Philipps-Universität Marburg
Der Präsident
Eing.: 25. 04. 2022
Tgb.-Nr.: Anl.:

Datenschutzkonzept des Demokratiezentrums Hessen an der Philipps-Universität Marburg

Stand: 30.03.2022

Projekt:	Demokratiezentrum Hessen an der Philipps-Universität Marburg
Laufzeit:	01.01.2020-31.12.2024
Durchführende Institution:	Demokratiezentrum Hessen Wilhelm-Röpke-Str. 6A 35032 Marburg 06421-2821110 kontakt@beratungsnetzwerk-hessen.de
Projektleitung:	Dr. Reiner Becker Wilhelm-Röpke-Str. 6A 35032 Marburg 06421-2824535 reiner.becker@uni-marburg.de
Verantwortliche:	Prof. Dr. Thomas Nauss Präsident der Philipps-Universität Marburg Biegenstraße 10 35037 Marburg 06421 28 26000
Datenschutzbeauftragter:	Dr. Rainer Viergutz Biegenstraße 10 35037 Marburg 06421 28 26000 datenschutz@uni-marburg.de

Inhalt

Inhalt 2

1. Einleitung 3

a. Zum Projekt 3

b. Zum Datenschutzkonzept 3

2. Datenerhebung 3

a. Art der Daten 3

b. Art der Verarbeitung 4

3. Rechtsgrundlage für die Erhebung 5

a. Einwilligung, Art. 6 Abs. 1 lit. a DSGVO 5

b. Datenverarbeitung für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen, Art 6 Abs. 1 lit. b DSGVO 5

c. Datenverarbeitung zur Erfüllung rechtlicher Verpflichtungen, Art. 6 Abs. 1 lit. c DSGVO 6

d. Datenverarbeitung zur Wahrnehmung öffentlicher Interessen gem. Art. 6 Abs. 1 lit. e DSGVO 6

4. Rechte der betroffenen Person 6

a. Auskunft über gespeicherte Daten 6

b. Widerruf, Löschung, Anonymisierung 6

c. Dauer der Speicherung 7

5. Technische und Organisatorische Maßnahmen 7

a. Zutrittskontrolle 7

b. Zugangskontrolle 8

c. Zugriffskontrolle 8

d. Trennungskontrolle 9

e. Pseudonymisierung 9

f. Wiedergabekontrolle und Eingabekontrolle 9

g. Verfügbarkeit und Belastbarkeit 9

h. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 9

i. Dienstleister 10

j. Incident Response-Management - Unterstützung bei der Reaktion auf Sicherheitsverletzungen 10

1. Einleitung

a. Zum Projekt

Rechtsextremismus, Antisemitismus, Rassismus oder Demokratiefeindlichkeit vorzubeugen und entgegenzuwirken – das ist Ziel und Aufgabe des „Beratungsnetzwerks Hessen – gemeinsam für Demokratie und gegen Rechtsextremismus". Seit 2007 berät es in solchen Fällen Hilfesuchende – Schulen, Eltern, Familienangehörige, Kommunen, Vereine, Diskriminierungsopfer und andere Betroffene – und bietet ein breites Spektrum entsprechender Präventionsmaßnahmen an. Die professionelle Beratung ist individuell, qualifiziert, vertraulich und kostenlos. Im Beratungsnetzwerk kooperieren zahlreiche relevante staatliche, nichtstaatliche und kirchliche Institutionen, Organisationen, Vereine, öffentliche und freie Träger aus ganz Hessen sowie landesweit eingesetzte mobile Beraterinnen und Berater, um sich gemeinsam für die beschriebenen Ziele und Aufgaben einzusetzen. Zentrale Anlauf- und Geschäftsstelle des Beratungsnetzwerks ist das Demokratiezentrum Hessen, das an der Philipps- Universität Marburg angesiedelt ist. Es vermittelt Ansprechpartner vor Ort, koordiniert die Beratung, Vernetzung und Prävention und dokumentiert die Arbeit des Beratungsnetzwerks Hessen. Finanziert wird die Arbeit des Beratungsnetzwerks und des Demokratiezentrums Hessen durch das Hessische Ministerium des Inneren und für Sport im Rahmen des Landesprogramms „Hessen – aktiv für Demokratie und gegen Extremismus" sowie durch das Bundesministerium für Familie, Senioren, Frauen und Jugend über das Programm „Demokratie leben! Aktiv gegen Rechtsextremismus, Gewalt und Menschenfeindlichkeit". Dem Demokratiezentrum zugeordnet ist seit 2021 die „Recherche- und Informationsstelle Antisemitismus Hessen" (RIAS Hessen). RIAS Hessen nimmt Meldungen zu antisemitischen Vorfällen entgegen und wertet diese nach einem standardisierten Verfahren für die Erstellung von Berichten aus. Die im Folgenden ausgearbeiteten Datenschutzrichtlinien sind auch für RIAS Hessen geltend.

