Derr Hessische Datenschutzbeauftragte

Hinweise, Checkliste und Ablauf zur Vorabkontrolle nach § 7 Abs. 6 Hessisches Datenschutzgesetz

Grundsätzliches zur Vorabkontrolle

Vor dem Einsatz oder der wesentlichen Änderung eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten ist nach § 7 Abs. 6 HDSG die sogenannte "Vorabkontrolle" durchzuführen. Dies ist eine Untersuchung, ob durch die beabsichtigte automatisierte Datenverarbeitung das in § 1 Abs. 1 Nr. 1 HDSG beschriebene Recht der informationellen Selbstbestimmung (das Datenschutzrecht als Persönlichkeitsrecht des Einzelnen) gefährdet wird. Die in Zusammenarbeit mit dem Hessischen Innenministerium und einigen behördlichen Datenschutzbeauftragten entwickelte inhaltliche Checkliste und das Ablaufschema bieten zwar für die meisten Fälle eine gute Orientierung, können aber nicht alle denkbaren Aspekte der Vorabkontrolle abdecken. Unterschiede in Intensität und relevanten Prüfungspunkten entstehen zwangsläufig wegen der unterschiedlichen Sensitivität der zu verarbeitenden personenbezogenen Daten, der unterschiedlichen Risikofaktoren und der unterschiedlichen Sicherheitskonzepte.
Die Checkliste und das Ablaufschema sind auf eine Vielzahl von Prüfungen automatisierter Verfahren anwendbar, z.B. wenn es um die datenschutzrechtliche Prüfung im Rahmen der Auswahl zwischen verschiedenen Softwareprodukten geht.
Nachfolgend sind besondere Fälle betrachtet, bei denen bereits vorhersehbar ist, dass eine Vorabkontrolle von diesem Schema abweichen kann:

- Bei **Verfahren**, die **speziell** für die Verarbeitung personenbezogener Daten im Rahmen einer bestimmten Aufgabenstellung **neu entwickelt** werden, ist die Checkliste parallel zur Entwicklung abzuarbeiten und dabei sind die in Betracht gezogenen Verfahrensalternativen datenschutzrechtlich zu bewerten.
- Bei **komplexen Verfahren**, die für die Verarbeitung personenbezogener Daten den Einsatz **verschiedener** Komponenten und Optionen ermöglichen (z.B. SAP/R3), wird die Vorabkontrolle nicht schon vor der prinzipiellen Entscheidung, welches Verfahren eingesetzt werden soll, erfolgen können. Sie lässt sich regelmäßig erst parallel zu Auswahl und Erprobung jener Komponenten durchführen, mit denen die personenbezogenen Daten verarbeitet werden, also wenn feststeht, welche Komponenten welche personenbezogenen Daten wie und auf welche Weise verarbeiten sollen. Auch die angebotenen Alternativen für ein Sicherheitskonzept sind von vielfältigen Randbedingungen abhängig, die nicht global, sondern nur für den konkreten Einsatz beurteilt werden können. Deshalb wird bei solchen Verfahren die Vorabkontrolle schrittweise parallel zu einer entsprechenden Konkretisierung erfolgen.
- Für **Standardverfahren, die** ohne Anbindung an eine bestimmte Verwaltungsaufgabe **übergreifend als "Werkzeug"** für verschiedene Aufgaben eingesetzt werden (z.B. einfache Telefonanlagen, Textverarbeitung), ist für die Einsatzfelder, bei denen personenbezogene Daten verarbeitet werden sollen, eine Vorabkontrolle durchzuführen. Ein Verfahrensverzeichnis ist für das Standardverfahren als solches nicht notwendig (Erlass des HMdI zu §§ 6 und 15 HDSG, StAnz 17/1999, S. 1226). Zweck der Vorabkontrolle solcher Verfahren ist festzustellen, ob der geplante Einsatz zur Verarbeitung personenbezogener Daten rechtmäßig ist; insbesondere muss sichergestellt sein, dass mögliche Risiken erkannt und durch entsprechende Sicherheitsmaßnahmen minimiert werden.

