***a.s.k. Datenschutz***

Sascha Kuhrau

Quick-Check Datensicherheit

und Datenschutz

Checkliste

Sascha Kuhrau

Quick-Check Datensicherheit und Datenschutz

Checkliste

a.s.k. Datenschutz - Datenschutz und Datensicherheit

Sascha Kuhrau

Schulstr. 16a

91245 Simmelsdorf-Hüttenbach / Bayern

**Innovationsstiftung**

**bayerische Kommune**

**Stiftungsvorstand**

Alexander Schroth, AKDB

Rudolf Schleyer, AKDB

**Kuratorium**

Dr. Jürgen Busse, Bayerischer Gemeindetag

Bernd Buckenhofer, Bayerischer Städtetag

Dr. Johann Keller, Bayerischer Landkreistag

Stefanie Krüger, Bayerischer Bezirketag

**Impressum**

**Herausgeber**

Innovationsstiftung Bayerische Kommune

c/o Anstalt für Kommunale Datenverarbeitung in Bayern – AKDB

Hauptverwaltung

Hansastraße 12-16

80686 München

Postfach 150140

80042 München

**Redaktionelle Bearbeitung**

Innovationsstiftung Bayerische Kommune

**Druck**

Innovationsstiftung Bayerische Kommune

© Innovationsstiftung Bayerische Kommune, München 2014

[www.bay-innovationsstiftung.de](http://www.bay-innovationsstiftung.de)

Sehr geehrte Anwenderin, sehr geehrter Anwender,

Ihnen liegt der *„Quick-Check Datensicherheit und Datenschutz“* der Innovationsstiftung Bayerische Kommune vor. Bevor Sie sich ans Werk machen, haben wir Ihnen die wichtigsten Fragen und Antworten zur Umsetzung als Hilfestellung in diesem Dokument zusammengefasst. Im Anschluss an diese FAQ finden Sie den eigentlichen Quick-Check.

Sollten Sie darüber hinaus Fragen zur Anwendung und Umsetzung des Quick-Checks haben, wenden Sie sich bitte an info@bay-innovationsstiftung.de

**Inhalt**

[**Wieso ein Check für Datensicherheit und Datenschutz?** 5](#_Toc402266397)

[**Was sind die Ziele dieses Quick-Checks?** 6](#_Toc402266398)

[**Konkurriert der Quick-Check mit einer Zertifizierung nach BSI IT-Grundschutz oder der ISO 27001?** 6](#_Toc402266399)

[**Ersetzt der Quick-Check die aktuell in Entwicklung befindlichen Sicherheitsrichtlinien des Freistaates Bayern?** 7](#_Toc402266400)

[**Wie gehe ich am besten mit diesem Quick-Check um?** 7](#_Toc402266401)

[**Macht es Sinn, die Prüfpunkte lediglich auf Basis der vorgegebenen Antwortmöglichkeiten zu betrachten?** 8](#_Toc402266402)

[**Muss ich alle Fragen beantwortet haben oder bei mir vor Ort umsetzen können?** 8](#_Toc402266403)

[**Welche Ergebnisse liefert mir der Quick-Check?** 8](#_Toc402266404)

[**Was sind die nächsten Schritte und kann ich identifizierte Schwachstellen selbst beheben?** 9](#_Toc402266405)

[**Wie oft sollte ich den Quick-Check wiederholen?** 10](#_Toc402266406)

[**Welche Quellen nutzt der Quick-Check und wie praxiserprobt sind diese?** 10](#_Toc402266407)

[**Welche Themen werden im Quick-Check behandelt?** 11](#_Toc402266408)

[**Wird die Linkliste aktualisiert und was mache ich, wenn ein Link veraltet ist?** 11](#_Toc402266409)

[**Und wie starte ich jetzt den Quick-Check?** 11](#_Toc402266410)

**Wieso ein Check für Datensicherheit und Datenschutz?**

*Höherer Technologie-Einsatz bedingt höhere Anforderungen an organisatorische und technische Sicherheits- und Schutzmaßnahmen. Dies macht auch vor Kommunen nicht halt. Rufen Sie sich alleine die Anzahl der Prüfpunkte der Kommunalen Prüfaufsicht früher und heute in Erinnerung und betrachten Sie deren Zunahme. Nicht nur Wirtschaftsunternehmen, sondern auch öffentliche Einrichtungen geraten immer mehr in den Fokus von „Hackern“, bewussten und zielgerichteten Angriffen von außen, um Systeme und Daten zu kompromittieren.*

*Hinzu kommen eine Vielzahl gesetzlicher Anforderungen zum Beispiel durch das Bayerische Datenschutzgesetz (BayDSG) für den öffentlichen Bereich und zahlreiche Spezialgesetze wie das Telekommunikationsgesetz (TKG) oder die Sozialgesetzbücher (SGB I – XII).*

*Auch der Bürger wird immer kritischer in Bezug auf den Umgang mit seinen persönlichen Daten. Während nicht-öffentliche Stellen einer Verpflichtung zur Selbstanzeige bei bestimmten Datenpannen unterliegen (§ 42a BDSG) sind öffentliche Stellen hiervon zurzeit (noch) ausgenommen. Doch Rufe werden lauter, dies anzugleichen. Der umstrittene und wieder zurückgezogene Entwurf des neuen Meldegesetzes im Jahr 2012 hat die Bürger für das Thema Datenumgang im kommunalen und behördlichen Bereich weiter sensibilisiert.*

*Diese Herausforderungen im Alltag des Tagesgeschäfts zu meistern, stellt hohe Ansprüche an die Beteiligten und Verantwortlichen. Mit dem praxisorientierten „Quick-Check Datensicherheit und Datenschutz“ wollen wir von der Innovationsstiftung Bayerische Kommune Sie dabei unterstützen.*

**Was sind die Ziele dieses Quick-Checks?**

*Check- und Prüflisten gibt es zuhauf, das Internet ist voll damit. Der Ihnen vorliegende Quick-Check soll Sie mit seinen Fragen, Antworten, Hilfestellungen, Tipps und Weblinks pragmatisch unterstützen. Ziel ist es, Ihnen praxisorientierte und erprobte Fragestellungen und Lösungswege an die Hand zu geben, mit denen Sie das Datensicherheits- und Datenschutzniveau Ihrer Kommune prüfen und verbessern können.*

*Dabei soll der personelle und finanzielle Aufwand einer Zertifizierung nach den unterschiedlichsten Normen wie BSI IT-Grundschutz oder ISO 27001 ebenso vermieden werden, wie der meist sehr theoretische Ansatz dieser Methoden.*

*Am Ende des Quick-Checks steht daher kein Zertifikat, aber auch kein aufwändiges Beratungsprojekt. Sie führen mit eigenen, internen Ressourcen eine erste Selbstbewertung des Schutzniveaus durch und identifizieren mögliche Schwachstellen. Diese können Sie im Nachgang mit internen Mitteln und / oder externer Unterstützung beseitigen.*

**Konkurriert der Quick-Check mit einer Zertifizierung nach BSI IT-Grundschutz oder der ISO 27001?**

*Nein. Wie bereits im Abschnitt zuvor dargelegt, ist es nicht Ziel des Quick-Checks in Konkurrenz zu diesen Zertifizierungsverfahren zu treten. Wir wollen Ihnen mit diesem Tool eine Hilfestellung bieten, Ihren Arbeitsalltag und Ihre IT-Struktur unter den Gesichtspunkten Datensicherheit und Datenschutz zu hinterfragen und zu bewerten. Um die Ergebnisse besser einschätzen und konkrete Maßnahmen zur Behebung von Schwachstellen entwickeln zu können, erhalten Sie mit den Fragestellungen und der beigefügten Linkliste bewährte und frei verfügbare Informationen bekannter Institutionen zur Sicherstellung eines Basis-Schutzniveaus. Auf Verweise zum BSI IT-Grundschutz haben wir in diesem Zusammenhang bewusst verzichtet, da sie in ihrer Vollständigkeit und Komplexität für die meisten kommunalen Anforderungen kaum handhabbar sind.*