b. Zum Datenschutzkonzept

Vorliegendes Datenschutzkonzept beschreibt in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte des Demokratiezentrums Hessen. Das Datenschutzkonzept kann auch als Grundlage für datenschutzrechtliche Prüfungen genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutzgrundverordnung (DSGVO) sowie des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) gewährleistet und nachgewiesen werden.

2. Datenerhebung

Personenbezogene Daten werden von uns erhoben, wenn Personen Kontakt mit dem Demokratiezentrum aufnehmen, zum Beispiel als Interessenten für eine Beratung, für eine Publikation, eine Veranstaltung oder Projektförderung. Dies geschieht durch die Registrierung für Online-Dienste, Kontaktaufnahme per Telefon oder E-Mail oder wenn sie im Rahmen bestehender Geschäftsbeziehungen Dienstleistungen nutzen.

a. Art der Daten

- Angaben zur persönlichen Identifikation
    - Vor- und Nachname, Anschrift, E-Mail-Adresse, Telefonnummer, Faxnummer
- Auftragsdaten
- Kundennummer, Auftragsnummer, Rechnungsdaten
    - Unternehmensbezogene Daten
    - Firmierung, Abteilung, Tätigkeit

- Daten zu Ihrem Online-Verhalten
    - IP-Adressen, Benutzernamen, Daten zu Ihren Besuchen auf unserer Website, in den Kundenportalen oder in der App, ausgeführte Aktionen auf unseren Websites und in den Kundenportalen, Ort des Zugriffs
- Informationen zu Ihren Interessen und Wünschen
    - Z.B. über Kontaktformulare oder über sonstige Kommunikationskanäle
- Informationen über Ihren beruflichen Werdegang
    - Z.B. Berufsausbildung, bisherige Arbeitgeber, sonstige Qualifikationen
- **Personenbezogene Daten Minderjähriger:** Angebote des Demokratiezentrums richten sich auch an Minderjährige. In allen Belangen der Datenverarbeitung, wo dies notwendig ist, wie beispielsweise bei Seminaranmeldungen, wird die schriftliche Einverständniserklärung der Erziehungsberechtigten eingeholt. Soweit erkennbar personenbezogene Daten Minderjähriger ohne Einwilligung der Erziehungsberechtigten verarbeitet werden, werden diese umgehend gelöscht.

b. Art der Verarbeitung

- Das Demokratiezentrum gibt personenbezogene Daten nur weiter, wenn gesetzliche Bestimmungen dies gebieten, die betroffenen Personen eingewilligt haben oder zur Erfüllung vertraglicher Verpflichtungen.
    - Hierzu zählt die Weitergabe der Daten an Beratungsteams, sofern die Betroffenen hierin eingewilligt haben.
    - Des Weiteren werden die anonymisierten Beratungsfälle von den Beratungsteams in eine Datenbank des Demokratiezentrums für das Berichtswesen und zu wissenschaftlichen Forschungszwecken eingegeben.
    - RIAS Hessen richtet sich in der Datenverarbeitung und der Datenlöschung bzw. Anonymisierung an den Richtlinien von RIAS Bund e.V. aus.

