COOKIE CHECKLISTE

- [ ] **Httponly Flag setzen**
- [ ] **Keine sensiblen Infos speichern**
- [ ] **Session Cookies verwenden**
- [ ] **Secure Flag setzen**
- [ ] **SameSite Flag setzen**
- [ ] **HostOnly Flag**
- [ ] **DSGVO beachten**
- [ ] **Session Fixation verhindern**

INMODIS
IT-Sicherheit für Ihr Unternehmen

COOKIE CHECKLISTE

Httponly Flag setzen

Das Httponly Flag verhindert, dass Cookies von JavaScript Skripten ausgelesen werden können.

Keine sensiblen Infos speichern

Sensible Informationen sollten möglichst nur auf Server Seite gespeichert werden um Manipulationen zu erschweren.

Session Cookies verwenden

Cookies sollten nur begrenzt gültig sein, etwa im Rahmen einer Session. Alternativ sollten sie ein Ablaufdatum (Expiration) haben.

Secure Flag setzen

Die Secure Flag verhindert, dass Cookies über unsichere Verbindungen (http) übertragen werden.

SameSite Flag setzen

Die SameSite Flag bietet Schutz gegen CSRF Angriffe und verhindert Anfragen, wenn diese von anderen Domains kommen.

HostOnly Flag

Beim HostOnly Flag sollte der Domain Parameter freigelassen werden um eine Verwendung von Cookies über Sudomains hinweg zu unterbinden.

DSGVO beachten

Im Rahmen der DSGVO muss der User der Verwendung von Cookies zustimmen, dafür sollte ein Pop Up angezeigt werden.

Session Fixation verhindern

Wenn Cookies mit __Host-(name) benannt werden, wird der Versuch einer Session Fixation zumindest erschwert.