



From CVR to security.txt

AN OVERVIEW OF DANISH COMPANIES'
STANCE ON VULNERABILITY DISCLOSURE

WHO THE HACK IS THIS GUY

- *Emil Christian Hørning*
- 7 years experience with Infosec
- Active bug bounty hunter with +100 reports
- Head of Hackers @ Defend Denmark
 - Danish local bug bounty platform
 - Got tired of there being so few Danish companies to hack
 - So started own adventure to promote Bug bounty in Denmark
 - Lots of really cool hackers already on the platform



How did this research start?

- In June when I scanned ~1.2 million .dk domains for security.txt
- What is security.txt ?

“When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. security.txt defines a standard to help organizations define the process for security researchers to disclose security vulnerabilities securely.”

– securitytxt.org

- Simply put, a .txt file that says how you can get in contact with the security team

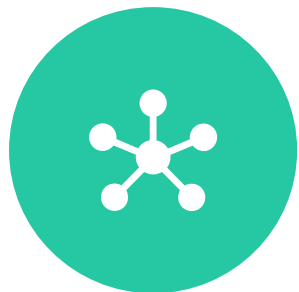


tryg.dk/.well-known/security.txt

The text shows a browser address bar with a lock icon, a shield icon, and a magnifying glass icon to the left of the URL "tryg.dk/.well-known/security.txt".

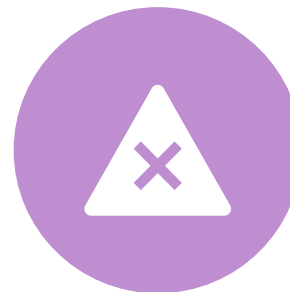
```
Contact: https://tryg.com/en/responsible-disclosure
Contact: mailto:irt@tryg.com
Preferred-Languages: en, da-DK, nb-NO, nn-NO, sv-SE
Policy: https://tryg.com/en/responsible-disclosure
Expires: Saturday, 30 Nov 2025 12:00:00 + 0200
```

Some quick terminology



Security.txt: RFC 9110 standard at `/.well-known/security.txt` or `/security.txt`.

"Here is how to contact us about security issues"



Vulnerability disclosure policy (VDP): A policy for how any external persons should handle vulnerabilities in the specific company



Bug Bounty Program (BBP): VDP + Financial/Gift rewards for finding and reporting security vulnerabilities



Coordinated Vulnerability Disclosure (CVD): The actual process after a report comes in.

What should we talk about ?

- Vulnerability disclosure adaptation in Danish Companies
 - How mature are Danish companies processes for handling unprompted reports of security issues

1

Not mature: No procedures in place, no proper contact method, no mention of security

2

Slightly mature: A security contact on the webpage. Maybe a **security.txt** – No formal CVD process

3

Mature: A VDP, outlining what to report and how to report it. Including a **security.txt**. Formalized CVD

4

Very mature: An active VDP with incentivization for finding vulnerabilities (Bug bounty or other rewards)

Why is it important

Radar Nyheder Debat Tip os Om Mere ▾

Gymnasier blev udsat for hackerangreb:

Helbredsoplysninger og andre data kan være lækket

It-sikkerhed 20. september 2024 kl. 05:00 5



blev hacket
historie være en
andre vandværk

Forsyningssikkerhed 12. februar kl. 12:00

B.T.
JILER 5. feb. 2025

der bekræf
tsning

> TV 2 Play

Log Ind



Nyheder Sport Vejr TV

Seneste

Korte videoer

Trump i Det Hvide Hus

Krigen i Ukraine

Politik

Krimi

Samfund

Udland

Business

Penge

Populær parkeringsapp ramt af hackerangreb

Parkeringstjenesten oplyser, at der er tale om "ikkefølsomme" oplysninger, men opfordrer alligevel kunder til at være opmærksomme på særligt én ting.

BETAL MED UDVALGTE APPS HER

Registreringen skal ske for korrekt områdekode/pladsnr. og nummeret

Brændt andre
ældre og virksomheder
blevet stjålet.

