Liquid Democracy und Online-Beteiligung

– wie es die Datenschützer gestalten würden

Dr. Thomas Probst

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Agenda

- Formen von Beteiligungsverfahren
- Beispiele
- Konzept von „Liquid Democracy“
- Technische Aspekte
- Schutzziele
- Anwendung der Schutzziele
- Maßnahmen zur Umsetzung der Schutzziele

(Mögliche) Beteiligungsverfahren

- Diskussionen (eher: Willensbildung statt Beteiligung)
  - gruppenintern
  - öffentlich
- Petitionen
  - individuelle Petition
  - Gruppenpetition
- Bürgerbeteiligung
  - informell: „Zukunftswerkstatt“
  - gesetzlich geregelte Beteiligungsverfahren (z.B. § 3 BauGB)
- Abstimmungen
  - öffentliche Abstimmungen
  - gruppeninterne Abstimmungen („Verein“)
  - geregelte Abstimmungen (Partei, Hauptversammlung)

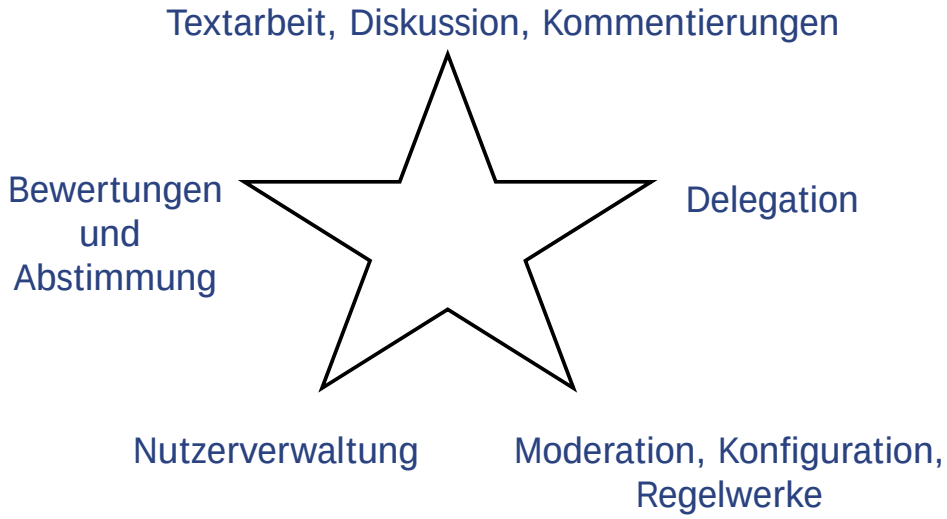
Spektrum der Funktionalitäten

- Individualinteressen => Vertraulichkeit
- Gruppeninteressen => Kollaborationstool

Interessen:

- formulieren => Textarbeit, z.B. Entscheidungsvorlagen
- vertreten => Abstimmungen, Bewertungen

Funktionalitäten von Beteiligungssystemen



Beispiele

- Liquid Feedback
  - Piratenpartei (einige Landesverbände, Bund)
  - geplant: Landkreis Friesland
- Adhocracy
  - Enquete-Kommission „Internet und Digitale Gesellschaft“ des Bundestages
  - ZEIT-Verlag: Zeitmagazin: „Das Heft Ihrer Wahl“

