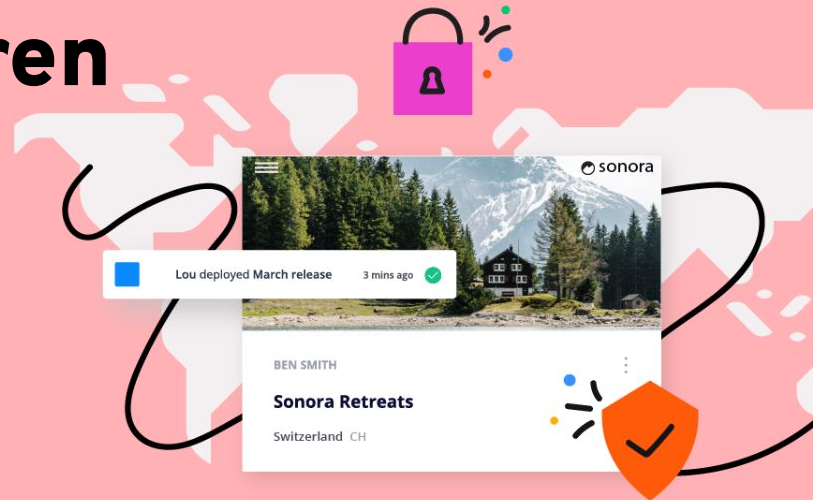


Websites und Anwendungen global aufsetzen, lokal ausführen

15 Juni 2023



Vorstellung



Patrick Boest
Solutions Architect



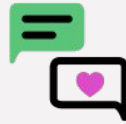
Viliyan Mihaylov
Agency Partner Manager
DACH

Die Suche nach Lösungen ist nicht nur eine technische Angelegenheit.

Es gilt zu bedenken:



Prozesse



Kommunikation



Organisation



Compliance

Sicherheit als “wichtiges Unterscheidungsmerkmal [...] um die digitalen Geschäftsentscheidungen Ihres Unternehmens, die Auswahl von Anbietern und Technologien sowie Investitionsstrategien zu steuern”.

— [AWS Security & Compliance](#)

7 Grundsätze für Privacy by Design

1. Proaktiv, statt reaktiv
2. Datenschutz als Standard
3. Ins Design eingebetteter Datenschutz
4. Volle Funktionalität
5. End-to-End Sicherheit
6. Sichtbarkeit und Transparenz
7. Respekt für die Privatsphäre der Nutzer

Quelle:

<https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>

**Kernaufgaben
identifizieren,
Sicherheits- und
Compliance-
Anforderungen
sinnvoll delegieren?**



Aspekte der Datenverwaltung



Erhebung



Speicherung



Zugang



**Nutzung /
Austausch**



Aufbewahrung

Modell der geteilten Verantwortung

Verantwortungsbereich	Platform.sh	Kunden
Physische und Umweltkontrollen	Durchgereicht an Hosting-Anbieter	X
Patch-Management	Patches und Korrekturen des Systems	Pflegt den Anwendungscode
Management der Konfiguration	Verwaltet die Konfiguration der Platform.sh Infrastruktur und Geräte	Verwaltet die sichere Konfiguration der Anwendung

Verantwortungsbereich	Platform.sh	Kunden
Zugangskontrolle	Bereitstellung von Zugangskontrollmechanismen	Effektive Nutzung der verfügbaren Zugangskontrollmechanismen
Backups	Automatisierte Erstellung & Deduplizierung von Backups	Optionale Erstellung zusätzlicher manueller Backups
Kapazitätsmanagement	Verwaltung der Kapazität der Infrastruktur	Kapazitätsmanagement auf Applikationsebene
Sensibilisierung und Fortbildung	Schulung der Mitarbeiter:innen von Platform.sh	Schulung der eigenen Mitarbeiter:innen und Nutzer:innen

**“One size does not fit all any longer” –
“Multinationale Unternehmen müssen
ihr DPP-Programm so gestalten und
anpassen, dass es den Anforderungen
der einzelnen Länder gerecht wird.”**

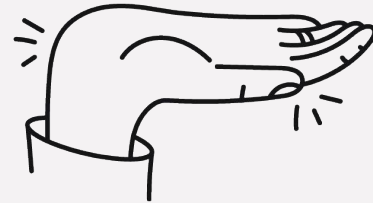
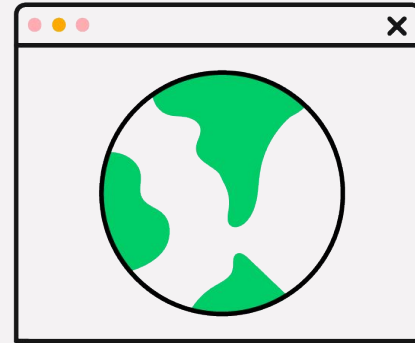
– [Ernst & Young Global](#)

Der Platform.sh

Ansatz:

GDPR everywhere

- Anwendung der Grundsätze der DSGVO auf alle personenbezogenen Daten, unabhängig der Herkunft
- Geringeres Potenzial für Datenschutzlücken
- Umfassende Anforderungen an den Schutz der Privatsphäre und des Datenschutzes




OWASP Top 10 Datenschutz - risiken



Eher organisatorisches Risiko



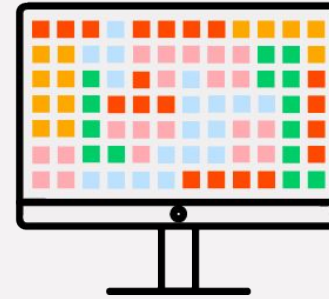
Eher technisches Risiko

1. Schwachstellen in Web-Anwendungen	
2. Datenabfluss beim Betreiber	 
3. Unzureichende Reaktion bei einer Datenpanne	 
4. Einwilligung für alles	
5. Intransparente Nutzungsbedingungen	
6. Unzureichende Löschung personenbezogener Daten	 
7. Unzureichende Datenqualität	 
8. Fehlendes oder unzureichendes Session-Ende	
9. Zugriff auf oder Änderungen von Benutzerdaten nicht möglich	 
10. Sammeln von Daten, die über den eigentlichen Zweck hinaus gehen	

Technische Risiken



**Infrastruktur & service
management - Ebene**



Applikationsebene

Integrierte bewährte Sicherheits- praktiken

- **Verschlüsselung von Daten im Ruhezustand und bei der Übermittlung**
- **Schutz vor Datenverlust und Ransomware**
- **Sicherheitsaktualisierungen und Stack-Management**
- **Verringerung des Risikos der versehentlichen Offenlegung von Daten**
- **Daten-Lokalisierung**

Compliance



SOC 2 Type 2



PCI Level 1 Compliant



Australian Privacy Principles

Thank you!

Patrick Boest

Solutions Architect, Platform.sh

patrick.boest@platform.sh

Viliyan Mihaylov

Agency Partner Manager, Platform.sh

viliyan.mihaylov@platform.sh

platform.sh 