Why is it important

Radar Nyheder Debat Tip os Om Mere ▾

Gymnasier blev udsat for hackerangreb:

Helbredsoplysninger og andre data kan være lækket

It-sikkerhed 20. september 2024 kl. 05:00 5



blev hacket
historie være en
andre vandværk

Forsyningssikkerhed 12. februar kl. 12:00

B.T.
JILER 5. feb. 2025

der bekræf
tsning

> TV 2 Play

Log Ind



Nyheder Sport Vejr TV

Seneste

Korte videoer

Trump i Det Hvide Hus

Krigen i Ukraine

Politik

Krimi

Samfund

Udland

Business

Penge

Populær parkeringsapp ramt af hackerangreb

Parkeringstjenesten oplyser, at der er tale om "ikkefølsomme" oplysninger, men opfordrer alligevel kunder til at være opmærksomme på særligt én ting.

BETAL MED UDVALGTE APPS HER

Registreringen skal ske for korrekt områdekode/pladsnr. og nummeret

Brændt andre
ældre og virksomheder
blevet stjålet.

Why is it important?

- The cybersecurity situation in Denmark is tense
- Regulations are knocking on the door
- The talent pool is growing rapidly in Denmark
 - Cybermesterskaberne
 - New Cybersecurity educations
 - More Focus, that's great!
- Larger chance of friendly hackers stumbling over vulnerabilities



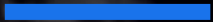
Raise your hand if
you know that your
company has a
vulnerability
disclosure policy