Bei dem Einsatz einer Telefonanlage wird deshalb z.B. zu untersuchen sein, welche Daten dort und

wozu gespeichert werden, ob dies von der Rechtsgrundlage gedeckt ist, wer Zugriff auf diese Daten hat und wann sie gelöscht werden müssen.
Vor dem Einsatz eines Textprogramms, mit dem auch personenbezogene Daten verarbeitet werden (und seien es nur Anschriften in Briefen), sollte die Stelle sich klar werden, für welche personenbezogene Arbeiten die Textverarbeitung eingesetzt werden soll. Für **weniger kritische** Einsatzfelder (z.B. Einsatz in der allgemeinen Verwaltung zum Schriftverkehr mit Firmen im Rahmen der Beschaffung, Schriftverkehr mit Bürgern und Behörden, bei dem außer der Anschrift kaum personenbezogene und keine sensitiven Daten ausgetauscht werden) wird die Vorabkontrolle schnell erledigt sein: Rechtsgrundlage der Verarbeitung ist § 11 HDSG, es sind nur geringe Risiken anzunehmen und es werden in der Regel einfache Maßnahmen der Zutritts-, Benutzer- und Zugriffskontrolle genügen.
Kritische und sensible Einsatzfelder gebieten strengere Anforderungen - z.B. im Sozialamt für die Bearbeitung von Anträgen, den Verkehr mit dem Gesundheitsamt; in der Personalabteilung für Personallisten mit Beurteilungsnoten, für Beurteilungen und Zeugnisse; in Prüfungsämtern für Zeugnisse, Beurteilungen und Notenlisten; im Krankenhaus für das Schreiben von Arztberichten und Gutachten. Die Rechtmäßigkeit ist hier sorgfältig zu prüfen und die dem höheren Risiko entsprechenden Sicherheitsmaßnahmen (z.B. Verschlüsselungen, spezieller Zugriffsschutz, spezieller Speicherort oder Netzabsicherung) und organisatorische Vorkehrungen müssen anhand des § 10 Abs. 2 HDSG im Einzelnen festgelegt werden. Für alle Anwendungskategorien sollten Löschungsfristen festgelegt werden.
Ist zu einem späteren Zeitpunkt beabsichtigt, ein Standardverfahren über das ursprüngliche Konzept hinaus für **neue** Anwendungsfelder der Verarbeitung personenbezogener Daten zu nutzen, liegt ein Fall der **Verfahrensänderung** vor. Für diese neuen Anwendungen ist eine Vorabkontrolle durchzuführen bzw. die ursprüngliche insoweit fortzuschreiben.

Checkliste

Die Vorabkontrolle nach § 7 Abs. 6 HDSG soll sicherstellen, dass durch die beabsichtigte automatisierte Datenverarbeitung das in § 1 Abs. 1 Nr. 1 HDSG beschriebene Recht der informationellen Selbstbestimmung (das Datenschutzrecht als Persönlichkeitsrecht des Einzelnen) nicht gefährdet wird. Diese Untersuchung stellt für die beabsichtigte automatisierte Verarbeitung personenbezogener Daten den Schutzbedarf und die Risiken fest und bewertet, insbesondere unter Berücksichtigung der technischen und organisatorischen Maßnahmen, ob Gefahren für das Persönlichkeitsrecht angemessen verhindert werden. Verfährt man nach dem nachfolgenden Schema, hat das den Vorteil, dass im Hinblick auf das ausgewählte Verfahren Doppelarbeit vermieden wird, weil bereits Festlegungen abgefragt werden, die ohnehin für das nach § 6 HDSG zu erstellende Verfahrensverzeichnis erforderlich sind.
Sind verschiedene Verfahrensalternativen vorhanden, sollte die Vorabkontrolle mit der Angabe dieser Alternativen beginnen. Folgender Ablauf ist - ggf. für jede Alternative - zu durchlaufen:
(Die als Klammerzusatz angegebenen Nummern beziehen sich jeweils auf die Nummerierung im Formular "Verfahrensverzeichnis")

1. Grundangaben

- zur datenverarbeitenden Stelle (Nr. 1)
- zur Zweckbestimmung (Nr. 2.1)
- zur Rechtsgrundlage (Nr. 2.3)
- zur Art der gespeicherten Daten (Nr. 3)
- zur Schutzbedürftigkeit der Daten, insbesondere bei sensitiven Daten im Sinne von § 7 Abs. 4 HDSG oder sonst besonders schutzbedürftigen Daten
- zum Kreis der Betroffenen (Nr. 4)
- zur Übermittlung (Nr. 5 und 10)
- zu den zugriffsberechtigten Personengruppen (Nr. 6)

- zu den Fristen für die Löschung (Nr. 9)

Dabei werden die meisten Angaben für alle Alternativen gleich sein.

