Privacy Impact Assessment

Ursula Sury

AUSGANGSLAGE

Das Thema bzw. der Begriff «Privacy Impact Assessment» kommt im Rahmen der Revision der Datenschutzgesetzgebung immer wieder vor.

Die EU-Datenschutzgrundverordnung (DSGVO) wird am 25. Mai 2018 wirksam und äussert sich in Artikel 35 der DSGVO zur Datenschutzfolgeabschätzung. Eine ähnliche Formulierung zur Datenschutzfolgeabschätzung findet man in Art. 20 zum Entwurf des neuen Bundesgesetzes über den Datenschutz (eDSG).

INHALT EINES PRIVACY IMPACT ASSESSMENTS

Wer Personendaten (berechtigterweise) bearbeitet, ist verpflichtet diese Bearbeitung in einer Art und Weise zu gestalten, dass möglichst keine Risiken für die betroffenen Personen entstehen. Dazu gehört sicher einmal die Einhaltung einer strikten Governance, insb. IT-Governance, worin genau festgelegt und vor allem sichergestellt wird, dass sowohl aktuell als auch in Zukunft nur die rechtlich zulässigen und somit vorgesehenen Bearbeitungen durchgeführt werden.

ORGANISATORISCHE MASSNAHMEN

Es muss organisatorisch sichergestellt werden, dass die damit beauftragten Personen klare Weisungen haben, welche Bearbeitungen sie vornehmen dürfen und dass sie unbedingt kontrolliert werden, ob sie sich an diese Weisungen halten. Dies ist ein sehr wichtiger Punkt, den über die Zeit gehen häufig ursprüngliche stringente Rahmenbedingungen vergessen und die Selbstorganisation und Kreativität der Mitarbeitenden kann dazu führen, das vergessen wurde, was ursprünglich an Datenbearbeitungen absolut untersagt wurde.

INFORMATIKSICHERHEIT

Ganz wichtig ist aber auch die Einhaltung einer strikten Informatiksicherheit. Das heisst das Sicherstellen, dass weder extern noch intern unbefugte Personen bei der Haltung oder bei der Übertragung von Daten zugreifen können sowie dass nur zulässige Bearbeitungen möglich sind. Dazu gehört auch das Erfordernis des «privacy by design» und «privacy by default».

WAS IST NEU?

Eigentlich sind die Forderungen des Gesetzgebers nicht neu, sondern es werden schon bestehenden Forderungen expliziert. Es ist schon unter den geltenden Gesetzgebungen in Europa und in der Schweiz so, dass Datenbearbeiter, ob sie das selbständig machen oder im Auftrag, alles unternehmen müssen, dass keine Risiken für betroffene Personen entstehen. Auch heute schon gibt es vorbildliche Unternehmungen, welche zum Beispiel im Rahmen der Projektdokumente bei Beginn zwingend verlangen, dass die Privacy-Themen mitbedacht und eingehalten werden.

UMSETZUNG EINES PRIVACY IMPACT ASSESSMENT

Ein Privacy Impact Assessment ist sicher zu Beginn jedes Projektes, in rechtlicher, organisatorischer und technischer Hinsicht notwendig.

Das bedeutet, dass man aufgrund des geplanten Projektes eine Risikoanalyse vornimmt und festhält, welche Gefahren konkret entstehen respektive entstehen könnten, diese bewertet und entsprechende Massnahmen einleitet. Sind mit der Bearbeitung grössere Risiken verbunden, ist es unumgänglich die Datenschutzaufsichtsstelle vor Projektstart zu informieren. Dazu äussert sich die EU-DSGVO in den Artikeln 29, 31 und 33 und der Entwurf zum Bundesgesetz über den Datenschutz in den Artikeln 27, 30 und 31.

Wird agil gearbeitet, und eigentlich ist, ob der Begriff verwendet wird oder nicht, jedes Projekt mehr oder weniger agil, dann ist es wichtig, dass laufend solche Assessments in adäquater Form durchgeführt werden. Dies weil sich das Projekt auf beliebigen Wegen weiterentwickeln kann und sich wieder neue Risiken ergeben können.

ZUSAMMENFASSUNG

- Wer Personendaten (berechtigterweise) bearbeitet, ist verpflichtet diese Bearbeitung in einer Art und Weise zu gestalten, dass möglichst keine Risiken für die betroffenen Personen entstehen (z.B. strikte Governance).
- Es muss organisatorisch sichergestellt werden, dass die beauftragten Personen klare Weisungen haben, welche Bearbeitungen sie vornehmen dürfen und dass sie unbedingt kontrolliert werden.
- Ganz wichtig ist die Einhaltung einer strikten Informatiksicherheit, beispielsweise durch «privacy by desing» und «privacy by default».
- Ein Privacy Impact Assessment ist zu Beginn jedes Projektes, in rechtlicher, organisatorischer und technischer Hinsicht notwendig.
- Bei Projekten ist eine Risikoanalyse vorzunehmen und es ist festzuhalten, welche Gefahren konkret entstehen respektive entstehen könnten. Diese sind zu bewerten und es sind entsprechende Massnahmen einzuleiten.
- Sind mit der Bearbeitung grössere Risiken verbunden, ist es unumgänglich die Datenschutzaufsichtsstelle vor Projektstart zu informieren.
- Wird agil gearbeitet, dann ist es wichtig, dass laufend solche Assessments in adäquater Form durchgeführt werden.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern - Informatik. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.