Bewertungen und Abstimmungen

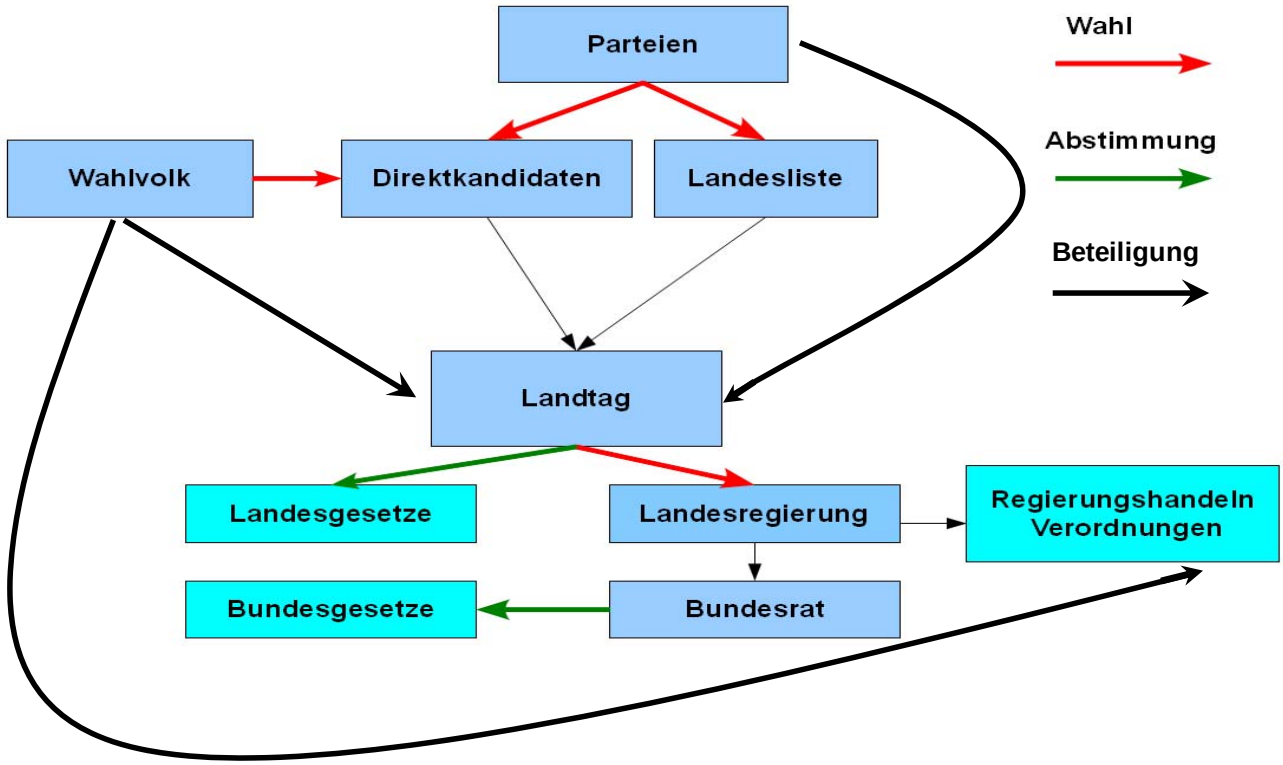
- Bewerten von Text-/Entscheidungsvorschlägen und Diskussionsbeiträgen (Relevanz)
- Abstimmen über Text-/Entscheidungsvorschläge (inkl. Quoren, Fristen, Veränderungssperren, etc.)
- Präferenzwahlen
  - Abstimmende geben Präferenzen in Form einer Rangliste an
  - Ermittlung des „besten“ Ergebnisses durch Condorcet-Methoden (z.B. Schulze-Methode)

Auf dem Weg zur repräsentativen Demokratie

- kein direkten Einflüsse der Wählerinnen und Wählerin Willensbildungs- und Entscheidungsprozesse

stattdessen:

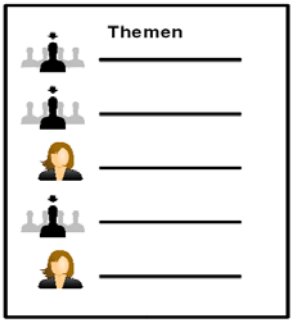
- Wahl von (Volks-)Vertretern, die eigenverantwortlich handeln
- Wahl auf Zeit
- häufig: Ketten von Auswahlprozessen („Repräsentanzketten“)



