

Hinweise zur Vorabkontrolle nach dem Berliner Datenschutzgesetz (BlnDSG)

Das am 30.7.2001 novellierte Berliner Datenschutzgesetz sieht vor, dass im öffentlichen Bereich Berlins vor Einführung einer automatisierten Verarbeitung mit besonders sensiblen personenbezogenen Daten eine Vorabkontrolle durchgeführt wird. Folgende Hinweise und Empfehlungen sollen den behördlichen Datenschutzbeauftragten bei der Durchführung der Vorabkontrolle als Hilfestellung dienen.

Wann ist eine Vorabkontrolle durchzuführen?

Nach § 5 Abs.3 Satz 2 BlnDSG gehört die Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung zum Sicherheitskonzept, wenn die zu verarbeitenden Daten einem Berufs- oder besonderem Amtsgeheimnis unterliegen oder zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden. In § 19 a Abs.1 Satz 3 Nr. 1 BlnDSG wird verfügt, dass bei besonders sensiblen Verarbeitungen eine Vorabkontrolle vom behördlichen Datenschutzbeauftragten durchzuführen ist.

Daraus ergibt sich die Notwendigkeit einer Vorabkontrolle, wenn

- ein Berufs- oder besonderes Amtsgeheimnis zu beachten ist (z.B. Arztgeheimnis, Sozialgeheimnis, Steuergeheimnis, Statistikgeheimnis, Personalaktengeheimnis, Geheimhaltungsvorschriften von Sicherheitsbehörden u.ä.);
- die Daten im Rahmen der Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden;
- die Verarbeitung besondere Kategorien personenbezogener Daten nach § 6 a BlnDSG betrifft (rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben)
- der behDSB zu dem Ergebnis kommt, dass die Verarbeitung der Daten mit besonderen Risiken für Rechte und Freiheiten von Betroffenen verbunden ist, obwohl die ers-

ten drei Gründe nicht vorliegen, z. B. wenn Daten verarbeitet werden, die dazu bestimmt sind, die Persönlichkeit der betroffenen Personen zu bewerten (z.B. Leistungs- oder Verhaltensdaten).

Wer führt die Vorabkontrolle durch ?

Die Durchführung der Vorabkontrolle obliegt nach § 19 a Abs. 1 Satz 3 Nr. 1 BInDSG dem behördlichen Datenschutzbeauftragten (behDSB).

Dies ändert nichts an der Verantwortlichkeit der datenverarbeitenden Stelle und deren Verpflichtung, die Rechtmäßigkeit der beabsichtigten Verarbeitungen insbesondere im Hinblick auf besondere Risiken der Betroffenenrechte zu prüfen und die Risiken durch angemessene Schutzmaßnahmen einzudämmen.

Wegen der Weisungsfreiheit des behDSB und der gesetzlichen Aufgabenzuweisung obliegt es ihm auch, in Zweifelsfällen zu entscheiden, ob eine Vorabkontrolle (von ihm) durchgeführt wird oder nicht. Grundlage und Voraussetzung dieser Entscheidung sind die Informationen aus der rechtzeitigen Unterrichtung über Vorhaben der automatisierten Datenverarbeitung nach § 19 a Abs. 3 Satz 3 BInDSG.

Handelt es sich bei den automatisierten Verarbeitungen um verwaltungsübergreifende Anwendungen, ist der BInBDI in jedem Fall bei der Vorabkontrolle zu beteiligen (§ 24 Abs.1 Satz 3 BInDSG).

Welche Unterlagen werden für die Vorabkontrolle benötigt?

Die Unterrichtung des behDSB nach § 19 a Abs. 3 Satz 3 BInDSG über Vorhaben der automatisierten Datenverarbeitung durch den Verfahrensverantwortlichen erfolgt idealer Weise mit folgenden Unterlagen:

- Verfahrensbeschreibung/ Sollkonzept/Pflichtenheft
- Entwurf der Dateibeschreibung nach § 19 Abs.2 BInDSG
- Risikoanalyse,

- Sicherheitskonzept mit Beschreibung der durchzuführenden technisch-organisatorischen Maßnahmen, dazu auch Sicherheitskonzepte übergeordneter Sicherheitsdomänen (etwa: Behördliches Sicherheitskonzept).
- Zeitpläne zur Einführung der Verarbeitung und der Umsetzung des Sicherheitskonzeptes
- Unterlagen über die Software und Hardware, die für die Beurteilung des Verfahrens relevant sind.

Was sind die Fragestellungen der Vorabkontrolle?

