - Microsoft 365 Copilot unter datenschutzrechtlicher Betrachtung
- [05-2025] DATENSCHUTZ-INFO | - Neue Angriffstrends im Bereich Informationssicherheit?
- [05-2025][02] DATENSCHUTZ-INFO | - Upgrade für die E-Mail-Sicherheit
- [06.00-2025] DATENSCHUTZ-INFO | - Umgang mit Mitarbeiterfotos nach Kündigung des Jobs
- [06.01-2025] DATENSCHUTZ-INFO | - Stand der Technik in der IT-Sicherheit
- [06.02-2025] DATENSCHUTZ-INFO | - Datenschutzkonformer Einsatz von ChatGPT
- [07-2025] DATENSCHUTZ-INFO | - Der Datenschutz kommt mit auf Geschäftsreise
- [08-2025] DATENSCHUTZ-INFO | - BSI-CS 155: „Upgrade für die E-Mail-Sicherheit“ - Empfehlung zur Stärkung der E-Mail-Sicherheit Ihrer Unternehmenskommunikation
- [09-2025] DATENSCHUTZ-INFO | -Ein Bild reicht aus: Hacker übernehmen gezielt iPhones
- [10-2025] DATENSCHUTZ-INFO | Datenschutz im Homeoffice für HR-Mitarbeitende: Worauf Personalabteilungen achten müssen

- [11-2025] DATENSCHUTZ-INFO | Support-Ende: Zehntausende Exchange-Server gefährdet - Pressemittelung des BSI vom 28.10.2025
- [11-2025][01] DATENSCHUTZ-INFO | Fotos von Veranstaltungen DSGVO-konform veröffentlichen
- [12-2025] IT-SEC & DATENSCHUTZ-INFO | React Server Components: Kritische Schwachstelle bedroht zahlreiche Webanwendungen

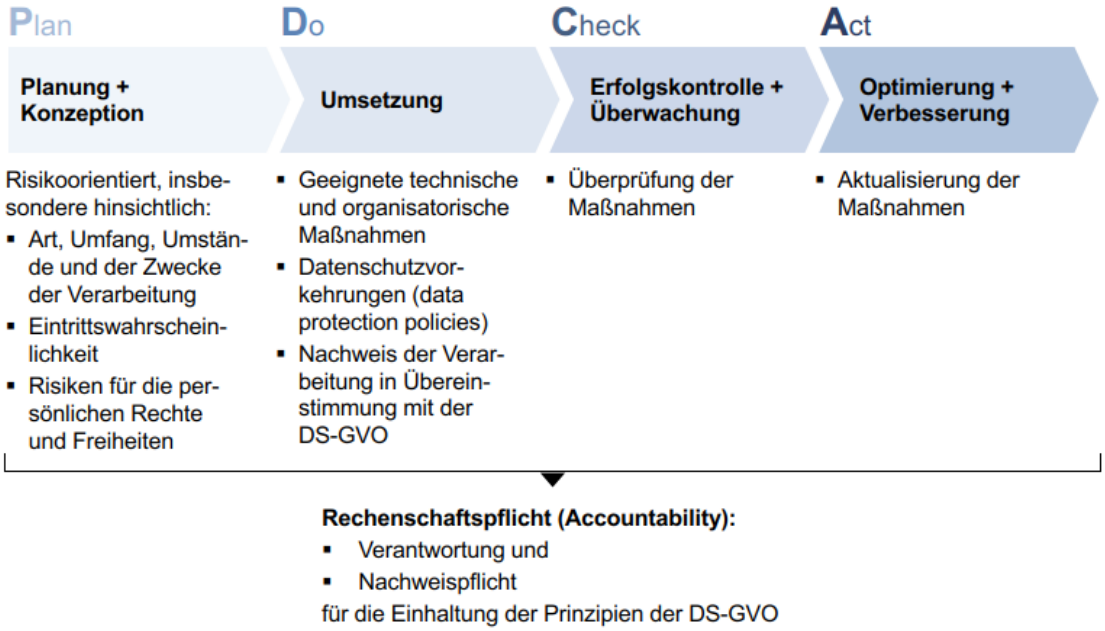
4.1.3. Datenschutzmanagement im Sinne eines Regelkreislaufes

55 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 Mitarbeiter 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

Mit dem implementierten Datenschutzmanagement wird sichergestellt, dass

- formale Anforderungen umgesetzt bzw. implementiert werden
- relevante Audits auf Basis eine Auditplanes durchgeführt werden
- datenschutzrelevante Prüffelder im risikoorientierten Focus des Datenschutzbeauftragten bleiben



56 Das Datenschutzmanagementsystem unterstützt den Datenschutzbeauftragten bei der Wahrnehmung seiner Aufgaben, dient der Erfüllung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO und ist beim Verantwortlichen im Datenschutzmanagementsystem **otris privacy** implementiert bzw. umgesetzt.

57 Folgende Prüfungshandlungen wurden im Rahmen des Datenschutzmandates durchgeführt:

- Prüfung technisch-organisatorischer Maßnahmen nach Art. 32 DSGVO
- Datenschutzrechtliche Betrachtung privaten E-Mail-Nutzung
- Datenschutzrechtliche Prüfung des Internetauftritts mittels eines automatisierten Audit-Tools
- Datenschutzrechtliche Prüfung Vernichtung von Daten
- Standortbegehung unter Datenschutz-Aspekten
- DSGVO-Compliance-Check (für Auftragsverarbeiter in Verbindung mit dem GCS-Zertifikat)

58 Über die Ergebnisse der Prüfungshandlungen wurde gesondert berichtet.

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

59 Kontrollen im Sinne des Art. 58 DSGVO durch die zuständige Datenschutzaufsichtsbehörde haben im Berichtszeitraum nicht stattgefunden.

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

60 Die Tätigkeiten des externen Datenschutzbeauftragten werden regelmäßig einer Qualitätssicherung durch die fachlich verantwortliche Stelle der GCS – Geno Corporate Services GmbH unterzogen.

61 Hinweise oder Feststellungen aus der Qualitätssicherung werden grundsätzlich in einem Maßnahmenplan aufgenommen. Die Bearbeitung von Hinweisen und Feststellungen wird durch die fachlich verantwortliche Stelle der GCS – Geno Corporate Services GmbH überwacht.

62 Sonderprüfungen durch die zuständige Aufsichtsbehörde fanden im Berichtszeitraum bei der Verantwortlichen Stelle nicht statt.

4.2. Verarbeitungstätigkeiten

4.2.1. Geplante Datenverarbeitungsvorhaben

63 Vor dem Einsatz von Software oder Hardware zur Verarbeitung personenbezogener Daten erfolgt – abhängig vom vorgesehenen Verwendungszweck – eine datenschutzrechtliche Prüfung und Freigabe hinsichtlich der Zulässigkeit der geplanten Verarbeitung.

64 Der Datenschutzbeauftragte wird über datenschutzrelevante Änderungen und geplante Verarbeitungsvorhaben rechtzeitig informiert.

65 Die Abstimmung erfolgt neben den regelmäßigen Anwesenheitszeiten im Unternehmen auch über die laufende Kommunikation per E-Mail, Telefon sowie mittels virtueller Webkonferenzsysteme.

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

66 Datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO werden im Rahmen der Leistungserbringung durch die Verantwortliche Stelle selbst als auch durch die eingesetzten Dienstleister grundsätzlich berücksichtigt.

67 Ebenso wird bei unternehmenseigenen Verfahren – wie etwa der individuellen Gestaltung von Formularen auf den jeweiligen Webpräsenzen sowie bei eigenentwickelten Anwendungen – die Vorgabe des Art. 25 Abs. 2 DSGVO konsequent beachtet.

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

68 Die Verarbeitung personenbezogener Daten erfolgt überwiegend auf Grundlage eines mit der betroffenen Person geschlossenen Vertrages oder im Rahmen vorvertraglicher Maßnahmen gemäß Art. 6 Abs. 1 lit. b DSGVO.

69 Soweit erforderlich, werden ergänzend Einwilligungen der betroffenen Personen nach Art. 6 Abs. 1 lit. a DSGVO eingeholt.

70 Darüber hinaus erfolgt eine Datenverarbeitung, sofern die Gesellschaft hierzu einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 lit. c DSGVO unterliegt.

71 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 im Datenschutzmanagementsystem otris privacy nachvollziehbar dokumentiert.

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

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

73 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)

74 Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO wird in Abstimmung mit den verantwortlichen Fachbereichen geführt und im Datenschutzmanagementsystem otris privacy dokumentiert.

Eine Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO für Auftragsverarbeiter wurde im Rahmen der vor Ort Tätigkeit in Abstimmung mit den verantwortlichen Fachbereichen durchgeführt.

Die Dokumentation findet ebenso im Datenschutzmanagementsystem otris privacy statt.

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

75 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.

76 Die Gesellschaft kommt ihrer Rechenschaftspflicht überwiegend durch den Einsatz des Datenschutzmanagementsystems **otris privacy** in Verbindung mit dem Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO in ausreichendem Maße nach.

77 Mittels des Datenschutzmanagementsystems (DSMS) werden idealerweise auch 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.

78 Zur Wahrnehmung der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO werden im Datenschutzmanagementsystem (DSMS) systematische Risikobewertungen der einzelnen Verarbeitungstätigkeiten durchgeführt. Dabei werden die jeweils implementierten technischen und organisatorischen Maßnahmen zur Risikominimierung dokumentiert.

79 Zudem wird die Entscheidung über die Durchführung oder das Absehen von einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO einschließlich einer etwaigen Schwellenwertanalyse nachvollziehbar festgehalten und eine Überprüfung durch den Datenschutzbeauftragten sichergestellt.

4.2.7. Datenschutzfolgenabschätzung (Art. 35 DSGVO)

80 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.

81 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.

82 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.

83 Neben konkreten Vorgaben zur Durchführung einer Datenschutz-Folgenabschätzung sieht die DSGVO in bestimmten Fällen vor, dass vor der Freigabe bzw. Aufnahme des produktiven Betriebs einer Verarbeitung eine Konsultation der zuständigen Aufsichtsbehörde zu erfolgen hat. Auch für diese vorherige Konsultation bestehen gesetzlich festgelegte Anforderungen.

84 Eine nicht legitimierte Verarbeitung von besonders sensiblen Daten gemäß Art. 9 DSGVO wird nach den aktuellen Feststellungen des Datenschutzbeauftragten und der erhaltenen Auskünfte gegenwärtig nicht durchgeführt.

85 Datenschutzfolgenabschätzungen nach Art. 35 DSGVO bei neuen Verarbeitungsverfahren in Verbindung mit besonders geschützten "sensiblen" Daten waren unter Berücksichtigung der erhaltenen Auskünfte im Berichtszeitraum nicht erforderlich.

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)

86 Die Verarbeitung und Speicherung von Beschäftigtendaten erfolgen grundsätzlich auf Grundlage des jeweiligen Anstellungs- bzw. Arbeitsvertrages. Für Zwecke der Personalverwaltung und der Entgeltabrechnung ist davon auszugehen, dass die Erstellung von Abrechnungen ohne den Einsatz informationstechnischer Systeme nicht möglich ist.

87 Die hierfür erforderliche IT-gestützte Verarbeitung personenbezogener Daten wird im Rahmen des Personalmanagements vorgenommen.

88 Für Beschäftigtendaten liegen Anstellungsverträge zugrunde.

89 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)

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

4.2.8.3. Verarbeitung personenbezogener Daten für Werbung

91 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)

92 Die Gesellschaft setzt keine Scoring- oder Ratingverfahren ein, die eine Profilbildung im Sinne des Art. 4 Abs. 4 DSGVO in Verbindung mit § 31 Abs. 1 Nr. 1 BDSG darstellen.