Personenbezogene Daten werden verarbeitet, um vertragliche Verpflichtungen zu erfüllen. Insbesondere gegenüber Banken und Finanzdienstleistern zur Abwicklung der finanziellen Angelegenheiten, außerdem gegenüber Partnergesellschaften und Förderpartnern, gegenüber Partnern aus der Wissenschaft und gegenüber strategischen Partnern.

c. Kategorien betroffener Personen

Bei den folgenden Personengruppen werden vom Demokratiezentrum Hessen Daten erhoben:

- Interessierte für eine Beratung
- Personen, die sich direkt bei RIAS Hessen melden, über Telefon oder das E-Mail-Kontaktformular sowie bezugnehmend auf die Meldungen, die über das Formular von RIAS Bund an RIAS Hessen gerichtet sind.
- Interessierte für Publikationen, Veranstaltungen, Förderungen
- Teilnehmer von Seminaren und Tagungen
- Mitglieder des Beratungsnetzwerks
- Vertragspartner und Dienstleister
- Newsletter-Abonnenten

3. Rechtsgrundlage für die Erhebung

a. Einwilligung, Art. 6 Abs. 1 lit. a DSGVO

Die informierte Einwilligung (Volltext siehe Anhang) ist Rechtsgrundlage der Datenverarbeitung. Die Einwilligung erfolgt bei der Benutzung der Kontaktformulare auf den Websites des Demokratiezentrums durch das Aktvieren eines entsprechenden Feldes; bei telefonischen Anfragen erfolgt die Einwilligung mündlich, bei Teilnahme an Veranstaltungen des Demokratiezentrums mit dem Eintrag auf einer Teilnehmerliste, die für Verwendungsnachweise obligatorisch sind, bei der Erstellung von Ton- und/oder Bildaufnahmen im Rahmen dieser Veranstaltungen durch eine schriftliche Einverständniserklärung. Mit der Einwilligung erklären sich die o.g. unterschiedlichen Personengruppen insbesondere dazu bereit, dass

- personenbezogene Daten erfasst und gespeichert werden,
- bei Beratungsanfragen personenbezogene Daten an entsprechende Beratungsteams übermittelt werden,
- anonymisierte Daten zu den Beratungsverläufen von den Forschenden und den Beratungsteams ausgewertet und durchsucht werden können.

RIAS Hessen erhebt Daten analog zum Vorgehen des Demokratiezentrums und arbeitet diese anonymisiert in die Jahresberichte ein. Im Arbeitsbereich Wissenschaft und Bildung werden die anonymisierten Vorfälle im Rahmen der adäquaten Wahrnehmung von Aufgaben im öffentlichen Interesse verwendet. (Vgl. 3.d.)

Mit Einholen der Einwilligung wird die betroffene Person über sein/ ihr Recht auf Auskunft und Widerruf informiert.

Gem. Art. 8 DSGVO in Verbindung mit Erwägungsgrund (38) zur Datenschutzgrundverordnung ist die Einwilligung von Minderjährigen nicht erforderlich:

- Gem. Art. 8 DSGVO ist die Einwilligung von Minderjährigen bei der Annahme von Angeboten von Diensten der Informationsgesellschaft grundsätzlich ab sechszehn Jahren rechtswirksam.
- Nach Erwägungsgrund 38 zur Datenschutzgrundverordnung ist die Einwilligung des Trägers der elterlichen Verantwortung im Zusammenhang mit Präventions- und Beratungsdiensten die einem Kind unmittelbar angeboten werden, nicht erforderlich.
    - Gem. Art. 1 Nr. 2 Informations-Richtlinie 98/34/EG handelt es sich um einen Dienst, soweit eine Dienstleistung im Fernabsatz, elektronisch und auf individuellen Abruf eines Empfängers erbracht wird.
    - Die Angebote des Demokratiezentrums werden zunächst via Internet oder Telefon (elektronisch) in Anspruch genommen, also ohne gleichzeitige physische Anwesenheit (Fernabsatz) durch eine individuelle Kontaktaufnahme des Interessenten (auf Abruf des Empfängers).
- Wird bei der Kontaktaufnahme deutlich, dass das Ziel des Minderjährigen keine Beratung ist, wird er auf seine Rechte hingewiesen.

b. Datenverarbeitung für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen, Art 6 Abs. 1 lit. b DSGVO

Personenbezogene Daten werden im Rahmen vorvertraglicher Korrespondenz verarbeitet. Die konkreten Zwecke hängen von der gestellten Anfrage ab. In Frage kommt hier beispielsweise Anfrage nach Informationen, Beratung oder Teilnahme an einer Veranstaltung.

c. Datenverarbeitung zur Erfüllung rechtlicher Verpflichtungen, Art. 6 Abs. 1 lit. c DSGVO
Das Demokratiezentrum verarbeitet personenbezogene Daten um den eigenen (bspw. steuerrechtlichen) gesetzlichen Verpflichtungen nachzukommen im erforderlichen Umfang.

