PLATTFORM-ENTWICKLUNG – VOM MODELL ZUM TOOL

CONSTANTIN BUSCHHAUS, ARVID BUTTING, STEFFEN HILLEMACHER, JUDITH MICHAEL, BERNHARD RUMPE, RWTH AACHEN

METHODE: MODELLGETRIEBENE ENTWICKLUNG – WAS IST DAS?

Bei der modellgetriebenen Softwareentwicklung steht das Modell im Mittelpunkt, um daraus Teile des Systems zu generieren. Diese Modelle beschreiben z.B. das Domänenwissen, die Struktur, das Verhalten oder graphische Oberflächen eines Programms.

Die Vorteile gegenüber konventioneller Softwareentwicklung bestehen darin, dass Modelle den ganzen Entwicklungsprozess begleiten und wie Software-Code laufend aktuell gehalten werden, da sie als zentrale Artefakte für die Generierung genutzt werden.

Im InviDas-Projekt verwenden wir einen modellgetriebenen Entwicklungsansatz und nutzen den MontiGem Generator zur Entwicklung der Datenschutzlotsin-Plattform. MontiGem ermöglicht die einfache Entwicklung von datenzentrierten Anwendungen.[1] Aus UML/P Klassendiagrammen[2] und Modellen für die Beschreibung von graphischen Nutzer*innenoberflächen (GUI) werden große Teile der Datenstruktur, der Kommunikation mit der Datenbank, der Zugriffskontrolle und der GUI generiert.

[BBH+23] C. Buschhaus, A. Butting, S. Hillemacher, J. Michael, B. Rumpe: Plattformentwicklung - vom Modell zum Tool. In: Wearables und Individuelle Digitale Souveränität, E. Schauermann (Eds.), pp. 20-22, Gesellschaft für Informatik, Apr. 2023.

DATENSCHUTZERKLÄRUNGEN ALS MODELL

Wir haben die Datenschutzerklärungen der sieben größten Hersteller von Smart Wearables (darunter Apple, FitBit und Garmin) auf ihre Gemeinsamkeiten und Unterschiede analysiert, um daraus ein wiederverwendbares Datenmodell für Datenschutzerklärungen zu erhalten.[3] Ein Kritikpunkt hierbei ist, dass nur selten Zusammenhänge zwischen Datenkategorien und den konkreten Daten beschrieben sind und Aussagen über die Verarbeitung der Daten zu generell formuliert sind, um sie als Nutzende tatsächlich nachvollziehen zu können.

Zudem haben wir den rechtlichen Rahmen der Datenschutzgrundverordnung untersucht und gemeinsam mit Rechtsanwält*innen des assoziierten Partners Planit Legal, die sich auf IT- und Datenschutzrecht spezialisiert haben, unser Modell auf Vollständigkeit überprüft. Im Folgenden beschreiben wir die wichtigsten Klassen des Datenmodells und ihre Funktion in der Plattform.

Die zentrale Klasse des Datenmodells[4] ist die Datenschutzerklärung, die Hersteller in der Plattform basierend auf ihrer originalen Datenschutzerklärung anlegen können. Jede Erklärung beinhaltet ein Datum, ab dem das Original gültig ist, und es ist ein Mindestalter angegeben, ab dem Nutzende der Erklärung rechtsgültig zustimmen können. Zusätzlich bilden vier weitere Klassen die relevanten Konzepte einer

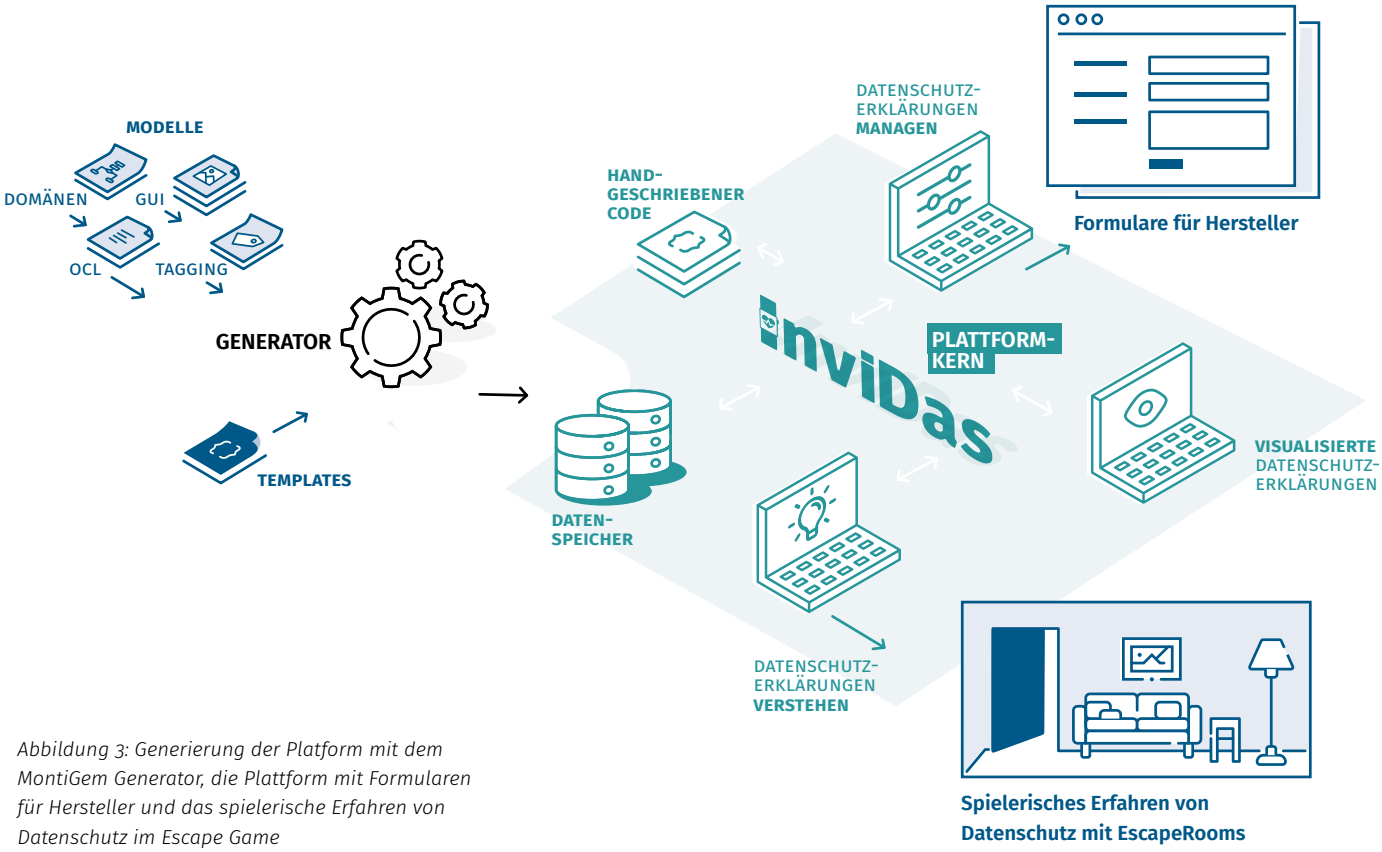

Abbildung 3: Generierung der Platform mit dem MontiGem Generator, die Plattform mit Formularen für Hersteller und das spielerische Erfahren von Datenschutz im Escape Game

Datenschutzerklärung ab: Dateneintrag, Datenkategorie, Datenverarbeitung, und Regionen. Dateneinträge und Datenkategorien liefern Details zu den Daten, die schützenswert sind. Beide haben einen Namen und Dateneinträge können durch Datenkategorien zusammengefasst werden, z.B. die Datenkategorie „Aktivitätsdaten" mit Dateneinträgen zu den gezählten Schritten und Pulsaufzeichnungen. Regionen geben an, wo die Datenschutzerklärung gültig ist.

Eine Datenverarbeitung wird an einem Ort und durch eine*n Akteur*in ausgeführt, wobei Nutzer*in, Hersteller und externe Datenbereitstellende möglich sind. Für jede Datenverarbeitung wird mindestens ein Zweck angegeben, der sich auf bestimmte Daten bzw. Datenkategorien der Verarbeitung bezieht und eine Rechtsgrundlage besitzen muss. Dem Zweck (1) kann widersprochen werden, ohne den Service des Herstellers zu beschränken, (2) er ist verpflichtend für die Nutzung des Wearables oder (3) er ist verpflichtend, um einen bestimmten Service zu nutzen. Es gibt verschiedene Formen der Datenverarbeitung und es existieren viele Begriffe, die eine ähnliche Bedeutung haben können. Um die Verständlichkeit zu erhöhen und einen Vergleich zu ermöglichen, wurden die Verarbeitungen für das Datenmodell und die Plattform auf drei Arten reduziert, die sich in ihren Charakteristiken unterscheiden und sich deshalb nachvollziehbar beschreiben lassen: die Erhebung bzw. Aufbereitung, die Speicherung und die Weitergabe. Die Erhebung bzw. Aufbereitung beschreibt den Vorgang der Datensammlung und weitere Verarbeitungen, die weder Speicherungen noch Weitergaben sind, darunter fällt z. B. die Analyse. Es wird unterschieden, ob sie einmalig stattfinden, z. B. beim Erstellen eines Nutzerkontos, kontinuierlich durchgeführt werden oder nur bei einer bestimmten Aktivität der Nutzenden.

Für die Datenspeicherung wird angegeben, wie lange diese andauert, entweder als Zeitspanne oder bis zu einem bestimmten Ereignis. Für die Datenweitergabe ist entscheidend, wer ihre Empfänger*in ist und in welchem Land die empfangende Instanz sitzt, da dort andere Datenschutzgesetze gelten können.

AUFBAU DER PLATTFORM

Die InviDas-Plattform nutzt den MontiGem Generator, um Programmcode für das Backend und Frontend der Anwendung zu generieren. Im Backend ist dies eine Java Anwendung, die das Apache TomEE Framework nutzt, ein Apache HTTP Webserver und eine Postgres Datenbank, in der die Daten der Hersteller eingepflegt werden können, jeweils in eigenen Docker Containern. Im Frontend generieren wir TypeScript und HTML Code in das Angular Framework.

Das Ziel der Plattform ist es, Datenschutzerklärungen von Smart Wearables besser verständlich zu machen. Hierfür müssen wir die Datenschutzverantwortlichen der Hersteller motivieren, ihre Datenschutzerklärungen in die Plattform einzupflegen, um einen Vergleich zwischen den verschiedenen Anbietern und Erklärungen zu erlauben. Dies ist über Formulare möglich (siehe Abb. 3). Die Plattform verfügt über ein Rechte-Rollen-Konzept, um es Herstellern zu ermöglichen ihre Daten einzupflegen. Zudem können Administrator*innen Accounts für Hersteller erstellen.

