**A.5.1 - Technisch – organisatorische Maßnahmen zur Reduzierung der festgestellten Risiken**  
  
Stand 11.07.2022

Version 1.2

Vorbemerkung: Dieses Dokument sollte im Zusammenhang mit A.5 (Risikoanalyse) eingesetzt werden und kann in A.4 (VVT) in der Spalte TOM als Quelle für die konkret wirkenden technisch-organisatorischen Maßnahmen referenziert werden.

1. Transparenz, Art. 5 Abs. 1 lit. a) DSGVO).

Ist die Transparenz gewährleistet, wenn die personenbezogenen Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten nicht informiert sind. | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen die Betroffenen über die Umstände der Datenverarbeitung informieren. | relevant | umgesetzt | Beleg für Umsetzung der Maßnahmen |
| Es werden personenbezogene Daten außerhalb der Verwaltung verarbeitet, z. B. von Bürgerinnen und Bürgern *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3)*  Es werden personenbezogene Daten in einem Bereich verarbeitet, indem Kundenverkehr stattfindet, z. B. im Bürgerbüro *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3,4)*  Es findet eine Auftragsverarbeitung statt *(In Betracht kommen z. B. die Maßnahmen Nrn. 7,8)*  Zwischen dem Betroffenen und dem Verantwortlichen besteht ein Über-/Unterordnungsverhältnis  *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3,4)*  Es werden personenbezogene Daten bei Dritten oder anderen Behörden erhoben *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3, 6)*  Es werden personenbezogene Daten an eine andere Stelle/Behörde weitergeleitet *(In Betracht kommen z. B. die Maßnahmen Nrn. 6, 11)*  Weitere Gefährdungen | 1. Die Betroffenen werden gem. Art 13 DSGVO informiert |  |  |  |
| 2. Die Betroffenen werden gem. Art. 16 ff DSGVO informiert |  |  |  |
| 3. Ein Prozess für Auskunftsansprüche ist festgelegt |  |  |  |
| 4. Veröffentlichung der Informationen zur Verarbeitung von personenbezogenen Daten (z.B. Online oder als Aushang  in Form einer Datenschutzerklärung) |  |  |  |
| 5. Dokumentation der Datenempfänger und Zeitspanne der Überlassung |  |  |  |
| 6. Ein Prozess zur Erstellung und Pflege des  Verarbeitungsverzeichnisses ist etabliert |  |  |  |
| 7. Ein Vertrag zur Auftragsverarbeitung ist abgeschlossen |  |  |  |
| 8. Es findet eine Dokumentation/Vertragsmanagement  der Auftrags- und Unterauftragsverhältnisse statt |  |  |  |
| 9. Dokumentation der Mandant\*innen und zugehörigen  Datenbereiche |  |  |  |
| 10. Festlegen verbindlicher Löschfristen |  |  |  |
| 11. Ein Prozess zur Weitergabe und zur Entscheidung  über die Weitergabe von Daten ist etabliert |  |  |  |
| 12. Bei Beschäftigtendaten: Die Datenverarbeitung wird  in einer Dienstvereinbarung beschrieben |  |  |  |
| 13. weitere Maßnahmen |  |  |  |

2. Zweckbindung Art. 5 Abs. 1 lit. b) DSGVO. Definition: Zweckbindung ist gewährleistet, wenn die Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Kontrollfragen:

* Ist gewährleistet, dass die personenbezogenen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und im Anschluss hieran nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden?
* Wie wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass die Verantwortlichen die personenbezogenen Daten der Betroffenen nicht dem Zweck entsprechend verarbeiten. | **Mögliche Maßnahmen**  Erläuterungen: Es müssen Maßnahmen zur Absicherung der Zweckbindung gefunden werden bzw. ein Prozess für die Überprüfung einer zulässigen Zweckänderung. | relevant | umgesetzt | Dokumentation |
| Es erfolgt eine Weitergabe von personenbezogenen Daten an eine andere Stelle für einen anderen Zweck *(In Betracht kommen z. B. die Maßnahmen Nrn.1, 6, 7)*  Durch die Verarbeitung werden Persönlichkeitsaspekte bewertet, z. B. werden Analysen/Prognosen erstellt über die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit einer Person in Bezug auf eine Tätigkeit, das Verhalten, den Aufenthaltsort  *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 5, 6 ,7)*  Es findet eine Zweckänderung statt *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 6, 7)*  Weitere Gefährdungen | 1. Erlass einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten |  |  |  |
| 2. Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten,  abgesicherten IT-System |  |  |  |
| 3. Physikalisch getrennte Speicherung auf gesonderten  Systemen oder Datenträgern |  |  |  |
| 4. Trennung von Produktiv- und Testsystem |  |  |  |
| 5. Versehen der Erhebungsformulare und Datensätze mit Zweckattributen und Datenfeldern |  |  |  |
| 6. Darstellung der Zwecke im Verzeichnis der  Verarbeitungstätigkeiten |  |  |  |
| 7. Verpflichtung der Mitarbeiter auf die Beachtung der  Anforderungen der DSGVO sowie des NDSG |  |  |  |
| 8 Entgegennahme von Weisungen nur von befugten  Mitarbeitern des Verantwortlichen bzw. Auftraggebers |  |  |  |
| 9. Anonymisierung und ggf. Pseudonymisierung von Telemetrie und Diagnosedaten |  |  |  |
| 10. weitere Maßnahmen |  |  |  |