**Ersetzt der Quick-Check die aktuell in Entwicklung befindlichen Sicherheitsrichtlinien des Freistaates Bayern?**

*Nein. Der Quick-Check dient einer zeitnahen und umfassenden Überprüfung der bekanntesten möglichen Schwachpunkte. Mittels des Quick-Checks können Sie bereits heute Ihr Sicherheits- und Schutzniveau vor Ort prüfen und einen Basis-Schutz sicherstellen. Wenn die Sicherheitsrichtlinien erarbeitet und veröffentlicht sind, justieren Sie einzelne Details einfach nach und widmen sich den zusätzlichen Punkten der Leitlinie, die in der Form möglicherweise nicht im Quick-Check enthalten sind.*

*Ein Beispiel: Der Quick-Check regt die Auseinandersetzung mit dem Thema Passwort (Länge, Zusammensetzung, Wechselintervalle etc.) an. Wichtig ist, dass Sie am Ende eine belastbare und dem Stand der Technik entsprechende Richtlinie implementiert haben und mit Ihren Mitarbeiter auch in der Praxis leben. Sollte der von Ihnen geschaffene Standard (beispielsweise acht Stellen) von der Vorgabe der zukünftigen Sicherheitsrichtlinie (eventuell zehn Stellen, keine Details zurzeit bekannt) abweichen, so können Sie dies einfach nachjustieren. Sie haben durch die Bearbeitung des Themas doch bereits jetzt schon einen wichtigen Beitrag für die Sicherheit der Systeme geleistet, ohne Doppelbelastung fürchten oder auf die Fertigstellung der Sicherheitsrichtlinie warten zu müssen.*

**Wie gehe ich am besten mit diesem Quick-Check um?**

*Bevor Sie sich an die Arbeit machen, sollten Sie sich über Ihre eigenen Ziele klar werden.*

*Wollen Sie lediglich für einige ausgewählte, bereits vorhandene Schutzmaßnahmen prüfen, ob und inwieweit diese ausreichend sind? In diesem Fall nehmen Sie sich das entsprechende Kapitel des Quick-Checks vor und bearbeiten die dort aufgeführten und für Sie zutreffenden Prüfpunkte.*

*Geht es Ihnen um einen umfassenden Basis-Schutz und Sie wollen zusätzlich vorhandene Lücken im Schutz-Niveau identifizieren? Dann sollten Sie den Quick-Check vollständig unter Einbeziehung verantwortlicher Stellen (z.B. IT-Sicherheitsbeauftragte, Personalverwaltung, Datenschutzbeauftragte) in Ihrer Kommune abarbeiten.*

**Macht es Sinn, die Prüfpunkte lediglich auf Basis der vorgegebenen Antwortmöglichkeiten zu betrachten?**

*Sie werden bei der Bearbeitung der einzelnen Prüfpunkte schnell feststellen, dass es hier nicht um die bloße Abarbeitung von Fragen und vorgegebenen Antworten geht. Bei sehr vielen Schutzmaßnahmen geht es selten um das reine Vorhandensein einer ganz speziellen Technik. Von daher sind die Antwortmöglichkeiten als beispielhafte Schutzmaßnahmen zu verstehen, die in einer ausgewogenen und abgestimmten Kombination das notwendige Schutzniveau erzeugen.*

*Interessanter ist daher in der Praxis stets der eingesetzte Mix an Schutzmaßnahmen, egal ob technisch erzwungen oder durch Dienstanweisungen vorgegeben. So kann z.B. eine Videoüberwachung im IT-Serverraum sinnvoll sein, wenn dieser über mehr als nur einen Zugang verfügt und zusätzlich mit Fenstern versehen ist. Liegt der Serverraum jedoch im inneren Schutzbereich des Gebäudes, ist fensterlos und lediglich über eine massive und stets verschlossene Zugangstür zu betreten, wäre eine Innenraum-Videoüberwachung eine übertriebene Maßnahme, die das Schutzniveau im Zweifel nicht mehr merklich anhebt. Hier wäre dann mehr Augenmerk auf sinnvolle Überwachung und Alarmierung bei Gefährdungssituationen wie Feuer, Wasser, Temperatur oder Stromausfall zu legen.*

**Muss ich alle Fragen beantwortet haben oder bei mir vor Ort umsetzen können?**

*Nein. Jedes Schutzsystem besteht aus einer Vielzahl unterschiedlicher Schutzschichten, ähnlich dem Zwiebelprinzip. Der innere, weiche und saftige Kern ist durch eine ausreichend hohe Zahl an Schichten von außen nach innen geschützt. So sollten Sie auch die einzelnen Fragen und Punkte dieses Quick-Checks verstehen. Es kommt nicht zwingend auf die Menge der Schutzschichten, sondern auf die vernünftige Auswahl und Kombination der Schichten an.*

**Welche Ergebnisse liefert mir der Quick-Check?**

*Für jeden einzelnen Prüfpunkt oder auch einen kompletten Themenbereich ersehen Sie ziemlich schnell, ob Ihre Schutzampel grün zeigt, Justierungen notwendig sind oder im schlimmsten Fall noch akuter Handlungsbedarf besteht.*

*Hierfür hat jeder Prüfpunkt neben dem Feld „Ergebnis“ eine sehr konkrete Antwortskala*

1. *Vollständig erfüllt*
2. *Fast erfüllt*
3. *Teilweise erfüllt*
4. *Nicht erfüllt*
5. *Nicht anwendbar*
6. *Aktuell in Arbeit*

*Haben Sie Punkt 1 bei der Frage als Bewertung angegeben, sollte das Schutzniveau hoch sein und kein weiterer Handlungsbedarf bestehen. Mit der 2 als Bewertung ist noch Zeit und Arbeit zu investieren, um letzte vorhandene Lücken zu schließen. Das Schutzniveau ist in diesem Fall jedoch bereits recht hoch. Kommen als Antwort nur Antwort 3 oder schlimmstenfalls Antwort 4 in Frage, dann besteht akuter Handlungsbedarf. Das Schutzniveau vor Ort weist jetzt Sicherheitslücken auf, die zeitnah und mit gemeinsamer Anstrengung aller Beteiligten geschlossen werden müssen.*

*Keine Kommune gleicht der anderen und IT-Systeme sind selten identisch. Von daher kann es durchaus vorkommen, dass einzelne Prüfpunkte für Sie nicht anwendbar sind. Für diesen Fall wählen Sie Antwort 5 „Nicht anwendbar“.*

*Sollten Sie bei der Überprüfung auf einen Punkt stoßen, der noch nicht vollständig umgesetzt, aber bereits in Arbeit ist, markieren sie diesen mit Antwort 6 „Aktuell in Arbeit“.*

*Für die Nachbearbeitung und Bewertung ist es wichtig, dass Sie nicht nur die Antwortskala unter „Bewertung“ nutzen, sondern in der Spalte „Ergebnis“ ganz konkret die Ist-Situation beschreiben. Welche Maßnahmen sind bereits vorhanden, wie sind diese konkret ausgestaltet, welche fehlen Ihrer Meinung nach noch?*

*Besonders wichtig ist es, nichts zu beschönigen! Eine solche Art der Kosmetik mündet zwar in ein positives Endergebnis, jedoch bleiben vorhandene Sicherheitslücken als bedrohliches und vielleicht auch für die Entscheidungsträger und haftenden Personen unbekanntes Risiko weiter im Hintergrund bestehen.*