Idee der „Liquid Democracy“

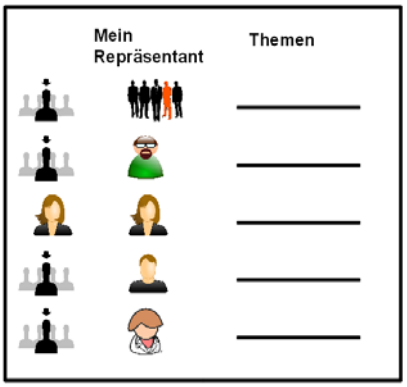
- keine *starre* Festlegung zwischen unmittelbarer Demokratie und repräsentativer Demokratie, sondern *flüssiger* Übergang
- individuelle Festlegungen, ob und inwieweit
  - direkter Einfluss oder
  - Delegation, d.h. Vertretung durch Repräsentanten erfolgen soll
- Festlegung erfolgt
  - themenspezifisch
  - personenspezifisch
  - dynamisch

Konsequenzen

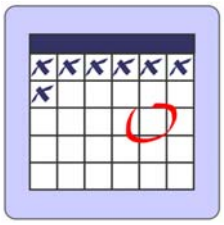


Dies erfordert Delegationssysteme, die

- themenspezifisch,
- personenspezifisch,



- dynamisch delegieren können



Technik und Konsequenzen

- Datenbank:
  enthält alle Inhalte, Nutzerkonten und Abstimmungen
- Webfrontend:
  Zugriff jederzeit und von überall her möglich; Web-Security
- Mandantenfähig:
  Trennung der Mandanten erforderlich
- Bereitstellung durch Dritte:
  Auftragsdatenverarbeitung

Welche Anforderungen gibt es?

Datenschutz-Schutzziele

Bisher: Formulierung technisch-organisatorischer Datensicherheitsmaßnahmen (TOM) in Form von *Kontrollen*

- Zutritts-, Zugangs-, Zugriffskontrollen,
- Weitergabe-, Eingabe-, Auftrags, Verfügbarkeitskontrollen,
- Abschottungsgebot

Gesetzliche Regelung:

- § 9 BDSG und Anlage
- § 78 a SGB X und Anlage
- § 5 LDSG-SH (alt)

Datenschutz-Schutzziele

Neuere Ansätze: Formulierung als **(Schutz-)Ziel**

... technische und organisatorische Maßnahmen ... müssen gewährleisten, dass

1. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),

2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),

...

Beispiele: § 5 Abs. 1 LDSG-SH, viele LDSGe

Datenschutz-Schutzziele in Schleswig-Holstein

- Verfügbarkeit: „da, wenn gebraucht“
- Integrität: „unversehrt“
- Vertraulichkeit: „nur Befugten zugänglich“

- Transparenz: „nachvollzieh- und überprüfbar“
- Intervenierbarkeit „Korrektur für Verantwortliche möglich“ „Betroffenenrechte ausübbar“
- Nicht-Verkettbarkeit „Daten- und Funktionsminimierung für Erforderlichkeitsprinzip + Zweckbindung“

Anwendung der Schutzziele: risikobasiert

§ 5 LDSG-SH:

Die Ausführung der Vorschriften dieses Gesetzes .....ist durch technische und organisatorische Maßnahmen sicherzustellen, die

nach dem **Stand der Technik** und der **Schutzbedürftigkeit der Daten** } **Einflussfaktoren**

erforderlich und **angemessen**.

