

Kurzgutachten für die Rezertifizierung des Produkts „TGPopen“ der 1&1 Internet AG nach der DSAVO Schleswig-Holstein

1. Einleitung

Rechtsgrundlage der Gütesiegelvergabe in Schleswig-Holstein ist § 4 Abs. 2 des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG-SH). Satz 1 fordert von öffentlichen Stellen des Landes Schleswig-Holstein, vorrangig Produkte einzusetzen, „deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde“. Auf Basis des Satzes 2 wurde die Landesverordnung über ein Datenschutzaudit (DSAVO) erlassen. Diese regelt die Erteilung des Gütesiegels des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Produkte die den Vorschriften über den Datenschutz und die Datensicherheit des Landes Schleswig-Holstein genügen, erfüllen in der Regel auch die Anforderungen des Bundesdatenschutzgesetzes. Insoweit ist das Gütesiegel ein auch für Wirtschaftsunternehmen relevantes Kriterium bei der Auswahl von Produkten. Gemäß § 1 Abs. 2 der DSAVO sind IT-Produkte im Sinne der Verordnung „Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen geeignet sind.“

Mit dem Produkt „TGPopen“ in der vorliegenden Version 2.0 können auch Dienststellen des Landes Schleswig-Holstein den Online-Nutzer/inne/n zielgerichtet Inhalte mit der für die Nutzer/innen höchsten Relevanz ausliefern. Somit ist das Produkt zur Nutzung durch öffentliche Stellen geeignet. Mit dem vorliegenden Gutachten wird überprüft inwieweit das Produkt „TGPopen“ den Vorschriften über den Datenschutz und die Datensicherheit genügt.

2. Zeitpunkt der Prüfung

24.10.2011 – 17.11.2013

3. Grund der Rezertifizierung – Änderungen des Produkts

Die Rezertifizierung des Produkts TGPopen war zum einen wegen des Ablaufs der Zertifizierung und zum anderen wegen Änderungen am Produkt erforder-

lich geworden. Hinzu kam, dass Ende Mai 2011 die Frist zur Umsetzung der Anforderungen aus der Richtlinie 2009/136/EG über den [Schutz personenbezogener Daten](#) in der elektronischen Kommunikation (sogenannten Cookie-Richtlinie oder auch E-Privacy-Richtlinie) abgelaufen ist. Nach einer Zeit der Rechtsunsicherheit wurde während des Rezertifizierungsverfahrens seitens des ULD entschieden, dass zu zertifizierende Produkte die Anforderungen umsetzen müssen.

4. Adresse des Antragstellers

United Internet Media AG
Brauwerstr. 48
76135 Karlsruhe

5. Adresse des Sachverständigen (technischer und rechtlicher Gutachter)

Dipl. Informatiker Werner Hülsmann
Datenschutzconsulting.info
Am Briel 49 – 78467 Konstanz
Tel.: 07531 / 380 08 02 oder 0177 / 28 28 681
E-Mail: wh@d-s-c.info – URL: <http://www.d-s-c.info>

6. Kurzbezeichnung:

TGPopen ist ein IT-Produkt für Vermarkter und Betreiber von Telemediendiensten (Websites) zur Steuerung von zielgruppenspezifischen Inhalten, wie z.B. Werbeeinblendungen. Durch den Einsatz des Produkts wird es dem Vermarkter oder dem Betreiber der Website möglich, den Online-Nutzern zielgerichtet Werbung oder andere Inhalte mit der für sie höchsten Relevanz auszuliefern. Die Ansprache erfolgt mithilfe ausgefeilter analytisch-statistischer Prognose-techniken (Hypervariate Similaritätsmodellierung™) auf Basis von pseudonymisierten Informationen. Die konkrete Einbindung eines Fragebogendienstleisters ist nicht Bestandteil der Begutachtung.

7. Detaillierte Bezeichnung:

TGPopen ist eine Dienstleistung für die zielgruppenspezifische Auslieferung von digitalen Inhalten wie z.B. Werbekampagnen. Dazu werden auf Basis einer pseudonymen Identität (Cookie) Browser-Nutzungsprofile der Online-Nutzung erstellt, daraus Zielgruppenzugehörigkeiten prognostiziert und diese über den

Browser einem Adserver-System oder anderen Telemediendiensten zur Verfügung gestellt. Der Adserver und die Telemediendienste selbst sind nicht Bestandteil von TGPopen.