2. Prüfung, ob

- die Art der gespeicherten Daten (Nr. 3)
- die Übermittlungen (Nr. 5 und 10)
- die Eingrenzung der Zugriffsberechtigten (Nr. 6)
- die Löschfristen (Nr. 9)

von der angegebenen Zweckbestimmung und Rechtsgrundlage (Nr. 2) gedeckt sind, insbesondere auch unter Berücksichtigung des Grundsatzes der Datensparsamkeit nach § 10 Abs. 2 HDSG. Ist dies nicht der Fall, muss geprüft werden, ob Änderungen im Verfahren möglich sind, die zu einem positiven Ausgang der Prüfung führen. Falls dies nicht möglich ist, ist die Alternative auszuschließen.

3. Prüfung, ob die Rechte der Betroffenen nach § 8 HDSG gewahrt sind.

- Können die erforderlichen Auskünfte, Berichtigungen, Sperrungen und Löschungen durchgeführt werden?
- Ist sichergestellt, dass der Betroffene in Fällen des § 8 Abs. 2 HDSG seine Rechte ohne unvertretbaren Aufwand geltend machen kann?

Auch hier ist im Negativfall die Nachbesserungsmöglichkeit zu prüfen und wenn auch diese mit negativem Ergebnis endet, ist die Alternative auszuschließen.

4. Risikofaktoren für einen Missbrauch der Daten sind zu ermitteln. Dies sind Gefahren für

- die Vertraulichkeit
- die Integrität
- die Verfügbarkeit

der Daten. Dazu gehören z.B. die Gefahr, dass Datenträger oder "Computerlisten" während des Transports gestohlen werden, Virenbefall, Gefahr von unbefugten Zugriffen. Ggf. sind Personengruppen, die für missbräuchliche Verwendung in Frage kommen, zu benennen.

5. Beurteilung der möglichen Folgen bei missbräuchlicher Verwendung der Daten, z.B.

- Gefahren oder Nachteile für die Betroffenen
- Schadensersatzansprüche
- finanzielle Schäden
- "Vertrauensschaden"

6. Angaben zu der Technik des Verfahrens:

- Einzelplatz (Nr. 8.1)
- bei vernetzten Rechnern auch Angaben zur Netzstruktur und Datenhaltung (Nr. 8.2)
- eingesetzte Software (Nr. 8.3)
- sowie zu den technischen und organisatorischen Maßnahmen nach § 10 HDSG (Nr. 7)

7. Abgleich der Risikofaktoren unter besonderer Berücksichtigung der Schutzbedürftigkeit der personenbezogenen Daten mit den getroffenen Sicherheitsmaßnahmen und Entscheidung, ob das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist. Ist das Restrisiko zu hoch, ist zu prüfen, ob eine Nachbesserung der Technik des Verfahrens oder der technischen und organisatorischen Maßnahmen eine positive Bewertung ergibt. Ist dies nicht der Fall, ist die Alternative auszuschließen. Bei vertretbarem Restrisiko endet die Vorabkontrolle dieser Alternative mit positivem Ergebnis.

