Die Belange des Datenschutzes bei Bewegungsdatensystemen

am Beispiel des Praxistest nextTicket

Verkehrsverbund Rhein-Ruhr AöR

Gelsenkirchen, 03.04.2019

Dipl.-Ing. Ralf Baumhoer, Datenschutzbeauftragter der VRR AöR

Agenda

- Systemübersicht
- Datenschutzrechtliche Anforderungen
- Umsetzung

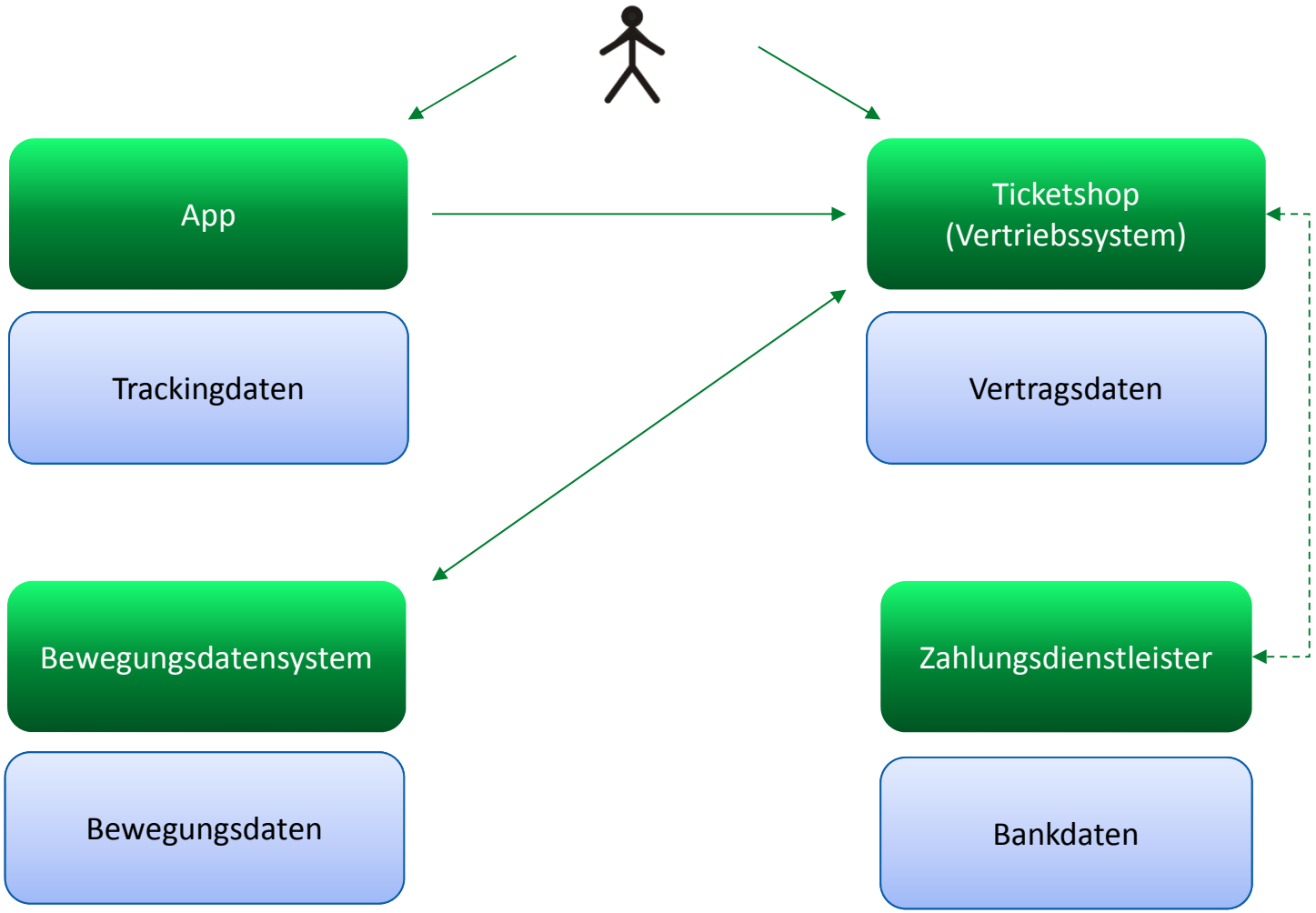
Projektpartner bei dem Praxistest

- Kundenvertragspartner ist die Bochum Gelsenkirchener Straßenbahn AG (Verkehrsunternehmen, VU,Bogestra)
- Betreiber des Systems : Verkehrsverbund Rhein-Ruhr AöR (VRR)
- Technischer Betrieb des Systems: Fa. MENTZ GmbH

Ziele des Praxistest:

- Funktionalität der Technik und Prozesse testen
- Akzeptanz bei den Kunden ermitteln
- Daten für statistische Auswertungen gewinnen

