Vorabkontrolle
... leicht gemacht

Orientierungshilfe

Der Landesbeauftragte für den Datenschutz Niedersachsen

1. Vorbemerkung

Wachsender Technikeinsatz in Wirtschaft und Verwaltung schafft neben vielen Vorteilen auch Gefahren und Risiken für die Gesellschaft und für die Rechte von Bürgerinnen und Bürgern. So kann der Ausfall von Computersystemen Leib und Leben der Betroffenen bedrohen (z.B. Ausfall von Geräten in der Flugsicherung und zur Überwachung lebenswichtiger Funktionen im Bereich der Medizin) oder die Existenz von Unternehmen gefährden (z.B. im Banken- und Versicherungsbereich). Auch kann das Recht auf informationelle Selbstbestimmung durch Verlagerung von Arbeitsabläufen auf computergestützte Systeme auf vielfältige Weise verletzt werden (z.B. ungewollte Preisgabe von personenbezogenen Daten durch fehlenden Zugriffsschutz, Einsatz von Expertensystemen in der Verwaltung zur automatisierten Sachbearbeitung ohne Beteiligung der Betroffenen).

Ziel der Vorabkontrolle ist es, die Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung zu überprüfen. Mit ihr werden die Abläufe der automatisierten Datenverarbeitung transparent gemacht, Gefahren für die Rechte der betroffenen Bürgerinnen und Bürger aufgezeigt, Risiken abgeschätzt und Sicherungskonzepte entworfen. Die Methodik ist auch allgemein geeignet, Lösungen für einen datenschutzgerechten Technikeinsatz zu finden.

Die nachstehende Orientierungshilfe will Handlungsempfehlungen für eine praxisgerechte Untersuchung der Folgen neuer Informations- und Kommunikationsanwendungen geben.

2. Gesetzliche Grundlage

Öffentliche Stellen des Bundes und der Länder sowie datenverarbeitende Stellen der Wirtschaft haben bei Einführung von automatisierten Verfahren **„Vorabkontrollen“** durchzuführen, die die spezifischen Risiken für die Rechte und Freiheiten der betroffenen Personen untersuchen. Entsprechende Rechtsvorschriften finden sich in:

- Artikel 20 der Datenschutzrichtlinie der Europäischen Union,
- § 4d Abs. 5 des Bundesdatenschutzgesetzes (BDSG) und
- § 7 Abs. 3 des Niedersächsische Datenschutzgesetzes (NDSG).

Eine Vorabkontrolle ist durchzuführen, wenn sensitive personenbezogene Daten verarbeitet werden oder die Verarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens. Automatisierte Verfahren dürfen nur eingesetzt oder wesentlich geändert werden, soweit derartige Gefahren durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können. Das Ergebnis der Vorabkontrolle und seine Begründung sind schriftlich festzuhalten.

Zuständig für die Vorabkontrolle ist der behördliche oder betriebliche Datenschutzbeauftragte. Er hat sich in Zweifelsfällen an seine Aufsichtsbehörde oder den zuständigen Landesbeauftragten für den Datenschutz zu wenden.

3. Empfehlung zu Methodik und Ablauf der Vorabkontrolle

In der ersten Analysestufe werden die geplanten neuen Technologien und die Verfahrensabläufe skizziert sowie die Anwendungsdaten beschrieben. In der zweiten Stufe werden Schwachstellen und mögliche Bedrohungen festgestellt und bewertet. Ziel dieser Untersuchungsstufe ist es, möglichst genaue Aussagen über die Gefahren und die daraus resultierenden Risiken zu gewinnen. Hieraus werden geeignete Sicherungsmaßnahmen abgeleitet.

Die Vorabkontrolle sollte wie folgt gegliedert werden:

1. **Systembeschreibung,**
2. **Rechtsgrundlage der Datenverarbeitung,**
3. **Gefahrenanalyse,**
4. **Risikoanalyse,**
5. **Datensicherungskonzept,**
6. **Beherrschung der Gefahren.**

3.1 Systembeschreibung

Für die Darstellung von IST-Zustand und von Planung kann auf die bewährten Verfahren der Systemanalyse zurückgegriffen werden.