4.2.8.5. Datenträgerentsorgung bzw. -vernichtung nach DSGVO (ISO/IEC 21964-1:2018)

93 Die datenschutzkonforme Entsorgung papiergebundener Unterlagen sowie die fachgerechte Vernichtung elektronischer Speichermedien, insbesondere nicht mehr benötigter Datenträger, erfolgt durch zertifizierte Dienstleister auf Grundlage vertraglicher Vereinbarungen und in Übereinstimmung mit den Vorgaben der ISO/IEC 21964-1:2018 (vormals DIN 66399).

94 Ein Konzept zur Löschung personenbezogener Daten ist implementiert.

4.3. Einbindung Externer

4.3.1. Auftragsverarbeitung als Auftraggeber (Art. 28 DSGVO)

95 Zur Durchführung der Geschäftsprozesse werden externe Dienstleister im Sinne einer Auftragsverarbeitung gemäß Art. 28 DSGVO eingesetzt.

96 Die Einhaltung der gesetzlichen Rahmenbedingungen des Art. 28 DSGVO wurde durch den Datenschutzbeauftragten geprüft und finden im Rahmen der Vertragsgestaltung Berücksichtigung.

97 Die Einhaltung der vom externen Dienstleister umgesetzten und vertraglich zugesicherten technischen und organisatorischen Maßnahmen wird regelmäßig überprüft. Dies erfolgt insbesondere auf Grundlage aktueller Testate, Prüfberichte oder Auszüge aus Berichten unabhängiger Stellen (z. B. Wirtschaftsprüfer, interne Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilungen, Datenschutz- oder Qualitätsauditoren), durch geeignete Zertifizierungen im Rahmen von IT-Sicherheits- oder Datenschutzaudits (z. B. nach BSI-Grundschutz) sowie – sofern erforderlich – durch Vor-Ort-Prüfungen durch den Datenschutzbeauftragten.

98 Darüber hinaus liegen weitere Auftragsverarbeitungen vor. Hier besteht für den Datenschutzbeauftragten Transparenz über die Vertragsverwaltung.

99 Neue Verträge werden dem Datenschutzbeauftragten zur Prüfung vorgelegt.

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

4.3.2. Auftragsverarbeitung als Auftragnehmer (Art. 28 DSGVO)

101 Die Gesellschaft erbringt Leistungen als Auftragsverarbeiter im Sinne des Art. 28 DSGVO.

102 Durch ein Testat der **Geno Corporate Services GmbH (GCS)** wurde bestätigt, dass die von der Gesellschaft vertraglich zugesicherten technischen und organisatorischen Maßnahmen tatsächlich umgesetzt und eingehalten werden.

4.4. Transparenzpflichten und Betroffenenrechte

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

103 In Abstimmung mit dem Datenschutzbeauftragten wurden Hinweise für Betroffene (Interessenten sowie Kunden) erstellt, um den Informationspflichten gemäß Art. 13, 14 und 21 DSGVO nachzukommen. Diese wurden in die etablierten Prozesse integriert.

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

104 Im Berichtszeitraum ergaben sich **keine Beschwerden** im Bezug zum Datenschutz.

105 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

106 Im Rahmen der Prüfungshandlungen der Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO, wird darauf geachtet, dass Regelungen zur Einhaltung der Betroffenenrechte in ausreichendem, gesetzlich gefordertem Maße enthalten sind.

4.4.3. Datenschutzvorfälle (Art. 33 und 34 DSGVO)

107 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.

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

109 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.**

110 Übersicht verhängter Bußgelder in **Deutschland 2025** (Auszug maßgeblicher Sachverhalte):