**Was sind die nächsten Schritte und kann ich identifizierte Schwachstellen selbst beheben?**

*Haben Sie den Quick-Check erfolgreich absolviert, dann herzlichen Glückwunsch! Sie kennen nun die größten und wichtigsten Schwachstellen im Datensicherheits- und Datenschutzniveau Ihrer Kommune. Mit dieser Erkenntnis können Sie jetzt in die konkrete Umsetzung gehen und die Schwachstellen sukzessive beseitigen.*

*In einem ersten Schritt sollten Sie die erkannten Schwachstellen nach Risiko sortieren. Dabei ist nicht nur der mögliche Schaden (monetär, Image, Rechtskonflikte etc.) zu berücksichtigen, sondern auch die Eintrittswahrscheinlichkeit. Haben Sie diese Sortierung vorgenommen, beziehen Sie den Kreis der Verantwortlichen mit ein, der für die weitere Umsetzung notwendig ist, sofern Sie die Verantwortlichen nicht bereits in die Risikoeinschätzung einbezogen haben.*

*Manche Schwachstelle lässt sich mit einfachen Mitteln beheben. So ist zum Beispiel eine fehlende Verpflichtung der Mitarbeiter auf das Datengeheimnis mittels der von der Bayerischen Landesdatenschutzbehörde zur Verfügung gestellten Textvorlage leicht nachzuholen.*

*Für andere Schwachstellen ist neben Zeit oft auch Budget notwendig. Auch hier unterstützt Sie der Quick-Check mit seiner Bewertung als Argumentationshilfe.*

*Zusätzlich finden Sie in der separaten Linkliste zu jedem Themenbereich weiterführende Tipps und Weblinks, mit denen Sie das Thema und den Umsetzungsbedarf vertiefen und einschätzen können.*

*Nun planen, konzeptionieren und budgetieren Sie die notwendigen Maßnahmen, die Sie zur Behebung der Schwachstellen ergreifen wollen / müssen. Diesen Maßnahmenplan legen Sie der Leitung oder dem / den Verantwortlichen für das Projekt „Quick-Check“ zur Diskussion und Freigabe vor.*

*Bei Bedarf können Sie auch externes Know-how zu Rate ziehen, z.B. das der AKDB.*

*Kleiner Tipp: Versuchen Sie nicht, bereichsübergreifende Probleme im Alleingang zu lösen. Stimmen Sie sich mit den Kolleginnen und Kollegen eng ab, zum Beispiel im Rahmen von Arbeitsgruppen oder Projektteams. „Gemeinsam sind wir stark“ ist keine Floskel aus einem Management-Ratgeber, sondern hat sich in der Praxis tausendfach bewährt.*

**Wie oft sollte ich den Quick-Check wiederholen?**

*Dies ist von dem jeweiligen Themenkomplex abhängig. Während ein Datenschutzbeauftragter (Kapitel 9 des Quick-Checks) zumeist langfristig bestellt und tätig ist, ändern sich technische Anforderungen sehr schnell. Sie machen auf jeden Fall nichts verkehrt, wenn Sie den Quick-Check und die daraus umgesetzten Maßnahmen im Jahresrhythmus erneut überprüfen. Haben Sie das Feld „Ergebnis“ sorgfältig und detailliert ausgefüllt, fällt diese Nachprüfung deutlich einfacher aus, als wenn Sie sich alle Informationen erneut beschaffen müssen.*

*Kommen neue IT-Infrastrukturen, Verfahren oder Arbeitsweisen unterjährig hinzu, dann empfiehlt sich die sofortige Prüfung anhand des Quick-Checks mit den dazu passenden und ausgewählten Prüfpunkten.*

**Welche Quellen nutzt der Quick-Check und wie praxiserprobt sind diese?**

*Der vorliegende Fragenkatalog ist das Ergebnis einiger hundert Auditierungen im öffentlichen und nicht-öffentlichen Bereich. Die ausgewählten Prüfpunkte entsprechen den Schwachstellen, die dabei in der Praxis die höchste Fehl- oder Fehlerquote aufgewiesen haben.*

*Angelehnt sind diese Prüfpunkte einerseits an die sogenannten „Technischen und Organisatorischen Maßnahmen“, die das Landesdatenschutzgesetz BayDSG fordert. Andererseits sind Musterdienstanweisungen beispielsweise für den IT-Betrieb der Bayerischen Spitzenverbände, aber auch Elemente des BSI IT-Grundschutzkatalogs eingeflossen. Weiterhin bieten alle Landesdatenschutzbehörden zahlreiche Formulare, Hilfestellungen und Prüflisten an, die themenabhängig integriert wurden.*

*Sie werden zahlreiche dieser Quellen etwa in den Weblinks bei den einzelnen Themenbereichen wiederfinden.*

**Welche Themen werden im Quick-Check behandelt?**

1. *Gebäudesicherheit und Sicherheitszonen*
2. *Zugang zu EDV-Systemen*
3. *Zugriffsschutzmaßnahmen*
4. *Berechtigungskonzepte und Protokollierung*
5. *Externe Dienstleister (Auftragsdatenverarbeitung)*
6. *Systemverfügbarkeit / Notfallmanagement*
7. *Richtlinien / Dienstanweisungen*
8. *Beschäftigtendatenschutz*
9. *Datenschutzbeauftragter*
10. *Verfahrensverzeichnis / Übersichten*

**Wird die Linkliste aktualisiert und was mache ich, wenn ein Link veraltet ist?**

*Nichts ist im Internet vergänglicher als ein Weblink. Wir werden die Linkliste daher in regelmäßigen Abständen prüfen und aktualisieren. Dies auch im Hinblick auf die sich zurzeit im Entstehen befindende Sicherheitsrichtlinie des Freistaats Bayern.*

*Sollten Sie im praktischen Einsatz nicht mehr aktive Links vorfinden oder selbst Vorschläge für die Linkliste haben, schreiben Sie uns bitte einfach an. Gerne nehmen wir auch Ihre Anregungen für weitere Ergänzungen der Linkliste entgegen.*

**Und wie starte ich jetzt den Quick-Check?**

*Zuerst sollte ein Hauptverantwortlicher für das Thema benannt sein. Dies muss nicht zwangsläufig derjenige sein, der den Quick-Check in der Praxis durchführt. Je nach Größe der zu prüfenden kommunalen Einrichtung empfiehlt sich im Zweifel der Einsatz einer Arbeitsgruppe, da die Themen teilweise bereichsübergreifend zu prüfen und abzuarbeiten sind. Zumindest sollten alle betroffenen Fachbereiche über die Maßnahme „Quick-Check“ vor Beginn der Prüfung in Kenntnis gesetzt werden.*

*Setzen Sie auf jeden Fall einen Zeitplan fest. In diesem definieren Sie entweder fixe Termine, zu denen einzelne Themenbereiche abgearbeitet sein sollen und / oder ein finaler Endtermin für die Bestandsaufnahme vereinbart wird. Damit vermeiden Sie ein „Versanden“ des Projekts oder eine Überpriorisierung anderer Aufgaben.*

*Versichern Sie sich der Unterstützung der einzubeziehenden Fachbereiche und deren Leiter. Im Zweifel sollte sich der Hauptverantwortliche um diesen Support kümmern.*