In der Vorabkontrolle ist zu prüfen, ob

- die vorgesehene Datenverarbeitung rechtlich zulässig ist, ob sie also durch eine Erlaubnisnorm aus § 6 BlnDSG gedeckt ist; besonders zu beachten sind dabei die Zulässigkeit und Umstände der Datenerhebung, Übermittlungen, vor allem in das Ausland;
- bei der Verarbeitung besonderer Kategorien personenbezogener Daten die Voraussetzungen nach § 6 a BlnDSG gegeben sind;
- die organisatorischen und technischen Voraussetzungen für die Gewährung der in § 7 BlnDSG zusammengefassten unabdingbaren Rechte der Betroffenen gegeben sind (vor allem: Auskunft, Benachrichtigung, Einsichtnahme, Berichtigung, Sperrung und Löschung);
- die Risikoanalyse nach § 5 Abs. 3 Satz 1 BlnDSG vollständig und gewissenhaft durchgeführt wurde;
- das Sicherheitskonzept alle in der Risikoanalyse erkannten Risiken vollständig so weit reduziert, dass die Restrisiken ausdrücklich als tragbar hingenommen werden können.

Checkliste zur Durchführung der Vorabkontrolle

Die folgende Checkliste führt beispielhaft auf, worauf aus der Sicht des Datenschutzes zu achten ist:

1. Prüfung der Vollständigkeit der zur Verfügung gestellten Unterlagen nach folgenden Kriterien:

- a) Grundangaben anhand der Dateibeschreibung nach § 19 Abs. 2 BlnDSG
- b) Dokumentation von Verfahren und Programmen soweit vorhanden
- c) Bei Auftragsdatenverarbeitung: Schriftliche Weisungen; Unterwerfungsklausel
- d) Technische Angaben:
 - da) Eingesetzte Hardware:
 - Einzelplatz-Anwendung
 - Mehrplatz-Anwendung: Netzstruktur und Datenhaltung
 - Schnittstellen
 - db) Eingesetzte Software
 - Standardprogramme
 - Anwendungsprogramme
 - Protokollierungen

2. Rechtliche Prüfung

- a) Prüfung, ob folgende Angaben von der angegebenen Zweckbestimmung und der Rechtsgrundlage gedeckt sind; insbesondere auch unter Berücksichtigung des Grundsatzes der Datenvermeidung nach § 5a BlnDSG:
 - Verfahren der Datenerhebung
 - Art der gespeicherten Daten (Beschreibung des Datensatzes)
 - Kreis der Betroffenen
 - Auswertungsmöglichkeiten für die Daten
 - Zugriffsberechtigungen auf die Daten
 - Übermittlungen (Umfang, Häufigkeit, Empfänger)
 - Lösungsfristen

b) Prüfung, ob die Rechte der Betroffenen nach § 7 BlnDSG gewahrt sind:

- Möglichkeit der Durchführung der erforderlichen Auskünfte, Berichtigungen, Einsichtnahmen,
- Sperrungen, Löschungen und Widerspruch;
- Sicherstellung, dass der Betroffene in Fällen des § 7 BlnDSG seine Rechte ohne unverhältnismäßigen Aufwand geltend machen kann.

3. Beurteilung der Sicherheitsmaßnahmen; Risikoabwägung

a) Ermittlung der Risikofaktoren für einen Missbrauch der Daten; insbesondere Analyse der Gefahren für die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz der Daten (z.B. Gefahr von unbefugten Zugriffen, Diebstahl von Datenträgern während des Transports, Virenbefall).

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

- Gefahren oder Nachteile für die Betroffenen
- Schadensersatzansprüche
- Finanzielle Schäden
- Vertrauensschäden

c) Abgleich der Risikofaktoren mit den getroffenen Sicherheitsmaßnahmen unter Berücksichtigung der IT-Sicherheitsstandards (gemäß IT-Sicherheitsrichtlinie) und Entscheidung, ob das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist. Ist das Restrisiko zu hoch, ist zu prüfen, ob eine technisch-organisatorische Nachbesserung eine positive Bewertung ergibt. Ist dies nicht der Fall, ist die Alternative auszuschließen.

Was ist in Zweifelsfällen zu tun?

Ergeben sich bei der Vorabkontrolle Zweifelsfälle, sollte zuerst versucht werden, diese zusammen mit den Verfahrensverantwortlichen auszuräumen. Gibt es weiterhin strittige Punkte, kann der BlnBDI konsultiert werden (§ 19a Abs.4 BlnDSG).

Der behDSB muss sich allerdings nicht an die Aufsichtsbehörde wenden, wenn er nach pflichtgemäßem Ermessen zu dem Schluss kommt, dass die beabsichtigte Datenverarbeitung unzweifelhaft rechtmäßig ist.

Wie ist die Vorabkontrolle zu dokumentieren?

Das Ergebnis der Vorabkontrolle ist aufzuzeichnen. Dabei ist schriftlich festzuhalten:

- Die Gegenstände der Prüfung,
- die Risikoabwägung,
- die Zweifelsfälle und deren Lösungsvorschläge,
- die Gründe für die Auswahl eventueller Alternativen und
- schließlich das Schlussergebnis der Vorabkontrolle.

Die schriftlichen Aufzeichnungen sind der Behördenleitung bzw. dem Verfahrensverantwortlichen zuzuleiten.

Das Ergebnis der Vorabkontrolle ist in die Dateibeschriftung nach § 19 Abs.2 Nr.11 BlnDSG aufzunehmen; es wird gleichermaßen Bestandteil des Sicherheitskonzepts.