Orientierungshilfe
„Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“

Herausgegeben vom
Arbeitskreis „Technische und organisatorische Datenschutzfragen“
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand 2. November 2009

Inhalt

1 Vorbemerkung

Personenbezogene Daten sind vor der Freigabe eines Systems nicht weniger schutzbedürftig als nach dessen Freigabe. Die Regelungen der Landesdatenschutzgesetze und des Bundesdatenschutzgesetzes gelten für die Verarbeitung personenbezogener Daten ungeachtet der Frage, ob die Datenverarbeitung bereits im Produktivbetrieb oder noch in einer Projektphase erfolgt.

Unabhängig von der jeweiligen Phase, in der sich ein Projekt befindet, ist eine *Dokumentation* erforderlich, der

- die definierten Ziele,
- die technischen Mittel und Instrumente,
- die Festlegung der einzelnen Projektphasen mit Beginn und Ende,
- die Benennung der verantwortlichen Personen und
- die Entscheidung der verantwortlichen Person über den Beginn einer Projektphase, die Dokumentation des Projektverlaufes sowie die Ergebnisse und Schlussfolgerungen

zu entnehmen sind.

Der Detaillierungsgrad dieser Dokumentation kann sich nach der Entwicklungsphase richten, in der sich ein Verfahren zur Verarbeitung personenbezogener Daten befindet.

Zu unterscheiden ist der *Projektbetrieb* von dem *Produktivbetrieb*.

2 Projektbetrieb

2.1 Funktionstest

Der Zweck des Funktionstests ist es, die grundsätzliche Verwendbarkeit von Programmen und Geräten für die nachfolgenden Projektphasen sicherzustellen.

Ein Test zeichnet sich durch die folgenden Merkmale aus:

- *Keine Anwender – nur Tester:* Es gibt außer einer sehr kleinen Gruppe von Testern keine regulären Anwender des Verfahrens.
- Keine Verbindungen zu anderen und keinen Datenaustausch mit anderen Verfahren im Produktivbetrieb: Ein Test findet in einer isolierten Testumgebung statt.

- *Keine personenbezogenen Daten:* In einem Test dürfen keine personenbezogenen Daten verarbeitet und auch nicht aus anderen Produktivsystemen übernommen werden. Echtdaten sind vor ihrer Übernahme in das Testverfahren zu anonymisieren.

In Funktionstests werden definitionsgemäß keine personenbezogenen Daten verarbeitet. Deshalb sind im Testbetrieb auch keine datenschutzrechtlichen Anforderungen zu erfüllen. Durch den Ausschluss von Verbindungen mit anderen Produktivsystemen der automatisierten Verarbeitung personenbezogener Daten, sind durch die Funktionstests auch bei *anderen* Verfahren keine gravierenden Auswirkungen auf deren Datenschutz- und Datensicherheitsniveau zu erwarten.

2.2 Integrations- und Abnahmetest

Der Zweck der Integrations- und Abnahmetests besteht darin, das Konzept und die Implementierung vor dem Auftreten von (z. B. im Funktionstest nicht erkannten) Designschwächen oder Implementierungsfehlern in einer quasi-produktiven Umgebung mit realistischen Lastszenarien abzusichern. Mit Hilfe von Integrations- und Abnahmetests sollen vor einem Pilotbetrieb (siehe Abschnitt 3.1) oder einer Freigabe des Regelbetriebs eventuell vorhandene oder vermutete Risiken ausgeschlossen werden, die unter den Bedingungen des Funktionstests nicht abgeschätzt werden konnten. Derartige Tests sind zeitlich streng limitiert auf detailliert beschriebene Szenarien zu beschränken.

Die Integrations- und Abnahmetests sollten nach Möglichkeit nicht mit personenbezogenen Daten durchgeführt werden.

Personenbezogene Daten dürfen nur im Rahmen zusätzlicher, minimierter Tests verwendet werden. Grundlegende Funktionen müssen bereits im Funktionstest mit ausreichend anonymisierten Daten überprüft werden. Auf derartige erste Funktionstests darf nicht wegen der ohnehin geplanten Integrations- und Abnahmetests verzichtet werden.

Zu Testzwecken darf eine Kopie der erforderlichen Originaldatensätze verwendet werden, wenn eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder falls sich im Ausnahmefall trotz Nachbildung im Funktionstest ein Fehler aus dem Produktionsbetrieb nicht ermitteln, sondern nur mit Originaldaten aufklären lässt. Unter diesen Voraussetzungen können personenbezogene Daten zu Testzwecken verwendet werden wenn,

- eine bereichsspezifische Rechtsvorschrift dies nicht ausdrücklich untersagt,
- eine Anonymisierung der Originaldaten für die vorgesehene Test-Konstellation mit einem unvertretbar hohen Aufwand verbunden wäre,
- die verantwortliche Stelle dem Vorgehen schriftlich zugestimmt hat,
- bei der Durchführung oder Auswertung des Tests die schutzwürdigen Belange der Betroffenen und die Datensicherheit angemessen berücksichtigt werden,
- sichergestellt ist, dass nur die für die Fehlerbehebung und Durchführung des Tests erforderlichen Personen die Daten nutzen können und
- Zugang zu diesen Daten nur Personen erhalten, die den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften unterliegen.