*Und jetzt frisch ans Werk!*

**Quick-Check Datensicherheit + Datenschutz**

**Geprüfte Stelle**

**Datum**

**Prüfer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Prüfpunkt** | **Erläuterungen / Fragen** | **Ergebnis(se)** | **Bewertung** |
| 1. **Gebäudesicherheit** | Art und Beschaffenheit des Gebäudes stellen einen nicht unerheblichen Beitrag zur Sicherheit. Das Gebäude stellt die äußerste Schutzschicht dar. | | |
| * 1. **Zutritt** | Je einfacher sich Zutritt ins Gebäude verschafft werden kann, umso höher das Sicherheitsrisiko. |  |  |
| * + 1. **Zutrittsmöglich-keiten** | Welche Zutrittsmöglichkeiten in das Gebäude bestehen?  Ist die genaue Lage und Anzahl bekannt?  Sind diese Türen stets verschlossen? Welche müssen zwingend für den öffentlichen Zugang zu den Bürozeiten geöffnet sein, z.B. Bürgerbüro? Welche Eingänge sollten verschlossen bleiben, um einen unbefugten Zutritt in Verwaltungsbereiche zu verhindern?  Wie sind die Türen gesichert? Schlüssel, Code-Eingabe, Code-Karte, biometrische Systeme?  Sind Türen nach Möglichkeit von außen nicht mit Türklinke ausgestattet, sondern mit einem nicht drehbaren Knauf?  Existieren weitere zu sichernde Zugänge durch Nebengebäude oder Tiefgarage? Wie sind diese gesichert?  Existieren Notausgänge und wie sind diese gegen unbefugtes Öffnen gesichert? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Besucher Empfang / Pforte** | Unberechtigte Besucher sollten frühzeitig am tieferen Eindringen in das Gebäude gehindert werden.  Existiert ein zentraler Empfang, der Besucher auf den richtigen Weg leitet?  Sind Pforte / Empfang durchgehend zu den Öffnungszeiten besetzt?  Wie ist sichergestellt, dass Personen nicht in sensible Bereiche wie Verwaltung, IT oder Personal gelangen?  Existieren Richtlinien für Mitarbeiter, worauf sie zu achten haben und wie mit auffälligen Personen umzugehen ist? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Schlüsselver-gabe** | Sind Ausgabe, Rücknahme, Tausch und Ersatz von Schlüsseln, Code-Karten, PINs nachvollziehbar dokumentiert und existieren hierfür feste Verfahrensweisen?  Ist den Mitarbeitern diese Verfahrensweise bekannt?  Wird deren Einhaltung regelmäßig überprüft? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Zusätzliche Schutzmaß-nahmen** | Weitere Maßnahmen, welche die Gebäudesicherheit signifikant erhöhen können:   * Bewegungssensoren für Außenbeleuchtung * Alarmanlage * Bewegungsmelder * Glasbruchmelder * Kontrollgänge, z.B. durch Wachschutz außerhalb der Öffnungszeiten |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Sicherheitszonen** | Eine interne Einteilung des Gebäudes in Sicherheitszonen unterstützt bei der Risikobewertung und Planung der notwendigen Schutzmaßnahmen |  |  |
| * + 1. **Planung** | Ist das Gebäude in verschiedene Sicherheitszonen unterteilt? Z.B.   * Bürgerbüro * Verwaltung * IT-Bereich * Archiv   Alternativ (wenn auch weniger differenziert):   * Zwingend öffentlich zugänglicher Bereich * Teilweise öffentlich zugänglicher Bereich * Interner Bereich ohne öffentlichen Zugang |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Schutzmaß-nahmen Übertritte** | Wie ist sichergestellt, dass Unbefugte nicht aus den öffentlich zugänglichen Bereichen in die internen Bereiche gelangen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Signalisation** | Sind nicht öffentlich zugängliche Bereiche entsprechend gekennzeichnet und diese Signalisation leicht zu erkennen? (nur sinnvoll, wenn es keine Schutzmechanismen wie verschlossene Tür zwischen öffentlichem und nicht öffentlichem Bereich gibt)  Wurde auf eine gesonderte Kennzeichnung sensibler Bereiche bewusst verzichtet? Schilder wie „Serverraum“, „Technikraum“ oder „Zutritt nur für Befugte“ sind eine Einladung. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Vermeidung** | Ist durch die gezielte Anlage der Sicherheitszonen gewährleistet, dass in Bereichen mit höherer Schutzstufe kein oder nur so wenig wie möglich Publikumsverkehr herrscht? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Serverraum** | In der heutigen Zeit ist der Serverraum oder der Bereich mit der Netzwerkverteiler-Technik der Bereich, den es besonders zu schützen gilt. Hier gilt, je mehr desto besser. Eine regelmäßige Überprüfung und Anpassung der Schutzmaßnahmen ist Pflicht. |  |  |
| * + 1. **Lage** | Liegt der Serverraum geschützt im Inneren des Gebäudes?  Verfügt er über möglichst nur eine Zugangstür?  Fenster sollten generell keine vorhanden sein, auch nicht ins Gebäudeinnere |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Fenster** | Sofern doch Fenster vorhanden sind, wie sind diese gesichert?   * Bruchfestes Glas * Sicherheitsglas * Vergitterung * Glasbruchmelder |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Türen** | Sind Türen mit ausreichend hoher Schutzklasse verbaut (Metall, Zargen, Sicherheitsschlösser, Aushebelschutz etc.)?  Sind diese mit separaten Schlüsseln oder Kreisen innerhalb des Schließsystems zu öffnen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Alarmierung** | Sind für alle relevanten Vorfälle Alarmierungen eingerichtet?   * Glasbruch * Tür steht zu lange offen oder nicht abgeschlossen * Bewegungsmelder * Videoüberwachung im Innenbereich |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Schutz vor Feuer / Wasser** | Liegt der Serverraum in einem eigenen Brandabschnittsbereich?  Sind brandschutztechnische Belange berücksichtigt?  Schwer brennbare Bodenbeläge, Vermeidung von Brandbrücken durch Kabelschächte, keine zusätzliche Nutzung als Lager (Papier, Putzmittel etc.) oder Archiv  Sind Brand- und Wassermelder installiert und wird deren Funktion regelmäßig geprüft? (Im Zweifel sind bereits im Handel erhältliche Melder ohne Anschluss an eine Hausmeldeanlage eine gute Lösung.)  Führen keine Wasser-Zu- und Ableitungen durch den Serverraum?  Ist der Serverraum nicht unter wasserführenden Räumen wie Küche / Sanitär im Stockwerk darüber eingerichtet?  Ist es möglich, den Serverraum nicht im Keller als wassersammelnder, tiefster Punkt zu betreiben? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Verschluss-sache** | Ist sichergestellt, dass diese Elemente stets verschlossen sind und nur ein beschränkter Mitarbeiterkreis Zugang hat?   * Netzwerkverteiler (auch im Gebäude) * Serverschränke * Patch-Schränke |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Lieferanten/ Externe Dienstleister** | Der ungeregelte Zutritt durch Lieferanten und externe Dienstleister stellt eine Bedrohung für die Sicherheit dar. |  |  |
| **1.4.1 Anlieferung /**  **Abholung** | Werden die getroffenen Schutzmaßnahmen durch entsprechende organisatorische Regelungen bei Anlieferung und Abholung nicht unterbrochen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| **1.4.2. Bewegungs-**  **freiheit** | Dürfen sich Lieferanten und externe Dienstleister nur unter Aufsicht in den höheren Sicherheitszonen, z.B. nicht-öffentlichen Bereichen, bewegen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| **1.4.3. Identitäts-**  **/Auftragsprüfung** | Werden die Identität des Externen und die Richtigkeit des Auftrags vor Zugriff auf Informationen (unabhängig ob elektronisch oder in Papierform) überprüft?  Werden Zugriff oder Übergabe protokolliert?  Wo werden diese Protokolle aufbewahrt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Zugang zu EDV-Systemen** | Hat sich jemand unbefugt Zutritt zu den Räumlichkeiten verschafft, stellen die Schutzmaßnahmen der EDV- Systeme eine weitere Hürde dar. Hier kann bereits mit wenigen Maßnahmen ein hohes Maß an Sicherheit gewährleistet werden. | | |