3. Datenminimierung Art. 5 Abs. 1 lit. c DSGVO.

Definition: Datenminimierung ist gewährleistet, wenn die Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind.

Kontrollfragen:

* Wie wird gewährleistet, dass personenbezogene Daten nur in dem Umfang erhoben und gespeichert werden, der zum Erreichen des verfolgten Zwecks notwendig ist?
* Wie wird gewährleistet, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind, Art. 5 Abs. 1 lit. c) DSGVO Wird eine große Menge personenbezogener Daten verarbeitet?
* Wie lange werden die personenbezogenen Daten gespeichert?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass mehr personenbezogene Daten über Betroffene als notwendig verarbeitet werden. | **Mögliche Maßnahmen**  Erläuterungen: Durch geeignete Maßnahmen müssen die Verantwortlichen den Umfang der Datenverarbeitung begrenzen. | relevant | umgesetzt | Dokumentation |
| Es werden personenbezogene Daten über die Erhebung hinaus gespeichert *(In Betracht kommen z. B. die Maßnahmen Nrn.1-11)*  Es fehlt an einer Löschfrist *(In Betracht kommen z. B. die Maßnahmen Nrn. 4, 7, 8)*  Die Löschfrist ist zu lang oder zu kurz bemessen  *(In Betracht kommen z. B. die Maßnahmen Nrn. 4, 7)*  Die personenbezogenen Daten werden automatisiert, z. B. in einem Fachverfahren verarbeitet  *(In Betracht kommen z. B. die Maßnahmen Nrn.1-11)*  Personenbezogene Daten werden durch einen elektronischen oder analogen Erhebungsvordruck erhoben *(In Betracht kommen z. B. die Maßnahmen Nrn.1 ,2 ,3 ,5 ,6, 9, 10, 11)*  Es wird ein umfangreicher Datensatz erhoben  *(In Betracht kommen z. B. die Maßnahmen Nrn.1-11)*  Es werden durch nicht notwendige/genutzte Module zusätzliche personenbezogene Daten erhoben *(In Betracht kommen z.B. die Maßnahme Nr 13)*  Weitere Gefährdungen | 1. Datenschutz durch Technikgestaltung  (data protection by design) |  |  |  |
| 2. Vornahme datenschutzrechtlicher Voreinstellungen  (data protection by default) |  |  |  |
| 3. Plausibilitätskontrolle zur Beschränkung der  Datenerhebung |  |  |  |
| 4. Regelmäßiges manuelles Auslösen der Löschung nicht benötigter Daten/Löschroutine |  |  |  |
| 5. Pseudonymisierung der Daten bei Weiterverarbeitung oder Übermittlung |  |  |  |
| 6. Regelmäßige Audits über den Datenumfang |  |  |  |
| 7. Festlegung verbindlicher Löschfristen |  |  |  |
| 7. a. Festlegung verbindlicher Löschfristen für Cloud Dienste |  |  |  |
| 8 Festlegung automatisierter Löschzyklen |  |  |  |
| 8.a Festlegung automatisierter Löschzyklen für Cloud Dienste |  |  |  |
| 9. Anonymisierung von Daten wenn Identifikation nicht mehr notwendig |  |  |  |
| 10. Erlass einer schriftlichen Dienstanweisung |  |  |  |
| 11. Versehen der Datensätze/Erhebungsformulare mit Zweckattributen und Datenfeldern |  |  |  |
| 12. Minimierung oder Vermeidung von Telemetrie- oder Diagnosedaten, (Privacy by default, einstellbar). |  |  |  |
|  | 13. Definition von Anwendungsfällen |  |  |  |
|  | 14. Weitere Maßnahmen |  |  |  |

4. Richtigkeit der personenbezogenen Daten Art. 5 Abs. 1.lit. d) DSGVO.

Definition: Richtigkeit ist gewährleistet, wenn die verarbeiteten Daten sachlich richtig und auf einem aktuellen Stand sind sowie Daten,   
die unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Kontrollfrage:

* Welche Umstände gefährden die Richtigkeit und Aktualität der verarbeiteten personenbezogenen Daten?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass inkorrekte Daten über die Betroffenen erhoben und weiterverarbeitet, z.B. übermittelt werden. | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen sicherstellen, dass die korrekten Daten bereits bei der Erhebung verarbeitet und Prüfroutinen etabliert werden und die Betroffenen ihre Korrekturrechte durchsetzen können | relevant | umgesetzt | Dokumentation |
| Es sind falsche personenbezogene Daten in Verwaltungsvorgängen enthalten *(In Betracht kommen z. B. die Maßnahmen Nrn.1, 5 ,6, 9, 10, 11)*  Fehlerhafte Zuordnung von Daten/Informationen zu Betroffenen / Verwechslungsfälle *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)*  Unklare Datenherkunft und –weitergabe  *(In Betracht kommen z. B. die Maßnahmen Nrn. 2, 3, 4)*  Schadsoftware *(In Betracht kommt z. B. die Maßnahmen Nr. 11)*  Weitere Gefährdungen | 1. Einrichtung eines Verfahrens zur Berichtigung von  Daten auf Antrag |  |  |  |
| 2. Nachweis der Herkunft von Daten |  |  |  |
| 3. Nutzung von De-Mail |  |  |  |
| 4. Nutzung des Post-Ident-Verfahrens/Basis-Dienst NDiG  (e-ID), EGVP /beA |  |  |  |
| 5. Unverzügliche Löschung unrichtiger Daten |  |  |  |
| 6. Eigenständige elektronische Berichtigung der Daten  durch die betroffene Person |  |  |  |
| 7. Zertifikatsbasierte Authentifizierung der Datenquelle |  |  |  |
| 8 Identitätsprüfung bei der Datenerhebung oder Anlieferung von Daten |  |  |  |
| 9. Nutzung eines Video-Ident-Verfahrens |  |  |  |
| 10. Unverzügliche Berichtigung unrichtiger Daten |  |  |  |
| 11. Virenscanner, Firewall, Software-Updates |  |  |  |
| 12. weitere Maßnahmen |  |  |  |

5. Speicherbegrenzung, Art. 5 Abs. 1 lit. e) DSGVO.

Definition: Speicherbegrenzung ist gewährleistet, wenn die verarbeiteten Daten in einer Form gespeichert werden, die die Identifizierung der   
betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Kontrollfrage:

* Wie wird gewährleistet, dass nach dem Erreichen des Verarbeitungszwecks die Identität der betroffenen Personen nicht mehr festgestellt werden kann?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass personenbezogene Daten länger über die Betroffenen verarbeitet werden, als erforderlich und das Risiko der unbefugten Datenverarbeitung steigt. | **Mögliche Maßnahmen**  Erläuterungen: Durch geeignete Maßnahmen ist sicherzustellen, dass personenbezogene Daten nur so lange verarbeitet werden (z.B. gespeichert bleiben) wie erforderlich. | relevant | umgesetzt | Dokumentation |
| Personenbezogene Daten werden zu statistischen Zwecken verarbeitet *(In Betracht kommen z. B. die Maßnahmen Nr. 1, 2)*  Personenbezogene Daten werden archiviert *(In Betracht kommen z. B. die Maßnahmen Nr. 3)*  Personenbezogene Daten werden zu statistischen Zwecken an eine andere Stelle weitergeleitet  *(In Betracht kommen z. B. die Maßnahmen Nr. 1, 2)*  Weitere Gefährdungen | 1. Frühzeitige Anonymisierung personenbezogener Daten |  |  |  |
| 2. Frühzeitige Pseudonymisierung personenbezogener  Daten |  |  |  |
| 3. Organisatorische Maßnahmen zur Archivierung |  |  |  |
| 4. Weitere Maßnahmen |  |  |  |

6. Vertraulichkeit, Art. 5 Abs. 1 lit. f) DSGVO; 32 Abs. 1 lit. b), Erwägungsgründe 39, 38 DSGVO.

Definition: Vertraulichkeit ist gewährleistet, wenn Unbefugte keinen Zugang zu den Daten und weder die Daten noch die Geräte, mit denen diese Verarbeitet werden, benutzen können. Vertraulichkeit ist darüber hinaus nur gewährleistet, wenn die personenbezogenen Daten vor unbefugter, unrechtmäßiger Verarbeitung oder unbeabsichtigtem Verlust geschützt sind.

