

Gliederungspunkt	<i>Frage/Hinweis</i>
1. Einleitung zum Projekt	<i>Wie nenne ich das Vorhaben? Worum geht es? Wer führt das Projekt durch bzw. ist die verantwortliche Stelle für das Projekt?</i>
2. Fachliche Hintergründe zum Projekt	<i>Warum wird das Projekt durchgeführt? Welche Probleme sind die Motivation für das Projekt bzw. welche Probleme sollen gelöst werden?</i>
3. Beschreibung und Zielsetzung des Vorhabens	<i>Welche fachlichen Anforderungen sind bekannt? Was soll die Lösung bzw. das Projektergebnis können?</i>
4. Rechtsgrundlage der Datenverarbeitung des Projekts	<p><i>Welche Rechtsgrundlage ermöglicht die Datenverarbeitung des Projekts bzw. wer/was erlaubt mir, das geplante Vorhaben durchzuführen? Damit verbunden ergeben sich die Gesetze, die bei der Konzeption zu berücksichtigen sind:</i></p> <p><i>a) Wirksame Einwilligung des Betroffenen; bspw. §§ 4 (1) und § 4a BDSG, LDSG (etwa § 4 DSG NW)</i></p> <p><i>b) Erlaubnis durch ein Gesetz; bspw. §§13 ff. bzw. 28ff. BDSG, LDSG (etwa §§12 ff DSG NW) oder andere Rechtsvorschriften (etwa §67a SGB X u.a., §10 GDSG NW)</i></p>
5. Beschreibung der datenschutzrechtlichen Rahmenbedingungen (Angaben zum Verfahrensverzeichnis)	<i>Tabellarische Ausführung; etwa nach Vorgabe §4e BDSG oder § 8 DSG NRW oder anderen, je nach zutreffendem Fall. Bitte gehen Sie die geforderten Angaben durch – je nach den für Sie geltenden gesetzlichen Grundlagen.</i>
6. Datenschutzbezogene Anforderungen	<i>Folgende Aspekte sollten beschrieben werden, insofern im Kontext des Projekts zutreffend:</i>
a) Geeignetheit	<i>Ist das Datenverarbeitungsverfahren geeignet den angestrebten Zweck zu erfüllen?</i>
b) Erforderlichkeit	<i>Sind das gewählte Gesamtverfahren, die Daten, die einzelnen Verarbeitungen überhaupt erforderlich, um den angestrebten Zweck zu erreichen? Geht es nicht ggf. mit weniger Eingriffen in die Persönlichkeitsrechte der Betroffenen?</i>
c) Grundsatz der Datenvermeidung und -sparsamkeit	<i>Welche Techniken lassen sich sinnvoll einsetzen, um den Personenbezug weiter einzuschränken, ohne dass der Zweck gefährdet wird? Sind nachfolgende Maßnahmen sinnvoll einsetzbar: Anonymisierung, Pseudonymisierung, Trennung von personenidentifizierenden Daten?</i>