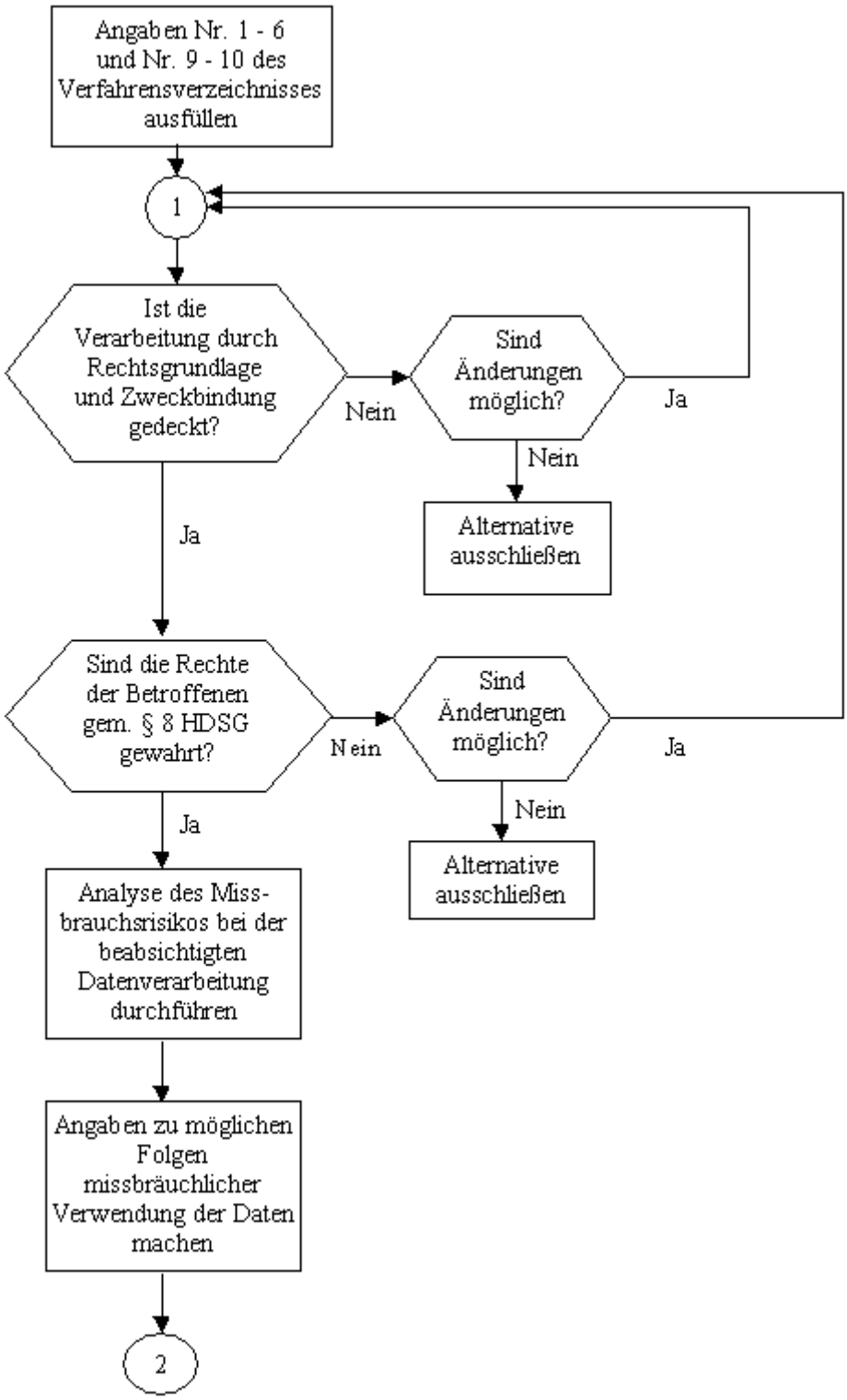
Schriftlich festzuhalten ist, welche Alternativen geprüft wurden, die Risikoabwägung und die Gründe für die Auswahl der Alternative.