Kontrollfrage:

* Welche Umstände können zu einer unbefugten Wahrnehmung, Offenlegung, Zerstörung oder einem unbefugten Verlust der personenbezogenen Daten führen?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass personenbezogene Daten durch Unbefugte erlangt und diese missbraucht werden können. | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen die Vertraulichkeit der personenbezogenen Daten sicherstellen. | relevant | umgesetzt | Dokumentation |
| Ein unbefugter Zutritt zu den Datenverarbeitungssystemen ist möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 2, 4, 5, 6,)*  Ein unbefugter Zugriff auf die personenbezogenen Daten ist möglich *(In Betracht kommen z. B. die Maßnahmen Nrn 1, 17, 18, 19, 24, 25, 26, 27, 28,32, 33, 56, 57, 61, 62, 63, 64, 65)*  Auf einem Datenträger gespeicherte personenbezogene Daten können unbefugt gelesen, kopiert, verändert oder entfernt werden *(In Betracht kommen z. B. die Maßnahmen Nrn 24, 42)*  Es können Personen auf die personenbezogenen Daten zugreifen, ohne dass dies für die Erledigung ihrer dienstlichen Aufgaben notwendig ist  *(In Betracht kommen z. B. die Maßnahmen Nrn 25, 26, 27, 28)*  Personenbezogene Daten werden im Rahmen des Mobilen Arbeitens oder im Homeoffice verarbeitet *(In Betracht kommen z. B. die Maßnahmen Nrn 1, 38, 39, 44, 45, 64, 65, 66)*  Bei mobilem Arbeiten oder Home-Office können Dritte wie Familienangehörige, Besucher etc. potenziell Zugriff auf personenbezogene Daten erhalten  *(In Betracht kommen z. B. die Maßnahmen Nrn 1, 38, 39, 44, 45, 64, 65, 66)*  Datenträger wie Notebooks, Akten, Smartphones, Tablets werden im Außendienst oder bei der Wahrnehmung externer Termine mitgenommen  *(In Betracht kommen z. B. die Maßnahmen Nrn 1, 38, 39, 44, 45, 51)*  „Offenes Haus“, d.h. Kunden oder Bürger können die Geschäftsräume der Verwaltung frei betreten  *(In Betracht kommen z. B. die Maßnahmen Nrn 1,17, 24, 28, 29, 30, 32, 38, 39)*  Die Verarbeitung der personenbezogenen Daten oder deren Offenlegung kann führen zu Diskriminierung, Identitätsdiebstahl-/betrug, finanziellen Einbußen, einer Rufschädigung, gesellschaftlichen Nachteilen, dem Verlust eines Berufsgeheimnisses, Verlust eines Pseudonyms *(In Betracht kommen z.B. die Maßnahmen Nrn. 1, 44, 45, 46, 49, 50, 51, 54, 60 -64, 65)*  Die Offenlegung der personenbezogenen Daten kann für den Betroffenen zu Diskriminierung, Identitätsdiebstahl, finanziellen Verlusten oder einer Rufschädigung führen. *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 44, 45, 46, 49, 50, 51, 54, 60 -64, 65)*  Bei einer unbefugten Offenlegung würden personenbezogene Daten bekannt, die Aufschluss über rassische oder ethnische Herkunft, politische Meinung, weltanschauliche Überzeugung oder Gewerkschaftszugehörigkeit geben *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 44, 45, 46, 49, 50, 51, 54, 60 -64, 65)*  Der Verlust von Datenträgern wie Akten oder mobilen Geräten (Tablets, Smartphones, Notebooks) ist potenziell möglich. *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 17, 22, 23, 24, 28, 29, 32, 33, 38, 39, 44, 45, 46, 65)*  Fehlgeleitete Nachrichten sind potenziell möglich  *(In Betracht kommen z. B. die Maßnahmen Nrn. 44, 49, 50, 60, 61, 62, 65)*  Im Fachverfahren oder im Windows-Filesystem bestehen zu weitgehende Zugriffsrechte *(In Betracht kommen z. B. die Maßnahmen Nrn. 23, 25, 26, 27)*  Zugriffsrechte werden oder wurden in der Vergangenheit nicht entzogen *(In Betracht kommen z. B. die Maßnahmen Nrn. 23, 25, 26, 27, 36)*  Mehrere Beschäftigte haben Zugriff auf personenbezogene Daten *(In Betracht kommen z. B. die Maßnahmen Nrn. 25, 26, 27)*  Unbefugte haben ein gesteigertes Interesse, personenbezogene Daten auszuspähen *(In Betracht kommen z. B. die Maßnahmen Nrn. 44, 45, 46, 60-64, 65)*  Die personenbezogenen Daten werden bei einer anderen Behörde abgefragt oder dahin weitergeleitet *(In Betracht kommen z. B. die Maßnahmen 49, 50, 60-64, 65)*  EDV-Verfahren werden unberechtigt / fehlerhaft genutzt / administriert *(In Betracht kommen z. B. die Maßnahmen Nrn. 25, 26, 27, 40, 41, 43, 55, 65)*  Ein unbefugtes Eindringen in EDV – Systeme durch Schadsoftware oder einen Angriff ist potenziell möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 44, 45, 46, 48, 57)*  Ein unbefugter Zugang zu den Räumen der Datenverarbeitungsanlagen ist potenziell möglich  *(In Betracht kommen z. B. die Maßnahmen Nrn. 3, 4, 5, 6, 7, 8, 9, 10, 12,13, 14, 15, 16)*  Ein unbefugter Zugang zu Büros oder Räumen ist potenziell möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 3, 6, 7, 8, 9, 10, 11, 14, 16, 18, 19, 20)*  Personenbezogene Daten werden im Windows-Filesystem abgelegt *(In Betracht kommt z. B. die Maßnahme Nr. 27)*  Weitere Gefährdungen | 1. Es gibt eine schriftliche Dienstanweisung zum Umgang  mit personenbezogenen Daten bei mobilem Arbeiten / Home-Office |  |  |  |
