Informatik Spektrum
https://doi.org/10.1007/s00287-020-01262-7

FORUM

Warum der Datenschutz essenziell für die Projektplanung ist – Weshalb ein Privacy Impact Assessment nötig ist

Ursula Sury[1]

Situation

Ein Unternehmen hat sich im vergangenen Jahr ausführlich mit der Einführung neuer Dienstleistungen auseinandergesetzt. Dabei sollen besonders schützenswerte Personendaten (Gesundheitsdaten) von den eigenen Kunden analysiert werden und die Ergebnisse Dritten dabei helfen, die Kunden besser zu verstehen und auf sie zugeschnittene medizinische Lösungen herzustellen.

Unzählige Arbeitsstunden und eine Machbarkeitsstudie haben schon einen großen Teil des beachtlichen Budgets für dieses Projekt aufgebraucht. Der Projektleiter möchte nun noch rechtliche Abklärungen treffen, bevor das Projekt auf den Markt geht.

Die Ernüchterung der Projektbeteiligten ist groß, als das juristische Gutachten darauf hinweist, dass eine solche Dienstleistung gegen den Datenschutz verstößt. Viel Geld und Zeit wurden mit dem Projekt in den Sand gesetzt.

Hätte man dieses Szenario verhindern können?

Die EU-DSGVO sowie der Entwurf des neuen Datenschutzgesetzes der Schweiz (Art. 16 E-DSG) sehen vor, dass in bestimmten Situationen eine Datenschutzfolgeabschätzung erstellt werden soll. Der Datenschutz fließt damit bereits in der Planung eines Projekts ein. Hätte man die rechtlichen Abklärungen früher gemacht, hätte viel Zeit und Geld gespart werden können.

✉ Ursula Sury
ursula.sury@hslu.ch

[1] Luzern, Schweiz

Was bedeutet PIA – Privacy Impact Assessment?

Ein Privacy Impact Assessment stellt eine systematische Analyse einer Datenverarbeitung hinsichtlich Privatsphäre und Datenschutz dar. Es handelt sich um eine Risikoabschätzung bzw. eine sogenannte „Datenschutzfolgenabschätzung“. Dies bedeutet, dass in bestimmten Fällen bei Datenverarbeitungen aus Sicht der Betroffenen evaluiert werden soll, inwiefern ein Risiko für die Rechte und Pflichten für jede einzelne Person durch die Datenverarbeitung besteht.

Bezüglich der Durchführung impliziert Art. 35 der EU-DSGVO eine zweistufige Prüfung. Zum einen ist von den verarbeitenden Stellen einzuschätzen, ob für die Betroffenen durch die Datenverarbeitung voraussichtlich ein hohes Risiko entsteht, zum anderen müssen sowohl der genaue Prozess der Datenerhebung und -verarbeitung als auch die geplanten Abhilfemaßnahmen zur Risikominderung beschrieben werden. Verantwortliche sollen daher für jeden Erhebungsprozess eruieren, was getan werden kann, um das jeweilige Risiko der Datenverarbeitung zu vermindern.

Wann muss eine Datenschutzfolgenabschätzung durchgeführt werden?

Die EU-DSGVO schreibt eine Datenschutzfolgenabschätzung in diesen Fällen vor:

- Wenn persönliche Aspekte natürlicher Personen automatisiert und systematisiert verarbeitet und bewertet werden und es aufgrund dessen zu Entscheidungen kommen kann, die gegenüber diesen Personen eine rechtliche Wirkung entfalten bzw. diese auf vergleichbare Weise einschränken.
- Wenn zu natürlichen Personen besondere Kategorien, wie z. B. politische Meinungen, religiöse und weltanschauliche Überzeugungen, ethische Herkunft sowie

Published online: 17 March 2020

genetische und biometrische Daten oder Informationen über strafrechtliche Straftaten und Verurteilungen verarbeitet werden.

Was gilt es in der Schweiz zu beachten?

Datenverantwortliche oder Datenverarbeiter sind gemäß dem E-DSG verpflichtet, eine Datenschutzfolgenabschätzung vorzunehmen, wenn die vorgesehene Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Dabei müssen sowohl Risiken als auch geeignete Maßnahmen umschrieben werden.

Datenverantwortliche haben dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) im Falle einer Datenschutzverletzung so rasch als möglich eine Meldung zu erstatten, wenn ein hohes Risiko für die Verletzung der Persönlichkeitsrechte der betroffenen Personen droht.

Der Inhaber der Datensammlung im Sinne des E-DSG ist für die Daten und insbesondere die Datenbeschaffung verantwortlich. Er entscheidet aber auch über den Zweck und den Inhalt der Datensammlung.

Der Datenschutzverantwortliche ist als Kontaktperson für alle Fragen rund um den Datenschutz zuständig. Alle Departemente, wie auch einige Bundesämter, ernennen einen Datenschutzverantwortlichen. Im privaten Sektor kann es sich um eine unabhängige Person handeln, der diese Aufgabe übertragen wird. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖP) ist darüber zu informieren, wer die Aufgabe wahrnimmt.

Die betroffene Person – also die Person, auf die sich im Projekt verwendete Daten beziehen – muss hinreichend informiert werden, wenn Daten beschafft werden, die sie betreffen. Die Auskunft muss vollständig und verständlich nach Art. 8 DSG sein. Die betroffene Person muss die Möglichkeit haben, ihre Einwilligung freiwillig zu geben, nachdem sie angemessen informiert wurde.

Ein solches Vorgehen ist für Unternehmungen essenziell, falls diese personenbezogenen Daten auswerten, welche ein erhöhtes Risiko für die Verletzung der Persönlichkeit der betroffenen Personen darstellen.

Fazit

Mit einer Einbindung des Datenschutzes in die Planung der Projekte kann ein wie oben beschriebenes Szenario verhindert werden. Es gilt den Datenschutz als aktiven Bestandteil einer Projektplanung aufzunehmen. Mit einfachen Mitteln lassen sich die Risiken, welche aus einem potenziellen Projekt heraus entstehen können, schnell und ohne großen Aufwand ermitteln. Somit stellt sich der Datenschutz auf eine Stufe mit dem Requirements Engineering. Zudem sollte bei großen Projekten allenfalls ein Datenschutzexperte oder die interne Rechtsabteilung mit ins Boot geholt werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern (CH) und Vizedirektorin an der Hochschule Luzern – Informatik. Sie ist zudem Dozentin für Informatikrecht in verschiedenen Nachdiplomstudien, welche am Institut für Wirtschaftsinformatik der Hochschule durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.