ch-direct
Direkter Verkehr Schweiz
Service direct suisse
Servizio diretto svizzero
Servetsch direct svizra

Das Wichtigste zur DSGVO

1. März 2018

Claudius Ettlinger, SBB AG / Matthias Kurmann, BLS AG

Einleitung

Am 25. Mai 2018 tritt die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft. Die DSGVO kann aufgrund ihres weitgefassten Anwendungsbereichs auch auf die Tätigkeit von Schweizer Unternehmen Anwendung finden. Davon betroffen sind auch ÖV-Unternehmen. Die nachstehenden Erläuterungen sollen einen Überblick über die inhaltlich wesentlichen Punkte der DSGVO verschaffen.

Was ist die DSGVO?

Die DSGVO ist das neue Datenschutzrecht der EU. Sie findet ab 25. Mai 2018 unmittelbar Anwendung.

Für wen gilt die DSGVO?

Sie gilt für Datenbearbeiter, die in der EU eine Niederlassung unterhalten. Sie gilt auch für ausländische Datenbearbeiter, wenn sie in der EU Waren oder Dienstleistungen anbieten, d.h. bewusst und gezielt Anstrengungen unternehmen, um potentielle Kunden mit Wohnsitz in der EU anzuwerben. Wer etwa Besuchern auf seiner Website die Möglichkeit gibt, „sein“ EU-Land anzuwählen oder wer nur schon Preise in Euro oder Versandkosten in EU-Mitgliedstaaten angibt, richtet sich zumindest auch an Kundschaft aus dem EU-Raum. Diese Kundschaft kann sich dann für die Bearbeitung ihrer Daten auf die DSGVO berufen. Zudem können auch bloss unentgeltliche Angebote wie Informations-Websites vom Anwendungsbereich der DSGVO erfasst werden, sofern die Website auch auf Personen in der EU ausgerichtet ist. Als Kriterien der Ausrichtung gelten bspw. die Sprach-Versionen oder die Angabe der internationalen Vorwahl.

Die DSGVO ist sodann anwendbar, wenn das Verhalten von Personen in der EU beobachtet wird. Abgezielt wird hier primär auf Internetsachverhalte, genauer das Web-Tracking. Wer also auf seiner Website Analyse-Tools (bspw. Google Analytics) einsetzt, um die Website-Besuche und das Klickverhalten auszuwerten, unterstellt sich insoweit der DSGVO.

Schliesslich werden auch gewisse Fälle von grenzüberschreitender Auftragsdatenbearbeitung erfasst.

Auf welche Vorgänge ist die DSGVO anwendbar?

Sämtliche Bearbeitungen von Daten, die sich auf natürliche Personen beziehen, werden erfasst. Das gilt u.a. für das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Verändern, (Aus)lesen, Abfragen, Verwenden, Übermitteln, Löschen, Vernichten, etc.

Wie funktioniert die DSGVO?

Die DSGVO verbietet grundsätzlich das Bearbeiten von Personendaten. Das bedeutet: Wer Daten bearbeitet, muss sich auf einen der vier Erlaubnistatbestände berufen können, nämlich:

(1) Einwilligung
Die Datenbearbeitung beruht auf einer wirksamen Einwilligung der betroffenen Person. Die Anforderungen an eine gültige Einwilligung sind generell etwas höher als in der Schweiz und setzen u.a. voraus, dass die Person vorgängig genau informiert wurde und wirklich freiwillig zustimmt. Darum ist es verboten, die Erfüllung eines Vertrags von der Einwilligung in weitere Datenbearbeitungen, die für die Vertragsabwicklung nicht erforderlich sind (z.B. für Werbezwecke), abhängig zu machen. Die Einwilligung muss zudem durch eine eindeutige, bestätigende Handlung zum Ausdruck gebracht werden. Vorangewählte Kästchen gelten nicht als gültige Einwilligung.

(2) Vertrag
Die Datenbearbeitung ist zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich.

(3) Gesetz
Die Datenbearbeitung ist erforderlich, um eine gesetzliche Pflicht zu erfüllen.

(4) Überwiegendes Interesse
Die Datenbearbeitung ist zur Wahrung eines berechtigten Interesses erforderlich, welches das Interesse der betroffenen Person übersteigt.

Welche Grundprinzipien gelten?

Es gelten die herkömmlichen Grundsätze der Datenbearbeitung: Personenbezogene Daten dürfen nur für die Zwecke bearbeitet werden, für die sie erhoben wurden und die für die Betroffenen nachvollziehbar sind (Grundsätze der Transparenz und Zweckbindung). Ausserdem dürfen sie nur soweit und solange bearbeitet werden wie für den festgelegten Verwendungszweck erforderlich ist (Grundsätze der Datenminimierung und Speicherbegrenzung). Unzulässig ist namentlich eine Datenerfassung auf Vorrat.

