brain-SCC
PORTALLÖSUNGEN

# Datenschutz

## Online-Dienste im brain- GeoCMS aus dem Blickwinkel des Datenschutzbeauftragten

Mit Antworten von Marcus Schilling

MGID Mitteldeutsche Gesellschaft für Informationssicherheit und Datenschutz mbH

Merseburg, 03.09.2020

brain-SCC
PORTALLÖSUNGEN

# Datenfelder

Was muss aus Sicht des Datenschutzes bei der Auswahl der zu erfassenden Datenfelder beachtet werden?

- es dürfen nur die Daten abgefragt werden, die für den jeweiligen Antrag erforderlich sind
- jede Erhebung personenbezogener Daten bedarf einer Rechtsgrundlage (Art. 6 DSGVO)
  - es dürfen nur die Daten abgefragt werden, die für den jeweiligen Antrag erforderlich sind
  - jede Erhebung personenbezogener Daten bedarf einer Rechtsgrundlage (Art. 6 DSGVO)
  - Einwilligung der Person (Art. 6 Abs. 1 lit. a) DSGVO)
  - Vertrag mit der betroffenen Person (Art. 6 Abs. 1 lit. b) DSGVO)
  - Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen (Art. 6 Abs. 1 lit. c) DSGVO)
  - Verarbeitung liegt im öffentlichen Interesse oder erfolgt in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e) DSGVO)
  - berechtigtes Interesse, welches dem Schutzinteresse des Betroffenen überwiegt (Art. 6 Abs. 1 lit. f) DSGVO)

- Grundsätze der DSGVO (Art. 5 DSGVO) sind einzuhalten:
  - Rechtmäßigkeit der Verarbeitung, Transparenz
  - Datenerhebung muss dem Zweck angemessen sein ("Datenminimierung")
  - Daten müssen unter gewährleistung eines angemssenen Sicherheitsniveaus verarbeitet werden
- "Verantwortlicher" ist die jeweilige Kommune; "Betroffener" ist jeweils der Antragsteller

brain-SCC
PORTALLÖSUNGEN

# Pflichtfelder und optionale Datenfelder

Welchen Einfluss hat diese Charakterisierung auf die Datenschutzerklärung?

- beide Daten unterliegen den gleichen Regeln der DSGVO (Rechtsgrundlage, Verarbeitungsgrundsätze, Löschfristen, ...)
- Verarbeitungsgrundlage ist aber ggf. unterschiedlich → freiwillige Angaben meist basierend auf Einwilligung (z.B. Titel im Namen für bessere Anrede im Schriftverkehr)
- Auf freiwillige Angaben ist jeweils explizit hinzuweisen. Zusätzlich ist darzustellen, wozu freiwillige Angaben erhoben werden und welche Folgen die Nichtbereitstellung hat (in der DSE oder in kurzen Erklärtexten auf dem Eingabeformular)

brain-SCC
PORTALLÖSUNGEN

# Erfassen von Anrede oder Geschlecht der Antragstellenden Person

## Sind beide Angaben gleich zu behandeln?

- Nein, diese Daten sind nicht gleich zu behandeln, solange die Frage der Anrede nicht darauf abzielt, das Geschlecht zu ermitteln, d.h. es muss grundsätzlich möglich sein, eine Anrede frei (unabhängig vom Geschlecht) auszuwählen
- Frage nach der Anrede sollte freiwillig sein
- Bsp.: Anrede für Formulierung in E-Mails (freie Auswahl) vs. Anrede für klinische Studien als "Ersatz" für die Angabe des Geschlechts

brain-SCC
PORTALLÖSUNGEN

# Datenschutzerklärung

## Welche Punkte müssen beim Erstellen einer Datenschutzerklärung berücksichtigt werden?

- Pflichtangaben:
  - Verantwortliche Stelle
  - Zwecke der Verarbeitung
  - Verarbeitete Daten und Rechtsgrundlage der Verarbeitung → bei Formularen aus dem jeweiligen Formular ersichtlich
  - Dauer der Verarbeitung, Geplanter Zeitpunkt der Löschung
  - Empfänger personenbezogener Daten
  - Aufklärung über die Rechte der betroffenen Personen wie Auskunft, Berichtigung, Löschung, Widerspruch, ... (Art. 15 - 22 DSGVO)
  - Kontaktdaten für Geltendmachung dieser Rechte (meist DSB, ggf. Datenschutzkoordinator der verantwortlichen Stelle selbst)
  - Geplante Übermittlung der Daten ins Ausland
  - Geplante Automatisierte Entscheidungsfindung

- Weitere Details abhängig von der Verarbeitung
- Grundsatz: Verarbeitung muss transparent und in klarer und verständlicher Weise dargestellt werden (Art. 12 DSGVO)

brain-SCC
PORTALLÖSUNGEN

# Datenschutzerklärung

Zu welchen Zeitpunkten der Benutzung eines Serviceportals müssen Nutzer einer Datenschutzerklärung zustimmen?