Datum	Summe	Unternehmen	Sachverhalt
07.03.2025	3.500 €	Polizeibeamter	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg erließ ein Bußgeld gegen einen Polizeibeamten. Dieser hatte die Melderegister-Daten einer Frau abgerufen, bei der er eine Verkehrskontrolle durchgeführt hatte. Sein Ziel war, die Person anhand ihres gespeicherten Lichtbilds nach einer persönlichen "Schönheitsskala" zu beurteilen.
25.03.2025	50.000 €	Unternehmen	Die Sächsische Datenschutz- und Transparenzbeauftragte verhängte zwei Bußgelder von je 20.000 EUR und 30.000 EUR gegenüber Unternehmen wegen unrechtmäßiger Videoüberwachung. Eines der Unternehmen, in der Hotelgastronomie tätig, überwachte den öffentlichen Verkehrsraum sowie eine zu ihm gehörende Bau-

			stelle, einen Gästeparkplatz und ein Nachbargrundstück mit Kameras, die auch Tonaufnahmen machten. Das zweite Unternehmen hatte Kameras auf seiner Baustelle installiert und betrieb diese auch tagsüber, obwohl sie angeblich zu Diebstahlschutzzwecken angebracht worden waren. In diesem Fall wurde auch gegen den Grundstücksbesitzer ein Bußgeld in unbekannter Höhe ausgesprochen.
25.03.2025	120.000 €	Unternehmen	Die Sächsische Datenschutz- und Transparenzbeauftragte erließ zwei Bußgelder gegen Unternehmen, die nur sehr verspätet auf Informationsanfragen reagiert hatten. In beiden Fällen halfen auch Zwangsmittel nichts. Eines der Unternehmen antwortete erst nach zwei Jahren, vier Monaten und fünf Zwangsgeldern, von denen vier bezahlt wurden. Bei dem anderen benötige es ein Jahr und vier Zwangsgelder, drei davon wurden bezahlt.
03.06.2025	45.000.000 €	Vodafone	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit untersuchte Vodafone. Dabei stellte sie fest, dass das Unternehmen die Auftragsverarbeiter, die es engagierte, nicht regelmäßig und umfassend genug datenschutzrechtlich überprüfte bzw. überwachte. So war es Mitarbeitenden der Partneragenturen möglich, Fake-Verträge zu erstellen oder bestehende Verträge zulasten der Kunden zu ändern. Die hierfür (Art. 28 Abs. 1 DSGVO) ausgesprochene Geldstrafe beträgt 15 Mio. EUR. Die BfDI sprach zudem eine Verwarnung wg. mangelhafter technischer und organisatorischer Maßnahmen zum Schutz verarbeiteter Daten aus. Eine Strafe von 30 Mio. EUR erließ die BfDI wegen Mängeln bei der Sicherheit von Authentifizierungs-Prozessen. Diese betrafen die Nutzung des Onlineportals "Mein Vodafone" in Verbindung mit der Unternehmens-Hotline. So konnten unbefugte Dritte eSIM-Profile abrufen. Die BfDI betonte, dass Vodafone seine Arbeitsabläufe und Systeme mittlerweile verbessert bzw. gegebenenfalls ersetzt hat.
30.09.2025	195.000 €	Unternehmen	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verhängte ein Bußgeld gegen ein Unternehmen. Dieses hatte von einem Auftragsverarbeiter Werbung per Post verschicken lassen. Als die Empfänger von ihren Betroffenenrechten Gebrauch machen wollten, reagierte der Bußgeldempfänger nicht fristgerecht.
30.09.2025	492.000 €	Finanz-Unternehmen	In ihrer Zwischenbilanz für die im Jahr 2025 verhängten Bußgelder berichtete der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit über eine Strafe für ein Finanz-Unternehmen. Dieses hatte mehrere Kreditanfragen trotz eigentlich guter Bonität der Antragsteller abgelehnt. Als diese daraufhin Informationsanfragen stellten, reagierte das Unternehmen nicht angemessen.

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

111 Übersicht verhängter Bußgelder **weltweit 2025** (Auszug maßgeblicher Sachverhalte):