3.2 Rechtsgrundlage der Datenverarbeitung

Datenverarbeitende Stellen sollten vor der Entscheidung zur automationsunterstützten Verarbeitung personenbezogener Daten prüfen, nach welcher gesetzlichen Regelung die Verarbeitung zulässig ist, und den Zweck die Datenverarbeitung konkret festlegen. Die Zulässigkeitsprüfung muss hinsichtlich jeder Verarbeitungsphase erfolgen (Erhebung, Speicherung, Übermittlung, automatisierter Abruf, sonstige Nutzung). Diese Prüfung ist selbstverständlich schon bei herkömmlicher Verarbeitung notwendig, sie sollte jedoch vor dem Einsatz neuer Technologien erneut vorgenommen werden. Als Rechtsgrundlage kommen - soweit die Datenverarbeitung nicht auf Grund wirksamer Einwilligung der Betroffenen erfolgt – das Bundesdatenschutzgesetz, Länderdatenschutzgesetze oder bereichsspezifische Gesetze in Frage (z.B. Meldegesetz, Personalausweis- und Passgesetz, Ausländergesetz, Gefahrenabwehrgesetz, Verfassungsschutzgesetz, Schulgesetz, Hochschulgesetz, Statistikgesetze, Baugesetzbuch, Sozialgesetzbuch, Straßenverkehrsgesetz). Personenbezogene Daten dürfen nur im erforderlichen Umfang verarbeitet werden. Die Rechte der Betroffenen (Auskunft, Berichtigung, Löschung usw.) müssen gewahrt bleiben.

3.3 Gefahrenanalyse

In der Gefahrenanalyse werden die bedrohten Objekte gegliedert nach Objektgruppen (z.B. Infrastruktur, Hardware, Software, Anwendungsdaten, Personen) erfasst und die Auswirkungen beschrieben. Dabei sollte der Detaillierungsgrad der Schutzbedürftigkeit des Verfahrens angepasst werden. Auch Zusammenfassungen der Anwendungsbereiche zu Gruppen gleicher Struktur bzw. gleichen Schutzbedarfs sind denkbar, um größere Transparenz zu erzielen und den Analyseaufwand zu reduzieren. In der Gefahrenanalyse ist von den Grundbedrohungen **„Verlust von Vertraulichkeit, Integrität und Verfügbarkeit“** auszugehen.

Für eine detaillierte Bewertung der Gefahren bieten sich zwei alternative Verfahren an, die Einordnung nach quantitativen oder nach qualitativen Wertmaßstäben. Beim **quantitativen** Verfahren werden alle schadensverursachenden Ereignisse auf einer numerischen Skala zusammengestellt, bewertet und summiert. Als Skala kann auch der Schadenswert genommen werden. Vorteil des quantitativen Verfahrens ist, dass seine Ergebnisse sehr detailliert sind und ein hohes Maß an Objektivität ermöglichen. Vergleiche mit alternativen Lösungen können so leicht durchgeführt werden. Nachteilig ist, dass sich manche Risiken nur sehr schwer numerisch bewerten lassen (z.B. der Ansehensverlust). Dadurch wird die Aussagegenauigkeit relativiert. Außerdem ist dieses Verfahren im Allgemeinen sehr arbeitsintensiv. Beim **qualitativen** Verfahren werden die möglichen Gefahren verbal beschrieben und nach einem vereinbarten Wertmaßstab klassifiziert (z.B. Gefährdung ist „niedrig“, „mittel“ oder „hoch“). Für eine möglichst vollständige Erfassung aller Gefahren bieten sich Checklisten an. Vorteil

des qualitativen Verfahrens ist, dass eine verbale Darstellung genügt und dabei eine lesbare, verständliche Auflistung aller Gefahren entsteht. Nachteilig ist die Unschärfe der Bewertung, die zudem subjektiv geprägt sein kann.

3.4 Risikoanalyse

Das Risiko wird bestimmt durch die **Wahrscheinlichkeit eines Schadenseintritts** und durch das **Ausmaß des Schadens.** Die Wahrscheinlichkeit für den Eintritt eines Schadens ergibt sich wiederum aus:

- dem **Missbrauchsinteresse** (Interesse Unbefugter, Daten zu missbrauchen: löschen, manipulieren, unbefugt nutzen).
  Ein hohes Missbrauchsinteresse liegt z.B. vor, wenn durch den Missbrauch von Daten persönliche Bereicherungen möglich erscheinen, Maßnahmen gegenüber Straftätern verhindert, Konkurrenten massiv benachteiligt und Entscheidungsträger erheblich beeinträchtigt werden können (Erpressung, Rache).
- dem **Aufwand**, der notwendig ist, um einen Schaden herbeizuführen,
- dem **Risiko**, bei einem Missbrauch entdeckt zu werden, und
- der **Verarbeitungshäufigkeit** (Häufigkeit der Vorgänge, bei denen ein Missbrauch oder eine sonstige Beeinträchtigung möglich ist).

Das **Ausmaß des Schadens** aus datenschutzrechtlicher Sicht ergibt sich aus der Beeinträchtigung der Betroffenen. Zur Einschätzung möglicher Risiken kann das LfD-Schutzstufenkonzept benutzt werden. Daneben sind der Verwendungszusammenhang der Datenverarbeitung, die Vielfalt der verfolgten Zwecke und die Komplexität des verwendeten Systems (z.B. behördeninterne Vernetzung, behördenübergreifende Vernetzung, landesweite Vernetzung, Einsatz multifunktionaler Chipkarten) bei der Risikoabschätzung zu berücksichtigen.