Die Identität des Browsers¹ wird im Prozess von TGPopen durch ein HTTP-Cookie repräsentiert. Der Wert des Cookies wird durch einen geeigneten Computeralgorithmus erzeugt. Dieser Wert selbst enthält keine Daten des Online-Nutzers, mit denen sich ein Personenbezug herstellen lässt.

Zur Sicherstellung der Pseudonymisierung werden alle Vermarkter und Portal-Betreiber, die TGPopen nutzen wollen, vertraglich verpflichtet, einen zur Verfügung gestellten unabhängigen IP-Anonymizer-Dienst zu nutzen. Dieser dient dazu, den Datenaustausch vom Browser zum TGPopen-Dienstleister bezüglich der IP-Adresse zu filtern. Der TGPopen-Dienstleister hat keinen Zugriff auf die Datenverarbeitungssysteme des IP-Anonymizer-Dienstes und damit auch nicht auf die IP-Adressen.

Die Bildung der Browser-Nutzungsprofile erfolgt mittels Beobachtung von Seitenabrufen durch die Browser (Webtracking). Dazu muss auf allen vermarkteten Webseiten im HTML-Code ein Abruf einer sehr kleinen, unsichtbaren Grafik von einem Server des TGPopen-Dienstleisters ausgelöst werden. Beim Abruf dieses Objekts überträgt der Browser Informationen, die den Seitenabruf charakterisieren. Neben der pseudonymen Identität des Cookies ist dies eine Klassifikation des Inhalts der besuchten Seite. Der TGPopen-Dienstleister zeichnet diese Abrufe auf und aggregiert sie mittels eines Hadoop-Frameworks zu statistischen Informationen bezogen auf die Identität des Browsers.

Die Browser-Nutzungsprofile fassen als Aggregat maximal den Beobachtungszeitraum der letzten acht Wochen zusammen. Bei Inaktivität des Benutzers über einen Zeitraum von mehr als acht Wochen wird sämtliche Information

¹ Es wird an dieser Stelle von einer Browseridentität und nicht von der Nutzeridentität gesprochen, da es grundsätzlich möglich ist und in der Praxis nicht selten vorkommt, dass mehrere Nutzer sich mit der gleichen Browseridentität im Web bewegen. Dies ist dann der Fall, wenn – beispielsweise im privaten Bereich – auf die Einrichtung von unterschiedlichen Benutzerkonten für verschiedene Nutzer eines PCs verzichtet wird.

des Browser-Nutzungsprofils von TGPopen verworfen und dieses Cookie nicht weiter verwendet.

Die Umwandlung von Browser-Nutzungsprofilen in Zielgruppenzugehörigkeiten erfolgt durch Anwendung von Prognosemodellen, welche aus den statistischen Kenngrößen der Online-Nutzung auf Zielgruppenzugehörigkeiten mit Bezug auf eine pseudonymisierte Browser-Identität schließen lassen. Die Zielgruppenzugehörigkeiten lassen sich unter anderem in soziodemografische Eigenschaften, Affinitäten zu Themengebieten, Zugehörigkeiten sowie einer geographischen Zuordnung zu den Nielsen-Gebieten zu einer Reihe spezieller Zielgruppen etc. einteilen. Bei der Zuordnung werden keine Gruppen gebildet, bei denen schon die Zugehörigkeit zu diesen Gruppen eine sensible Information darstellt (wie z.B. schwanger, etc.).

Die Prognose-Modelle selbst werden von Zeit zu Zeit dadurch verfeinert, dass zufällig ausgewählten Online-Nutzern beim Besuch einer durch TGPopen vermarkteten Website eine Online-Befragung präsentiert wird, an der freiwillig teilgenommen werden kann. Die Antworten der Nutzer sind ebenfalls auf das Cookie von TGPopen bezogen. Durch Korrelationsanalyse der gegebenen Antworten mit den statistischen Informationen des Browser-Nutzungsprofils derselben pseudonymisierten Browser-Identität wird eine Verbesserung der Prognosequalität der Modelle erreicht. Die konkrete Einbindung eines Fragebotendienstleisters ist nicht Gegenstand der Begutachtung.