Working with friendly hackers

The good

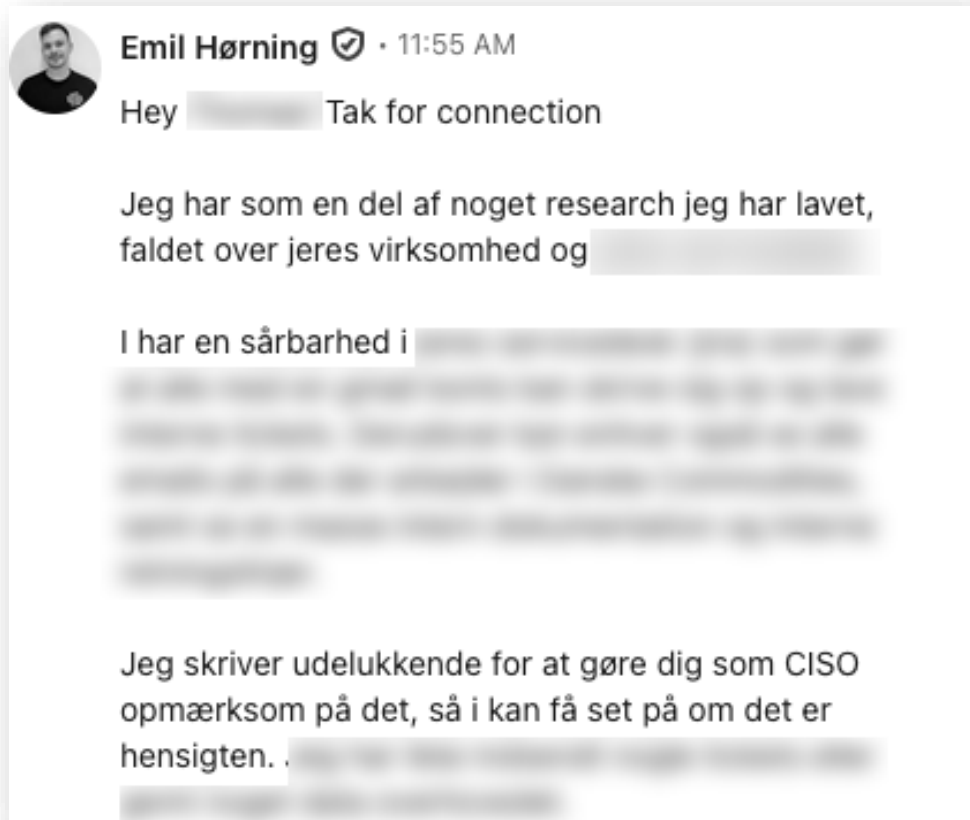
The bad

The ugly

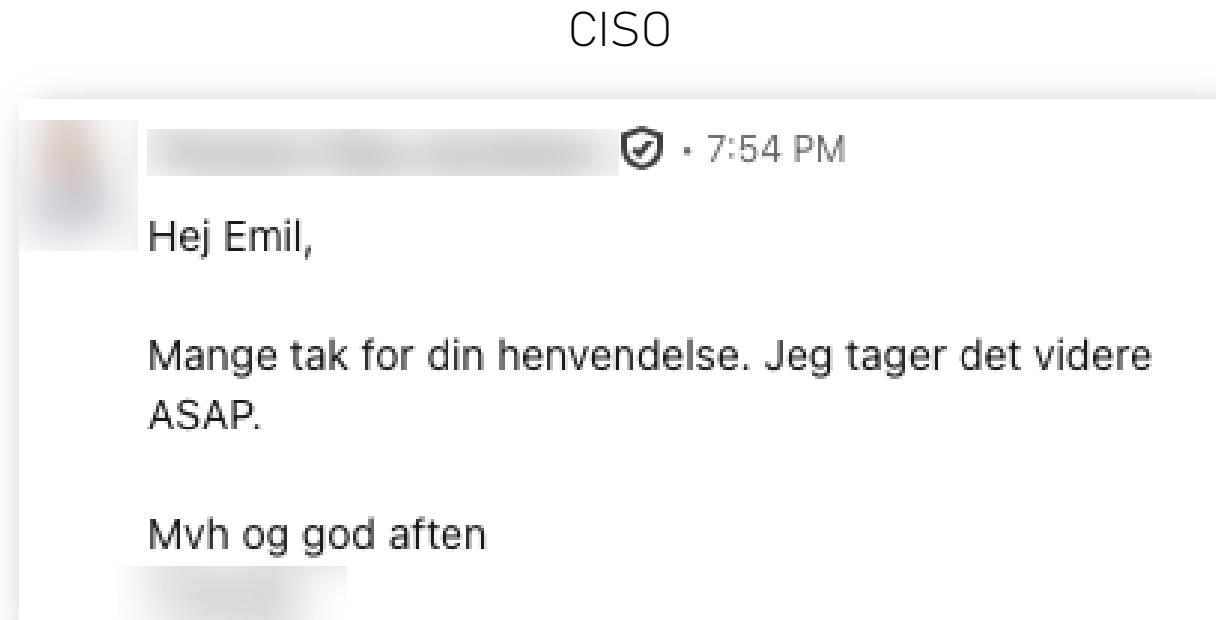


Working with friendly hackers – The good

Day 1



EN: I did some research, You have a vulnerability here, just letting you know



EN: Thanks for letting me know!

Working with friendly hackers – The good

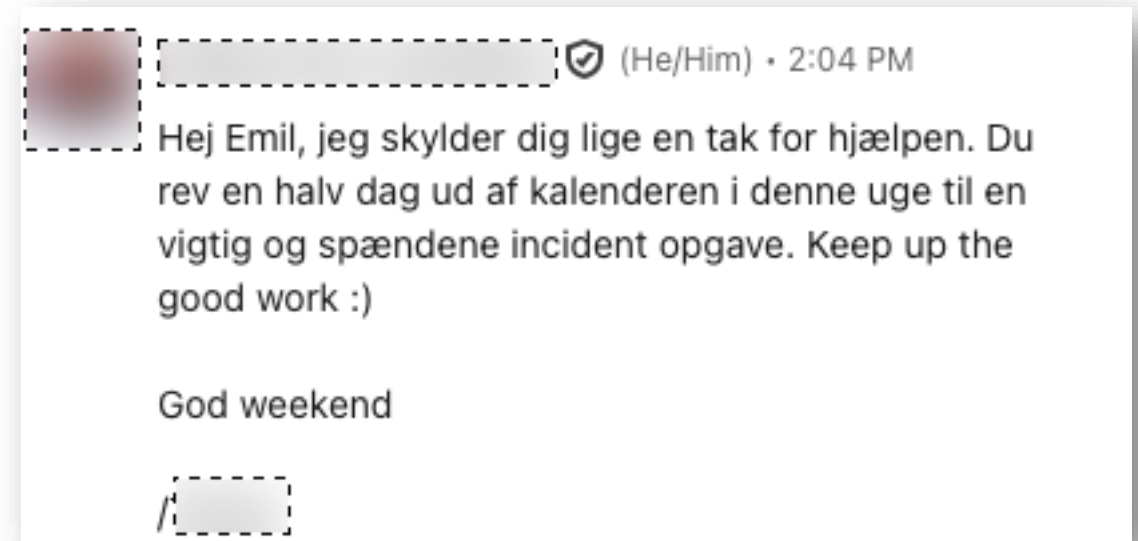
Day 2

CISO



EN: Thanks for letting us know again and for the good Process. As a thanks we will send you a hoodie, what is your size?