d. Datenverarbeitung zur Wahrnehmung öffentlicher Interessen gem. Art. 6 Abs. 1 lit. e DSGVO
Die Verarbeitung der personenbezogenen Daten liegt im öffentlichen Interesse und dient der Wahrnehmung der Forschungsaufgaben der Universität. Die Verarbeitung ist rechtmäßig, da folgende Voraussetzungen erfüllt werden:

- Die Verarbeitung der Daten ist für die wissenschaftlichen Zwecke erforderlich, da durch die anonymisierte Auswertung der dokumentierten Beratungsfälle das Angebot der Mobilen Beratung fortlaufend qualitativ weiterentwickelt wird. zudem dienen diese Zahlen bzw. die Statistik für das Berichtswesen gegenüber den Mittelgebern des Bundes und des Landes Hessen.
- Die Interessen der Forschenden an der Verarbeitung der Daten überwiegen das Interesse der betroffenen Personen an der Nicht-Verarbeitung. Dies betrifft die Aufbewahrung der anonymisierten dokumentierten Beratungsfälle deren Informationsgehalt für folgende Beratungsfälle in a) derselben Region und/oder b) im selben inhaltlichen Kontext von zentraler Bedeutung ist. Den Interessen der Betroffenen wird durch die vorherige vollständige Anonymisierung ihrer Daten ausreichend Rechnung getragen, da Rückschlüsse auf ihre Person im Rahmen der Forschungstätigkeit nicht länger möglich sind.

4. Rechte der betroffenen Person

a. Auskunft über gespeicherte Daten
Betroffene Personen haben das Recht, Auskunft über die gespeicherten Daten zu erhalten, die sie betreffen. Der Antrag auf Auskunft ist schriftlich an das Demokratiezentrum zu stellen. Dieses erzeugt einen maschinenlesbaren Ausdruck der Daten und händigt ihn der betroffenen Person aus.

b. Widerruf, Löschung, Anonymisierung
Betroffene haben das Recht, vom Demokratiezentrum Auskunft zu erhalten, welche ihrer personenbezogenen Daten verarbeitet werden. Sofern diese Informationen nicht (mehr) stimmen, können die Betroffenen die Berichtigung der Daten verlangen, b ei unvollständigen Angaben Ergänzungen. Sofern die Daten an Dritte weitergegeben wurden, werde diese bei entsprechender Rechtslage hierüber informiert.

Die unverzügliche Löschung der Daten wird vollzogen, sobald keiner der in Art. 6 DSGVO genannten Zulässigkeitstatbestände erfüllt ist. Gründe für den Wegfall der Rechtsgrundlage können sein:

- Die personenbezogenen Daten werden nicht länger für diejenigen Zwecke benötigt, für die sie erhoben wurden.
- Die Einwilligung aufgrund derer die Daten verarbeitet wurden, wurde widerrufen und es fehlt an einer sonstigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person widerspricht der Verarbeitung und es bestehen keine vorrangigen Gründe für eine Datenverarbeitung.
- Die Daten der betroffenen Person wurden unrechtmäßig verarbeitet.
- Die personenbezogenen Daten müssen zur Erfüllung einer gesetzlichen Verpflichtung gelöscht werden.

Die Einschränkung der Datenverarbeitung kann in folgenden Fällen verlangt werden:

- Die Richtigkeit der Daten wird von der betroffenen Person bestritten und das Demokratiezentrum hatte noch keine Gelegenheit sich von der Richtigkeit der Daten zu überzeugen.
- Die personenbezogenen Daten werden zwar nicht mehr für die ursprünglichen Zwecke verarbeitet, werden jedoch noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.
- Gegen die Verarbeitung wurde durch die betroffene Person Widerspruch eingelegt, es steht jedoch noch nicht fest, ob die Interessen des Demokratiezentrums die berechtigten Interessen der betroffenen Person überwiegen.

