

# DATENSCHUTZ

FÜR SCHWEIZER UNTERNEHMEN UND INSTITUTIONEN

## DATENSCHUTZ AKTUELL

**Cookiebanner:  
EUR 60 Mio. Busse  
gegen Facebook  
Ireland Limited**

Mehr dazu auf Seite 3

## DATENSCHUTZ IM ARBEITSVERHÄLTNISS

**Was gilt es beim Ein-  
satz von E-Recruiting-  
Software aus daten-  
schutzrechtlicher  
Sicht zu beachten?**

Mehr dazu auf Seite 5

## DATENSCHUTZ AUS DER PRAXIS

**Google Analytics  
und die Datenschutz-  
aufsichtsbehörden –  
ein eine Verortung**

Mehr dazu auf Seite 9



# Cookiebanner: EUR 60 Mio. Busse gegen Facebook Ireland Limited – Teil II: Folgen des Entscheids der CNIL vom 31.12.2021

Facebook Ireland Limited wurde mit Entscheid der französischen Datenschutzaufsichtsbehörde CNIL vom 31. Dezember 2021 mit EUR 60 Mio. wegen Verstössen gegen die Cookie-Pflichten gebüsst. Im ersten Teil des Artikels, erschienen in der Februar-Ausgabe 2022 des Newsletters, wurde der Entscheid der CNIL detailliert vorgestellt. In diesem abschliessenden Teil II werden dessen Folgen mittels Fragen nach der Best Practice sowie allfälligen Auswirkungen dieses Entscheids auf Schweizer Unternehmen thematisiert.

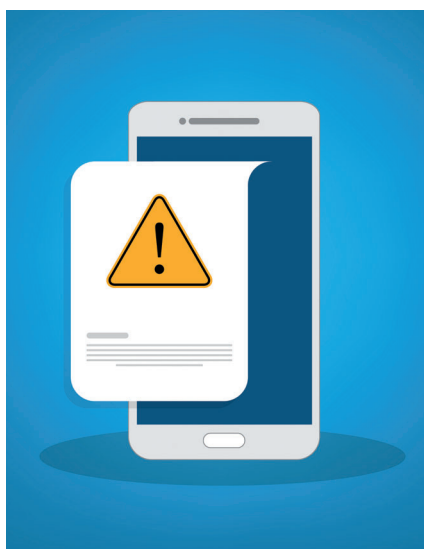
## ■ Von Reto Fanger

### Kurzer Rückblick auf Teil I

Die CNIL hatte im Rahmen einer Online-Überprüfung am 8. April 2021 festgestellt, dass bei einem Besuch von Facebook dem Nutzer ein Pop-up-Fenster mit der Überschrift «Cookies von Facebook in diesem Browser akzeptieren» erscheine und dass am unteren rechten Rand dieses Fensters zwei Schaltflächen mit den Überschriften «Dateieinstellungen verwalten» und «Alle akzeptieren» zu sehen seien.

Nach Auffassung der CNIL besuche ein Webnutzer in der Regel eine Vielzahl von Websites. Das Surfen im Web zeichne sich durch Schnelligkeit und Flüssigkeit aus. Die Tatsache, dass man auf «Dateieinstellungen verwalten» klicken und verstehen müsse, wie die Seite aufgebaut sei, auf der man Cookies ablehnen kann, könne den Nutzer entmutigen, wenn er das Ablegen von Cookies dennoch ablehnen möchte.

Das Angebot einer Wahl durch Facebook wurde dabei von der CNIL nicht in Abrede gestellt. Aber die Art und Weise, wie diese Ablehnung im Kontext des Surfens im Web ausgedrückt werden könne, verzerre die Wahl zugunsten einer Zustimmung, sodass die Wahlfreiheit beeinträchtigt werde. Nach Ansicht der CNIL würden diese Modalitäten den Nutzer eher zur



Annahme verleiten, dass es letztlich nicht möglich sei, seine Navigation fortzusetzen, wenn er das Ablegen von Werbecookies abgelehnt habe, da der gesamte Weg zur Ablehnung von Cookies auf einer Information beruhe, die auf die Annahme von Cookies verweise.

Dieser Eindruck werde durch die wenig explizite Schaltfläche «Dateieinstellungen verwalten» im Rahmen des ersten Fensters noch verstärkt, die nicht klar auf die Existenz von Möglichkeiten zur Ablehnung von Cookies hinweise. Die Tatsache, dass letztendlich keine Cookies abgelegt würden, habe keinen Einfluss auf die Verwirrung, die durch diesen widersprüchlichen Informationspfad entstehe, der dem Nutzer

das Gefühl geben könne, dass es nicht möglich sei, die Ablage von Cookies abzulehnen, und dass er diesbezüglich keine Kontrollmöglichkeiten habe.

Die CNIL war daher der Auffassung, dass das Unternehmen den Mechanismus zur Ablehnung von Cookies komplizierter gestalte als denjenigen zur Annahme, was in Wirklichkeit darauf hinauslaufe, die Nutzer von der Ablehnung von Cookies abzuhalten und sie dazu zu bringen, die Einfachheit der Schaltfläche «Cookies annehmen» zu bevorzugen.

Folglich würden die Informationen, die in Frankreich ansässigen Nutzern, welche die Seite «facebook.com» besuchen, zur Verfügung gestellt werden, sowie die Modalitäten zur Einholung der Zustimmung, die ihnen vom Unternehmen auf dieser Website angeboten würden, nicht den Bestimmungen von Art. 82 des französischen Datenschutzgesetzes entsprechen, wie sie durch die verstärkten Anforderungen an die Zustimmung gemäss DSGVO erhellt würden.

