SECURITY / PRIVACY STANDARDS

INTRODUCTION

This document should briefly outline the measures and efforts of PlanRadar to provide modern and high standards for data security, privacy and service availability for our SAAS.

INFRASTRUCTURE/HOSTING

AWS Security Whitepaper
https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

AWS Privacy Whitepaper
https://d1.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf

Information on AWS compliance and certifications
https://aws.amazon.com/compliance/

Configuration management
We follow the principles of immutable infrastructure and infrastructure as code.
In case of error/failure the system can be regenerated based on its templates and source code.
We use chef and docker for our infrastructure.

High availability / Scalability
AWS makes our system responsive to high load spikes and it will automatically provision more resources if that is necessary. Our customers will not experience performance impacts

DDOS / Webvulnerability Protection
Our webapplication is shielded and protected with the cloudflare (*www.cloudflare.com*) web proxy system.

SOFTWARE DEVELOPMENT

Implementation
Our system is based on modern, robust and battle proven open source technology.
Our web application is developed with ruby on rails in its latest version (5.2). Our mobile clients are developed in Java, Objective-C and .NET .
All data transfer is done via HTTPS/TLS and the data is encrypted at rest. (In our relational database and in our object storage).
All images ,plans and document assets are stored in the highly durable amazon s3 storage system.
https://aws.amazon.com/s3/?nc1=h_ls

OWASP
In our implementation we follow the security by design principle.
https://www.owasp.org/index.php/Security_by_Design_Principles

TDD
All our core functionality is implemented with the methodology of test driven development.
This ensures that we can minimize the amount of bugs or side effects in our system.

PROCESSES

Employees
All our employees but especially in support and engineering are aware of data privacy / security and get trainings and SOPs for a responsible treatment of our customers data.
All employees only get the minimum necessary access to our IT systems.
Customer data is only accessible by small selected group of support and operation engineers.

Incident management
Security and privacy incidents are collected on every point of contact and then routed to the responsible organizational unit. Our logging systems detect anomalies in system usage and sent automated alarms if necessary.
We have written procedures for disaster recovery and backup restores.

Access
Access to administrative systems is limited to certain ips and vpns and protected by 2 factor authentication.

ISO/IEC 27001 Information Security Management Certification
We want to finish our certification for development and operations until Q2 2020

Penetration tests
We do penetration tests about once a year with external consultants.