d) Verhältnismäßigkeit der Datenverarbeitung/Übermaßverbot	<i>Ist die Art und Weise der Verarbeitung, um den Zweck zu erreichen, verhältnismäßig? Die Frage ist insbesondere bei der Datenverarbeitung von besonderen Arten personenbezogener Daten (z.B. medizinische Daten) oder dem Einsatz einer automatisierte Einzelentscheidung (etwa §6a BDSG) bedeutsam. Welches Missbrauchsrisiko besteht für den Betroffenen, wenn Daten in „falsche“ Hände gelangen? Steht das Risiko in einem vertretbaren Verhältnis zum Nutzen der Datenverarbeitung?</i>
e) Zweckbindung, Aufbewahrungsfristen	<i>Bitte beschreiben Sie den Zweck der Datenverarbeitung. Stellen Sie sich bei der Antwort einen Text vor, der einen Betroffenen erläutert, in was und warum er einwilligen soll und warum. Zwecke sind regelmäßig zeitbegrenzt oder anlassbegrenzt: Welche Fristen gelten daher bei unserem Datenverarbeitungsvorhaben für die Daten? Wie lange dürfen/müssen die Daten aufbewahrt werden? Wie sieht unser Lösch- und Sperrkonzept aus? Wie wird geregelt, bzw. wie wird sichergestellt, dass die Daten nicht für andere Zwecke genutzt werden?</i>
f) Betroffenenrechte	<i>Welche Rechte von Betroffenen sind zu erfüllen (z.B. Recht auf Auskunft, Berichtigung, Widerruf etc.)?</i>
	<i>Hinweis: Die nachfolgenden Unterpunkte betrachten Datenschutzanforderungen ausgehend von den Daten und abstrahieren von konkreten Technologien. Zu den Anforderungen s. „Datenschutz und Telemedizin“, Bultmann et al., 2002, S. 10-13.</i>
g) Wahrung der Vertraulichkeit	<i>Ist bei dem Projekt die Vertraulichkeit und/oder die Schweigepflicht zu wahren? Welche Anforderungen sind hieran zu stellen? Wie wird sichergestellt, dass die Daten nicht von Unbefugten eingesehen werden können?</i>
h) Authentizität (Zurechenbarkeit)	<i>Wie wird die Eindeutigkeit der Urheberschaft eines Dokuments/eines Eintrages sichergestellt?</i>
i) Integrität der Daten	<i>Welche Anforderungen an die Integrität (Unversehrtheit der Daten) sind für das Projekt essentiell? Wie wird die Unverändertheit und Vollständigkeit der Daten sichergestellt? (Hinweis: Dies schließt auch den korrekten Zeitpunkt der Erstellung/Bearbeitung mit ein.)</i>
a) Verfügbarkeit	<i>Welche Anforderungen bestehen an die Verfügbarkeit der Datenverarbeitungssysteme und der Daten?</i>
j) Revisionsfähigkeit	<i>Ist es bei dem Projekt wichtig, dass Änderungen an Daten protokolliert werden, d. h., dass das System revisionsfähig ist? Wie wird sichergestellt, dass unberechtigte Manipulationen an den Daten aufgedeckt und nachvollzogen werden können?</i>
b) Validität	<i>Welche Anforderungen an die Qualität der Daten sind gegeben, um den Zweck zu erreichen? Sind die Daten aktuell und in einer für den Verarbeitungszweck genügenden Qualität? Relevant etwa bei Bilddokumenten, um den medizinischen Zweck erreichen zu können.</i>

c) Rechtssicherheit	<i>Besteht die Notwendigkeit, dass die Daten ggf. vor Gericht als Beweismittel angesehen werden? Wie wird dies sichergestellt? Ist für die Gerichtsverwertbarkeit der Einsatz einer qualifizierten elektronischen Signatur vorzusehen?</i>
d) Nicht-Abstreitbarkeit von Übermittlungen	<i>Besteht die Notwendigkeit, dass Übermittlungen so dokumentiert werden, dass sowohl Sender und Empfänger das Versenden bzw. das Erhalten nicht abstreiten können? Wie wird sichergestellt dass die Urheberschaft an einer Information oder einer Änderung daran (ggf. gerichtsfest) nachgewiesen werden kann?</i>
e) Nutzungsfestlegungen	<i>Können für personenbezogene Daten/Dokumente der Kreis der Nutzer und deren Nutzungsrechte (z.B. lesen, schreiben, ändern) abgestuft geregelt werden? Wie wird dieses sichergestellt (eventuell durch Rollenkonzepte)?</i>
f) Aspekte aus Anlage zu § 9 Satz 1 BDSG bzw. §10 DSG NW – je nach Trägerschaft	<p><i>Hinweis: Die in manchen Gesetzen genutzte technisch-organisatorische Sicht wie in §9 BDSG zielen vorrangig auf technische Aspekte von Datenverarbeitungsvorhaben. Durch die zunehmende Vernetzung von Datenverarbeitungsvorhaben und dadurch die Einbeziehung mehrerer Beteiligter – wie dies bei elektronischen Aktensystemen der Fall ist, wandelt sich zunehmend das Bild von stationären hin zu mitunter komplex vernetzten elektronischen Datenverarbeitungsverfahren. Dieser Technologiewandel schlug in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2002 in der Ausarbeitung der Hilfestellung „Datenschutz und Telemedizin“ von Bultmann et al nieder (s. oben), in der zu einer abstrakteren Betrachtung mit Hilfe von Sicherheitszielen geraten wird. Diese nun mehr auf die Daten orientierte Sichtweise wurde beispielsweise auch im Datenschutzgesetz des Landes NRW aufgegriffen (vgl. §10 DSG NRW).</i></p> <p><i>Ggf. entsprechend der Anlagen Ergänzungen vornehmen, wo zielführend und notwendig.</i></p>
7. Implementierte Datenschutzmaßnahmen	<i>Zu den unter 6 identifizierten Datenschutzanforderungen: Welche Maßnahmen werden als erforderlich zur Erfüllung der oben genannten Datenschutz-Anforderungen identifiziert? Beispiele wären etwa die Datentrennung, Pseudonymisierung, Zugriffskontrolle/rollenbasierte Zugriffskonzepte, Verschlüsselung, etc.</i>
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung	<i>Bitte beschreiben bzw. skizzieren Sie Ihre ausgearbeitete Gesamtlösung. Der Leser soll einen Überblick über das konzipierte Verfahren erhalten.</i>

9. Ggf. IT-Sicherheitskonzept	<i>Das IT-Sicherheitskonzept ist kein expliziter Schwerpunkt eines Datenschutzkonzeptes, kann jedoch vielfach einen vertieften Einblick in die Konzeption/Umsetzung geben. Insofern Sie bereits IT-Sicherheitskonzeptionen zielführend einsetzen können oder zur Hand haben, bietet sich dieses Kapitel oder alternativ die Beilegung als Anhang an. Zur Erstellung eines IT-SiKo zur konkreten technischen Umsetzung bietet sich das Vorgehen nach BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, Kapitel 4 an.</i>
10. Konzeptuelle Risikobetrachtung	<i>Bei dieser konzeptuellen Risikobetrachtung ist nicht zwingend die klassische Risikoanalyse aus der IT-Sicherheits-Analyse gemeint. Vielmehr sollen anhand der unter 8 beschriebenen Lösung/Konzeption mögliche Angriffsszenarien durchspielt werden (etwa: Unbefugte Person gibt sich für einen Patienten aus und verlangt die Löschung seiner Daten; beim Übertragen von Röntgenbildern per eMail werden die eMails abgefangen, um sie zu lesen usw.)? Bitte skizzieren Sie, wie groß/relevant das Risiko dieser Angriffsszenarien ist und welche Maßnahmen die jeweiligen Angriffsszenarien abwehren würden? Wenn Sie dies für alle wesentlichen Angriffsszenarien durchgearbeitet haben, prüfen Sie, welche Restrisiken anhand der getroffenen Maßnahmen noch verbleiben: Ist das verbleibende Restrisiko durch weitere verhältnismäßige Maßnahmen reduzierbar oder ist das Risiko vertretbar oder müssen ggf. Einschränkungen beim angestrebten Zweck gemacht werden?</i>
11. Anlagen	<i>Bitte fügen Sie z.B. Musterdokumente für Patienteninformation, Patienteneinwilligung sowie eine Auflistung der erhobenen, verarbeiteten und genutzten Daten(felder) bei.</i>

Kontakt:

Eric Wichterich: e.wichterich@ztg-nrw.de

Lars Treinat: l.treinat@ztg-nrw.de