| 2. Alarmanlage |  |  |  |
| 3. Wachpersonal |  |  |  |
| 4. Zugangskontrollsystem |  |  |  |
| 5. Unterteilung in Sicherheitszonen |  |  |  |
| 6. Sicherheitsschlösser |  |  |  |
| 7. Schlüsselregelung |  |  |  |
| 8. Schließsystem mit Chipkarte |  |  |  |
| 9. Schließsystem mit Transponder |  |  |  |
| 10. Schließsystem mit Codesperre |  |  |  |
| 11. Manuelles Schließsystem |  |  |  |
| 12. Biometrische Zugangssperren |  |  |  |
| 13. Ausweispflicht |  |  |  |
| 14. Personenkontrolle |  |  |  |
| 15. Festlegung befugter Personen |  |  |  |
| 16. Einbruchhemmende Fenster und Türen |  |  |  |
| 17. Geräte- und Gehäuseversiegelung |  |  |  |
| 18. Auf Datenschutz verpflichtetes Reinigungspersonal |  |  |  |
| 19. Auf Datenschutz verpflichtetes Wartungspersonal |  |  |  |
| 20. Festgelegte Reinigungszeiten |  |  |  |
| 21. Beaufsichtigung von Wartungstätigkeiten |  |  |  |
| 22. Zugangsbeschränkung nach Endgerät |  |  |  |
| 23. Zeitliche Zugangsbeschränkung |  |  |  |
| 24. Benutzerkonto für jeden Mitarbeiter |  |  |  |
| 25. Implementierung eines Rollen- und  Berechtigungskonzept („Least Privilege“, „Need to know“) |  |  |  |
| 25. a Berechtigungsgruppen sind so klein wie möglich |  |  |  |
| 25. b Überprüfungskonzept für Rollen- und Berechtigungskonzept |  |  |  |
| 26. Nach Verarbeitungszweck differenziertes  Berechtigungskonzept |  |  |  |
| 27. Steuerung der Zugriffsmöglichkeiten |  |  |  |
| 28. Arbeiten mit individuellen Benutzerkennungen |  |  |  |
| 29. Dem Zweck angemessene Passwortrichtlinien |  |  |  |
| 30. Regelmäßige Passwortwechsel |  |  |  |
| 31. Single Sign-on |  |  |  |
| 32. Authentifikation mit Passwort |  |  |  |
| 33. Authentifikation mit SmartCard oder vergleichbarer Multi-Faktor Authentifizierung |  |  |  |
| 34. Authentifikation über Verzeichnisdienste |  |  |  |
| 35. Biometrische Authentifikation |  |  |  |
| 36. Regelungen beim Ausscheiden von Mitarbeitern |  |  |  |
| 36. a Regelungen beim Wechsel von Zuständigkeiten von Mitarbeitern |  |  |  |
| 37. Sperren der Bootkonfiguration (BIOS, UEFI) |  |  |  |
| 38. Automatische Abmeldevorgänge |  |  |  |
| 39. Kontosperrung nach mehrmaliger Falscheingabe  des Passworts |  |  |  |
| 40. Aufteilung der Administratorrechte unter verschiedenen Personen |  |  |  |
| 41. Vergabe von Administratorrechten an minimale Anzahl von Personen |  |  |  |
| 41. a Vergabe der Administratorrechte auf das erforderliche Maß begrenzen („Least Privilege“, „Need to know“) |  |  |  |
| 42. Sicheres Löschen von Datenträgern, z. B. durch mehrmaliges Überschreiben vormaliger Inhalte mit Zufallswerten |  |  |  |
| 43. Differenzierung administrativer Aufgaben |  |  |  |
| 44. Dateiverschlüsselung |  |  |  |
| 45. Datenträgerverschlüsselung |  |  |  |
| 46. Verschlüsselung von Datenbanken / Services |  |  |  |
| 47. Sperrung der Nutzung von persönlichem  Cloudspeicher am Arbeitsplatz-PC |  |  |  |
| 48. Verhinderung nicht-autorisierter Cloud-Synchronisation durch Drittanbietersoftware |  |  |  |
| 49. Übermittlung von Daten in anonymisierter Form |  |  |  |
| 50. Übermittlung von Daten in pseudonymisierter Form |  |  |  |
| 51. Sichere Behältnisse bei physischem Transport |  |  |  |
| 52. Zuverlässiges Transportpersonal |  |  |  |
| 53. Identitätsnachweis des Transportpersonals |  |  |  |
| 54. Datenträgervernichtung nach DIN 66399 |  |  |  |
| 55. Nach Verarbeitungszweck differenziertes  Berechtigungskonzept |  |  |  |
| 56. Logische Mandantentrennung (z.B. durch inklusive separate Verschlüsselungsmaßnahmen und -schlüssel) |  |  |  |
| 57. Physikalisch getrennte Speicherung und Verarbeitung |  |  |  |
| 58. Trennung von Produktiv- und Testsystem |  |  |  |
| 59. Fernlöschung von mobilen Endgeräten |  |  |  |
| 60. E-Mail-Verschlüsselung mit S/MIME |  |  |  |
| 61. E-Mail-Verschlüsselung mit OpenPGP |  |  |  |
| 62. Durchgängige E-Mail-Verschlüsselung  bei der E-Mail-Übertragung |  |  |  |
| 63. Transportverschlüsselte Datenübertragung |  |  |  |
| 64. Datenkommunikation über VPN-Tunnel |  |  |  |
| 65. Mitarbeiterschulungen |  |  |  |
| 66. Bei mobilem Arbeiten oder Home-Office sollten die [Empfehlungen](https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html?__blob=publicationFile) (Stand 15. November 2019) des Bundesbeauftragten für den Datenschutz berücksichtigt werden) |  |  |  |
| 67. Datenklassifizierung (z.B. Vertraulich vs. Öffentlich) |  |  |  |
| 68. Ein System zur Authentifizierung („Single Point of Authentication“) |  |  |  |
| 69. Einschränkung des Zugriffs aus Drittstaaten |  |  |  |
| 70. Einsatz von anerkannt zertifizierten Systemen (Rechenzentrum, Service, Dienstleister), z.B. BSI C5, ISO 27001, ISO 27701, etc |  |  |  |
| 71. Weitere Maßnahmen |  |  |  |

