Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

zwischen

(nachfolgend „Auftraggeber“ genannt)

und

news aktuell GmbH
Mittelweg 144
20148 Hamburg

– Auftragsverarbeiter –
(nachfolgend „Auftragnehmer“ genannt)

(beide gemeinsam nachfolgend „Vertragsparteien“ genannt)

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1. Gegenstand der Vereinbarung, Art und Zweck der Verarbeitung

Präambel
Der Auftragnehmer bietet mit der Anwendung „zimpel“ die Möglichkeit zur Verarbeitung personenbezogener Daten des Auftraggebers. Diese Zusatzvereinbarung konkretisiert die diesbezüglichen datenschutzrechtlichen Verpflichtungen der Vertragsparteien. Sie findet Anwendung auf alle Tätigkeiten und Prozesse, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogenen Daten („Daten“) des Auftraggebers verarbeiten.

(1) Die Tätigkeit des Auftragnehmers umfasst die Bereitstellung einer Anwendung zur Erfassung, Speicherung und Verwaltung der o.g. Daten und – sofern diese Zusatzfunktion gebucht wurde - zum Aussand von Pressematerial per e-Mail an die jeweiligen Kontakte.
(2) Eine Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer ist darüber hinaus nicht vorgesehen.

(3) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt.

2. Art der personenbezogenen Daten, Kategorien betroffener Personen
Die Art der zu verarbeitenden Daten sind Namen und geschäftliche Adress- und Kontaktdaten von Medien und Journalisten, mit denen der Auftraggeber in Kontakt steht und die er selbst über die Anwendung „zimpel“ des Auftragnehmers erfasst, verarbeitet und pflegt. Zusätzlich zu den Kontaktdaten wie Name, Postanschrift des Mediums, Telefonnummer oder eMail Adresse können zu den einzelnen Kontakten Angaben zum Tätigkeitsfeld wie z.B. Position oder Zuständigkeiten erfasst werden, außerdem Notizen in einem Freitextfeld.

3. Dauer dieser Vereinbarung
(1) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Hauptvertrages inkl. möglicher Verlängerungen bzw. Folgeverträge oder -Aufträge in gleicher Sache. Mit dem Ende der Leistungsvereinbarung gemäß 1. endet diese Vereinbarung automatisch.

(2) Der Auftraggeber kann unabhängig von den Regelungen im Hauptvertrag diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Vereinbarung vorliegt. Nach der Kündigung darf der Auftragnehmer keine personenbezogenen Daten des Auftraggebers mehr verarbeiten. Die Vertragsparteien verpflichten sich, in einem solchen Fall auch den Hauptvertrag aufzulösen.

4. Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). I.d.R. wird die Dateneingabe, -Pflege und Nutzung innerhalb und außerhalb der Anwendung durch den Auftraggeber eigenständig vorgenommen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf expliziten Wunsch und dokumentierte Weisung des Auftraggebers.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5. Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer verpflichtet sich, dafür zu sorgen, dass die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Beschäftigten auch nach der Beendigung ihrer Tätigkeit und dem Ausscheiden aus dem Unternehmen des Auftragnehmers aufrecht bleibt. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6. Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten und dieses bei gegebenem Anlass, mindestens aber jährlich, durchführen.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem **Anlage „zimpel / Technisch-Organisatorische Maßnahmen zum Datenschutz“** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate

Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

7. Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Derzeit werden keine Subunternehmer im Rahmen der vertragsgegenständlichen Auftragsverarbeitung eingesetzt.

(2) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Die Auslagerung auf Subunternehmer ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Subunternehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten schriftlich oder in Textform gegenüber dem Auftragnehmer Einspruch gegen die geplante Auslagerung erhebt.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Subunternehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(6) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8. Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Soweit betroffene Personen gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit ausüben können, stellt der Aufragnehmer sicher, dass sie die Daten, die sie dem Auftraggeber bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten können.

(3) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder die betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(4) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten und vor Erhalt einer ausdrücklichen schriftlichen Weisung des Auftraggebers keine Handlungen gegenüber der betroffenen Person vornehmen.

9. Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG-neu oder einer anderen gesetzlichen Bestimmung dazu verpflichtet, einen Datenschutzbeauftragten zu benennen oder hat der Auftragnehmer freiwillig einen Datenschutzbeauftragten benannt, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten zum Zweck der direkten

Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Auftraggeber unverzüglich anzuzeigen.

Als Datenschutzbeauftragte ist beim Auftragnehmer

Frau Vera Walter, datenschutz@newsaktuell.de, Tel.: 040/4113-38277

bestellt.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich (Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10. Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen oder Beendigung dieser Vereinbarung kann der Auftraggeber mittels einer speziellen Export-Funktion seine Daten im Tabellenformat gesammelt aus der Anwendung exportieren. Der Auftragnehmer hat alle kundeneigenen Daten des Auftraggebers anschließend umgehend aus der Anwendung zu löschen.