Systemkomponenten



Relevante Datenschutzgesetze

- Durch die Laufzeit des Projektes fiel es sowohl unter das alte Datenschutzgesetz (Bundesdatenschutzgesetz alt) als auch unter die neue EU-Datenschutzgrundverordnung (EU-DSGVO) sowie unter das BDSG-neu
- Es musste daher von Anfang an den Erfordernissen der DSGVO und des BDSG-neu genügen
- Deren Umsetzung und Konsequenzen für das Projekt waren zum Projektstart neu und zum Teil unbestimmt
- Nachdenklich machte auch die Höhe der möglichen Bußgelder bei Rechtsverstößen in der DSGVO

Anforderungen der EU-Datenschutzgrundverordnung an Datenverarbeitung

Artikel 5:

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben sowie Transparent
- für festgelegte, eindeutige und legitime Zwecke
- dem Zweck angemessen sowie auf das notwendige Maß beschränkt
- und sachlich richtig

verarbeitet werden

- Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es zur Identifikation erforderlich ist
- Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet

Umsetzung

- Die Datenschutzbeauftragten (Bogestra,VRR) waren vom Start des Projektes an einbezogen. Bei dem Design und der technischen Ausgestaltung des Projektes während der Lasten- und Pflichtenheftphase flossen von Anfang an Datenschutzaspekte ein, z.B.:
  - Die Daten sowohl des Vertriebssystems als auch des Bewegungsdatensystems wurden strikt auf technisch getrennten Servern gespeichert bzw. verarbeitet und wurden nur zur Rechnungsstellung zusammengeführt
  - Wegen der besonderen Sensibilität der Daten (Bewegungsdaten) kam nur eine Verarbeitung bzw. Hosting in Deutschland, mindestens im europäischen Wirtschaftsraum in Frage
  - Das Tracking (Aufzeichnen der Bewegungsdaten durch die App) wurde nach einer definierten Zeit automatisch beendet
  - Bewegungsdaten wurden nach einer definierten Frist vollständig anonymisiert
  - Keine Übermittlung in Drittstaaten

Umsetzung

- Das Projekt wurde im bestehenden Datenschutzarbeitskreis der VRR AöR mit Verkehrsunternehmen diskutiert
- Datenschutzbestimmungen und Datenschutzkonzept wurden durch externen RA geprüft
- Nach Vorlage eines Lastenheftes wurde erstmalig die Landesdatenschutzbeauftragte (LDI NRW) einbezogen und danach mehrfach informiert (z.B. nach Fertigstellung Pflichtenheft)
  - Diese forderte u.a. eine Datenschutzfolgeabschätzung, deren Kern Identifikation von Datenschutzrisiken und Maßnahmen zu ihrer Abwehr, z.B. durch technische und organisatorische Maßnahmen, sind

- Es wurde eine Risikofolgenabschätzung in erster Linie im Bereich der Datensicherheit und wirtschaftlicher Risiken durchgeführt

Umsetzung

- Anwendung des Art. 26 DSGVO durch Betriebsvertrag und Vertrag zur Verarbeitung zwischen Bogestra und VRR, in denen z.B. folgendes vereinbart wurde:

  - Klare Regelungen zu Verantwortlichkeiten und Haftungsfragen
  - Zugriff auf die Kundendaten durch den VRR nur für den Zweck der Aufrechterhaltung des technischen Betriebs
  - Für datenschutzrechtliche Weisungen an den technischen Betreiber (Mentz) stimmen sich Bogestra und VRR vorher ab
  - Durchgriffsrecht der verantwortlichen Stelle (Bogestra) im Gefahrenfall auch auf Subunternehmer wie z.B. Hoster, um schnell reagieren zu können
  - Vereinbarungen, welche Daten (nach Anonymisierung) durch die VRR AöR statistisch ausgewertet werden dürfen
  - Vereinbarung, wie mit den Daten nach Abschluss des Praxistest umgegangen wird

Umsetzung

- Während des Testbetrieb gab es einen datenschutzrelevanten Vorfall von dem 8 Kunden betroffen waren:
  - Die Rechnungsdaten einer einzelnen Fahrt (Name, postalische Anschrift, Fahrtenpreis) wurden über einen Link an Dritte gesendet
  - Alle Beteiligten wurden sofort informiert
  - Der Vorfall wurde sofort umfassend der LDI übermittelt
  - Der Vorfall hatte keine weiteren Folgen

Fazit

Der Praxistest war, auch aus Datenschutzsicht, erfolgreich, da grundlegende Sachverhalte und Probleme durchdacht und umgesetzt wurden, einschließlich von Fehlerfällen, aus denen man bekanntlich am meisten lernt.

Vielen Dank für Ihre Aufmerksamkeit!


VRR