

Privacy Impact Assessment (PIA)

Jana Ehlers und Matthias Hauß

Was ist ein Privacy Impact Assessment?

Ein Privacy Impact Assessment (PIA) ist eine systematische Analyse der Auswirkungen einer Anwendung auf Privatsphäre und Datenschutz. Ziel ist die Sicherstellung der Konformität zu entsprechenden gesetzlichen und regulatorischen Vorgaben und das Identifizieren von Schutzmaßnahmen und alternativen Prozessen, um das Konformitätsniveau zu erhöhen und eventuelle Risiken zu minimieren. Eine PIA stellt somit eine Datenschutzfolge- und Risiko-Abschätzung dar.

PIAs sind seit einigen Jahren im englischsprachigen Raum gebräuchlich, in Deutschland jedoch noch nicht weit verbreitet. Im April 2011 wurde auf EU-Ebene ein Framework für die Durchführung von PIAs bei RFID-Anwendungen veröffentlicht. Dieses PIA-Framework wurde von der RFID-Wirtschaft als Reaktion auf eine Richtlinie der EU zur Datenschutzwahrung in RFID-gestützten Anwendungen erstellt und 2011 sowohl von der Europäischen Kommission als auch von der Artikel-29-Gruppe (dem unabhängigen Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) gebilligt.

Was kann ein PIA leisten?

PIAs helfen intern bei dem datenschutzgerechten Umgang mit personenbezogenen Daten und damit bei der Erhöhung der Compliance.

Zusätzlich können sie auch zur Außenwirkung beitragen. PIAs können dabei helfen, Datenschutz- und Privatsphäre-Bedenken in der Öffentlichkeit, bei Interessensvertretern und bei Behörden zu zerstreuen und das Vertrauen in die untersuchten Verfahren und Systeme zu erhöhen. So werden PIAs in den Ländern, in denen sie verbreitet sind, auch zunehmend von Datenschutzbeauftragten, Behörden und Unternehmen als Nachweis eines angemessenen Umgangs mit dem Datenschutz anerkannt.

Um diese Wirkungen zu erzielen, sind folgende Aspekte bei der Durchführung eines PIAs zu beachten:

- Ein PIA sollte vor der konkreten Implementierung technischer Systeme durchgeführt werden, um noch die Möglichkeit zu einer Änderung zu haben, sollten Risiken identifiziert werden, die eine Anpassung erforderlich machen. Insofern ist ein PIA nicht immer eine finale Datenschutz-Betrachtung, sondern schafft eventuell weiteren Handlungsbedarf.
- Ein PIA muss mit ausreichender Gründlichkeit durchgeführt werden und nicht nur relevante Gesetze, sondern auch gesellschaftliche Werte und allgemeine Erwartungen an Datenschutz und Privatsphäre berücksichtigen.

- Ein PIA sollte transparent durchgeführt werden, damit die Ergebnisse auch anerkannt werden. Die Vorgehensweise und der Bericht sollten nachvollziehbar sein und offengelegt werden.

Was ist bei Durchführung eines PIA zu tun?

Es gibt gegenwärtig keine generell verbindliche Vorgehensweise für die Durchführung von PIAs.

In Deutschland existieren derzeit zwei Rahmenwerke, die ein Vorgehen bei PIAs für RFID-Anwendungen beschreiben.

Das Framework der RFID-Industrie, „Rahmen für die Folgenabschätzung in Bezug auf den Datenschutz und die Wahrung der Privatsphäre bei RFID-Anwendungen“, eignet sich dank seines hohen Abstraktionsniveaus als Grundlage für die Ausarbeitung einer Vorgehensweise bei PIAs verschiedenster RFID-Anwendungen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erläutert in seinen "Technical Guidelines RFID as Templates for the PIA Framework", wie man die BSI-eigenen „Technischen Richtlinien für den sicheren RFID-Einsatz“ nutzen kann, um der Verpflichtung zur Erstellung eines PIAs auf Basis des EU-Frameworks effizient nachzukommen.

Für Anwendungen außerhalb der RFID-Technologie existieren zurzeit keine deutschen PIA-Richtlinien-Werke. Eine Ableitung eines geeigneten Prozesses aus den RFID-spezifischen Rahmen für PIA-Vorgehensweisen ist aber möglich.

Ein PIA-Prozess, wie er in den Rahmenwerken beschrieben wird, besteht aus einer Anfangsanalyse und einer Risikoabschätzung.

In der Anfangsanalyse wird ermittelt, ob und wie personenbezogene Daten durch die zu untersuchende Anwendung verarbeitet werden und ob und in welchem Umfang somit ein PIA für notwendig gehalten wird.

An die Anfangsanalyse schließt dann die eigentliche Risikoabschätzung an. Hier werden nach einer umfassenden Beschreibung der Anwendung mögliche Risiken für zu erreichende Datenschutzziele ermittelt und abgeschätzt. Darauf aufbauend werden mögliche Maßnahmen zur Reduktion der festgestellten Risiken abgeleitet und analysiert.

Zum Abschluss werden die Schlussfolgerungen aus der Risikoabschätzung dokumentiert.

Ein Privacy Impact Assessment endet entweder mit einer Freigabe der Anwendung für den Betrieb, wenn keine erheblichen Risiken verbleiben und somit den einschlägigen Vorschriften entsprochen wird, oder mit der Empfehlung von Folgenminderungsmaßnahmen, nach deren Abschluss eine erneute Datenschutzfolgeabschätzung stattfinden sollte. Es stellt damit ein wirksames Mittel zur Erhöhung der Compliance bezüglich des Datenschutzes dar.