(2) Der Auftragnehmer weist auf Wunsch dem Auftraggeber in Textform mit Datumsangabe nach, dass er sämtliche Daten gelöscht und somit keine Daten des Auftraggebers zurückbehalten hat.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Dazu kann der Auftraggeber oder ein beauftragter Prüfer die eingesetzte Infrastruktur und Anwendungen des Auftragnehmers prüfen. Der Auftraggeber stimmt die Durchführung der Inspektionen dabei mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Der Auftragnehmer erteilt dem Auftraggeber zudem unverzüglich konkrete Auskunft im Einzelfall.

12. Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden

gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

(2) Der Auftragnehmer haftet dem Verantwortlichen gegenüber entsprechend auch für die Einhaltung datenschutzrechtlicher Vorgaben durch die Subunternehmer, die er zur Erfüllung seiner Aufgaben einsetzt. Das Verschulden von Subunternehmern ist dem Auftragnehmer wie eigenes Verschulden zuzurechnen.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen, wenn der Auftraggeber einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist.

13. Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Abschluss dieser Vereinbarung unwirksam oder undurchführbar werden, so wird die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung hiervon nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen und datenschutzrechtlichen Zielsetzung, welche die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben, am nächsten kommt. Dasselbe gilt auch im Falle einer unbeabsichtigten Regelungslücke.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Änderungen und/oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses. Mündliche Nebenabreden zu dieser Vereinbarung bestehen nicht.

(5) Dies Vereinbarung unterliegt deutschem Recht.

(6) Alle Leistungen des Auftragnehmers in Zusammenhang mit der Erfüllung seiner Pflichten aus dieser Vereinbarung sind mit der Vergütung aus dem Hauptvertrag abgegolten.

(7) Der Anhang „zimpel / Technisch-Organisatorische Maßnahmen zum Datenschutz", Stand 01.08.2023, ist Bestandteil dieser Vereinbarung.

Ort, Datum:	
Stempel, Unterschrift Auftraggeber	

Hamburg,	2023
na•news aktuell Ein Unternehmen der dpa-Gruppe news aktuell GmbH Mittelweg 144, 20148 Hamburg Telefon (040) 4113-32850, Fax (040) 4113-32855 info@newsaktuell.de, www.newsaktuell.de Vera Walter Rechtsreferentin und Datenschutzbeauftragte	
Stempel, Unterschrift Auftragnehmer	

zimpel / Technisch-Organisatorische Maßnahmen zum Datenschutz

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren

Standort Rechenzentrum: Am Firmensitz in Hamburg

Technische Maßnahmen	Organisatorische Maßnahmen
• Automatisches Zugangskontrollsystem • Mehrere Zwischentüren, alle nur mit persönlicher Chipkarte bzw. Schlüssel und Tip Key zu öffnen • Videoüberwachung des Haupteingangs • Zugang zum Rechenzentrum nur aus dem Inneren des Firmengebäudes • Alarmanlage mit Sicherheitsdienst	• Zutritt nur für speziell autorisiertes IT-Personal • Zugangskarte, Schlüssel und Tip Key-Ausgabe nur an speziell berechtigtes IT-Personal inkl. Dokumentation • Zutritt für Gäste nur in Begleitung autorisierter IT-Mitarbeiter • Protokollierung von Besuchen • Außerhalb der Arbeitszeiten zusätzliches Passwort des IT-Personals erforderlich • 24/7 Rufbereitschaft bei Alarmauslösung • Bei Alarmauslösung: Telefonischer Kontakt des Wachdienstes inkl. Kennwortabfrage • Bei Alarmauslösung: Zutritt für Wachdienst nur in Anwesenheit von autorisiertem IT-Mitarbeiter oder nach Freigabe

Zugriffskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme und Anwendungen von Unbefugten genutzt werden