Hinweis auf Datenschutzverordnung § 4 Abs. 2 DSVO:
Sicherheitskonzept, **Risikoanalyse**

Anwendung der Schutzziele: situationsabhängig

- Schutzziele können in einem **Spannungsverhältnis** zueinander stehen
- Beispiele:
  - Gute Verfügbarkeitslösungen (Backup, Duplikation, Auslagerung, Onlinespeicher) können Vertraulichkeit gefährden
  - bestmögliche Integrität (z.B. Vollprotokollierung mit Manipulationsschutz) beeinflusst Intervenierbarkeit (z. B. Berichtigung/Löschung von Betroffenendaten)
- Konsequenz: **situationsabhängiges Ausbalancieren** erforderlich

Anwendung der Schutzziele auf Beteiligungssysteme

Vorgehen:

1) Schutzbedarf in Bezug auf die Datenschutz-Schutzziele ermitteln:
   - Kategorisierung: normal hoch sehr hoch
   - Schadenspotential bei Verletzung des Schutzziels ermitteln
   - hohes Schadenspotential => hoher Schutzbedarf

2) aus den Schutzbedarfen Maßnahmen ableiten

Gegenstand von Beteiligungsverfahren

- Diskussionen
  - gruppenintern
  - öffentlich
- Petitionen
  - individuelle Petition
  - Gruppenpetition
- Bürgerbeteiligung
  - informell
  - gesetzlich geregelte Beteiligungsverfahren (z.B. § 3 BauGB)
- Abstimmungen
  - öffentliche Abstimmungen
  - gruppeninterne Abstimmungen („Verein“)
  - geregelte Abstimmungen (Partei, Hauptversammlung)

Szenario I

Szenario:
Online-Diskussionen im örtlichen Modelleisenbahnverein

Anzahl der Teilnehmer: 60

Betreiber der Plattform: technikaffines Vereinsmitglied

Diskussionsgegenstände:
Veränderungen an der bestehenden Modellbahnanlage

Anwendung der Schutzziele auf Beteiligungssysteme

Szenario: Online-Diskussion im Modelleisenbahnverein

Schutzbedarfe:

Verfügbarkeit:	normal
Integrität:	normal
Vertraulichkeit:	normal
Transparenz:	normal
Nicht-Verkettbarkeit:	normal
Intervenierbarkeit:	normal

Die Folgen von Schutzzielverletzung sind bei diesem Szenario überschaubar.

Szenario II

Szenario: Online-Petitionen

Petition Art. 17 Grundgesetz:

Jedermann hat das Recht, sich einzeln oder in Gemeinschaft mit anderen schriftlich mit Bitten oder Beschwerden an die zuständigen Stellen und an die Volksvertretung zu wenden.

Grundsatzbeschlüsse des Petitionsausschusses des Schleswig-Holsteinischen Landtages der 18. Wahlperiode vom 19. Juni 2012:

Nr. 3: Vertraulichkeit von Sitzungsunterlagen und Petitionsakten

Nr. 4: Entscheidung in Eilfällen

Szenario II: Petitionen

Szenario:

Online-Petitionen

Anzahl der Teilnehmer: 100.000

Betreiber der Plattform: Landtag/Bundestag

Daten: Einzel- und Gruppenpetitionen

14.08.2012

Szenario II: Online-Petition

Schutzbedarfe:

Verfügbarkeit:	normal (?)
Integrität:	hoch
Vertraulichkeit:	hoch
Transparenz:	hoch
Nicht-Verkettbarkeit:	hoch
Intervenierbarkeit:	normal

Szenario III: Bauplanung

Szenario: Bürgerbeteiligung Bauplanung

Anzahl der Teilnehmer: 1000

Betreiber der Plattform: Verwaltung

Diskussionsgegenstände: Planungen, Bauleitpläne

hier offen: informell: Zukunftswerkstatt, öffentliche Diskussion
formell: Öffentlichkeitsbeteiligung bei Bauleitplänen

Szenario III: Bauplanung, informelle Verfahren

Schutzbedarfe:

Verfügbarkeit:	normal
Integrität:	hoch (andernfalls Manipulationsvorwurf)
Vertraulichkeit:	normal
Transparenz:	hoch (andernfalls Manipulationsvorwurf)
Nicht-Verkettbarkeit:	hoch (Sicht nach außen)
Intervenierbarkeit:	normal