| * 1. **Passwortsicherheit** | Muss ein Nutzer sowohl beim Login an seinem PC-Arbeitsplatz als auch in den einzelnen Verfahren ein sicheres Passwort eingeben?  Existieren Richtlinien, wie ein sicheres Passwort auszusehen hat (Mindestlänge, Zusammensetzung, Lebensdauer)?  Sind diese Richtlinien an alle Mitarbeiter schriftlich kommuniziert?  Werden diese Richtlinien durchgängig beim Login (Gruppenrichtlinie und in den Verfahren) technisch erzwungen?  Sind die Mitarbeiter angewiesen, die Richtlinien eigenverantwortlich einzuhalten, wenn es keinen technischen Zwang innerhalb des Verfahrens gibt?  Sind die Mitarbeiter für die Notwendigkeit entsprechend sensibilisiert, z.B. im Rahmen einer Schulung Datenschutz und Datensicherheit? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Geräteschutz** | Sind folgende Maßnahmen an den Arbeitsgeräten ergriffen?   * Bootreihenfolge auf Festplatte als erstes Medium eingestellt * Auswahl der Bootreihenfolge beim Systemstart abgeschaltet * BIOS-Passwort gesetzt * Wenn vorhanden, Schutz vor Gehäuseöffnung eingerichtet bzw. Warnmeldung aktiviert * USB-Ports wenn möglich deaktiviert |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Umgang mit sowie Speicherung und Lagerung von Administrations- und Dienstekenn-wörtern** | Es existieren personenbezogene Administrations-Accounts zwecks Nachvollziehbarkeit?  Der eigentliche Administrations-Account „Admin“ wird nur im Notfall genutzt?  Voreingestellte Admin-Passwörter (Auslieferungszustand) werden direkt bei der ersten Nutzung geändert?  Alle wichtigen Kennwörter sind in einem besonders geschützten Passwortcontainer abgelegt (mit eingeschränktem Zugriff) und in ausgedruckter Form im Datenschutz-Tresor hinterlegt?  Für Dienste sind separate Admin-Accounts eingerichtet, diese laufen nicht auf dem allgemeinen „Admin“ oder auf personenbezogenen Accounts? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Zugriffsschutzmaßnahmen** |  | | |
| * 1. **Erzwungener Login** | Ohne Anmeldedaten ist weder der System-Login noch der Zugriff auf relevante Verfahren möglich? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Manueller Logout** | Alle Mitarbeiter sind gehalten, sich bei Verlassen des Arbeitsplatzes (auch für kurze Zeit) manuell vom System abzumelden?  Dies wurde schriftlich kommuniziert, sinnvollerweise mit einer Erklärung, z.B. Windows-L auf Windows Geräten?  Zusätzlich kann über die IT ein Logout-Icon auf dem Desktop der Anwender eingerichtet werden?  Prüfen Sie, ob es sinnvoll ist, die Abmeldung auch aus den Fachverfahren vorzuschreiben bei Abwesenheit von x Minuten. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Bildschirmschoner mit Kennwort-abfrage** | Als zusätzliche Schutzmaßnahme sollte nach spätestens 10 Minuten der Bildschirmschoner mit Kennwortabfrage automatisch starten.  Sofern das manuelle Logout nicht sichergestellt ist, ist die Startzeit des Bildschirmschoners entsprechend zu verkürzen. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Verschlüsselung / Signaturverfahren** | Sind Dateien, Verzeichnisse und Laufwerke mit schutzbedürftigen Daten nach dem aktuellen Stand der Technik verschlüsselt?  Sind mobile Datenträger (Sticks) und Geräte (Notebooks, Tablets, Smartphones) in die Verschlüsselung mit einbezogen?  Kommen bei elektronischer Übertragung entsprechende Signatur- und Verschlüsselungsverfahren zum Einsatz (gerade bei Kommunikation außerhalb des bayerischen Behördennetzes)?  Sind die Mitarbeiter für diese Maßnahmen sensibilisiert? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Berechtigungskonzept** | Ein nachvollziehbares und administrierbares Berechtigungskonzept ist eines der Herzstücke eines funktionierenden Schutzkonzepts.  Neueinstellungen, ausscheidende Mitarbeiter oder z.B. Aushilfen / Praktikanten, die mehrere Bereiche durchlaufen, stellen eine große Herausforderung für ein funktionsfähiges Berechtigungskonzept dar. | | |
| * 1. **Gruppen- versus Einzelberechti-gungen** | Existieren nachvollziehbare Gruppen, mittels derer Nutzer ihre Zugriffsrechte zugeteilt bekommen?  Wird auf die Nutzung von Einzelberechtigungen weitestgehend verzichtet?  Sind möglichst wenig rekursive Gruppen vorhanden (Gruppen, die im schlimmsten Fall mehrmals ineinander verschachtelt sind)?  Wurde das Berechtigungskonzept seit Einführung regelmäßig auf Aktualität und Sicherheit geprüft (z.B. auch mittels externer Tools wie 8Man für das Active Directory)? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Verfahren der Zugriffsvergabe** | Gibt es ein festes Verfahren mittels dessen Zugriffsrechte vergeben und entzogen werden, z.B. bei Anforderung eines Arbeitsplatzes, Wechsel eines Mitarbeiters, Ausscheiden etc.?  Existiert hierfür ein Formular (Papierform oder elektronisch), auf dem alle relevanten Informationen und Arbeitsschritte festgehalten werden (Anforderung, Grund, Prüfung, Freigabe, Bestätigung der Umsetzung)? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Umgang bei zeitweisen Beschäf-tigungen oder bei Ausscheiden** | Ist auch der Rechteentzug für zeitweise Beschäftigungsverhältnisse oder bei Ausscheiden klar geregelt?  In der Praxis zeigt sich, der IT-Bereich erfährt mit als Erstes, wenn ein neuer Arbeitsplatz benötigt wird, ist jedoch das letzte Glied in der Kette, wenn es um die Information eines ausgeschiedenen Mitarbeiters geht. Risiko: weiterhin bestehende Zugriffsmöglichkeiten, z.B. von außen auf die Systeme durch den ehemaligen Mitarbeiter etc. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Systemprotokolle** | Ist bekannt, welche Systemprotokolle aktiviert sind und was konkret aufgezeichnet wird (Login, Logout, Fehlversuche, Sicherheitsverstöße etc.)?  Wann werden diese durch wen, wie oft ausgewertet?  Ist geregelt, was beim Feststellen von Verstößen konkret erfolgt?  Wie wird mit identifizierten Sicherheitsproblemen umgegangen?  Für welche Dauer werden diese Protokolle vorgehalten? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Zugriff, Änderung, Löschung** | Kann in den Systemen und Verfahren die datenschutzkonforme Protokollierung von Zugriffen auf Daten, deren Änderung und Löschung sichergestellt werden?  Wird diese umgesetzt?  Wer kontrolliert dies wann, wie oft?  Was passiert mit diesen Protokollen im Anschluss? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Dokumentation** | Ist das Berechtigungskonzept schriftlich dokumentiert und aktuell? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Externe Dienstleister (Auf-tragsdatenverarbeitung)** | Das Bundesdatenschutzgesetz (§ 11 BDSG) und das bayerische Landesdatenschutzgesetz (Art. 6 BayDSG) schreiben eine besondere Verfahrensweise *VOR* dem Einsatz externer Dienstleistern vor, wenn deren Tätigkeit direkt personenbezogene Daten betrifft oder durch deren Tätigkeit der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (z.B. IT-Support, Fernwartung etc.) Dabei gilt es, zahlreiche Aspekte zu Datenschutz und Datensicherheit zu prüfen, noch bevor mit der Zusammenarbeit begonnen wird. | | |