7. Integrität, Art. 32 Abs. 1 lit. b) DSGVO, Art. 5 Abs. 1 lit. f) DSGVO.

Definition: Integrität ist gewährleistet, wenn personenbezogene Daten vor dem unbeabsichtigten Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten mithin vollständig, unverändert und unversehrt sind.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass die personenbezogenen Daten nicht ausreichend gegen unbefugte Veränderung geschützt sind. | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen die Integrität der personenbezogenen Daten sicherstellen. | relevant | umgesetzt | Dokumentation |
| Die unbefugte oder unbemerkte Änderung personenbezogener Daten ist potenziell möglich  *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 18, 21, 23)*  Die Manipulation von Daten, ihres Urhebers oder des Bezugs zu anderen Datenobjekten ist potentiell möglich, etwa beim Datenaustausch auf dem Transportweg *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3, 10, 11, 19, 20, 21)*  Die Manipulation personenbezogener Daten oder von (Papier-)Akten durch einen Angreifer/Hacker von außen ist potenziell möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 6, 7, 8, 9, 13, 14, 15)*  Die Manipulation von personenbezogenen Daten oder (Papier-)Akten durch eine\*n Innentäter\*in ist potenziell möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 23)*  Weitere Gefährdungen | 1. Protokollierung |  |  |  |
| 2. Signieren elektronischer Dokumente |  |  |  |
| 3. Signieren von E-Mails |  |  |  |
| 4. Anwendung von Prüfsummenverfahren |  |  |  |
| 5. Überwachung von Fernwartungsaktivitäten |  |  |  |
| 6. Sperren externer Schnittstellen wie USB |  |  |  |
| 7. Intrusion Detection System |  |  |  |
| 8. Einsatz von Virenschutzlösungen |  |  |  |
| 9. Application Layer Firewall |  |  |  |
| 10. E-Mail-Signierung mit S/MIME |  |  |  |
| 11. E-Mail-Signierung mit OpenPGP |  |  |  |
| 12. Verschlüsselung der Internetpräsenz |  |  |  |
| 13. Packet Filter Firewall |  |  |  |
| 14. Dedizierte Netze für Systeme mit sensiblem Daten |  |  |  |
| 15. Automatisierte Updateprozesse für Betriebssysteme,  Anwendungen und Dienste |  |  |  |
| 16. Differenzierte Berechtigungen für unterschiedliche  Transaktionen |  |  |  |
| 17. Differenzierte Berechtigungen für Datenobjekte |  |  |  |
| 18. Plausibilitätskontrolle bei der Datenverarbeitung |  |  |  |
| 19. Inhaltsverschlüsselte Datenübertragung |  |  |  |
| 20. Regelung zum Umgang mit mobilen Datenträgern |  |  |  |
| 21. Verschlüsselung von mobilen Datenträgern |  |  |  |
| 22. E-Mail-Gateway mit Filterfunktion |  |  |  |
| 23. Paginierung von Akten |  |  |  |
| 24. Weitere Maßnahmen |  |  |  |

