Pipedrive's Road to ISO 27001 Certification and SOC2 Type II Attestation

pipedrive

About us

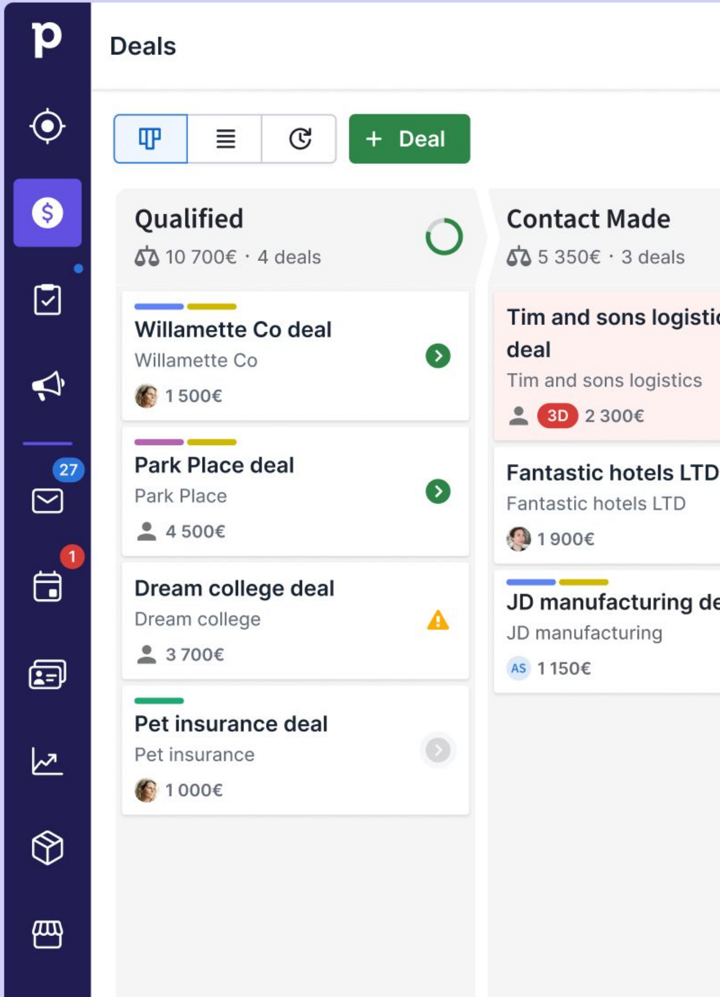
Anneli Kärner

Information Security
Compliance Manager

Ats Onemar

Head of Information Security

pipedrive



Deals

Qualified
10 700€ · 4 deals

Willamette Co deal
Willamette Co
1 500€

Park Place deal
Park Place
4 500€

Dream college deal
Dream college
3 700€

Pet insurance deal
Pet insurance
1 000€

Contact Made
5 350€ · 3 deals

**Tim and sons logistic
deal**
Tim and sons logistics
3D 2 300€

Fantastic hotels LTD
Fantastic hotels LTD
1 900€

JD manufacturing de
JD manufacturing
AS 1 150€

Agenda

1 **Intro to the subject**

Pipedrive, ISO 27001, SOC2 Type II

2 **The Past**

Where we started from

3 **The Change**

What we did

4 **Choosing External Auditor**

Why we are so proud of it

5 **Into the Future**

Where we want to go

What is what

Pipedrive, ISO27001, SOC2 Type II

Pipedrive is a *SaaS company* with over 100 000 customers, offices in 8 countries, Europe and US. 850+ employees, 55+ nationalities.

Pipedrive as a *product* is a sales CRM system designed for salespeople and sales teams across all industries. Its purpose is to help companies streamline pipeline management with features for sales management, sales forecasting and lead management.

ISO 27001 is an international standard for information security management systems (ISMS) that provides a framework for establishing, implementing, maintaining, and continually improving the management of information security within an organization.

SOC2 Type II attestation is independent assessment about the effectiveness of a service organization's controls related to security, availability, processing integrity, confidentiality, or privacy over a specific period of time.

The Past

Where we started from

Auditing peers

- Adequate to cover ISO requirement, but not enough to challenge for improvement

Maintenances as a control

- Collecting audit evidence in systematic and documented form, all year round - but looking at the same thing

InfoSec vs the organization

- Knowledge about auditing and participation was limited mostly to InfoSec department

Management reviews

- Mandatory reports to Executives in a regular basis

The Change

What we did

Included most of the organization into the audit

Team got the **trust** and freedom to act

Communicated the change and the audit goals

Asked before audit - **what would bring value** from the report, **where is the risk**

If you don't understand the requirement - **challenge it**

Train hard (internal audit), **fight easy** (external audit)

CISO in all the interviews (internal, external) - mostly listening

Site audits **in person**

Choosing external auditor

Why we are so proud of it

- ✓ We don’t want a tick in the box!
- ✓ Auditor needs to challenge us
- ✓ Auditor needs to understand our business
- ✓ Assessors name on certificate already means something
- ✓ Some visible improvements:
  - Quality (end to end)
  - No surprise policy
  - Teams feedback

pipedrive

Into the Future

Creating a stronger Internal Audit function

Focus on:

- Objectivity and independence
- Variation of auditing skills
- Avoiding organization’s audit fatigue
- Automation of evidence collection (SOC2)
- Improving maturity of the audit program

More attention to our core - technology

Current speed of product development, change in engineering environment and new SaaS possibilities is unprecedented.

- Constantly adopting new cloud technologies
- Policy as Code / Infrastructure as Code
- Policy Based Access Control
- Changing / improving agile development practices
- AI explosion for tools, product and code

Thank you!

Any questions? Contact us!

Anneli Kärner

anneli.karner@pipedrive.com

Ats Onemar

ats.onemar@pipedrive.com

pipedrive