Datum	Summe	Unternehmen	Sachverhalt
27.01.2025	4.000.000 €	GENERALI ESPAÑA, SOCIEDAD ANONIMA DE SEGUROS Y REASEGUROS (Generali Spanien)	Nach einem Cyber-Angriff auf die Systeme der Generali beschwerten sich mehrere betroffene Privatpersonen, deren Daten inkl. Ausweiskopien und IBANs abgeflossen waren, bei der spanischen Datenschutzbehörde. Die daraufhin eingeleitete Untersuchung ergab, dass es nicht nur an technischen und organisatorischen Maßnahmen zum Schutz verarbeiteter Daten mangelte, sondern dass es auch keine ausreichende Risiko- und Folgebewertung des Vorfalls gegeben hatte.
03.03.2025	1.000.000 €	LIGA NACIONAL DE FÚTBOL PROFESIONAL (Spanien)	Die LIGA NACIONAL DE FÚTBOL PROFESIONAL (LNFP) hatte für den Zugang zu Teilen einiger Stadien auf biometrischen Daten basierende Kontrollmaßnahmen eingeführt. Die Untersuchung ergab, dass die LNFP keine Datenschutz-Folgeabschätzung durchgeführt hatte, bevor sie die Kontrollen in Betrieb nahm. Die Liga muss die Gesichtserkennung nun abstellen, bis sie den Abschluss einer Folgeabschätzung nachweisen kann.
18.03.2025	3.500.000 €	Caixabank (Spanien)	Die spanische Datenschutzbehörde reagierte auf die Beschwerde einer Privatperson. Diese hatte mehrere Konten bei der Caixabank, von denen sie sich eins mit einer Miteigentümerin teilte. Bei einem anderen war ihre Mutter Bevollmächtigte. Rief nun die Person, die Miteigentümer zweier der Konten war, "CaixaBankNow" auf und sah ihre Kontostände ein, konnte sie auch auf das dritte Konto zugreifen, zu dem sie keine Verbindung hatte. Die Untersuchung der AEPD ergab, dass es seitens der Bank keine datenschutzfreundliche Technikgestaltung gegeben hatte, was zu der in der Beschwerde beschriebenen Offenlegung führte. Die Datenverarbeitung erfolgte somit nicht unter Gewährleistung eines angemessenen Sicherheitsniveaus.
27.03.2025	3.692.263 €	Advanced Computer Software Group Limited (Vereinigtes Königreich)	Nachdem die Advanced Computer Software Group Limited 2022 Opfer einer Ransomware-Attacke wurde, strengte das Information Commissioner's Office eine Untersuchung gegen das Unternehmen an. Dabei stellte das ICO Mängel bei den zum Datenschutz implementierten technischen und organisatorischen Maßnahmen fest.
28.03.2025	150.000.000 €	Apple (USA)	Die französische Wettbewerbsbehörde verhängte ein Bußgeld gegen Apple. Grund war das von dem Tech-Giganten implementierte App Tracking Transparency (ATT)-System, das ihm zwischen April 2021 und Juli 2023 eine Marktvorherrschaft im Bereich der App-Verbreitung für iOS und iPadOS verschaffte.
02.05.2025	530.000.000 €	TikTok Technology Limited (China)	Die irische Datenschutzbehörde verhängte ein Bußgeld von 530.000.000 EUR gegen TikTok Technology Limited. Hintergrund war eine Untersuchung der Behörde, welche die Datenübermittlung von EU-Nutzern an chinesische Server seitens TikTok betraf. Zunächst behauptete das Unternehmen, keine Daten europäischer Benutzer auf seinen Servern