Welche Rechte haben die betroffenen Personen?

Die DSGVO gewährt den Personen, welche von der Bearbeitung ihrer Daten betroffen sind, umfangreiche Rechte. Gegenüber dem schweizerischen Recht werden diese sog. Betroffenenrechte etwas ausgebaut. Die betroffenen Personen können verlangen, dass:

(1) sie umfangreich über Datenbearbeitungen informiert werden. Die Informationen sind vom Datenbearbeiter bei jeder Beschaffung von Personendaten unaufgefordert zu erbringen.

(2) sie detailliert Auskunft erhalten über Datenbearbeitungen, welche sie betreffen;

(3) unrichtige Daten berichtigt werden;

(4) gewisse Daten gelöscht oder bestimmte Datenbearbeitungen nicht durchgeführt werden;

(5) sie bei gewissen automatisierten Entscheiden von einem Menschen angehört werden;

(6) ihnen ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format herausgegeben werden.

Welche neuen Sorgfaltspflichten bringt die DSGVO mit sich?

(1) Datenbearbeitungsverzeichnis
Wer personenbezogene Daten bearbeitet, muss neu ein Verzeichnis aller relevanten Datenbearbeitungen führen. Darin muss für jeden Bearbeitungsprozess eine Reihe von Informationen dokumentiert und beschrieben werden (bspw. Zweck, Verantwortung, Art der Daten, spezifische Risiken, etc.).

(2) Nachweispflicht
Die Datenbearbeiter müssen nachweisen können, dass sie die Datenbearbeitungsgrundsätze einhalten.

(3) Datenschutz-Folgenabschätzung
Heikle Datenbearbeitungen, die mit vermutlich hohen Risiken für die betroffenen Personen verbunden sind, erfordern eine Risikoabschätzung und Konsultation der Aufsichtsbehörde, falls sich die hohen Risiken bestätigen. Eine Datenschutz-Folgeabschätzung wird insbesondere angebracht sein, wenn neue Technologien eingeführt und neuartige Datenbearbeitungsvorgänge eingesetzt werden.

(4) Meldepflichten
Datenschutzverstösse mit möglichen Risiken für Betroffene müssen der Behörde innert 72 Stunden und bei hohen Risiken auch den Betroffenen gemeldet werden. Es sind entsprechende interne Prozesse aufzusetzen und zu dokumentieren.

(5) Privacy by Design und by Default
Eigene Datenbearbeitungen müssen so ausgestaltet sein, dass sie die Einhaltung des Datenschutzes sicherstellen, während Standardeinstellungen datenschutzfreundlich zu sein haben.

(6) Bestellung eines Vertreters
Unternehmen ohne eigene Niederlassung in der EU müssen in der Regel einen Vertreter ernennen.

Unter welchen Voraussetzungen erlaubt die DSGVO die Weitergabe von Daten?

Die Datenweitergabe und deren Zweck müssen transparent gemacht werden. Zudem muss der Datenübermittler nachweisen können, dass ein Erlaubnistatbestand (z.B. Vertragserfüllung) gegeben ist. Zu beachten ist, dass bereits die blosse Einräumung eines Zugriffs als Datenbearbeitung zu betrachten ist.

In der Praxis häufig sind Fälle, in denen ein Auftraggeber (sog. Controller) ein anderes Unternehmen (sog. Processor) damit beauftragt, Personendaten (bspw. Mitarbeiter- oder Kundendaten) in seinem Auftrag und für seine Zwecke zu bearbeiten. Bei dieser sog. Auftragsdatenverarbeitung muss sich der Auftraggeber vom Beauftragten vertraglich Weisungs- und Kontrollrechte einräumen lassen. Der Beauftragte darf die Daten demnach nur nach den Weisungen des Auftraggebers bearbeiten. Dieser bleibt aber für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich.

Die Übermittlung von Daten in Länder ohne angemessenes Datenschutzniveau (wie bspw. die USA) ist ohne besondere Vorkehrungen wie Datenschutzverträge oder Zertifizierungen nicht erlaubt.

Was passiert bei Verstössen gegen die DSGVO?

Es drohen Bussen von bis zu 4% des weltweiten Jahresumsatzes oder EUR 20 Mio. – was immer höher ist. Wie häufig die zuständigen Aufsichtsbehörden Sanktionen aussprechen und von diesem Bussenrahmen tatsächlich Gebrauch machen werden, lässt sich derzeit kaum abschätzen.

Daneben verfügen die von einer Datenbearbeitung betroffenen Personen über verschiedene Möglichkeiten, ihre Rechte auf zivilrechtlichem Weg durchzusetzen.