### Best Practice ...?

Die CNIL hatte ihre Empfehlung zu Cookies und anderen Trackern aus dem Jahr 2013 angesichts der Entwicklungen aufgrund des Inkrafttretens der DSGVO angepasst und dazu am 4. Juli



# Was gilt es beim Einsatz von E-Recruiting-Software aus datenschutzrechtlicher Sicht zu beachten?

Was müssen Arbeitgebende resp. Stellenausschreibende datenschutzrechtlich beachten, wenn sie Softwarelösungen von Drittdienstleistern für Online-Bewerbungen (sog. E-Recruiting-Software) einsetzen? Wie werden dabei die Datenschutzrechte der Mitarbeitenden resp. Bewerbern gewahrt? Wie sich zeigen wird, betreffen die datenschutzrechtlich notwendigen Massnahmen primär die Transparenz, die Regelung des Auftragsbearbeitungsverhältnisses und die Wahrung der Datensicherheit.

■ Von Michael Kuhn und Marcel Isch

## 1. Was ist eine E-Recruiting-Software?

Unter Softwarelösung für Onlinebewerbungen verstehen wir konkret die Verwendung von Drittsoftware, welche die Administrierung von Online-Bewerbungen vereinfacht und digitalisiert (sog. E-Recruiting-, SaaS-Recruiting- oder Bewerbermanagement-Software). Beim Einsatz einer solchen E-Recruiting-Software gilt es einiges zu beachten, um sicherzustellen, dass die Datenschutzrechte der Mitarbeitenden resp. Bewerbenden gewahrt werden, denn dadurch werden Personendaten durch ein Drittunternehmen (Softwareanbieter) bearbeitet und gespeichert.

## 2. Wie kann eine E-Recruiting-Software eingesetzt werden?

Eine solche E-Recruiting-Software kann den gesamten Recruiting-Workflow abbilden: von der Stellenausschreibung auf der eigenen Website, in Jobbörsen und relevanten Foren über die Ablage und das Prüfen der eingereichten Bewerbungsunterlagen, die Vereinbarung eines Vorstellungsgesprächs, das Abhalten eines Videointerviews bis zur Personalauswahl und allenfalls sogar bis zur Vertragsgestaltung (Erstellen eines Arbeitsvertrages). Zudem decken solche Tools teilweise auch die Analyse und Auswertung der Bewerbungsprozesse ab (z.B. welches sind die effektivsten

Ausschreibungs-kanäle und Bewerberquellen oder wie präsentiert sich der Time-To-Hire-Durchschnitt?).

## 3. Relevanz im Lichte des neuen totalrevidierten Schweizer Datenschutzgesetzes

Mitarbeiterdatenschutz ist ein zentrales Thema, welches oft in den Hintergrund gerät, weil regelmässig vergessen resp. unterschätzt wird, dass das Datenschutzrecht auch auf die Bearbeitung eines Unternehmens der Personendaten ihrer Mitarbeitenden und Bewerbenden Anwendung findet.

Das Thema Mitarbeiterdatenschutz wurde in der Schweiz bisher wenig beachtet, weil das geltende Schweizer Datenschutzgesetz (nachfolgend DSG) die Erkennbarkeit einer Personendatenbearbeitung als ausreichend betrachtet. Das neue totalrevidierte Schweizer Datenschutzrecht, welches voraussichtlich am 1. September 2023 in Kraft gesetzt wird (nachfolgend E-DSG), sieht in Art. 19 dahingegen eine aktive Informationspflicht vor, insbesondere was den Bearbeitungszweck und die Weitergabe der Personendaten betrifft.

Hinzu kommt, dass das E-DSG im Vergleich zum DSG die Datenschutzrechte der Datensubjekte (und damit eben auch der Bewerbenden und

Mitarbeitenden) deutlich ausweitet. Zu denken ist hier beispielsweise an das Auskunftsrecht (Art. 25 E-DSG), das Recht auf Datenherausgabe oder -übertragung (Art. 28 E-DSG), das Recht auf Datenberichtigung (Art. 6 Abs. 5 E-DSG und Art. 32 Abs. 1 E-DSG) sowie das Recht auf Datenlöschung (Art. 32 Abs. 2 lit. c E-DSG).

Hinsichtlich der Inkraftsetzung des E-DSG ist der Handlungsbedarf im Zusammenhang mit dem Mitarbeiterdatenschutz deshalb gross.

## 4. Nicht im Anwendungsbereich der EU-Datenschutz-Grundverordnung

Der erwähnte Handlungsbedarf für Schweizer Arbeitgebende rührt dabei auch daher, dass Unternehmen, welche bereits Massnahmen zur Umsetzung der am 25. Mai 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung (nachfolgend **DSGVO**) ergriffen, den Mitarbeiter- resp. Bewerberdatenschutz regelmässig ausgeklammert haben. Grund dafür ist, dass die Bearbeitung von Mitarbeiter- resp. Bewerberpersonendaten durch Schweizer Arbeitgebende resp. Stellenausschreibende in der Regel nicht in den extraterritorialen Geltungsbereich der DSGVO fällt, welcher sich auf die Bearbeitung von Personendaten von Datensubjekten, welche sich in der EU befinden, beschränkt (was