			in China abgelegt zu haben. Dies berichtigte TikTok jedoch im April 2025. Das Unternehmen entdeckte im Februar 2025 auf dessen Servern doch Daten von europäischen TikTok-Benutzern. Als Ursache wurde ein Fehler angegeben. Diese Daten waren nach Ansicht des DPC nicht nach den Standards geschützt, die die DSGVO verlangt.
23.06.2025	3.960.392 €	McDonald's Polska (Polen)	Die polnische Datenschutzbehörde untersuchte McDonald's Polska und den von ihm engagierten Auftragsverarbeiter 24/7 Communication. McDonald's hatte 24/7 Communication engagiert, um Mitarbeiter-Daten zu verarbeiten. Bei 24/7 Communication gab es jedoch keine angemessenen technischen und organisatorischen Maßnahmen zum Schutz verarbeiteter Daten. So gab es keine Risiko-Folgeabschätzung. Gleiches gilt für McDonald's Polska. Die implementierten technischen und organisatorischen Maßnahmen waren mangelhaft.
05.09.2025	150.000.000 €	Shein/Infinite Styles Services Co. (China/Irland)	Die französische Datenschutzbehörde CNIL ging gegen Infinite Styles Services Co., die irische Niederlassung von Shein, vor. Beim Besuch der Shein-Webseite legte diese auf den Endgeräten der Nutzer Cookies ab, ohne hierfür die Zustimmung der Nutzer einzuholen. Erst danach wurden Informationsbanner zur Einwilligung angezeigt, doch diese enthielten unvollständige Daten. Lehnte ein User ab, speicherte die Seite trotzdem neue Cookies und las bereits abgelegte weiterhin aus.
08.09.2025	325.000.000 €	Google (Google LLC, Google Ireland Limited)	Die französische Datenschutzbehörde CNIL ging nach einer Beschwerde der None Of Your Business (NOYB)-Organisation vom 24. August 2022 gegen Google LLC und Google Ireland Limited, beide Teil von Google, vor. In den Postfächern des Google Mail-Dienstes schaltete das Unternehmen in einigen Ordnern Werbung zwischen den Nachrichten, der von der Aufmachung her den tatsächlich erhaltenen E-Mails sehr ähnlich war. Dies geschah ohne Zustimmung der Nutzenden, was die CNIL als unrechtmäßig einstufte. Darüber hinaus drängte das Unternehmen seine Nutzer bei der Kontoeinrichtung dazu, Tracker zu aktivieren, und informierte nicht ausreichend über die geplante Nutzung. Damit waren erteilte Einwilligungen nach Ansicht der CNIL ungültig.
10.09.2025	1.800.000 €	S-Bank (Finnland)	Die finnische Datenschutzbehörde untersuchte die S-Bank. Diese hatte 2022 eine neue Authentifizierungsmethode für ihr Online-Banking implementiert, die jedoch eine gravierende Sicherheitslücke enthielt. Über diese war es monatelang möglich, sich in den Account anderer Kunden einzuloggen. Die Behörde stellte gravierende Mängel bei den implementierten Datenschutzmaßnahmen fest, die schon bei der Einschätzung möglicher Schwachstellen vor Einrichtung der Tools begannen.

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

5. Planung 2026

112 Für das Jahr 2026 wurden nachfolgend aufgeführte Punkte in die Planung aufgenommen, um die datenschutzrechtlichen Anforderungen auch im Hinblick auf die Datenschutzgrundverordnung konform zu erfüllen.

- Umsetzung der Anforderungen der DSGVO, des BDSG sowie weiterer datenschutzrechtlich relevanter Gesetze unter Mitwirkung der Gesellschaft
- Fortführung des Datenschutzmanagementsystems (PDCA)
- Durchführung von Audits und Prüfungshandlungen
  - Prüfung technisch-organisatorischer Maßnahmen nach Art. 32 DSGVO
  - Beherrschung von „Schatten-IT“
  - Sicherheit von Betriebsmitteln
  - Datenschutzrechtliche Prüfung Vernichtung von Daten
  - Standortbegehung unter Datenschutz-Aspekten
  - Prüfung der Webseite(n) unter Datenschutzaspekten
  - KI/Copilot und Datenschutz
  - Microsoft 365 Identity Management

  - für Auftragsverarbeiter: DSGVO-Compliance-Check (Jährliches Audit als Basis für das GCS-Zertifikat)

- Prüfung/Überwachung der Auftragsverarbeitungverhältnisse im Sinne des Art. 28 DSGVO
- Weiterentwicklung des Löschkonzeptes und Dokumentation in otris privacy
- Sensibilisierungsmaßnahmen zum Datenschutz (koordinierende Rolle)
- Durchführung eine Security-Awareness-Kampagne (koordinierende Rolle)
- Beratende Unterstützung bei der Einführung neuer rechtlicher Anforderungen

qualifiziert signiert
Frank Gundlach
27.01.2026
10:11:14 +01

27.01.2026

Datum

Frank Gundlach
Datenschutzbeauftragter