LUX

Informationspaket für
den Datenschutz

Präambel

Das folgende Dokument soll als Handreichung für Personen dienen, die mit dem Datenschutz beauftragt sind und verstehen wollen, welche rechtlichen Folgen die Nutzung von LUX haben könnte. Es geht dabei um eine inhaltliche Darstellung der Konfigurationsmöglichkeiten und der Funktionsweise. Diese ist unter Anderem auch wichtig, um den Besucher der Website korrekt über die Verwendung seiner Daten zu informieren (Datenschutzerklärung).

Eine rechtliche Bewertung der einen oder anderen Nutzungsweise des Produkts können und dürfen wir nicht abgeben. Ob das Produkt datenschutzkonform verwendet wird, liegt allein in der Verantwortung des Betreibers. Das ergibt sich bereits daraus, dass der Betreiber über den Zweck der Datenverarbeitung bestimmt und dieser für die rechtliche Bewertung maßgeblich ist.

Einführung und Zweck

LUX ist eine Erweiterung für das weit verbreitete Content-Management-System (CMS) TYPO3. Es hat zum Ziel, das Surf-Verhalten individueller Website-Besucher zu analysieren, den Besuchern individuell angepasste Inhalte zu präsentieren und die Besucher ggf. zu identifizieren. Die dabei gewonnen Daten sollen es ermöglichen, Marketing-Maßnahmen individualisiert und gezielt zu treffen (Lead-Generierung).

Unter welchen Voraussetzungen werden Daten gesammelt?

Das Speichern der Daten kann per Konfiguration von unterschiedlichen Voraussetzungen abhängig gemacht werden:

- Opt-In, z.B. über Cookie-Banner, d.h. das Tracking wird erst gestartet durch eine Aktion des Benutzers und findet vorher nicht statt. Die Zustimmung des Benutzers wird immer im Browser des Nutzers gespeichert, auch wenn ansonsten Fingerprinting aktiv ist.
- Opt-Out: Stoppt weiteres Erfassen von Daten (jedoch erfolgt keine rückwirkende Löschung). Das Opt-Out wird ebenfalls im Browser des Benutzers gespeichert. Der entsprechende Eintrag kann nicht zur Identifikation genutzt werden.
- Unabhängig von der oberen Einstellung können über die “Email4Link” Erweiterung Downloads nach hierfür spezifischem Einverständnis getrackt werden. Sofern ansonsten kein Tracking aktiv ist, wird dann nur getrackt, welche Downloads der Besucher vorgenommen hat.
- Browser nicht im „Do-not-Track-Modus“

Ihre Notizen

Betriebsmodus der Besucher-Wiedererkennung

Für die Verknüpfung von Seitenaufrufen muss LUX den jeweiligen Besucher wiedererkennen. Hierfür werden zwei unterschiedliche Verfahren angeboten:

1. Vergabe einer eindeutigen Identifikation und Speicherung derselben im Browser bzw. auf dem Gerät des Besuchers im sog. „Local Storage“. Datenschutzrechtlich ist diese Technologie mit (First-Party)-Cookies gleichzusetzen.
2. Fingerprinting, d.h. Speicherung einer Kombination von Merkmalen auf dem Server, die vom Gerät des Besuchers stammen und in Kombination mit einer gewissen Wahrscheinlichkeit die Wiedererkennung desselben Besuchers ermöglichen.

Zu 1: Die Speicherung erfolgt analog zur Speicherung eines Cookies auf Seiten des Besuchers. Es werden also Daten auf dem Gerät des Besuchers abgelegt.

Zu 2: Das Fingerprinting nutzt die Tatsache, dass die Summe aller Eigenschaften, wie Browser-Typ und -Version, Bildschirmauflösung, Fenstergröße etc. in der Gesamtschau die Identifikation ermöglicht. Für bestimmte Betriebssysteme oder Geräte ist das jedoch nicht immer eindeutig möglich.

Nachträgliche De-Anonymisierung

Je nach Konfiguration kann LUX sehr viele verschiedene Informationen zum Surfverhalten des Besuchers speichern. Im Falle von ausgefüllten Formularen, z.B. Kontakt-Formularen, kann LUX die dort eingegebenen Daten des Besuchers dembereits gespeicherten Besuchsverlauf hinzufügen und somit rückwirkend einen Personenbezug herstellen.

Welche Daten können gesammelt werden?

Welche Daten tatsächlich gesammelt werden, ist frei konfigurierbar. Zu den gesammelten Daten können gehören:

- Besuchte Seiten, z.B. auch, welche News-Seiten besucht wurden
- Vom Besucher in Formulare eingegebene Daten[1]
- Verwendete Suchbegriffe
- Anklicken von auf der Website dargestellten Links
- IP-Adresse des Besuchers, ggf. „gekürzt“

Wo werden die Daten gespeichert?

Die Daten werden auf dem Webserver gespeichert, auf dem das CMS betrieben wird. Datenschutzkonforme Auswahl und Betrieb von Betreiber und Servern ist dadurch unkompliziert.

Wer erhält Zugriff auf die Daten?