Technische Maßnahmen	Organisatorische Maßnahmen
• Zugriff nur mit Benutzername und Passwort • Login mit 2-Faktor-Authentifizierung in kritischen Bereichen • Passwort-Verschlüsselung auf aktuellem technischen Stand (Salt & Hash) • Adminrechte-Vergabe nach dem Prinzip der Notwendigkeit • Automatische Desktopsperre an Mitarbeiter-Rechnern • Anti-Viren-Software auf allen Laptops • Festplattenverschlüsselung aller Laptops • Remote-Zugriff auf Anwendungen im internen Firmennetz nur per VPN • Firewalls immer auf neuestem Stand der Technik • Firewall-Architektur für das interne und externe Netz inkl. DMZ • Schutz vor DDOS- und weiteren potenziellen Angriffen durch Filterung des Web-Traffic • Logisch getrennte Logs • Datenverarbeitung aller Systeme ausschließlich im firmeneigenen Netz	• Zentrale Rechtevergabe • Zugriff durch news aktuell auf kundeneigene Daten nur für speziell berechtigte Administratoren • Passwort-Richtlinie für Mitarbeiter • Allgemeine Richtlinien zum Datenschutz • Vertraulichkeitsverpflichtung Mitarbeiter • Sensibilisierung und Online-Trainings für Informationssicherheit für alle Mitarbeiter • Externer Aktenvernichtungsservice für Papierdokumente • Sichere Löschung von Daten auf Datenträgern vor Wiedereinsatz oder Vernichtung

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

Technische Maßnahmen	Organisatorische Maßnahmen
• Trennung von Test- und Produktivumgebung • Trennung der kundeneigenen Daten von den Systemdaten durch Rechtesystem	• Steuerung über Berechtigungskonzept • Festlegung von Datenbankrechten

Pseudonymisierung/Anonymisierung

Maßnahmen, die gewährleisten, dass bei personenbezogenen Daten entweder keine Möglichkeit zur Identifizierung des Betroffenen besteht (Anonymisierung), oder eine Identifizierung nur unter Hinzuziehung separater Informationen möglich ist (Pseudonymisierung)

Technische Maßnahmen	Organisatorische Maßnahmen
• Anonymisierung aller Daten, die in der Anwendungsentwicklung genutzt werden • Anonymisierung aller Daten, die für Testverfahren genutzt werden	• Interne Anweisung, personenbezogene Daten im Fall einer Weitergabe zu anonymisieren / pseudonymisieren

Eingabekontrolle

siehe nächste Seite

Maßnahmen, die gewährleisten, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder gelöscht worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
• Technische Protokollierung der Eingabe, Änderung und Löschung von Daten in der zur Anwendung gehörenden Mediendatenbank • Automatische Überwachungsprotokolle für verschiedene beteiligte Systeme	• Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes • Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (keine Benutzergruppen) • Dokumentation, mit welchen Programmen welche Daten eingegeben, geändert und gelöscht werden können

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten während einer elektronischen Übertragung oder eines Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass dokumentiert ist, an welche Stellen eine Übermittlung vorgesehen / erfolgt ist.

Technische Maßnahmen	Organisatorische Maßnahmen
• Verschlüsselte Kommunikation der Anwendung durch SSL-Zertifikate • Verschlüsselung auch im internen Netz • Protokollierung von Zugriffen und Abrufen	• Vorabprüfung jeglicher Datenüberlassungen oder -weitergaben außerhalb der normalen Funktionalität durch Teamleitung und/oder Datenschutzbeauftragte • Keine Weitergabe über Datenträger; sofern unumgänglich, nur in pseudonymisierter oder anonymisierter Form • Dokumentation aller Verarbeitungen im Kundenauftrag

Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, nach einem physischen oder technischen Zwischenfall wiederhergestellt werden können und Systeme auch unter Belastung fehlerfrei funktionieren.

Technische Maßnahmen	Organisatorische Maßnahmen
• Brandmeldeanlage und Brandschutztüren im Rechenzentrum • Sauerstoffreduzierung Rechenzentrum als Brandschutzmaßnahme • Klimatisierung Rechenzentrum inkl. Überwachung • USV (unterbrechungsfreie Stromversorgung, Notstromeinspeisung) • Alarmanlage Rechenzentrum mit Wachdienst • Redundanz aller wichtigen Systeme und Daten • Regelmäßige Vulnerability Scans • Backup- und Recovery Konzept	• Kontrolle des Sicherungsvorgangs • Doppelte Datensicherung in zwei physikalisch getrennten Räumen • Existenz eines Notfallplans / Wiederanlaufplans

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Jährlicher Compliance Check durch die Datenschutzbeauftragte und die Informationssicherheitsbeauftragte
- Regelmäßige Abstimmung von Projekten mit der Informationssicherheitsbeauftragten und/oder Datenschutzbeauftragten
- Fortlaufende Dokumentation von Änderungen

Weitere Maßnahmen / Allgemeines

- Leitlinie IT-Sicherheit und Datenschutz
- Datenschutz- und Sicherheits-Prinzipien in der Entwicklung
- Pair Programming / 4 Augen Prinzip in der Entwicklung
- Incident-Response-Prozess
- Automatisiertes Monitoring aller kritischen Systeme inkl. Benachrichtigungsfunktion
- Zeitnahes Einspielen von Sicherheitsupdates und Patches
- Regelmäßiger Einsatz von Code-Scanning-Tools

Stand: August 2023