| * 1. **Technische und organisatorische Maßnahmen (TOM)** | Wurde der externe Dienstleister vor Vertragsabschluss auf ein ausreichend hohes Niveau im Bereich Datenschutz und Datensicherheit geprüft? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Dokumentation der Prüfung** | Wurden die Prüfungen und die Ergebnisse schriftlich dokumentiert?  Sofern es Nachfragen an den Dienstleister gab, sind diese der Dokumentation beigefügt?  Sofern das Schutzniveau nicht ausreichend nachgewiesen und belegt werden kann, muss von einer Beauftragung und Zusammenarbeit abgesehen werden! |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Wiederholung der Prüfung** | Die Prüfung aktueller technischer und organisatorischer Maßnahmen (TOM) ist in regelmäßigen Abständen zu wiederholen (üblicherweise alle 1-2 Jahre).  Wird dies durchgeführt und das Ergebnis ebenfalls protokolliert?  Sollten sich Verschlechterungen am Schutzniveau ergeben, sollte der Dienstleister diese zeitnah beheben. Ansonsten ist der Anbieter zu wechseln. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Vereinbarung zur Auftragsdatenverar-beitung** | Für die rechtskonforme Umsetzung ist eine schriftliche Vereinbarung notwendig, die über die übliche vertragliche Regelung der Zusammenarbeit wie Tätigkeit und Honorar hinausgeht. Früher übliche Klauseln wie „Die Parteien vereinbaren sich an die jeweils gültigen Datenschutzgesetze zu halten“ sind ungültig.  Wurde eine der aktuellen Rechtslage entsprechende Vereinbarung mit dem Dienstleister *VOR* Aufnahme der Zusammenarbeit geschlossen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Überprüfen bestehender Vereinbarungen** | Wurden langfristig bestehende Vereinbarungen jeweils der aktuellen Rechtslage z.B. nach Novellierungen angepasst?  Sollte dies versäumt worden sein, gilt die Vereinbarung als ungültig. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Umfang der Vereinbarung** | Regelt die Vereinbarung alle vorgeschriebenen Punkte wie z.B.   * Bezeichnung des Verfahrens, * Zweck und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung, * Art der gespeicherten Daten, * Kreis der Betroffenen, * Art der regelmäßig zu übermittelnden Daten und deren Empfänger, * Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung, * verarbeitungs- und nutzungsberechtigte Personengruppen, * im Fall des Art. 6 Abs. 1 bis 3 die Auftragnehmer, [Auftragsdatenverarbeitung] * Empfänger vorgesehener Datenübermittlungen in Drittländer. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Notfallkonzept / Verfügbar-keit der Systeme** | Erst im Fall einer gravierenden Störung oder eines Notfalls zeigt sich, ob die Maßnahmen aus diesem Prüfpunkt erfolgreich umgesetzt wurden. Dies lässt sich auch durch ausführliche Tests teilweise nicht ausreichend simulieren. Umso wichtiger ist eine konsequente Prüfung und Umsetzung identifizierter Schwachstellen. | | |
| * 1. **Firewall** | Wird eine dem Stand der Technik entsprechende Firewall-Lösung zum Schutz vor Zugriffen von außen eingesetzt, entweder als Hard- oder Softwarelösung?  Sind die Funktionen der Firewall bekannt und dokumentiert?  Wer überprüft die Firewall und deren Konfiguration auf Aktualität? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Virenschutz** | Sind sowohl client- als auch serverseitig geeignete Virenschutzmaßnahmen installiert?  Werden Updates sowohl auf dem Server als auch auf Clients sichergestellt? Wie wird dies getan?  Werden Mitarbeiter über außerordentliche, aktuelle Bedrohungen informiert? Wenn ja, wie? Wenn nein, warum nicht? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **WLAN** | Sofern WLAN eingesetzt wird:   * Existiert eine Übersicht über alle Zugangspunkte / Hotspots? * Wurde auf ausreichend sichere Ver-schlüsselung WPA/WPA2 geachtet? * Sind weitere Schutzmechanismen im Einsatz wie MAC-Filter etc.? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Backup / Recovery** | Nicht nur die Sicherung an sich ist wichtig. Die zu sichernden Daten müssen nach Dringlichkeit der Wiederherstellung klassifiziert sein, geeignete Backupverfahren und Zyklen ausgewählt sein sowie regelmäßig Wiederherstellungstests durchgeführt werden. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Sicherungs-konzept** | Existiert ein Sicherungskonzept, aus dem hervorgeht:   * Wichtigkeit der Verfahren und Daten? * Sicherungsart? * Sicherungsrhythmus? * Verantwortlichkeiten? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Technik** | Ist die Art der Sicherung noch zeitgemäß?  Ist mittels der eingesetzten Sicherungstechnik ein zeitnahes Recovery möglich?  Sind ausreichend Schutzmaßnahmen wie Verschlüsselung, Brandschutz etc. berücksichtigt? (Ungeeigneter Klassiker: Tapeloader im Serverraum in Endlosschleife)  Bei Sicherung auf Wechselmedien: Werden diese regelmäßig ausgetauscht, um Ausfällen vorzubeugen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Lagerung der Datensicherung** | Werden die Sicherungsmedien (Tape, Wechselplatte, NAS) außerhalb des Serverraums gelagert?  Möglichst in einem anderen Brandabschnitt?  Ist ein Datensicherungstresor vorhanden nach Norm S 60 / 120 DIS?  Bei Online-Backup: Sind die Datenübertragung und der Online-Speicher nach aktuellem Stand verschlüsselt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Beschreibung** | Existiert eine genaue Beschreibung des Backups und der Maßnahmen für ein erfolgreiches Recovery für den Fall der Nichtverfügbarkeit der Hauptverantwortlichen für das Backup?  Ohne eine solche Beschreibung wird das Zurückspielen zum unkalkulierbaren Risiko, z.B. bei Ausfall der verantwortlichen Mitarbeiter bei Krankheit, Dienstreise oder Ausscheiden.  Wird diese Beschreibung zeitnah angepasst, wenn sich etwas am Sicherungskonzept verändert?  Wer ist dafür verantwortlich? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Recovery-Tests** | Die Erfolgsmeldungen der Datensicherungssoftware können täuschen. Trotz positiver Meldung sind durchaus Backups nicht mehr les- und wiederherstellbar im Ernstfall.  Werden regelmäßige (Intervall 3-6 Monate) Überprüfungen der Backups auf Funktionsfähigkeit durchgeführt?  Beschränkt sich der Recovery-Test nicht auf einzelne Dateien, sondern werden auch komplette Server-Umgebungen getestet?  Wird das Ergebnis entsprechend dokumentiert?  Werden Fehlversuche analysiert und deren Ursache zeitnah abgestellt?  Werden auch diese Maßnahmen schriftlich dokumentiert?  Wer ist für die Durchführung der Tests und die weitere Bearbeitung verantwortlich? Ist dies schriftlich dokumentiert und dem Verantwortlichen bekannt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * + 1. **Umgang mit älteren Sicherungen** | Im Laufe der Zeit finden Wechsel der Sicherungssysteme (Hardware und Software statt).  Ist sichergestellt, dass ältere Sicherungen (z.B. Jahressicherungen) auch nach einem Wechsel noch verfügbar sind, z.B. durch Überspielen auf neue Sicherungstechnik?  Dies ist gerade im Hinblick auf Aufbewahrungsfristen wichtig, sofern keine anderweitige elektronische Archivierung stattfindet. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Sicherheitsbe-auftragter** | Existiert ein Sicherheitsbeauftragter?  Ist dieser vom Fachwissen her für die Aufgabe geeignet?  Verfügt dieser über ausreichend zeitliche Ressourcen, um seine Aufgaben wahrnehmen zu können? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Brandschutzgeräte** | Existieren ausreichend Brandschutzgeräte gerade im IT-Bereich / Serverraum?  