Die Bereitstellung der Zielgruppenzugehörigkeiten erfolgt mittels Abruf der Zielgruppenmerkmale durch den Browser im Rahmen eines Seitenabrufs. Das ausliefernde System, der Zielgruppen-Server, ist Bestandteil von TGPopen. Beim Abruf der Zielgruppenmerkmale ist das Cookie des Browsers bekannt und dient dem Zielgruppen-Server als Schlüssel. Die Zielgruppenzugehörigkeiten sind in Abstimmung zwischen TGPopen-Dienstleister und dem Vermarkter oder Website-Betreiber so verschlüsselt, dass nur dieser den Inhalt der Zielgruppenmerkmale nutzen kann. Dadurch wird einem Missbrauch des Zielgruppen-Servers von TGPopen vorgebeugt.

Zur Umsetzung der Anforderungen aus Art 5 Abs. 3 der sogenannten E-Privacy-Richtlinie (oder „Cookie-Richtlinie“) wird in der begutachteten Version die Möglichkeit angeboten eine Opt-In-Variante zu benutzen, d.h. ein Tracking wird nur vorgenommen, wenn durch ein aktives Opt-In des Nutzers ein auswertbares Cookie gesetzt wird. Dieses Opt-In kann jederzeit widerrufen werden, in diesem Fall wird ein Opt-Out-Cookie gesetzt, dessen Inhalt nur aus der Opt-Out-Markierung besteht. Mit Setzen dieses Cookies wird die Browser-Identität sofort und dauerhaft unkenntlich gemacht. Dadurch können in TGPopen ab sofort keine Browser-Nutzungsprofile mehr erstellt werden, und die Steuerung der Auslieferung zielgerichteter Werbung und anderer Inhalte wird unmittelbar unterbunden. Das bereits erstellte Browser-Nutzungsprofil und die Zielgruppenzugehörigkeiten werden sofort unbrauchbar und automatisch durch den technischen Prozess verworfen.

TGPopen stellt auch einen Opt-Out-Dienst bereit, der von den vermarkteten Portalen aus angesprochen werden kann. Benutzt ein Endanwender diesen Opt-Out-Dienst, wird das oben beschriebene Opt-Out-Cookie gesetzt.

Die Do-Not-Track-Option (DNT) der gängigsten Browser wird durch eine entsprechende Konfiguration ebenfalls berücksichtigt.

In der aktuellen Version erfolgt das Auskunftersuchen des Nutzers auf manuellen Weg. D.h. der Nutzer kann unter Angabe seiner Cookie-ID über die auf der zur Verfügung gestellten Infoseite angegebenen E-Mail-Adresse erfahren, für welche Themengebiete der Nutzer (bzw. sein Nutzungsverhalten) erachtet wird. Im zweiten Quartal 2014 soll diese manuelle Beauskunftung durch eine webbasierte Auskunft ersetzt werden. Dann reicht ein Klick auf den Link zum „Themenmonitor“ und der Nutzer erhält die zu seinem Nutzungsverhalten zugeordneten Themengebiete in der Abstufungen hoch, mittel und niedrig. Sollten (wegen nicht erteiltem oder widerrufenem Opt-In) keine Daten vorliegen, wird der Nutzer auch hierüber informiert.

7.1. Tools, die zur Herstellung des IT-Produkts verwendet wurden

- Programmiersprachen: JavaScript, Java, SQL, Python, AWK und andere
- Key Value Store: Hadoop
- Webserver: Apache
- Datenbanken: MySQL

7.2. Zweck und Einsatzbereich

Zweck und Einsatzbereich des Produkts TGPopen ist die relevanzgesteuerte Einblendung von Werbung und anderen Unterinhalten bei der Auslieferung von Inhalten in Telemediendiensten (Websites).

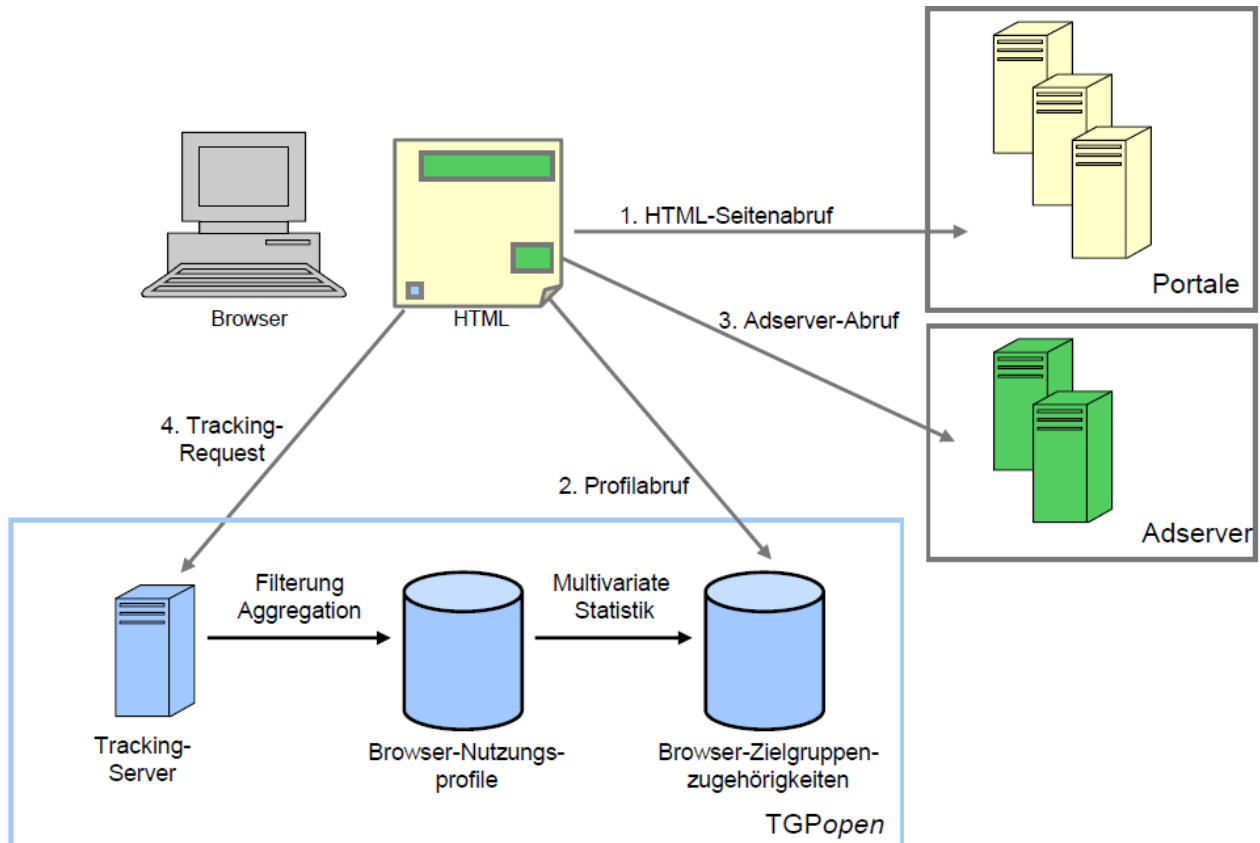
Grundsätzlich ist das Produkt auch bei allen Behörden und sonstige öffentlichen Stellen des Landes Schleswig-Holstein einsetzbar, sofern sie über das Medium Internet/World Wide Web Telemediendienste erbringen und deren Inhalte zielgruppenspezifisch ausprägen wollen.

7.3. Modellierung des Datenflusses

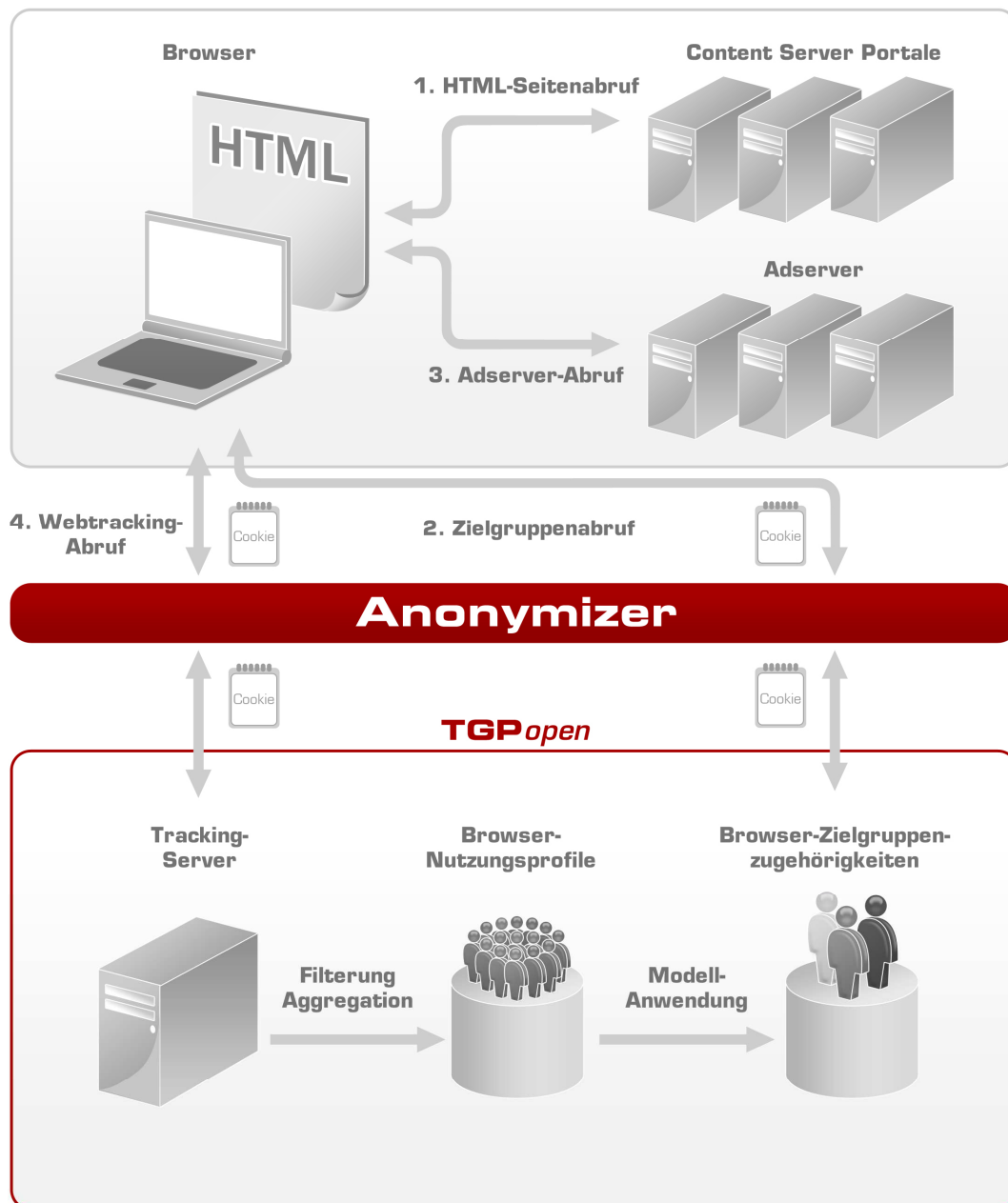
Der Abruf des Inhalts einer Website, die mit TGPopen vermarktet wird, durch einen Internet-Browser setzt sich mindestens aus vier wesentlichen Datenabrufen zusammen:

1. Abruf des HTML-Codes des Seiteninhalts vom Content-Server eines Portals. Im HTML-Code sind alle folgenden Unteraufrufe enthalten. Dieser technische Dienst ist nicht Teil von TGPopen.
2. Abruf der kodierten Browser-Zielgruppenzugehörigkeit vom Zielgruppen-Server des TGPopen-Dienstleisters unter Übermittlung des Cookies. Dieser Abruf wird an den IP-Anonymizer gerichtet, der eine Weiterleitung an den Server des TGPopen-Dienstleisters unter Herausfilterung der IP-Adresse vornimmt.
3. Abruf von Online-Werbung oder anderer gesteuerter Inhalte unter Vorlage der kodierten Browser-Zielgruppenzugehörigkeit von einem Adserver oder anderen Telemediendienst, die nicht Teil von TGPopen sind.

4. Abruf der Webtracking-Grafik vom Webtracking-Server des TGPopen-Dienstleisters unter Übermittlung des Cookies und der Content-Klassifikation der abgerufenen Seite. Dieser Abruf wird an den IP-Anonymizer gerichtet, der eine Weiterleitung an den Server des TGPopen-Dienstleisters unter Herausfilterung der IP-Adresse vornimmt.



Schematische Darstellung eines Websiteaufrufs mit Profilabruf

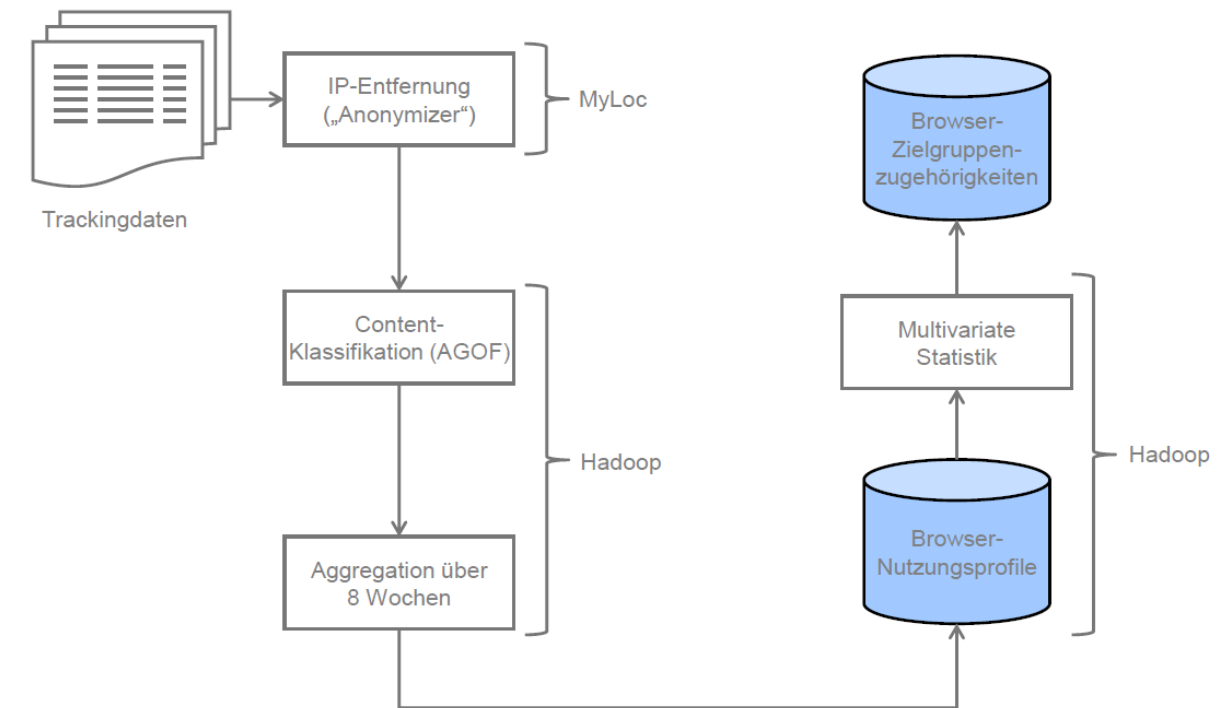


Darstellung der Einbindung des Anonymisierungsdienstleisters

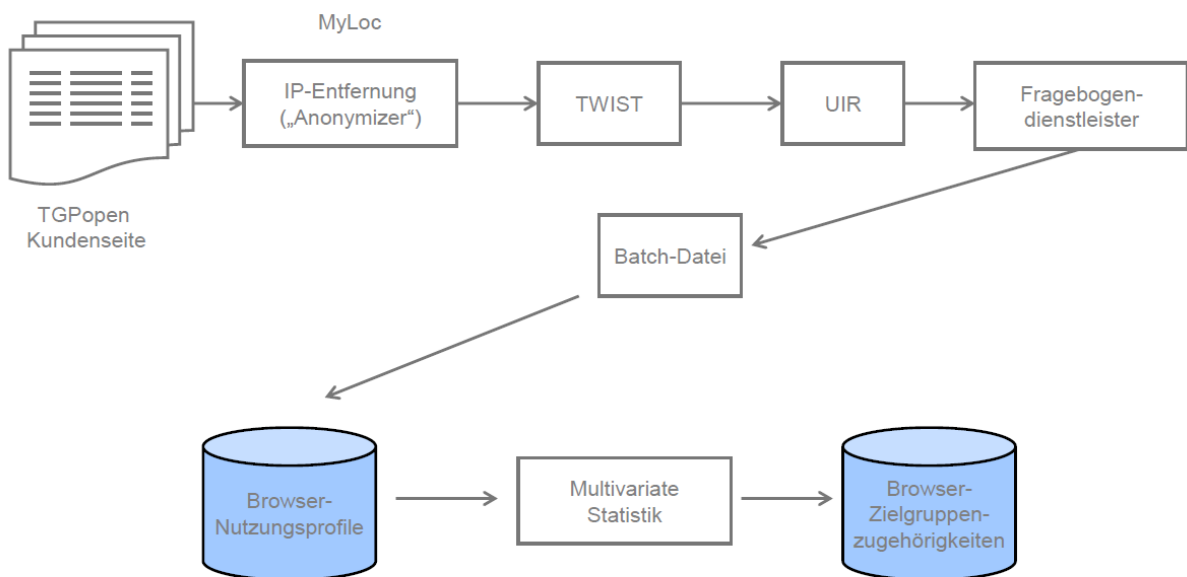
Innerhalb des TGPopen-Systems finden nebenläufig zum oben beschriebenen Online-Prozess zwei grundlegende Datenverarbeitungsschritte statt:

1. Erstellung von Browser-Nutzungsprofilen durch Filterung und Aggregation der Webtracking-Informationen
2. Ermittlung von Browser-Zielgruppenzugehörigkeiten durch Modellanwendungen (Hypervariate Similaritätsmodellierung™) auf die Browser-Nutzungsprofile und Bereitstellung auf dem Zielgruppen-Server

7.3.1. Anonymisierung, Klassifikation und Aggregation der Nutzungsdaten



7.3.2. Datenfluss bei der Fragebogennutzung



Auch beim Einsatz des Fragebogens wird der Anonymisierungsdienst genutzt, so dass auch der externe Fragebogendienstleister nicht die Original-IP-Adresse des Nutzers erhält.

8. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog Version 1.2

