



info@socialwave.de
Tel: +49 89 21546472
Fax: +49 89 21544713

Informationen zur DSGVO Anpassung von Socialwave

Am 25. Mai 2018 tritt die neue Europäische Datenschutzgrundverordnung in Kraft - kurz DSGVO. Diese Verordnung betrifft alle Bereiche in denen Daten von Kunden oder Nutzern erfasst und gespeichert werden.

Das wichtigste: Ihr Socialwave WLAN ist auf die DSGVO vorbereitet!

Als Kunde von Socialwave müssen Sie sich folglich um nichts kümmern - das haben wir schon für Sie erledigt. In dieser E-Mail möchten wir Sie umfassend informieren, wie wir das Socialwave WLAN auf die DSGVO vorbereitet haben.

Warum ist offenes WLAN ist von der DSGVO betroffen?

Laut Erwägungsgrund 30 zur Datenschutz-Grundverordnung werden insbesondere dynamische IP-Adressen, welche bei Netzwerkverbindungen zwangsläufig gespeichert werden, als Bestandteil persönlicher Daten angesehen. Diese sind nach der DSGVO besonders schutzbedürftig.

Welche Daten werden bei der Verbindung zum WLAN gespeichert?

- Dynamische IP-Adresse
- MAC-Adresse (eindeutige Kennung des Geräts)
- Startzeitpunkt und Dauer der Nutzung
- Verbrauchtes Datenvolumen
- Je nach Login ggf. Social Media Account bzw. E-Mail Adresse

Unsere Anpassungen:

Um die Daten Ihrer Gäste und Kunden, die das Socialwave WLAN nutzen, bestmöglich zu schützen haben wir unterschiedliche Anstrengungen unternommen. Diese Anpassungen führen dazu, dass Ihr Socialwave WLAN DSGVO-konform ist.

Hier finden Sie eine detaillierte Erläuterung:

1.) Verschlüsselung des kompletten Login-Vorgangs via HTTPS

Erläuterung: Die DSGVO verlangt, dass persönliche Daten ausschließlich sicher, verschlüsselt übertragen werden.

Was wir tun: HTTPS ist ein Verfahren um den Datenverkehr auf Webseiten zu verschlüsseln, so dass dieser nicht von Dritten abgehört werden kann. Sie erkennen dies am vorangestellten "https://" und einem Schloss-Symbol in der Adresszeile Ihres Internet-Browsers.

2.) Sicherung des Basisgerätes

Erläuterung: Die DSGVO verlangt, dass Datenspeicher mit persönlichen Daten gegen fremden Zugriff gesichert sind. Einige Daten, wie z. B. dynamische IP-Adressen oder die MAC-Adresse des verwendeten Gerätes werden lokal im Basisgerät gespeichert. Das Basisgerät ist somit der Datenspeicher.

Was wir tun: Im Gegensatz zu vielen haushaltsüblichen Routern sind beim Socialwave Router fast alle Zugangsmöglichkeiten (z. B. Telnet, FTP, API) gesperrt, so dass etwaige Einfallstore für Angreifer gar nicht erst bestehen. Andere Zugangsmöglichkeiten wie z. B. SSH, Webfig) sind mit Maßnahmen wie "fail2ban" besonders geschützt.

3.) Verständliche Datenschutzhinweise mit Ansprechpartner

Erläuterung: Die DSGVO schreibt vor, dass Datenschutzhinweise für Jedermann verständlich formuliert sein müssen. Außerdem ist ein Ansprechpartner anzugeben, an den sich Nutzer direkt wenden können um ihre Daten anpassen zu lassen, die Nutzung einzuschränken oder die Löschung zu verlangen.

Was wir tun: Auf der Loginseite findet sich unter "Datenschutzhinweise" eine verständliche Erklärung und eine einfache Anleitung um als Nutzer Einsicht in die gespeicherten Daten zu erhalten um diese einschränken, verändern oder löschen zu lassen.

4.) Nachvollziehbarkeit der Datennutzung

Erläuterung: Die DSGVO verlangt, dass anhand eines Protokolles nachvollziehbar ist, wer welche Daten wann verwendet hat.

Was wir tun: Zu diesem Zweck muss sich jeder Mitarbeiter, der auf Datensätze zugreift im System mit seinem Namen per Login authentifizieren. Das Login erhält jeder Mitarbeiter erst nach Zustimmung zu einer Vertraulichkeitsvereinbarung. Anschließend loggt das System welcher Mitarbeiter wann welchen Kundendatensatz aufgerufen hat und welche Daten verändert wurden.

5.) Automatisches Löschen der Daten

Erläuterung: Die DSGVO verlangt, dass Daten nicht länger als nötig aufbewahrt werden. Für Nutzer muss es transparent sein, wann die Daten gelöscht werden.

Was wir tun: Wir löschen...

- die Verbindungsdaten im Router automatisch nach 24 Stunden
- die Accountdaten automatisch nach dem der jeweilige Nutzer 365 Tage lang inaktiv war (also sich an keinem Socialwave WLAN eingeloggt hat)
- oder nach spätestens 7 Tagen auf Anfrage des Nutzers

6.) Transparenz und Auskunftspflicht für gespeicherte Daten

Für alle gespeicherten Daten muss für Nutzer verständlich dargestellt werden wann diese Daten, wie und warum gespeichert werden, wie sie geschützt werden, wer darauf Zugriff hat, ob sie Dritten zur Verfügung gestellt werden und wann bzw. wie sie gelöscht werden. Hierfür steht das gesamte Socialwave Team zur Auskunft zur Verfügung. Wenn ein Kunde um Löschung seiner Daten bittet, geschieht dies durch einen Socialwave Mitarbeiter spätestens 7 Werktagen nach Kontaktaufnahme.

Bei Rückfragen können Sie uns gerne telefonisch unter 089/21546472 oder per Mail unter info@socialwave.de kontaktieren.

Mit besten Grüßen,

Mario Schilling
Geschäftsführer der Socialwave GmbH