Die Anonymisierung der Daten erfolgt, wenn kein Antrag auf Löschung gestellt wird und der Datenbestand eine faktische Anonymisierung zulässt. Die Beratungsfälle werden von den Berater*innen vollständig anonymisiert in die Falldatenbank eingegeben.

c. Dauer der Speicherung

- Gemäß den geltenden Datenschutzbestimmungen speichert das Demokratiezentrum Ihre personenbezogenen Daten nicht länger, als sie für die Zwecke der jeweiligen Verarbeitung benötigt werden. Sofern die Daten nicht mehr zur Erfüllung vertraglicher oder gesetzlicher Pflichten benötigt werden, werden sie regelmäßig gelöscht.
- RIAS Hessen löscht diese Daten nach 18 Monaten; die anonymisieren Daten stehen für die Wahrnehmung von Aufgaben im öffentlichen Interesse weiter zur Verfügung.
- Personenbezogene Daten werden nur dann über diese Aufbewahrungsfristen hinaus befristet aufbewahrt, wenn einer der folgenden Gründe vorliegt:
    - Es müssen handels- bzw. steuerrechtliche Aufbewahrungspflichten eingehalten werden: Die Fristen zur Aufbewahrung vorrangig nach den Regelungen des Handelsgesetzbuches und der Abgabenordnung liegen bei bis zu zehn Jahren.
    - Zum Erhalt von Beweismitteln im Falle rechtlicher Streitigkeiten im Rahmen der gesetzlichen Verjährungsvorschriften.
    - Zu wissenschaftlichen Forschungszwecken, soweit die Verarbeitung für solche Zwecke erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen.

5. Technische und Organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen werden vorgenommen, um die datenschutzrechtlichen Bestimmungen einzuhalten:

a. Zutrittskontrolle

Maßnahmen zur Zutrittskontrolle haben das Ziel, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden:

- **Zutritt zu Gebäuden und Räumlichkeiten**: Die Gebäude und Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, sind nur durch definierte Zutrittsstellen betretbar. Die Räumlichkeiten sind durch elektronische oder mechanische Schließanlagen gesichert.
- **Serverräume/Rechenzentrum**: Die Server zur Datenhaltung und -verarbeitung befinden sich in verschlossenen, zutrittsbeschränkten Räumen des Hochschulrechenzentrums (HRZ). Weitere Maßnahmen des HRZ: Alarmanlage, Schlüsselregelung inkl. Liste, Protokoll der Besucher*innen.

b. Zugangskontrolle

Maßnahmen zur Zugangskontrolle haben das Ziel zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- **Kennwortschutz**: Login an Datenverarbeitungssystemen ausschließlich mit Benutzername und Passwort möglich. Das Passwort dient dem sicheren Zugang unter anderem zu Datenverarbeitungssystemen und gewährleistet, dass nur berechtigte Personen auf bestimmte Daten Zugriff haben.
- **Vergabe von Benutzerrechten**: Die Vergabe von Benutzerrechten für Systeme erfolgt ausschließlich durch Systemadministratoren. Für diese Benutzerrechte gelten folgende Vorgaben:
    - Eigenes Benutzerkonto für jede natürliche Person
    - Anmeldeprozess mit Benutzerkennung und Passwort
    - Passwort-Vorgaben sowie deren zwingende Einhaltung
- **Datenhaltung**: Die Speicherung und Aufbewahrung personenbezogener Daten erfolgt ausschließlich auf passwortgeschützten Gruppenlaufwerken, die durch das Hochschulrechenzentrum betreut werden.
- Fernzugriffe erfolgen über VPN. Der VPN-Zugang wird neben einem Passwort mittels Zwei-Faktor-Authentifizierung geschützt.
- **Automatische Sperrung von Bildschirmen**: Automatische Sperrung der Bildschirme erfolgt nach 15 Minuten.

c. Zugriffskontrolle

- **Protokollierung von Zugriffen**: Über die Vergabe von verschiedenen Berechtigungen oder durch die Vergabe von verschiedenen Rollen und Profilen wird der Zugriff gesteuert für: Einsichtnahme, Veränderung und Löschung aller Transaktionen und/oder Objekte.
  Kontrollierter Zugriff auf personenbezogene Daten durch:
    - definierte Benutzergruppen
    - Protokollierung des Zugriffs auf personenbezogene Daten (Lesen, Ändern, Löschen)
    - Firewall und Virenschutz mit automatisierter regelmäßiger Aktualisierung, Verschlüsselung lokal gespeicherter Daten
    - Trennung von Systemdateien unterschiedlicher Anwendungen
    - Trennung von Benutzerdateien verschiedener Benutzer
    - Verwaltung der Benutzerrechte durch Administrator*innen

d. Trennungskontrolle

- **Trennungskontrolle durch Systeme sowie Berechtigung** (siehe Zugang und Zugriffsberechtigung)
  - Daten zu unterschiedlichen Zwecken werden getrennt verarbeitet und getrennt gespeichert.
  - Klare Trennung von Benutzerdateien verschiedener Benutzer

e. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechend technischen und organisatorischen Maßnahmen unterliegen. Für die Wahrnehmung von Aufgaben im öffentlichen Interesse kann dies auch die Forderung nach einer Änderung von identifizierbaren Merkmalen umfassen.