9. Zusammenfassung der Prüfungsergebnisse

Das Produkt TGPopen kann in datenschutzrechtlich zulässiger Weise von öffentlichen Stellen des Landes Schleswig-Holstein und im nichtöffentlichen Bereich dazu eingesetzt werden, um auf Telemediendiensten (Websites) zielgruppenspezifische Inhalte einzubinden. Die Anforderungen an den Datenschutz werden von dem Produkt in insgesamt vorbildlicher Weise erfüllt.

Es werden technische und organisatorische Maßnahmen getroffen, die eine Anonymisierung der IP-Adressen und damit eine Pseudonymisierung der Nutzer/innen sicherstellen. Die Anonymisierung der IP-Adressen erfolgt im Rahmen einer datenschutzrechtlich zulässigen Datenverarbeitung im Auftrag des jeweiligen Website-Betreibers, der die Dienste von TGPopen nutzt. Der Datenaustausch zwischen dem Browser des Nutzers und TGPopen erfolgt ausschließlich über den dazwischen geschalteten Anonymisierungsdienst. Dadurch ist sichergestellt, dass im Bereich von TGPopen zu keiner Zeit die IP-Adresse des Nutzers vorliegt.

Die Auswertung der Browser-Nutzungsinformationen durch das Produkt TGPopen erfolgt in ausschließlich pseudonymer Weise unter Zuhilfenahme von Cookies. Bei Nutzung der Opt-In-Option entspricht das Produkt der Anforderung aus Art 5 Abs. 3 der sogenannten E-Privacy-Richtlinie. Daher stellt die opt-in-Lösung in der Regel die einzusetzende Lösung dar.