Sind diese frei zugänglich angebracht? (nicht hinter Türen, zugestellt mit Material etc.)  Existieren deutliche und ausreichend viele Hinweisschilder auf die Standorte der Brandschutzgeräte? (Im Zweifel sind das mehr Hinweise als sie der Brandschutz rechtlich vorsieht.)  Werden die Brandschutzgeräte regelmäßig gewartet / geprüft? Sind nachvollziehbar ALLE Geräte in den Wartungszyklus integriert (Problem Einzelanschaffungen)?  Sind Mitarbeiter in die Brandbekämpfung eingewiesen oder dafür speziell ausgebildet? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Brandmeldesystem** | Wird das Brandmeldesystem regelmäßig geprüft und das Ergebnis dokumentiert?  Sind ausreichend Brandmelder vorhanden (in der Praxis werden meist mehr benötigt als der Brandschutz vorschreibt)?  Ist die automatisierte Benachrichtigung der richtigen Ansprechpartner im Falle eines Auslösens sichergestellt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **USV** | Sind relevante Systeme vor Stromausfällen mittels unterbrechungsfreier Stromversorgung gesichert?  Werden die USV regelmäßig gewartet (Akkuprüfung, Austausch)? Werden diese Arbeiten protokolliert?  Melden die USV kritische Zustände nicht nur per Leuchtanzeige, sondern ebenfalls für Meldesysteme wie Email / SMS?  Werden lediglich einfache USV eingesetzt oder intelligente Systeme, die entsprechende Notaktivitäten einleiten (Information an Nutzer, Schließen der Datenbanken, Herunterfahren der Systeme etc.)?  Wer ist für die Betriebssicherheit und Funktionsfähigkeit der USV konkret verantwortlich?  Sind ausreichend Netzersatzgeräte, z.B. Katastrophenschutzeinrichtungen, vorhanden? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Überwachung / Monitoring** | Sind alle verfügbaren Monitoring Systeme im IT-Bereich installiert / aktiviert wie:   * Temperatur? * Feuchtigkeit? * Unbefugter Zutritt / Einbruch? * Fehlerhafte Backups? * Fehlermeldungen der USV? * Verstöße gegen Sicherheitsrichtlinien auf den Systemen?   Ist sichergestellt, dass der Empfänger von Alarm-SMS/-Email mit den eingehenden Informationen handlungsfähig ist?  Wie ist der Einsatz außerhalb der Öffnungszeiten geregelt?  Sind die Empfänger aktuell oder laufen die Meldungen eventuell ins Leere?  Wer ist für die Einrichtung und Konfiguration des Monitorings verantwortlich?  Sind die informierten Mitarbeiter ausreichend geschult und eingewiesen, was im Meldefall zu tun ist? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Dokumentation** | Eine ausführliche Dokumentation ist das A und O für die erfolgreiche Umsetzung eines Notfallkonzepts. Ohne diese Informationen kann nicht gewährleistet werden, kritische Verfahren zeitnah wieder anfahren zu können. Folgende Informationen sollten mindestens verfügbar und aktuell sein:   * Netzwerkübersichten der eingesetzten Technik und Systeme * Leitungsübersicht (interne Verkabelung) und externe Leitungen, inkl. Beschreibung der Patchfeld-Systematiken * Detailliertes Verfahrensverzeichnis (Übersicht aller relevanten Verfahren im Haus mit genauer Beschreibung der Verantwortlichkeiten, Funktionen, Daten, Berechtigungen, Schutzmaßnahmen etc.) – im Zweifel fragen Sie Ihren Datenschutz-beauftragten * Übersicht über externe Zulieferer (Strom, Wasser, TK, Datenleitungen, Hardware, Software etc.) mit Ansprechpartnern, Rufnummern, (Rahmen-)Vertragsdaten, Leistungsbeschreibung in Kurzform * Übersicht über externe Dienstleister, z.B. für Installation, Wartung, Konfiguration, Support, Fehlerbehebung etc. mit Ansprechpartnern, Rufnummern, Vertragsdaten und Leistungsbeschreibung * Verzeichnis der im Einsatz befindlichen Hard- und Software sowohl für Server als auch Arbeitsplätze * Übersicht über auf den Geräten installierte Standardsoftware und darüber hinaus installierte Zusatzsoftware * Klassifizierung der eingesetzten Systeme und Verfahren nach Dringlichkeit für eine Wiederherstellung (siehe nächsten Punkt Risikoanalyse) |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Risikoanalyse** | Wurde eine Risikoanalyse durchgeführt, aus der hervorgeht:   * Welche Risiken bedrohen die Funktionsfähigkeit der Systeme? * Identifikation kritischer und weniger kritischer Systeme und Verfahren. * Maximal tolerierbare Ausfallzeit von Systemen und Verfahren (im Detail).   Wann wurde die Risikoanalyse zuletzt durchgeführt (1 x jährliche Überprüfung)? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Notfallplan** | Wurde ein Notfallplan auf Basis der Risikoanalyse erstellt und bekanntgemacht?  Wo wird dieser Notfallplan aufbewahrt? Empfehlenswert: elektronische Kopie sowie stets aktuelle Papierversion z.B. in Datenschutztresor.  Sind alle notwendigen Handlungsabläufe nachvollziehbar dokumentiert, auch für z.B. externe Kräfte oder Personen, die nicht an der Erstellung beteiligt waren?  Sind die Organisationsstruktur und die Verantwortlichkeiten für die Wiederanlauf-maßnahmen klar vorgegeben, um eine reibungs- und konfliktlose Umsetzung zu gewährleisten?  Werden die Notfallmaßnahmen regelmäßig getestet und mit den Mitarbeitern Notfallübungen abgehalten? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Richtlinien / Anweisungen als organisatorische Maßnahmen** | Sind folgende Richtlinien / Anweisungen vorhanden:   * Nutzung des Email-Accounts / Webzugangs zu geschäftlichen / privaten Zwecken? * Klassifizierung von (personenbezogenen) Daten und der Umgang damit? * Manuelle Sperre des Desktops bei Verlassen des Arbeitsplatzes? * Clean desk? * Vertretungszugriffe statt Passwortweitergabe? * Passwort-Richtlinie für Verfahren ohne technische Zwangsmaßnahme für Passwortkonventionen? * Umgang mit Email-Archivierung? * Entsorgung von Daten in Papierform oder auf elektronischen Medien? * Verhalten bei Datenpannen und Sicherheitsverstößen?   Wann wurden diese zuletzt aktualisiert?  Entsprechen diese noch den rechtlichen Vorschriften und technischen Anforderungen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Umgang mit mobilen Geräten / Datenträgern** | Existiert eine Verpflichtung zur Verschlüsselung von Geräten wie Laptops, Tabs, Smartphones sowie Speicherkarten, USB Sticks etc.?  Wurde kommuniziert, dass Login-/Zugangsdaten auf mobilen Geräten z.B. für VPN, Email, Verfahren, etc. nicht gespeichert werden sollen, sofern keine Verschlüsselung und Gerätesperre vorliegen (VPN Zugangsdaten sollten NIE abgespeichert werden!)?  Sind zusätzliche Sicherheitssperren aktiv, z.B. PIN / Passwort bei Smartphones? (Keine Gesten, da zu unsicher.)  Ist die Meldepflicht bei Verlust bekannt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Sicherheitsrichtlinie** | Neben den detaillierten Richtlinien und Anweisungen sollte den Mitarbeitern eine zusammenfassende Sicherheitsrichtlinie bekannt gemacht werden.  Sinnvollerweise geschieht dies in Verbindung mit einer kurzen Schulungs-/Trainingseinheit (z.B. Aware-Kampagne „Der unsichtbare Dritte“). |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Beschäftigte / Mitarbeiter** | Ein nicht unerhebliches Risiko für Datensicherheit und Datenschutz geht – bewusst oder unbewusst – von den eigenen Mitarbeitern aus.  Neben der Entwicklung und Bekanntmachung von Richtlinien und Anweisungen sind daher weitere Maßnahmen zur Sensibilisierung und Umsetzung rechtlicher Anforderungen notwendig. | | |
| * 1. **Schulungen Datenschutz und Datensicherheit** | Werden Mitarbeiter bei der Einstellung im Rahmen einer Präsenzveranstaltung oder eines Online-Trainings (möglichst mit Zertifikat) auf die Themen Datenschutz und Datensicherheit sensibilisiert?  Finden regelmäßig, spätestens alle zwei Jahre, besser häufiger, Auffrischungen statt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Datengeheimnis** | Sind nachweislich alle Mitarbeiter schriftlich auf das sogenannte „Datengeheimnis“ nach § 5 verpflichtet, z.B. im Anschluss an eine Schulung Datenschutz und Datensicherheit? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Fernmeldege-heimnis** | Es empfiehlt sich, Mitarbeiter mit Außenkontakt (Bürgerbüro, Telefonzentrale, Ansprechpartner für Bürger etc.) sowie Mitarbeiter mit regelmäßigem Zugriff auf Verbindungsdaten (z.B. IT-Mitarbeiter) auf das Fernmeldegeheimnis nach § 88 TKG zu verpflichten.  Ist diese Verpflichtung erfolgt?  Ist sie in Schriftform erfolgt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Prozess Einstellen / Wechsel / Aus-scheiden von Mitarbeitern** | Existiert ein nachvollziehbarer Prozess für alle Beteiligten (Personal, IT, Verwaltung etc.) für neue, wechselnde und ausscheidende Mitarbeiter?  Sind darin auch enthalten   * Anforderung IT-Arbeitsplatz? * Zugriffsberechtigungen (Einrichtungen / Entzug)? * Ausgabe / Rücknahme von IT-Equipment? * Sicherheitsunterweisung? * Schulung Datenschutz und Datensicherheit? * Verpflichtungen?   Ist der Datenschutzbeauftragte in die Entwicklung und Pflege dieses Prozesses aktiv involviert? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Datenschutzbeauftragter** | Ein aktiver Datenschutzbeauftragter ist ein wichtiger Beitrag zur Datensicherheit, nicht nur zum Datenschutz. Seine Maßnahmen beschränken sich in der Praxis nicht auf personenbezogene Daten, sondern beinhalten jedwede Art von schützenswerter Information. | | |
| * 1. **Bestellpflicht** | Öffentliche Stellen sind verpflichtet, einen Datenschutzbeauftragten (DSB) zu bestellen.  Mehrere öffentliche Stellen können sich einen DSB teilen, sofern er seinen Aufgaben als DSB nach wie vor im ausreichenden Maß nachkommen kann.  Wurde ein Datenschutzbeauftragter bestellt? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Bestellurkunde** | Wurde der Datenschutzbeauftragte korrekt schriftlich bestellt und seine Aufgaben klar definiert (z.B. Stellenbeschreibung)? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Fachkunde** | Hat der (zu bestellende) DSB ausreichend Fachkunde als Voraussetzung für die Tätigkeit als DSB?  Die Fachkunde muss vor der Bestellung vorliegen.  Hinweis: Bei der Auswahl der Qualifizierungskurse ist darauf zu achten, dass Crash-Kurse oft nicht das notwendige Grundwissen für die Ausübung dieser Tätigkeit vermitteln. Empfohlen sind mindestens drei Tage, besser fünf Tage. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Ressourcen** | Dem DSB müssen ausreichend zeitliche, finanzielle und räumliche Ressourcen zur Verfügung stehen.  Ist dies (gerade in Anbetracht einer Bestellung zusätzlich zum eigentlichen Aufgabenbereich) gewährleistet? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Vermeidung einer Pro Forma Bestellung** | Verfügt der DSB nicht über die notwendige Fachkunde, besucht er keine regelmäßigen Weiterbildungen, kann er seiner Tätigkeit aufgrund mangelnder Ressourcen nicht nachkommen, spricht man von einer sogenannten Pro-forma-Bestellung.  Diese wird in einschlägigen Kommentaren zum deutschen Datenschutzrecht als eine Nichtbestellung betrachtet, was einen erheblichen Verstoß gegen die bestehenden Datenschutzgesetze darstellt. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Interessenkonflikte** | Ist der Datenschutzbeauftragte frei von Interessenkonflikten zu seinen anderen Tätigkeiten?  Bei Mitarbeitern im Bereich IT, Personal, Marketing, Behördenleitung, Bereichsleitung kann in der Regel ein Interessenkonflikt angenommen werden. Diese Mitarbeiter scheiden für eine gültige Bestellung daher aus. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Reporting / Unterstützung** | Hat der DSB ein exklusives Vortragsrecht an den Geschäfts-/Behördenleiter?  Erhält er von diesen die notwendige Rückendeckung für seine Tätigkeit und die Umsetzung notwendiger Maßnahmen? |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Einbeziehung** | Wird der DSB rechtzeitig von den Fachbereichen einbezogen, z.B. bei Änderung bestehender Verfahren oder Einführung neuer Verfahren?  Hier besteht eine Bringschuld gegenüber dem DSB. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Das datenschutz-rechtliche Freigabe-verfahren** | Sowohl der erstmalige Einsatz als auch wesentliche Änderungen von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedürfen grundsätzlich gem. Art. 26 BayDSG der vorherigen schriftlichen Freigabe durch den behördlichen Datenschutzbeauftragten der das Verfahren einsetzenden öffentlichen Stelle.  Ist diese Vorgehensweise als fester Bestandteil der Arbeitsabläufe implementiert?  AKDB-Verfahren werden gemäß Art. 26 Absatz 1 Satz 2 BayDSG als bereits freigegeben betrachtet. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
|  |  |  |  |
| 1. **Verfahrensverzeichnis** | Unsere Datenschutzgesetze verpflichten jede Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt, zum Führen eines sogenannten Verfahrensverzeichnisses.  Dieses muss auf Verlangen der Schutzbehörden jederzeit vorgelegt werden können.  Unterschätzen Sie den Zeitaufwand für dessen Erstellung und Pflege nicht. Wenn die Anforderung kommt, ist es für gewöhnlich zu spät, um das Verzeichnis fristgerecht noch erstellen und vorlegen zu können. | | |
| * 1. **„Verfahrensver-zeichnis für jedermann“** | Existiert eine grobe Übersicht der Aufgabenbeschreibung und betroffenen personenbezogenen Daten samt Kreis der Betroffenen?  Für gewöhnlich ist dies recht schnell und einfach zu erstellen.  Auf Verlangen ist diese jedermann zur Verfügung zu stellen.  Achtung: Detailgrad darf kein Sicherheitsrisiko darstellen. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Detailliertes Ver-fahrensverzeichnis** | Wurde eine umfangreiche Übersicht über ALLE IT-gestützten Verfahren, mit denen personenbezogene Daten verarbeitet werden, erstellt?  Diese Übersicht enthält neben der Beschreibung der Verfahren detaillierte Angaben wie zum Beispiel   * eingesetzter Hard- und Software, * Berechtigungskonzepte, * Schutzmaßnahmen, * Angaben zu den verarbeiteten Daten, * verantwortliche Mitarbeiter, * Löschfristen, * Angaben zu involvierten externen Dienstleistern, * Inkrafttreten des Verfahrens, * Nachweis der Aktualitätsprüfung. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |
| * 1. **Zuständigkeiten** | Die Datenschutzgesetze sehen vor, diese Verzeichnisse durch den DSB führen zu lassen. Die Meldung von Verfahren, das Einliefern aller relevanten Informationen sowie deren regelmäßige Aktualisierung obliegen den Fachbereichen als verantwortliche Stelle unter Einbeziehung des IT-Bereichs / -Verantwortlichen. |  | Vollständig erfüllt  Fast erfüllt  Teilweise erfüllt  Nicht erfüllt  Nicht anwendbar  Aktuell in Arbeit |

**Abschlusskommentar**

**Abschlussbewertung**

Ohne Mängel, kein Handlungsbedarf

Wenige Mängel, es besteht Handlungsbedarf

Zahlreiche Mängel, diese sollten zeitnah abgestellt werden

Gravierende Mängel, akuter Handlungsbedarf