Risikobereiche

Generell sind die technischen und organisatorischen Maßnahmen zu treffen, die in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Missbrauch gewährleisten. Es hat sich bewährt, für alle eingesetzten Systeme einen einheitlichen Grundschutz festzulegen (vgl. 3.5). Auf diese Weise wird ein weitgehend einheitlicher Sicherungsstandard erreicht, der eine flexible Verarbeitung von personenbezogenen Daten ermöglicht und bei Verfahrensänderungen grundsätzlich erneute umfangreiche Sicherheitsbetrachtungen überflüssig macht. Wenn auf diese Weise keine wirkungsvolle Absicherung aller Gefährdungen möglich ist, sind Zusatzmaßnahmen zu treffen. Die erforderlichen Zusatzmaßnahmen sind an den folgenden Risikobereichen zu orientieren:

Geringes und mittleres Risiko

Geringer bzw. mittlerer Schutzbedarf besteht bei Daten der Schutzstufen A bis C sowie bei Daten der Schutzstufe D mit geringer Verarbeitungshäufigkeit und geringem Missbrauchsinteresse. Für diesen Risikobereich reichen Grundschutzmaßnahmen aus. Grundschutzmaßnahmen sind im Allgemeinen angemessen, solange der finanzielle und personelle Aufwand hierfür einen geringen Bruchteil des Gesamtaufwandes für das Verfahren ausmacht.

Hohes Risiko

Hoher Schutzbedarf besteht bei Daten der Schutzstufe D und hoher Verarbeitungshäufigkeit oder hohem Missbrauchsinteresse. Hierfür sind über den Grundschutz hinaus Zusatzmaßnahmen zur Datensicherung zu treffen. Dies kann im Einzelfall bedeuten, dass der finanzielle und personelle Aufwand

für Schutzmaßnahmen in der gleichen Größenordnung wie der gesamte sonstige Aufwand für das Verfahren liegt. Technische Maßnahmen sind gegenüber organisatorischen Maßnahmen vorzuziehen.

Sehr hohes Risiko

Sehr hoher Schutzbedarf besteht bei Daten der Schutzstufe D mit hohem Mißbrauchsinteresse und hoher Verarbeitungshäufigkeit sowie generell bei Daten der Schutzstufe E. Die Aufwendungen für erforderliche Zusatzmaßnahmen können im Einzelfall den sonstigen Aufwand für das Verfahren übersteigen. Technische Maßnahmen sind organisatorischen Maßnahmen vorzuziehen.

3.5 Datensicherungskonzept

Aus der Gefahren- und Risikoanalyse ist ein Sicherheitskonzept zu entwickeln. Die zu treffenden technischen und organisatorischen Maßnahmen sind zu beschreiben und zu bewerten. Für den Grundschutzbereich bieten die IT-Grundschutzkataloge[2] empfehlenswerte Maßnahmen an. Die Kataloge werden stets aktualisiert, sodass die Empfehlungen dem Stand der Technik entsprechen. Es berücksichtigt Bereiche wie Organisation, Personal, Infrastruktur und geht konkret auf die EDV-Technik ein, z.B. Personal Computer, Unix-Systeme oder TK-Anlagen.

Man kann davon ausgehen, dass ca. 80 % der IuK-Anwendungen durch den Einsatz von Standard-Sicherungsmaßnahmen ausreichend geschützt werden können. Aus den IT-Grundschutzkatalogen lassen sich die der eigenen Risikolage entsprechenden Sicherheitsmaßnahmen auswählen, ohne ein individuelles Sicherheitskonzept aufstellen zu müssen. Für die verbleibenden 20 % der IuK-Anwendungen mit höherem Schutzbedarf oder beim erstmaligen Einsatz neuer Technologien ist dagegen ein individuelles Sicherheitskonzept aufzustellen.

4. Dokumentation

Die Untersuchungsergebnisse sind zu dokumentieren. Die Dokumentation muss für die Entscheider verständlich formuliert werden. Die Ergebnisse sollten bekanntgemacht werden, um das Gebot hinreichender Transparenz zu erfüllen. Sie sollten zumindest anderen Verwaltungen zugänglich sein, damit Stellen, die ähnliche Projekte planen, sich frühzeitig über mögliche Gefahren und Risiken sowie die gewählten Sicherungskonzepte informieren können und mehrfacher Untersuchungsaufwand für vergleichbare Projekte vermieden wird.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzkataloge