Endbericht
netidee Projekt 1829 – DSGVO Tool

Einleitung

Ich danke dem netidee Förderprogramm der Internet Privatstiftung Austria für die Möglichkeit dieses Tool umsetzen zu können. Als größten Gewinn betrachte ich rückwirkend all die Erfahrung und Lerneffekte, die ich im Zuge des Projektes mit allen Höhen und Tiefen, Erfolgen und Verzögerungen habe sammeln dürfen! Ich bin sehr zuversichtlich, dass die Kooperation mit der Datenschutz NGO zustande kommt und dazu beitragen wird, das Tool weiterzuentwickeln und den Datenschutz zu unterstützen.

Projektbeschreibung

Ziel ist eine Website, wo man automatisiert eine gültige Datenanfrage an eine Vielzahl von Firmen schicken kann. Die Website soll auch am Smartphone (responsive; Ausweisupload per Handykamera) funktionieren. Diese Möglichkeit soll einer möglichst großen Menschengruppe bekannt gemacht werden. Die App soll opensource sein damit sie für die übrigen EU-Länder übersetzt und umgesetzt werden kann (Skalierung). Für Firmen gibts (mittels einer optional übermittelten maschinenlesbaren .csv Datei mit den Anfragedaten) eine Möglichkeit um Anfragen automatisiert zu verarbeiten.

Status Quo der Ziele:
Alle Arbeitspakete fertiggestellt.

- Die Webapp launchte im Q2 2018 (www.daten-auskunft.at). Web-App funktioniert im Browser am Smartphone (ausgezeichneter Erfolg). Quellcode ist veröffentlicht auf: https://github.com/mialbr/daten-auskunft

- 18 Firmen-Kontakte stehen zur Verfügung (Projektvorgabe waren 10)

- Medienarbeit: Während mit diversen PR-Aktionen viele Journalisten erreicht wurden bzw die Reichweite von Newslettern sehr hoch war, wurde die angestrebte Veröffentlichung in reichweitenstarken Medien nicht erreicht. Trotz aller Bemühungen (vor allem auch mit tatkräftiger Hilfe seitens Netidee), hat man es nicht in der Hand Medienecho zu erzwingen. Ein erneuter Versuch der Medienarbeit erscheint nach dem Sommerloch im Herbst sinnvoll.

- Ziel war auch, dass Firmen am DSGVO Tool für eine Automatisierung teilnehmen und die optional mitgesendete maschinenlesbare .csv nutzen. Dies wurde leider nicht erreicht. Die DSGVO ist immer noch ein Schreckgespenst im Bereich der Wirtschaft – ein erneuter Vorstoß erscheint sinnvoll, sobald Unternehmen, die Mindestanforderungen der DSGVO weitgehend erfüllt haben.

- Datenanfragen 6 Monate nach Launch: Ziel:200, ausgezeichnet: 600. Nach aktuellem Stand wurden 180 Anfragen innerhalb von 2 Monaten nach Launch durchgeführt. Das vorrangige Ziel von 200 scheint realistisch erreicht zu werden.

Zum Projektverlauf:

- Alle Pakete bis auf eines konnten im angestrebten Zeitrahmen erledigt werden (Geringfügig länger dauerte die Programmierung der Webapp und API). Aufgrund der Verzögerung bei der API Planung, hat sich der gesamte Verlauf um 3 Monate nach hinten verschoben (siehe Netzplan).
- Der Launch selber wurde in Absprache mit Netidee auf Q2 verschoben (Mail vom 03.04.2018; siehe Begründung weiter unten). Die App launchte 2 Wochen nach Inkraftreten der DSGVO. Begründung für Launch nach der DSGVO:
  - Datenanfragen werden erst mit der DSGVO ein wirklich mächtiges Instrument. Ich befürchte, dass bis zum 25.5. Anfragen generell eher nicht beantwortet werden, weil bis dahin rechtlich noch nicht (wirklich) zwingend, und alle mit den Vorbereitungen für die DSGVO beschäftigt sind. Ich habe die rechtlichen Inhalte im generierten Anschreiben bereits für die DSGVO formuliert, also für geltendes Recht nach 25.5.
  - Weiters erschien die Chance für Berichterstattung nach dem 25.5 viel höher.

Endbetrachtung:

- Ich danke dem netidee Förderprogramm der Internet Privatstiftung Austria für die Möglichkeit dieses Tool umsetzen zu können. Als größten Gewinn betrachte ich rückwirkend all die Erfahrung und Lerneffekte, die ich im Zuge des Projektes mit allen Höhen und Tiefen, Erfolgen und Verzögerungen habe sammeln dürfen! Ich bin sehr zuversichtlich, dass die Kooperation mit der Datenschutz NGO zustande kommt und dazu beitragen wird, das Tool weiterzuentwickeln und den Datenschutz zu unterstützen.

Verlauf der Arbeitspakete

Arbeitspaket 1 wurde durchgeführt:

- Vertrag unterschrieben, Detailprojektplan (Arbeitsblatt Arbeitspakete)

erstellt und abgenommen, detaillierte Liste Projektergebnisse mit Lizenz und Ort der öffentlichen Bereitstellung erstellt und abgenommen (Arbeitsblatt Projektergebnisse); erste Förderrate beantragt

Arbeitspaket 2 wurde durchgeführt:

- DSGVO Anforderungen recherchiert:
  - Da die DSGVO ein sogennanter hybrider Unionsakt ist, also sowohl Merkmale einer sofort anwendbaren Verordnung als auch einer von den Mitgliedstaaten erst umzusetzenden Richtlinie hat, sind die Auswirkungen rein prinzipiell zur Zeit noch nicht zu 100% klar. Jedoch sind die Regelungen, die das Projekt betreffen, in der Art als direkt anwendbare Verordnung formuliert sind und daher schon jetzt klar und so konnten für das DSGVO-Tool alle offenen Fragen geklärt werden.

Arbeitspaket 3 wurde durchgeführt:

- Rechtliche Ausgestaltung und Formulierungen für rechtswirksame Anfrage recherchiert.
- Es sollten Kontakte für mindestens 10 Anfrageadressaten aufgelistet werden (aktueller Stand: 18).
- Eine erste Erkenntnis war, dass verschiedene Adressaten verschiedene Identifizierungsdaten für eine wirksame Anfrage benötigen. Ausserdem zeigte sich, dass manche Anbieter (zB Friends of Merkur) ein Email als Anfrage akzeptieren, während manch andere auf Schriftform zB Fax beharren. Mit der DSGVO wird das vereinfacht: ein formloser Antrag sowie eine Identifikation per Ausweis sind ausreichend. Damit sind viele Hindernisse ab Mai 2018 beseitigt. Vorausdenkend wird die App für Regelungen der DSGVO designt, weil das die Komplexität erheblich reduziert und Nutzerfreundlichkeit erhöht, was einen Launch ab Geltung der DSGVO bedingt.

Arbeitspaket 4+5 wurde durchgeführt:

13.02.2017-24.02.2017

- Konzept, Features und Prozesse für die Webapp definiert
- Design, Texte und Struktur der Website vorbereitet.
- Funktionen, Abläufe und Usability von API konzipiert und geplant

Die API wurde wie im Zwischenbericht geschildert umgesetzt: "Bei der Konzeption der API standen wir vor dem Problem eine Übermittlung der Daten an den Nutzer sicherheitskonform zu gestalten. Bei Variante eins wäre die Webapp nicht nur bei der Anfrage sondern auch bei der Datenübermittlung der Mittler zwischen anfragender User und beantwortender Firma. Bei Variante zwei würde die Datenübermittlung direkt zwischen User und Firma ablaufen.

Bei Variante 1 waren mehrere Zugänge denkbar, wo mit diversen Verschlüsselungssystemen die Daten des Nutzers per Email versendet werden können. Jedoch verlangt der Prozess dann zunehmend mehr technische Kenntnisse vom Nutzer, bzw verlangt die Installation von zusätzlichen Tools auf Seite des Nutzers. Dies widerspricht dem Ziel, die Datenanfrage einem größtmöglichen (auch technisch unversierten) Interessentenkreis zugänglich zu machen. Je mehr der Ablauf vereinheitlicht wird, indem die Webapp die Verschlüsselung unternimmt, desto mehr der übermittelten persönlichen Nutzerdaten müssen am Server der App (zwischen)-gespeichert werden, und desto größer wird das Sicherheitsrisiko. Eine langfristige Sicherheitspflege, also laufende Serverupdates, übersteigt auch die Ressourcen des Projekts.
Aufgrund dieser Erkenntnisse haben wir den Entschluss getroffen, dass mit der API die Anfrage an die Firmen übermittelt wird, und die Übermittlung der Daten direkt zwischen User und Firmen stattfindet.
Wir haben lange über Variante 1 nachgedacht, weil wir gerne eine höchstmöglich elegante Lösung erzielen wollten. Dadurch kam es zu einem höheren Zeitaufwand in AP 5 und zu einer Verzögerung von 2 Monaten. Auf die Gesamtkosten hat es keinen Einfluss, weil sich anderweit eingeplante Leistungen (für Variante 1) als nicht notwendig herausgestellt haben."

Arbeitspaket 6 wurde durchgeführt:

27.02.2017 - 31.03.2017

- Server/Plattform wählen
- Verschlüsselung, Frontpage aufsetzen
- Website aufgesetzt laut Konzept

Bei der Wahl der Server bestand initial das Problem den größtmöglichen Datenschutz für die Nutzer zu gewährleisten und das Finden eines Serverstandortes in einem der wenigen Länder mit hohem Datenschutzniveau und Resilienz gegenüber Überwachungsmöglichkeiten. Da jedoch das Konzept so gestaltet wurde, sodass die Nutzerdaten direkt – ohne Umweg über die Webapp – an den Nutzer übermittelt werden und nur die Email der Nutzer als einzige persönliche Daten – und diese nur verschlüsselt – gespeichert werden, ist die Datenschutzproblematik entschärft. Durch Datenvermeidung ist der Schaden eines Datenlecks absolut minimiert.
Daher wurde bei der Wahl des Servers/Plattform weniger auf den Standort und vor allem auf Skalierbarkeit, Kosten und professionelle und regelmäßige Sicherheitsupdates geachtet. Pythonanywhere.com erfüllt diese Bedingungen (Serverpflege wird zu 100% vom Plattformanbieter übernommen) und wird für die App genutzt.

Arbeitspaket 7 wurde durchgeführt:

03.04.2017-02.06.2017

- Codierung der Anfragefunktion
- Anfragefunktion funktioniert per Webapp im Desktopbrowser (ausgezeichnet: auch am Smartphone).
- Ziel: Man kann aus mindestens 10 Adressaten wählen, seine Daten eingeben, Anfrage wird rechtswirksam abgeschickt.

  Aktuell: Man kann aktuell aus 18 Adressaten wählen, Dateneingabe funktioniert sowohl am Desktop als auch am Handy. Herausforderung waren vor allem Sicherheitsaspekte, die umso schwerer wiegen, als das mit einer großen Zahl User-generierten Eingaben gearbeitet wird, die auch als Einfallstor für Attacken genutzt werden kann. Da sich die App thematisch um Datenschutz dreht, aber gleichzeitig viele persönliche Daten verarbeitet werden (Name Anschrift, Geburtsdatum, Ausweisbild) wäre ein Datenleck der Super-Gau für das Projekt und das darüberliegende Ideal, persönliche Daten automatisiert anfordern/kontrollieren zu können. Daher wurde viel Arbeit in eine Absicherung der Prozesse gesteckt. Vorallem in AP 8 wurde das Testen sehr ausgiebig unternommen und Fehler beseitigt.

Arbeitspaket 8 wurde durchgeführt:

- Eine automatisierbare maschinenlesbare Anfragedatei wurden konzipiert, und pro hinterlegten Anfragekontakt kann definiert werden, ob eine Anfrage standardmäßig nur als Brief versendet wird, oder ob auch eine maschinenlesbare .csv Datei mit allen zur Anfragebearbeitung nötigen Daten mitgesendet wird. Ein Anfrageadressat kann damit die Anfrage in sein Firmensystem hineinladen und automatisiert weiterverarbeiten.
- Haupttätigkeit in AP 8 waren vor allem Testen, und Fehlerbehebung – wie in AP 7 beschrieben, war ein Vermeidung von Datenlecks und die Minimierung der Dauer, während der persönliche Daten am Server gespeichert sind eine Sine Qua Non.

Arbeitspaket 9

- Es wurde recherchiert, ob eine Vereinbarung für die Übermittlung bzw Nutzung der .csv Datei notwendig ist. In erster Linie scheint es nicht zwingend nötig zu sein. Sollte die sich .csv in Zukunft größerer Beliebtheit erfreuen, dann kann natürlich eine Ausweitung dieses Services angedacht werden und dann sind die rechtlichen Aspekte von AP 9 neu zu denken.

Arbeitspaket 10 Kontakte suchen, Termine ausmachen, durchführen, Vereinbarungen treffen, API Anbinden, Rücksprache und Koordination, Beratung und Unterstützung bei Anbindung

- Beratung und Unterstützung sowie Koordination waren leider nicht nötig, da sich keine Firma fand um die API zu nutzen. Die aufgetriebenen Firmen-Kontakte waren im Frühjahr zu sehr beschäftigt mit der

dringenden Umsetzung der DSGVO. Wie vorhin beschrieben ist die DSGVO immer noch ein Schreckgespenst im Bereich der Wirtschaft – ein erneuter Vorstoß erscheint sinnvoll, sobald Unternehmen, die Mindestanforderungen der DSGVO weitgehend erfüllt haben.

Arbeitspaket 11

- Aussendungen (Kurzerklärung) sowie Blog-Postings wurden verfasst.
- Mehrere PR-taugliche Anschauungsbilder wurden erstellt, die auch für das Rollup genutzt wurden.
- Weiters fand die Erstellung eines tollen Videos auf Initiative von Netidee statt.
- Kooperationen wurden vor allem mit anderen Datenschutz NGOs geschmiedet. Eine große medial bekannte österreichische Datenschutz NGO erklärte sich interessiert in der Zukunft zu kooperieren und gemeinsam an der Weiterführung und Weiterentwicklung der App zu arbeiten.

Arbeitspaket 12 Kampagnen starten und Journalisten Kontaktieren, Design der Website auffrischen, Launch:

- In Zusammenarbeit mit Netidee wurden Journalisten kontaktiert bzw eigene Kontakte zu Journalisten genutzt, das vorgestellte Medienecho wurde aber leider nicht erreicht.
- Eine Verbreitung über den Newsletter einer Arbeitnehmer-Organisation ist noch im Laufen.
- Für den Launch wurde das Design der Webapp komplett überarbeitet und neu gestaltet, um eine interessantes und ansprechendes Erlebnis zu bieten und ohne überladener Gestaltung von der Funktionalität abzulenken und gleichzeitig die responsiveness zu bewahren (Nutzbarkeit sowohl am PC als auch Smartphones).

Arbeitspaket 13 Dokumentation, Userguides schreiben und Veröffentlichung der opensource Komponente. Formales während des Projektes und am Projektende. Die nötige Dokumentation und Berichterstattung wurde fertiggestellt.

Liste der Projektergebnisse

- Projektendbericht (dieses Dokument (CC-BY Sharelike-3.0 AT))

- Entwickler-DOKUMENTATION des Projektergebnisses für andere Entwickler ("Dritte"), die das Projektergebnis nach Projektende nutzen/weiterentwickeln wollen (https://www.netidee.at/dsgvo-tool (CC-

BY Sharelike-3.0 AT))

- Anwender-DOKUMENTATION des Projektergebnis für Anwender, die das Projektergebnis nach Projektende nutzen wollen ("Bedienungsanleitung") (https://www.netidee.at/dsgvo-tool (CC-BY Sharelike-3.0 AT))

- Veröffentlichungsfähiger Einseiter (https://www.netidee.at/dsgvo-tool (CC-BY Sharelike-3.0 AT))

- SW Webapp für Datenanfragen bzw SW API für Firmen (https://github.com/mialbr/daten-auskunft (MIT))

Verwertung der Projektergebnisse in der Praxis

- Die erstellte Software für Flask(Python) wird selber weiterbetrieben und unter www.daten-auskunft.at der Öffentlichkeit gratis zur Verfügung gestellt. Durch den kostengünstigen Betrieb kann das Service auch in Zukunft angeboten und die App damit verwertet werden. Es ist davon auszugehen, dass das Thema Datenschutz nicht weniger wichtig werden wird, sonder eher das Gegenteil eintreten wird. Damit sind die Projektergebnisse vor allem ein erster Schritt, auf dem in Zukunft aufgebaut und erweitert werden kann. Die ersten hundert Nutzungen sind bereits erfolgt.

Öffentlichkeitsarbeit/ Vernetzung

- Siehe AP 11 +12

Geplante Aktivitäten nach netidee-Projektende

- Wie gesagt, sind die Projektergebnisse vor allem ein erster Schritt, auf dem in Zukunft aufgebaut und erweitert werden kann:
  - Erweiterung der Liste der auswählbaren Firmen
  - Erneuter Versuch Firmen zur automatisierten Verarbeitung zu motivieren
  - Nochmalige PR-Offensive im Herbst
  - Programmierung eines Backends, um die Erweiterung und Anpassung der App zu erleichtern und eine Portierung in andere Sprachen für andere Länder zu erleichtern

Anregung für Weiterentwicklung durch Dritte

  - Unterstützung bei der Programmierung eines Backends, um die Erweiterung und Anpassung der App zu erleichtern
  - Portierung in eine andere Sprache bzw die App für andere Länder aufsetzen, um dort auch automatisierte Anfragen anzubieten.
  - Hinweise geben, welche Firmen sinnvollerweise noch in die Liste aufgenommen werden sollen.