8. Verfügbarkeit, Art. 32 Abs. 1 lit. b) DSGVO.

Definition: Verfügbarkeit ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss gewährleistet sein, dass die Verfügbarkeit und der Zugang zu den personenbezogenen Daten nach einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass die betroffenen Personen oder die befugten Verantwortlichen nicht mehr auf die Daten zugreifen können. | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen sicherstellen, dass ein Zugriff auf die personenbezogenen Daten möglich bleibt oder wieder wird. | relevant | umgesetzt | Dokumentation |
| Die Zerstörung oder der Diebstahl von Hardware/Servern ist potenziell möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 2, 3, 5,12)*  Potenziell droht der Verlust von Akten *(In Betracht kommt z. B. die Maßnahmen Nrn. 1 bei elektronisch geführten Akten)*  Ein Angriff auf Hard-/Software ist potenziell möglich *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3, 5,6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17)*  Es ist potenziell möglich, dass IT – Systeme oder IT –Anwendungen durch einen Angriff mit Schadsoftware nicht oder nicht in vollem Umfang genutzt werden können *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 2, 3, 5,6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17)*  Das Wiederanfahren der IT – Systeme/IT – Anwendungen bei einem Angriff wird durch mangelnde Vorkehrungen verhindert oder verzögert *(In Betracht kommen z. B. die Maßnahmen Nrn. 1, 7, 8, 9)*  Es ist potenziell möglich, dass ein Angriff zugleich die Datensicherung angreift  Der Ausfall von Hard-/Software durch Elementarschäden (Brand, Regen, Hochwasser, Wassereinbruch, Corona) ist potenziell möglich  Es ist potenziell möglich, dass infolge von defekter Hard-/Software, fehlender Stromversorgung oder einer gestörten Netzwerkverbindung IT – Anwendungen/IT – Systeme nicht ordnungsgemäß funktionieren  Weitere Gefährdungen | 1. Sicherungs- und Wiederherstellungskonzept  (Backup und Recovery) |  |  |  |
| 2. Automatisiertes Anfertigen von Datensicherungen (Backup) |  |  |  |
| 3. Daten und Datensicherung sind voneinander getrennt |  |  |  |
| 4. Aufbewahrung von Datenträgern in gegen Elementarschäden gesicherten Behältnissen |  |  |  |
| 5. Aufbewahrung der Datensicherung in einem anderen Brandabschnitt |  |  |  |
| 6. Festgelegte Zuständigkeiten für die Datensicherung |  |  |  |
| 7. Regelmäßiger Test der Datenwiederherstellung |  |  |  |
| 8. Notfallplan bei Kompromittierung oder Angriffen |  |  |  |
| 9. Notfallplan zur Wiederinbetriebnahme von Servern  oder Diensten |  |  |  |
| 10. Datenträgerspiegelung (RAID) |  |  |  |
| 11. Datenreplikation |  |  |  |
| 12. Vermeidung lokaler Datenspeicherung |  |  |  |
| 13. Redundante IT-Systeme |  |  |  |
| 14. Virtualisierte Infrastruktur |  |  |  |
| 15. Automatisches Benachrichtigungssystem  bei Ausfall oder Angriffen |  |  |  |
| 16. Intrusion Detection System |  |  |  |
| 17. Intrusion Prevention System |  |  |  |
| 18. weitere Maßnahmen |  |  |  |