Sofern die Opt-Out-Version genutzt wird, wird dem Endnutzer die Möglichkeit geboten, jederzeit durch Nutzung einer Opt-Out-Option der Auswertung seines Nutzungsverhaltens gemäß § 15 TMG zu widersprechen. Der Website-Betreiber, der TGPopen einsetzt, wird vertraglich verpflichtet, auf diese Opt-Out-Möglichkeit deutlich hinzuweisen. Die Opt-Out-Variante kann nur dann datenschutzkonform eingesetzt werden, wenn das Opt-In durch den TGPopen einsetzenden Websitebetreiber oder Vermarkter anderweitig sichergestellt wird.

Das pseudonyme Browser-Nutzungsprofil wird von TGPopen aufgrund analytisch-statistischer Modelle durch eine Zielgruppenzugehörigkeit ersetzt. Nur diese Zielgruppenzugehörigkeit wird über den Anonymisierungsdienst für die Einblendung zielgruppenrelevanter Inhalte an den Browser zurückgemeldet. Die Modellbildung und Abbildung der pseudonymen Browser-Nutzungsprofile auf die Zielgruppenzugehörigkeit erfolgen ebenfalls in datenschutzrechtlich zulässiger Weise. Die gelegentliche Befragung zufällig ausgewählter Nutzer/innen, die der Verbesserung der Modellbildung dient, erfolgt auf freiwilliger Basis ebenfalls in pseudonymer Form. Dabei wird der Fragebogendienstleister im Rahmen einer Auftragsdatenverarbeitung durch den TGPopen-Dienstleister eingebunden. Die Einblendung des Fragebogens sowie die Rückmeldung der Antworten erfolgen ebenfalls über den dazwischen geschalteten Anonymisierungsdienst.

Die konkreten datenschutzrechtlichen Vorgaben aus dem BDSG bzw. LDSG und dem TMG sind von der jeweiligen verantwortlichen Stelle, also dem Website-Betreiber einzuhalten. Die 1&1 Internet AG hat die erforderlichen organisatorischen Maßnahmen getroffen, um auf die Einhaltung dieser datenschutzrechtlichen Anforderungen hinzuwirken und stellt die erforderlichen Mustervereinbarungen insbesondere mit dem Anonymisierungsdienstleister zur Verfügung.

10. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das Produkt TGPopen fördert den Datenschutz durch konsequente Beachtung der Prinzipien von Datenvermeidung und Datensparsamkeit. Sämtliche Datenverarbeitungen basieren auf der pseudonymen Identität des Browser-Cookies. Die Herstellung eines konkreten Personenbezugs ist nicht erforderlich und im technischen Prozess nicht möglich.

Im Einzelnen wurden folgende Maßnahmen getroffen, um dem Datenschutz Rechnung zu tragen:

1. Entfernung der IP-Adresse: Diese dient der Verhinderung der Personenbeziehbarkeit. Sie ist als technischer Prozess in der Hoheit und Verantwortung eines unabhängigen Drittanbieters realisiert.
2. Entfernung des Referers: Diese verhindert die Nachvollziehbarkeit der Clickstreams (Surfpfade).
3. Content-Klassifikation: Konkrete URLs der Seitenabrufe werden durch Content-Kategorien gemäß AGOF ersetzt.
4. Zeitliche Aggregation: Die Entfernung der Zeitreiheninformation von Seitenabrufen verhindert die Nachvollziehbarkeit der Clickstreams (Surfpfade)
5. Profiltransformation durch Modellanwendung: Pseudonyme Browser-Nutzungsprofile werden durch Zielgruppenzugehörigkeiten ersetzt.
6. Bereitstellung eines Opt-Out-Mechanismus: Dieser kann gemäß § 15 TMG von Endanwendern zum Widerspruch gegen die Erstellung der pseudonymen Nutzungsprofile genutzt werden.
7. Einblendung der „i-Icon-Information“: Der Portal-/Websitebetreiber wird verpflichtet ein sogenanntes „i-Icon“ einzublenden, mit der der Nutzer auf das Webtracking sowie auf die Opt-Out-Möglichkeit hingewiesen wird.
8. Anbieten einer Opt-In-Version
9. Berücksichtigung der Do-Not-Track-Einstellungen (DNT) der gängigsten Browser
10. Nutzer/innen können Auskünfte zur Profilvereinerung auf der Infoseite des TGPopen-Dienstleisters unter dem Punkt "Auskünfte" anfordern.