f. Wiedergabekontrolle und Eingabekontrolle

- **Elektronische Verschlüsselungstechniken**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, unter anderem durch Verschlüsselung, Virtual Private Networks (VPN). Die Datenübertragung erfolgt über verschlüsselte Netzwerkverbindungen, die dem aktuellen Stand der Technik entsprechen.
- **Entsorgung und Wiederverwendung von Datenträgern**: Vor einer Wiederverwendung oder Entsorgung von Datenträgern findet stets deren vollständige (physikalische) Löschung nach dem jeweiligen Stand der Technik statt. Die Benutzung von mobilen Datenträgern wird auf ein Minimum reduziert.
- **Entsorgung von analogen Akten**: Analoge Ausdrucke und Akten oder Bestandteile von Akten werden datenschutzkonform und sachgerecht entsorgt, sobald ihr Verwendungszweck nicht länger gegeben ist. Dies betrifft auch handschriftliche Notizen bei Beratungsfällen oder der Annahme von Meldungen bei RIAS Hessen.
- **Verarbeitung personenbezogener Daten auf Datenträgern in nicht elektronischer Form**:
  - Die Datenträger werden vor dem Zugriff Nichtberechtigter in verschlossenen und gesicherten Räumen oder Behältnissen aufbewahrt.
  - Nach Wegfall aller Rechtsgrundlagen für die Verarbeitung werden die Datenträger unwiderruflich gelöscht oder vernichtet. Die Löschung bzw. Vernichtung wird dokumentiert.

g. Verfügbarkeit und Belastbarkeit

- Back-Up-Systeme: Durch regelmäßige Backups ist sichergestellt, dass personenbezogene Daten regelmäßig gesichert werden und wiederhergestellt werden können.
- Nach Fortfall aller Zwecke für die Verarbeitung, beziehungsweise der gesetzlichen Aufbewahrungsfristen werden die Daten unverzüglich und unwiderruflich gelöscht.
- Weitere Maßnahmen: Feuer- und Rauchmeldeanlagen, Feuerlöschanlage, Klimatisierung, USV, Schutzsteckdosen und Temperaturüberwachung im Serverraum, Verwendung von RAID-Systemen, Existenz eines Notfallplans

h. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Etabliertes Datenschutz-Management:

i. Dienstleister

Um sicherzustellen, dass bei den Dienstleistern dieselben datenschutzrechtlichen Standards wie im Demokratiezentrum eingehalten werden, hat das Demokratiezentrum entsprechende Verträge zur Auftragsverarbeitung abgeschlossen. Diese Verträge regeln unter anderem:

- Dritte erhalten nur dann Zugriff auf die Daten, wenn sie diese zur Erledigung der an sich übertragenen Aufgaben benötigen;
- Mitarbeiter der Dienstleister erhalten nur dann Zugriff auf die personenbezogenen Daten, wenn sie sich explizit zur Einhaltung der datenschutzrechtlichen Regelungen verpflichtet haben;
- Bei den Dienstleistern werden technische und organisatorische Maßnahmen eingehalten, welche die Datensicherheit und den Datenschutz gewährleisten;
- Dass die Daten nach Beendigung der Auftragsverarbeitung gelöscht werden und dieser Vorgang dokumentiert wird.

j. Incident Response-Management - Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Maßnahmen zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen werden realisiert durch:

- Einsatz von Spamfiltern
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen
- Dokumentierter Prozess zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und ISB in Sicherheitsvorfälle
- Dokumentation von Sicherheitsvorfällen via Ticketsystem

Marburg, den 22.04.22	Marburg, den 22.4.22	Marburg, den
Dr. Reiner Becker Leiter Demokratiezentrum	Dr. Susanne Urban Projektleitung RIAS Hessen	Dr. Rainer Viergutz Behördlicher Datenschutzbeauftragter