- Einer DSE muss nicht zugestimmt werden → käme sonst einer Einwilligung gleich, der jederzeit (möglicherweise rückwirkend) widersprochen werden könnte
- Stattdessen Bestätigung der Kenntnisnahme als Nachweis für den Verantwortlichen
- Information muss stets vor der ersten Datenerhebung erfolgen
- In Bezug auf Serviceportal:
  - DSE muss jederzeit im Portal zugänglich sein (in Bezug auf Verarbeitungen durch das Portal)
  - Kenntnisnahme sollte im Registrierungsprozess bestätigt werden
  - spezielle (antragsbezogene) Informationen sind im Antragsprozess zur Verfügung zu stellen (z.B. abweichende verantwortliche Stelle, Empfänger, Speicherfristen, ...) (in Bezug auf Verarbeitung durch die Antragsstellung)

brain-SCC
PORTALLÖSUNGEN

# Datenschutzerklärung

Ist für jeden Online-Dienst eine eigene Datenschutzerklärung notwendig – und wenn ja in welchem Umfang?

- Um Transparenz zu gewährleisten, muss jeder Online-Dienst eine passende DSE haben. Werden mehrere gleichartige Dienste betrieben, kann diese ggf. auch zu einer Erklärung zusammengefasst werden
- passende DSE muss aber stets erreichbar sein
- In Bezug auf einzelne Dienste des Serviceportals:
  - Es gilt eine allgemeine DSE des Portalbetreibers (Verantwortlicher, Verarbeitungen auf der Webseite, Empfänger von Daten beim Browsen auf der Webseite, etc.)
  - abweichende Regelungen können bei den einzelnen Dienstleistungen separat angegeben werden (abweichende Empfänger von Daten, abweichende Speicherfristen, etc.)

brain-SCC
PORTALLÖSUNGEN

# Datenspeicherung

Wie lange dürfen Daten im Serviceportal für Sachbearbeiter gespeichert werden?

- Eine Verarbeitung (d.h. auch Speicherung) der Daten darf solange erfolgen, wie es für den Zweck erforderlich ist, für den sie erhoben wurden
- entfällt der Zweck (egal, ob Erfüllung oder Wegfall aus anderen Gründen), muss die Verarbeitung beendet werden
- eine Löschung muss dann erfolgen, sobald geltende Löschfristen abgelaufen sind
- für den Zeitraum zwischen Zweckentfall und Ablauf der Löschfrist sind Daten zu archivieren und der Zugriff darauf einzuschränken

brain-SCC
PORTALLÖSUNGEN

# Zuschauerfragen

Wo gibt es verlässliche Templates für eine Datenschutzerklärung?

- Verlässliche Templates kann es nicht geben, da die Verarbeitungen stets unterschiedlich gestaltet sind.
- Datenschutzgeneratoren bieten in Bezug auf bestimmte Verarbeitungen Texte, die häufig richtig sind

  → Problem: Generatoren benötigen jemanden, der den Generator korrekt konfiguriert
- Die meisten generierten Texte sind entweder unvollständig oder enthalten zu viele Verarbeitungen, die nicht stattfinden → rechtswidrig
- Hilfe ist erhältlich vom eigenen oder externen Datenschutzbeauftragten, bei Fragen zu bestimmten Verarbeitungen durch Dienstleister ggf. auch bei DSB der Dienstleister
- Grundsätzlich gilt es, für jede Verarbeitung die Angaben aus Artikel 13 DSGVO in sinnvoller und verständlicher Weise zur Verfügung zu stellen

brain-SCC
PORTALLÖSUNGEN

# Zuschauerfragen

Wenn eine Datenschutzerklärung 60 Seiten beträgt, weil in ein Portal so viele Dienste eingebunden hat, liest das noch jemand außer Anwälte?

- eine 60 seitige DSE ist grundsätzlich unzumutbar und verstößt gegen die Grundsätze der Verständlichkeit und Transparenz und wird vermutlich nicht vollständig gelesen
- bei so vielen eingebundenen Diensten sollte man sich folgende Fragen stellen:
  - als Nutzer: Sollte diese Webseite wirklich genutzt werden?
  - als Betreiber: Benötige ich wirklich all diese Dienste?
- Gerade bei längeren DSE kann man eine Kurzübersicht über die Verarbeitungen mit den wichtigsten Fragen der eigentlichen DSE voranzustellen: Wer erhebt welche Daten zu welchen Zwecken für wie lange und welche Rechte und Entscheidungsmöglichkeiten hat der Betroffene? Dies sollte in Stichpunkten auf eine DIN A4-Seite passen.