Der Kopierzugriff auf die Originaldaten ist zu protokollieren. Nach Beendigung des Tests ist die benutzte Kopie der Originaldaten unverzüglich aus dem Testbereich zu löschen bzw. im Testbereich zu anonymisieren. Die Verwendung von Originaldatenkopien mit Anlass,

Begründung, Umfang und Dauer, die getroffenen Sicherheitsmaßnahmen sowie die vorangehenden Tests mit Testdaten sind revisionssicher zu dokumentieren.

Der/die behördliche Datenschutzbeauftragte bzw. – soweit ein solcher nicht bestellt wurde – der/die Landesdatenschutzbeauftragte sowie die betroffenen Daten verarbeitenden Stellen – soweit nicht mit der Fachlichen Leitstelle identisch – sind vorab zu informieren.

Die Integrations- und Abnahmetests müssen in einer definierten und kontrollierten Umgebung stattfinden.

Gegenstand der Integrations- und Abnahmetests ist insbesondere auch der Test und die eventuell notwendige Korrektur der erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen. Sie dienen als Grundlage für die Erstellung des Sicherheitskonzepts und der Risikoanalyse für den späteren Regelbetrieb. Die Durchführung von Integrations- und Abnahmetests ist Voraussetzung, um das System unter Sicherheitsgesichtspunkten für den Regelbetrieb freigeben zu können.

Werden personenbezogene Daten im Integrations- und Abnahmetest verwendet, dann bedarf es hierzu zumindest einer Kurzfassung eines IT-Konzeptes sowie eines auf die Testbedingungen angepassten Sicherheitskonzeptes.

3 Produktivbetrieb

3.1 Pilotbetrieb

Der Zweck des Pilotbetriebs besteht darin, einen Echtbetrieb in einem nach zeitlich und sachlich begrenzten Bereich durchzuführen, um die definierten Anforderungen technischer und organisatorischer Art erfahrungsgestützt auf ihre Praxistauglichkeit prüfen und gegebenenfalls verändern zu können.

Innerhalb des Pilotbetriebs wird in der Regel der führende Datenbestand bearbeitet. Ist beispielsweise eine stichtagsbezogene Umstellung von Alt- auf Neuverfahren erforderlich, kann ein Parallelbetrieb zwischen Alt- und Neuverfahren vorübergehend erforderlich sein. Es sollte aber kein Parallelbetrieb stattfinden, bei dem ein eventuell noch vorhandenes Alt-Verfahren das führende System bleibt. In einem Piloten dürfen in einem zeitlich definierten Rahmen personenbezogene Daten verarbeitet werden.

Voraussetzung für einen Pilotbetrieb ist ein IT-Konzept, aus dem sich der Zweck des Verfahrens sowie das Ziel des Pilotbetriebes ergeben.

Soweit im Piloten personenbezogene Daten verarbeitet werden, bedarf es eines vollständigen Sicherheitskonzepts und einer auf dem Sicherheitskonzept aufbauenden Risikoanalyse. Wird der Pilotbetrieb nur in einem einschränkten Umfang aufgenommen, kann sich auch das Sicherheitskonzept auf diesen begrenzten Funktionsumfang beschränken. Entspricht der Pilot bereits dem Regelbetrieb der Verarbeitung personenbezogener Daten, so hat sich das Sicherheitskonzept vollständig an diesen Anforderungen zu orientieren.

Sollen im Piloten die Wirksamkeit der in dem Sicherheitskonzept beschriebenen technischen und organisatorischen Maßnahmen unter Realbedingungen überprüft werden, so muss das Sicherheitskonzept Aussagen über die Minimierung der gegebenenfalls für personenbezogene Daten auftretenden Risiken treffen.

Ein Pilotbetrieb bedarf grundsätzlich der Freigabe durch die Leitung, wenn personenbezogene Daten verarbeitet werden. Für den Pilotbetrieb kann die Freigabe auch an eine „befugte Person“ delegiert werden.

3.2 Regelbetrieb

Der Zweck des Regelbetriebes besteht darin, ein automatisiertes Verfahren gemäß den definierten Anforderungen und vereinbarten Zielen zu betreiben. Die geltenden Regeln zur ordnungsgemäßen Verarbeitung personenbezogener Daten sind zu beachten.

Der Regelbetrieb erfolgt mit der Freigabe durch die Leitung. Die Freigabe hat schriftlich zu erfolgen.

Vor dem Beginn des Regelbetriebs sind die eingesetzten Programme und Sicherheitsmaßnahmen zu testen. Solche Tests dürfen beispielsweise mit personenbezogenen Daten von Personen durchgeführt werden, die für das Verfahren verantwortlich oder Mitarbeiter des Projekts sind und diesen Tests zugestimmt haben. Gut dokumentierte Funktionstests, Integrations- und Abnahmetests aus den vorherigen Projektphasen können den Aufwand für die notwendigen Tests vor der Freigabe des Verfahrens erheblich reduzieren.