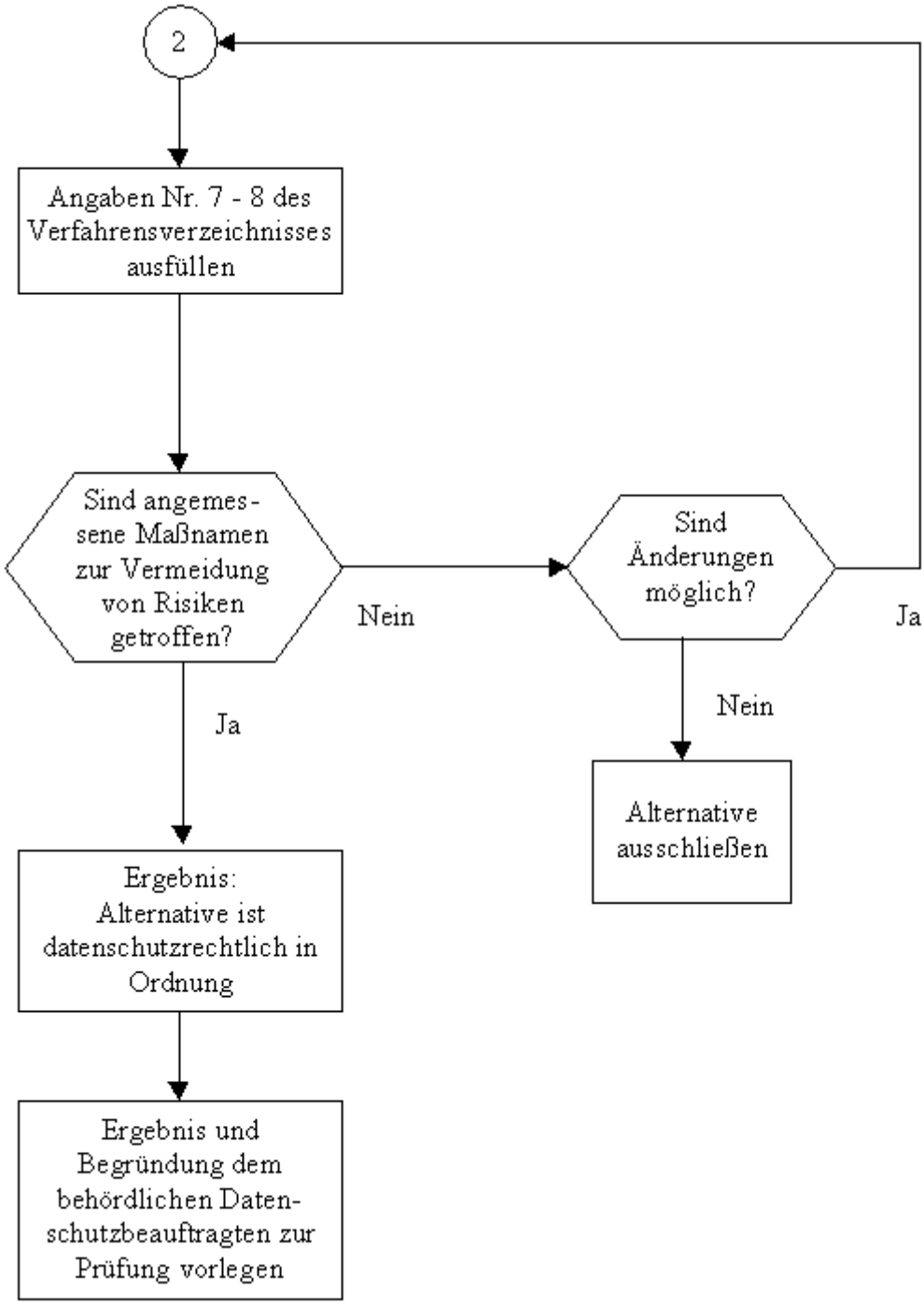
Das Ergebnis der Vorabkontrolle und die Begründung sind dem behördlichen Datenschutzbeauftragten zur Prüfung vorzulegen.

Anliegendes Ablaufschema soll die Reihenfolge der Schritte optisch veranschaulichen.

Ablauf einer Vorabkontrolle

Zunächst ist für die Prüfung der Verfahrensalternativen jeweils wie folgt zu verfahren:


Angaben Nr. 1 - 6 und Nr. 9 - 10 des Verfahrensverzeichnisses ausfüllen
1
Ist die Verarbeitung durch Rechtsgrundlage und Zweckbindung gedeckt?
Nein
Sind Änderungen möglich?
Ja
Nein
Alternative ausschließen
Ja
Sind die Rechte der Betroffenen gem. § 8 HDSG gewahrt?
Nein
Sind Änderungen möglich?
Ja
Nein
Alternative ausschließen
Ja
Analyse des Miss-brauchsrisikos bei der beabsichtigten Datenverarbeitung durchführen
Angaben zu möglichen Folgen missbräuchlicher Verwendung der Daten machen
2



Für alle Alternativen ist die Prüfung nach diesem Ablaufschema durchzuführen. Für die Auswahlentscheidung eines Verfahrens sind alle verbliebenen Alternativen datenschutzrechtlich zu bewerten.

Nach § 7 Abs. 6 HDSG ist schriftlich festzuhalten, welche Alternativen geprüft wurden, die Risikoabwägung und die Gründe für die Auswahl der Alternative.

Stand: 09.04.2008
Recherchiert und im Layout geändert am 04.11.2014;
Gefunden unter www.datenschutz.hessen.de/tf001.htm