Szenario III: Bauplanung, formelle Verfahren

Schutzbedarfe:

Verfügbarkeit:	hoch
Integrität:	hoch
Vertraulichkeit:	hoch
Transparenz:	hoch
Nicht-Verkettbarkeit:	normal
Intervenierbarkeit:	normal

Szenario IV: Parteiarbeit

Szenario: Parteiarbeit

Anzahl der Teilnehmer: 10.000

Betreiber der Plattform: Partei; Dienstleister involviert

Gegenstände: Erstellung von Meinungsbildern, Anträgen, Abstimmungen

hier offen: informell / formell (Parteitagsbeschlüsse?)

Szenario IV: Parteiarbeit

Schutzbedarfe:

Verfügbarkeit:	hoch
Integrität:	hoch
Vertraulichkeit:	?
Transparenz:	hoch
Nicht-Verkettbarkeit:	?
Intervenierbarkeit:	hoch

Funktionsbeispiele und Gestaltungsvorschläge

Gestaltungsvorschläge: Nutzerkonten

- Klarnamen(zwang) in Abhängigkeit von Zweck möglich
- meist pseudonyme Nutzung prinzipiell möglich (durch Entkopplung von Nutzerkonto und Identität)
- auch ohne Aufdeckung der bürgerlichen Identität denkbar, z. B. neuer Personalausweis: pseudonyme Zertifikate, Prüfung von Gruppenberechtigungen (Anwohner ja/nein)
- zu klären: nur ein Konto pro Person? Wie überprüft? („Sockenpuppen“)
- anonyme Nutzung:
  falls kein Reputationsaufbau => keine sinnvolle Delegation
- Löschung muss möglich sein (Intervenierbarkeit)

Gestaltungsvorschläge: Nutzerkonten II

Nicht-Verkettbarkeit:

- Pseudonymwechselmöglichkeit wünschenswert (unterbricht Reputation => Nicht-Verkettbarkeit)
- Nachvollziehbarkeit von Pseudonymwechseln: teilweise sinnvoll. Für wen nachvollziehbar? Wie leicht?
- denkbar: themenindividuelle Pseudonyme bei einem Nutzerkonto
- bei Mehrmandantenbetrieb:
  - mandantenspezifische Nutzerkontenverwaltung sinnvoll (schränkt aber „Single-Sign-on“ ein)
  - häufig E-Mail-Adresse als mandantenübergreifender Identifier (Verkettbarkeit) => klare Abschottung zwischen Mandanten erforderlich

Gestaltungsvorschläge: Integrität

- Anwendungs-Administratoren sind „sehr mächtig“ (Konfiguration, Quoren, Nutzerverwaltung)
  => Anwendungs-Administration ist (ggf. in der Datenbank) zu protokollieren und zu kontrollieren
- Datenbank-Administratoren sind „allmächtig“
  => Datenbank-Administration ist *außerhalb* der Datenbank zu protokollieren und zu kontrollieren
- Entkopplung von Anwendungs-, Datenbank- und Plattform-Administration („Gewaltenteilung“)
- je nach Integritätsanforderung:
  Umfang, Aufbewahrungsdauer und Schutz der Protokolldaten im Hinblick auf alle Schutzziele

Aspekte der Vertraulichkeit: Abstimmungen

- zahlreiche Wahl- und Abstimmungsverfahren:
  - Abstimmung per Handzeichen
  - namentliche Abstimmung
  - geheime Abstimmung: Stimmzettel + Wahlurne
  - Briefwahl
- jeweilige Vor- und Nachteile für die Überprüfbarkeit von: Stimmberechtigung, Stimmabgabe (ja/nein/wieviele), Stimme
- Vertraulichkeit gegenüber wem: Gruppe? Öffentlichkeit? Veranstalter?
- Delegation: legitimes Interesse, dass Abstimmungsverhalten nachverfolgbar ist?
- Unterschied zwischen „jetzt für die Gruppe nachvollziehbar“ und „für alle Zeiten dokumentiert“

Gestaltungsvorschläge: Vertraulichkeit

- Administratoren: siehe „Integrität“
- zu klären:
  Ist die Plattform
  - öffentlich zugänglich?
  - gruppenintern zugänglich?