brain-SCC
PORTALLÖSUNGEN

# Zuschauerfragen

Ist die Verschlüsselung von besonders schützenswerten personenbezogenen Daten (bspw. Kinderdaten) verpflichtend im Sinne einer TOM oder kann darauf auch verzichtet werden? Ich meine damit keine Transportverschlüsselung, sondern die Speicherung. Bzw. Archivierung

- TOMs (Technische und Organisatorische Maßnahmen) müssen einen angemessenen Schutz gewährleisten
- Wo nötig oder mit nicht übermäßigem Aufwand möglich, sollte eine Verschlüsselung eingesetzt werden
- Notwendigkeit ist über eine Risikoabschätzung zu ermitteln
- Bei besonders schützenswerten Informationen wird die Risikoabschätzung meist zugunsten der Verschlüsselung ausfallen, gerade bei mobilen Geräten
- Es kann noch andere Wege der Einschränkung des Zugriffes auf besonders schützenswerte Daten geben, bei Diebstahl von Datenträgern hilft aber nur die Verschlüsselung
- Achtung! Auch verschlüsselte personenbezogene Daten bleiben personenbezogene Daten im Sinne der DSGVO!

brain-SCC
PORTALLÖSUNGEN

# Zuschauerfragen

Ein weiterer Grundsatz ist die datenschutzfreundliche Voreinstellung. Wir fragen nur Daten ab die wir brauchen - andere Abfragen, also freiwillige Angaben müssen gekennzeichnet sein. Was bedeuten würde, wir würden freiwillige Angaben kennzeichnen?

- Datenschutzfreundliche Voreinstellungen beziehen sich auf Konfigurationsmöglichkeiten für Nutzer → diese sollen ohne Eingriffserfordernis des Nutzers so voreingestellt sein, dass die datensparsamste Konfiguration getroffen wird.
- Bei der Erhebung freiwilliger Daten geht es um den Grundsatz der Datenminmierung (Art. 5 (1) c) DSGVO) und die rechtmäßige Datenverarbeitung (Art. 5 (1) a) DSGVO bzw. Art. 6 (1) DSGVO).
- Wenn keine Notwendigkeit für die Erhebung von Daten gegeben ist, sondern diese aus reinem Servicegedanken (z.B. für gezieltere Anreden) erhoben werden, sollte auf die Erhebung verzichtet werden oder diese Angaben müssen freiwillig sein.
- Freiwillige Angaben müssen klar getrennt von erforderlichen Angaben erhoben werden
- In der DSE ist darauf hinzuweisen, für welchen Zweck freiwillige Angaben erhoben werden und welche Folgen die Nichtbereitstellung der Daten hat.

brain-SCC
PORTALLÖSUNGEN

# Zuschauerfragen

Empfehlen Sie eine Versionierung für Datenschutzerklärungen und wenn ja welche Tool könnten Sie empfehlen?

- Es reicht, das Datum der letzten Aktualisierung der Datenschutzerklärung auf der Webseite zu kennzeichnen
- Für registrierungspflichtige Dienste empfiehlt es sich, auf Änderungen in der DSE für Bestandskunden hinzuweisen
- Eine Versionierung hilft nur zum Nachweis der korrekten Informationen zu einem bestimmten Zeitpunkt im Falle eines Rechtsstreites oder Beschwerde einer betroffenen Person
- Wir nutzen zur Versionierung Subversion (SVN). Eine konkrete Empfehlung habe ich aber nicht.

brain-SCC
PORTALLÖSUNGEN

# Zuschauerfragen

Gibt es derzeit irgendeine Möglichkeit eine Webstatistik ohne Einwilligung des Nutzers [zu erstellen]? Bspw. über alternative Methoden um Nutzerprofile zu erstellen ohne Cookies.

- Einwilligungen und Informationen über ein Cookie-Banner sind nicht abhängig von Cookies, sondern davon, ob personenbezogene Daten verarbeitet (erhoben, gespeichert, übertragen, ...) werden.
- Eine Einwilligung ist immer dann erforderlich, wenn personenbezogene Daten verarbeitet werden, die nicht für den Betrieb der Webseite unbedingt erforderlich sind (Nutzertracking, Werbung, etc.)
- Die anonymisierte, statistische Auswertung von Serverlogs auf dem eigenen System (ohne Übertragung an Dritte) kann aber ohne eine Einwilligung durchgeführt werden. Das Analyse-Tool Matomo lässt sich so konfigurieren, dass lediglich solche Serverlogdaten in anonymisierter Form zu Webstatistiken aufbereitet werden. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) nutzt derzeit selbst Matomo ohne eine Einwilligung, siehe https://www.lda.bayern.de/de/datenschutz.html. (Stand 09/2020).

# Vielen Dank für Ihre Aufmerksamkeit!

**Kontakt**
brain-SCC GmbH | Tel. 03461 2599510
www.brain-scc.de | info@brain-scc.de