9. Belastbarkeit der Systeme, Art. 32 Abs. 1 DSGVO.

Belastbarkeit ist gewährleistet, wenn die verwendete IT-Infrastruktur, d.h. Räumlichkeiten, Hard- und Software, Netze und Dienste, möglichst widerstandsfähig, robust und resilient sind.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können sich daraus ergeben, dass durch Angriffe auf die IT-Infrastruktur eine Verarbeitung der personenbezogenen Daten nicht möglich ist. | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen die Verarbeitung der personenbezogenen Daten auch dann gewährleisten, wenn ein Angriff auf die Verfügbarkeit erfolgt. | relevant | umgesetzt | Dokumentation |
| Es ist potenziell möglich, dass die IT – Infrastruktur infolge hoher bestimmungsgemäßer Zugriffe nicht ordnungsgemäß funktioniert  Es ist potenziell möglich, dass infolge von defekter Hard-/Software, fehlender Stromversorgung oder einer gestörten Netzwerkverbindung IT – Anwendungen/IT – Systeme nicht ordnungsgemäß funktionieren  Ein Angriff auf Hard-/Software ist potenziell möglich  Der Ausfall von Hard-/Software durch Elementarschäden (Brand, Regen, Hochwasser, Wassereinbruch, Corona) ist potenziell möglich  Personenbezogene Daten können nicht in angemessener Zeit verfügbar gemacht oder abgerufen werden *(In Betracht kommen z. B. die Maßnahmen Nrn.)* | 1. Lastausgleich (load balancing) der  Netzwerkkomponenten |  |  |  |
| 2. Lastausgleich der (load balancing) der Server |  |  |  |
| 3. Lastausgleich (load balancing) der Dienste |  |  |  |
| 4. Automatische Skalierung virtueller Systeme |  |  |  |
| 5. Unterbrechungsfreie Stromversorgung |  |  |  |
| 6. Überspannungsschutz |  |  |  |
| 7. Klimaanlage in Serverräume |  |  |  |
| 8. Feuer- und Rauchmeldeanlagen |  |  |  |
| 9. Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen |  |  |  |
| 10. Feuer- und Rauchmeldeanlagen |  |  |  |
| 11. Feuerlöscher/automatisches Löschsystem |  |  |  |
| 12. Automatisches Benachrichtigungssystem bei  Erreichung der maximalen Auslastung |  |  |  |
| 13. IT-Komponenten verfügen über die erforderliche  Leistungsfähigkeit |  |  |  |
| 14. Schutz vor Wassereinbruch |  |  |  |
| 15. Schutz vor Hochwasser |  |  |  |
| 16. Eignung der Räumlichkeiten/des Baus |  |  |  |
| 17. Weitere Maßnahmen |  |  |  |

10. Besondere Anforderungen aus dem jeweiligen Fachrecht oder Gefährdungen für bestimmte besonders schützenswerte Datenkategorien (Art. 9, 10 DSGVO i. V. m. § 17 NDSG, §§ 34, 35 NDSG, § 11 VgV)

Erläuterung: Bei der Verarbeitung besonders schützenswerter Daten i. S. d. Art. 9, 10 DSGVO schreibt § 17 NDSG die Einhaltung bestimmter Maßnahmen und Gewährleistungsziele vor. §§ 34, 35 NDSG schreiben ihrerseits bei der Bearbeitung von Ordnungswidrigkeiten die Einhaltung bestimmter Maßnahmen und Gewährleistungsziele vor. Ähnliche Anforderungen können sich aus dem jeweils einschlägigem Fachrecht ergeben. Die zu treffenden Maßnahmen können jedoch mit den in Ziff. 1-10 genannten Maßnahmen identisch sein. Es wird daher empfohlen, zunächst zu prüfen, ob etwaige besondere Anforderungen nicht schon erfüllt sind.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potenzielle Gefährdungen**  Erläuterung: Potenzielle Gefährdungen können  sich daraus ergeben, dass ... | **Mögliche Maßnahmen**  Erläuterungen: Die getroffenen Maßnahmen müssen ... | relevant | umgesetzt | Dokumentation |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Fazit

Bei Umsetzung und Einhaltung der bereits implementierten technisch-organisatorischen Maßnahmen besteht eine geringe Wahrscheinlichkeit des Schadenseintritts. Die Eintrittswahrscheinlichkeit entspricht dem E-Wert 1.

*Anhaltspunkt: Ereignisse kommen quasi nie vor, sind höchst selten oder nahezu undenkbar ("30 bis 100-jähriges Hochwasser")*

Die bisher umgesetzten technisch-organisatorischen Maßnahmen ergeben eine mittlere Wahrscheinlichkeit des Schadenseintritts. Die Eintrittswahrscheinlichkeit entspricht dem E-Wert 2.

*Anhaltspunkt: Ereignisse sind bereits vorgekommen oder grundsätzlich denkbar ("voraussehbare Besonderheiten")*

Trotz Umsetzung und Einhaltung der bereits implementierten technisch-organisatorischen Maßnahmen besteht eine hohe Wahrscheinlichkeit des Schadenseintritts. Die Eintrittswahrscheinlichkeit entspricht dem E-Wert 3.

*Anhaltspunkt: Ereignisse treten regelmäßig auf und zeichnen sich ab. (Keine Frage mehr des "OB", sondern des nächsten "WANN")*

Dokumentenlenkung

|  |  |  |  |
| --- | --- | --- | --- |
| Letzte Änderung | Datum | Autor | Anmerkungen |
|  |  |  |  |
|  |  |  |  |