  Welche Nutzeraktivitäten sollen für wen offen liegen:
  - Texte und Beiträge zu Diskussionen?
  - Delegationen (An wen wurde delegiert? Von wem wurde delegiert?)
  - Abstimmungsverhalten („Delegierter“ als Überbringer der eigenen Stimme oder mit Entscheidungsvollmacht?)

Gestaltungsvorschläge: Nicht-Verkettbarkeit

- sinnvolle Einrichtung von Nutzerkonten (namentlich, pseudonym, nur ein Konto pro Nutzer, ...)
- Funktionalitäten begrenzen:
  Ist beispielsweise eine Übersicht über alle Bewertungen/Diskussionsbeiträge erforderlich? Für wen?

- Löschung von Daten (sofern vorhanden) nach festgelegten Fristen:
  - Teilnahme an Abstimmungen
  - Stimmen
  - Delegationen

Gestaltungsvorschläge: Transparenz

- keine irreführenden Angaben über Urheber von Beiträgen
- Funktionalität muss durchschaubar sein (insbesondere für Delegationen)
- Nachverfolgung/Historisierung von Textbeiträgen und Kommentierungen sinnvoll
- Aufbewahrungsdauern, Archivierung, Übermittlungen festlegen und bekannt geben
- Protokollierung administrativer Tätigkeiten
- Bereitstellung von Datenbank(teil)en für externe Überprüfung (Download): schwierig:
  - komplette Anonymisierung schwierig, da Korrelationen möglich (z.B. Zeitvergleiche, Schreibstilvergleiche)
  - Löschung später nicht mehr möglich
- Beispiel für gegenseitige Beeinflussung der Schutzziele Transparenz und Nicht-Verkettbarkeit

Gestaltungsvorschläge: Verfügbarkeit

- Maßnahmen abhängig von Verfügbarkeitsanforderungen
- Verfügbarkeitsanforderungen anhängig vom Einsatzszenario
- ggf. rechtliche Auswirkungen bei Ausfall
- typische Anforderungen:
  - gespeicherte Inhalte verfügbar
  - Online-Zugang verfügbar
- ebenso: abhängig von Ausweichmöglichkeiten (z.B. Papierabstimmung, manuelle Verfahren)

Gestaltungsvorschläge: Intervenierbarkeit

- Nutzerkonten müssen sperr- und löschbar sein
  =>Umfang der zu löschenden Daten festlegen!
- Delegationen: müssen vom Delegator leicht änderbar sein
- auch Abweichungen von der Delegation im Einzelfall („hier stimme ich selbst“) sollten möglich sein
- zu klären: sollen Delegationen abgelehnt werden können? Dies würde erfordern, dass Delegierte Delegatoren erkennten und unterscheiden können
- Auskunftsrechte:
  für eigene Beiträge relativ leicht umsetzbar

Schlussfolgerungen

- Anforderungen sind situationsabhängig (Beispiele in den verschiedenen Szenarien)
- technische Grundlagen von Beteiligungssystemen: wichtig, da große Informationsdichte und Einflussmöglichkeiten an zentraler Stelle
- andere Aspekte können bei der Nutzung („zur Laufzeit“) festgelegt werden:
  - durch Konfiguration der Systeme
  - durch Entkopplung bei der Vergabe von Nutzerkennungen

Vielen Dank für Ihre Aufmerksamkeit.

Haben Sie noch Fragen?

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
Holstenstraße 98
24103 Kiel
Tel.: 0431-988 1200

mail@datenschutzzentrum.de
www.datenschutzzentrum.de