Der Zugriff erfolgt über das Backend des TYPO3 CMS. Die Personengruppe, welche Zugriff auf die von LUX gesammelten Daten zugreifen kann, kann eingestellt werden.[2]

1 Ein spezieller, in der Standardkonfiguration nicht aktivierter Modus, erlaubt das Aufzeichnen der Eingaben in Formularfelder, BEVOR das Formular vom Benutzer abgesendet wird. Dieses Verhalten wird in den meisten Fällen für den Besucher überraschend sein und sollte daher vor dem Einsatz datenschutzrechtlich geprüft werden.

2 Sofern mehrere Websites innerhalb derselben TYPO3-Instanz verwaltet und mittels LUX getrackt werden, ist es derzeit nicht möglich, die zugriffsberechtigten Personengruppen auf einzelne Websites einzugrenzen. Ein entsprechendes Feature ist für eine der nächsten Versionen in Planung.

Ihre Notizen

Wie und wohin werden die Daten übertragen?

Die primäre Datenhaltung erfolgt auf dem Webserver. Datenübertragung erfolgt beim Aufrufen der Auswertungen im Backend durch die berechtigten Personen über einen Webzugriff. Der Betreiber hat sicherzustellen, dass Webzugriffe verschlüsselt stattfinden (https).

Durch die Speicherung der primären Daten auf den Systemen des Betreibers ist der Betrieb von LUX ohne den Transfer der Besucherdaten an einen Drittanbieter oder gar in ein Drittland möglich. Ein Abgleich der Daten mit Tracking-Profilen großer Internet-Anbieter findet nicht statt.

Konfigurierbare Datenübertragungen:

- Workflows, die eine der folgenden Wege aktivieren
  - → Übertragung als E-Mail an eine vorgegebene Adresse
  - → Übertragung an ein Drittsystem (z.B. Slack oder CRM)
  - → Automatischer Versand von Berichten
- API-Zugriff auf die im BE-Modul sichtbaren Daten
- CSV-Download der im BE-Modul sichtbaren Daten
- Übertragung von IP-Adressen an entsprechende Informationsdienste, um eine Ort bzw. ein Firmennetzwerk zu identifizieren
- Übertragung von die Person identifizierenden Daten an Gravatar oder Google zum Zweck der Darstellung eines Bildes im Backend

Bei Nutzung einer oder mehrerer dieser optionalen Datenübertragungs-Wege ist jeweils durch den Betreiber zu prüfen, ob die Übertragung datenschutzrechtlich zulässig ist.

Zu den beiden letzten Punkten sind diese ergänzenden Informationen relevant:

1. Optional kann eingestellt werden, ob eine IP-Adresse automatisch in einen Ort umgewandelt werden soll oder nicht. (siehe **Hier**)
2. Optional kann eingestellt werden, ob im BE-Modul über Gravatar oder die Google Bildersuche ein Bild eines Leads nachgeladen werden soll (siehe **Hier**)

Wann werden Daten gelöscht?

Eine automatische Löschung von Daten lässt sich per “Scheduler-Task” konfigurieren. Mögliche einstellbare Kriterien sind, z.B. das Alter der Daten, die gelöscht werden sollen.
Löschung von unidentifizierten und/oder identifizierten Datensätzen. An Hand Alter der letzten Aktivität. Weitere Selektionskriterien sind möglich.

Manuell:

Löschung je nach Konfiguration ergänzt um Eintragung in eine Denylist: Manuell oder per Workflow. Datensatz wird von Identifikation entkoppelt und erhält Markierung “Denylist”.

Ihre Notizen

Dokumentation für Integration und Inbetriebnahme

- Wir empfehlen, ausgehend von der Standardeinstellung die Wahl jeder Option datenschutzrechtlich zu hinterfragen und deren Zulässigkeit abzuklären.
- Sofern Seitenbesucher eine Zustimmung abgeben, kann es zu Nachweiszwecken sinnvoll sein, den zugehörigen Ablauf einmalig aus Sicht des Besuchers per Videoaufzeichnung bzw. Screenshots zu dokumentieren und zu verwahren. Nach jeder Änderung des Ablaufs bzw. der angezeigten Texte ist der Vorgang zu wiederholen.
- Wesentliche Änderungen an der Konfiguration oder an den Texten, die den Besucher über die Verwendung seiner Daten informieren, erfordern ein erneutes Opt-In.
- Die Benutzergruppe, die Zugriffsrechte auf das LUX-Backend-Modul erhält, sollte sorgfältig ausgewählt sein und darf keine Personen enthalten, die nicht mit diesen Daten arbeiten müssen.
- Sofern mehrere Domains von der gleichen TYPO3/LUX-Instanz verwaltet werden, muss darauf geachtet werden, dass der Benutzer der Verwendung auf allen beteiligten Websites zustimmt.

Schlussbemerkung

Bei der Konfiguration von LUX und insbesondere bei der Auswahl der zu aktivierenden Optionen ist jeweils im Einzelnen eine datenschutzrechtliche Prüfung erforderlich. Dieses Dokument soll die dafür nötigen Informationen liefern.
Bei Unklarheiten oder fehlenden Informationen bitten wir um Rückmeldung z.B **via GitHub**.

Ihre Notizen