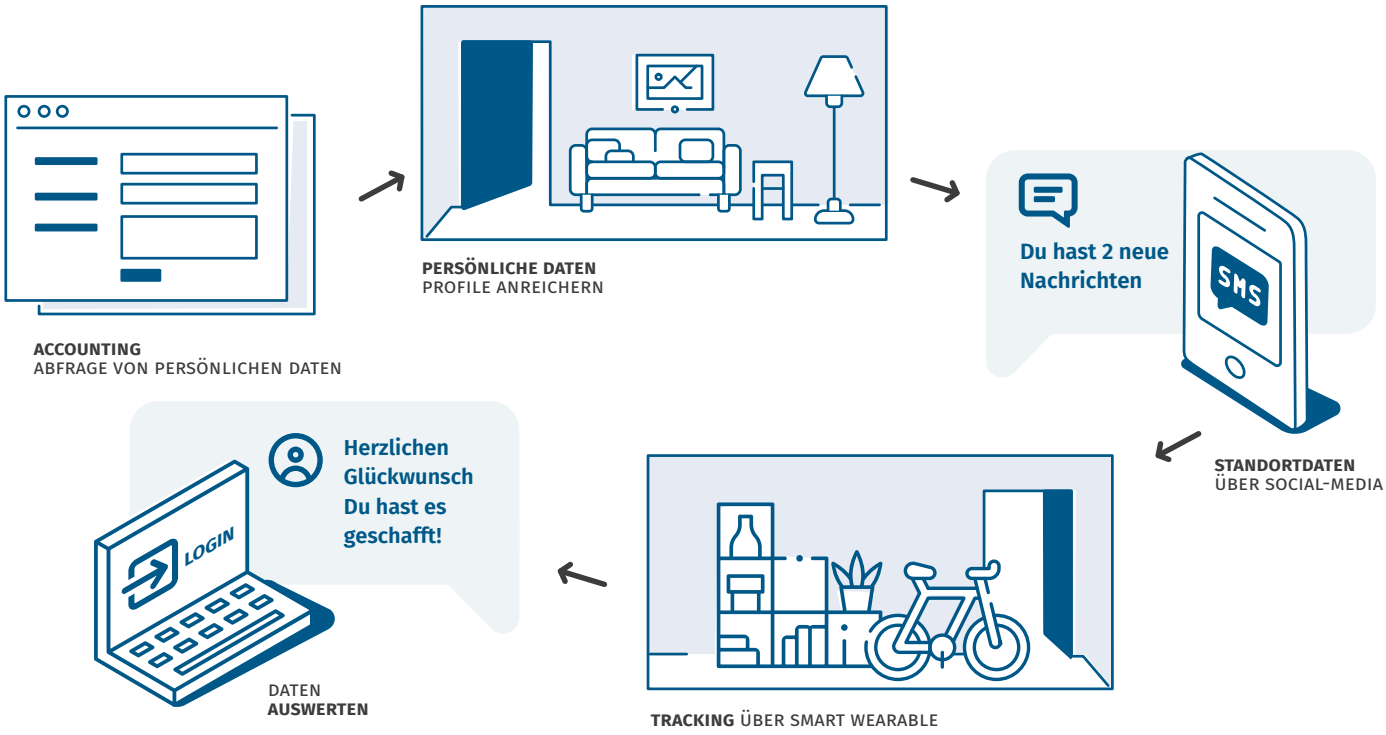

Abbildung 4: Datenschutz im Escape Game spielerisch erfahren

DATENSCHUTZ GAMIFIZIEREN

Gamifizierung beschreibt die Einbettung von spielerischen Elementen in seriöse Kontexte mit dem Ziel, das Engagement, die Motivation und die Beteiligung zu fördern. Beispiele für solche spielerischen Elemente sind Punktewertungen, Bestenlisten, Abzeichen, Herausforderungen und andere Anreize. Der Ansatz der Gamifizierung basiert auf der Idee, dass Menschen einen intrinsischen Spieltrieb haben und sich an Belohnungen durch Gewinne und Leistungen erfreuen.

Im Projekt wurde das Konzept der Gamifizierung durch ein Escape Game umgesetzt, das den Spielenden den Umgang mit Datenschutz und personenbezogenen Daten näherbringen soll. Diese Lektionen sind in die für den Spielfortschritt erforderlichen Schritte integriert.

Zu Beginn des Spiels wird der*die Spieler*in dazu aufgefordert, persönliche Daten anzugeben, deren Angabe eigentlich nicht erforderlich ist und das Spielerlebnis nicht verändert. Dies soll Spielenden vermitteln, dass personenbeziehbare Daten nicht immer vollständig angeben werden müssen, um spezifische Dienstleistungen zu nutzen.

Das Ziel des Spielverlaufs ist es, den Standort einer Person herauszufinden, um dieser einen Streich zu spielen. Dazu bieten sich den Spieler*innen im Verlauf des Spiels zwei Möglichkeiten. Einmal über den Social-Media-Status der gesuchten Person sowie über die Trackingfunktion der Fitnessuhr, die bereits auf der Herstellerseite im Kundenprofil eingeloggt ist. Die Spieler*innen sollen dabei lernen,

(1) dass Standortdaten in den falschen Händen missbraucht werden können,
(2) dass die Ortung über Smart Wearables sehr genau ist und somit ein größeres Missbrauchspotenzial besteht, und
(3) dass jede Person für den Schutz ihrer Daten mitverantwortlich ist, z.B. wenn es darum geht ein geeignetes Passwort auszuwählen oder zu verhindern, dass anderen Personen durch Unachtsamkeit Zugriff auf die eigenen Daten ermöglicht wird.

---

[1] *https://www.se-rwth.de/research/MontiGem*
[2] *https://www.mbse.se-rwth.de/book1*
[3] A. Butting, N. Conradie, J. Croll, M. Fehler, C. Gruber, D. Herrmann, A. Mertens, J. Michael, V. Nitsch, S. Nagel, S. Pütz, B. Rumpe, E. Schauermann, J. Schöning, C. Stellmacher, S. Theis: *Souveräne digitalrechtliche Entscheidungsfindung hinsichtlich der Datenpreisgabe bei der Nutzung von Wearables. In: Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg, pp. 489-508, Springer Fachmedien Wiesbaden, Apr. 2022.*
[4] *Modeling Privacy Policies of Smart Watches: A Reuseable Generic Data Structure Model: https://zenodo.org/record/5898204*