Senior Security Engineer



EN: Thanks for the help and for giving me an interesting task keep up the good work

Working with friendly hackers – The bad



friend 08/29/2023, 11:01 AM

Just accidentally found a pretty big security vuln at <redacted>...



me 08/29/2023, 11:09 AM

My dude
Hahaha



friend 08/29/2023, 11:12 AM

Literally a website with a live feed of all customer data for everyone ordering books from <redacted>



me 08/29/2023, 11:16 AM

Dude what



friend 08/29/2023, 11:16 AM

Including their email addresses, ID numbers, addresses, names, and phone numbers?
I doubt that part



friend 08/29/2023, 11:19 AM

Isn't that a massive GDPR violation?



me 08/29/2023, 11:20 AM

Is it a GET request?
Gotta check what my downstairs neighbor is borrowing, haha



friend 08/29/2023, 11:20 AM

Seriously, yeah, just a GET



friend 08/29/2023, 1:13 PM

That's where, using F12, I could get a live feed of all personal info + ID numbers of people borrowing books from Danish libraries

Working with friendly hackers – The bad

3 MONTHS LATER



me 11/29/2023, 2:45 PM

Any update on that library thing? It's been like 3 months



friend 11/29/2023, 2:47 PM

They never got back to me, but the site is down now

Working with friendly hackers – The ugly

1. In 2016 a Danish father finds a simple IDOR in his kindergardens software
2. He contacts the vendor Infoba
They don't respond back to him (No timeline)
3. He finds more vulns
4. Later he pops an XSS on the kindergarden personnels site
5. This makes Infoba report him to the police



EN: "Father convicted of hacking sons kindergarden"

Working with friendly hackers – The ugly



The ethical hacker

Good

Is curious when he sees something suspicious

Reports the issues to the vendor

Ugly

Doesn't wait long for a response before trying more

Performs an actual **attack** against the site



Infoba Decision makers

Good

Says they take security seriously if reported in good faith

Ugly

Has no policy for vulnerability disclosure

Does not give a timely answer of acknowledgement when receiving a report

What is ideal in regards to working with friendly hackers?

- Tryg does it well



```
← → ↻ tryg.dk/.well-known/security.txt
Contact: https://tryg.com/en/responsible-disclosure
Contact: mailto:irt@tryg.com
Preferred-Languages: en, da-DK, nb-NO, nn-NO, sv-SE
Policy: https://tryg.com/en/responsible-disclosure
Expires: Saturday, 30 Nov 2025 12:00:00 + 0200
```

What is ideal?

- Tryg does this well
- Clear purpose
- Explains legal situation (Do not hack us, but let us know)
- What is in scope (tell us about these issues)
- What is out of scope (what don't we want to hear about)
- Here is how to reach us
- We don't know about the internal procedure (CVD)

 [About us](#) [Investor](#) [Governance](#) [Press](#) [Sustainability](#) [Careers](#) [RSA](#)

Purpose: Tryg strives to make our customers and partners feel "tryg", i.e. safe and secure.

Hence it's important for us, our customers, and our partners to know that any threat to us and them is handled effectively and efficiently, which is why we maintain these responsible disclosure guidelines giving clear directions to anyone on how to report security issues to us for swift action.

Intended audience: This guideline is aimed to be read and followed by any individual, who believe to have found a security issue in Tryg's in-scope assets.

Legal boundaries >

In scope >

Out of scope >

How to report a security issue

If you detect a security issue in our in-scope assets, please email us at irt@tryg.com.

Please include the string "Responsible disclosure" in the subject to ensure proper handling of your email.

When reporting a security issue, please include these points:

- Description of the security issue with as many details as possible.
- Please describe the attack chain, which can lead to an impact to Tryg using the security issue discovered.
- Screenshot(s).
- Any thoughts on how we can mitigate the security issue.
- Contact details and preferred method of follow-up conversation (e.g. email, Skype, Teams or phone).

You must ensure that your email is sent with ≥TLS1.2 ("forced TLS") and a cipher suite currently considered secure.

If you can't ensure forced TLS, you may use the (fool-proof) option of emailing us the relevant information in a .zip- or .7z-file within a regular email to the above address, the file encrypted with a secure algorithm and password.

Deliver this password via an alternative communication channel. Please contact us to arrange this alternative communication channel (probably a text, phone call or a virtual meeting room depending on your preference).

After receiving your report, we will make our best efforts to respond to you within 15 business days.

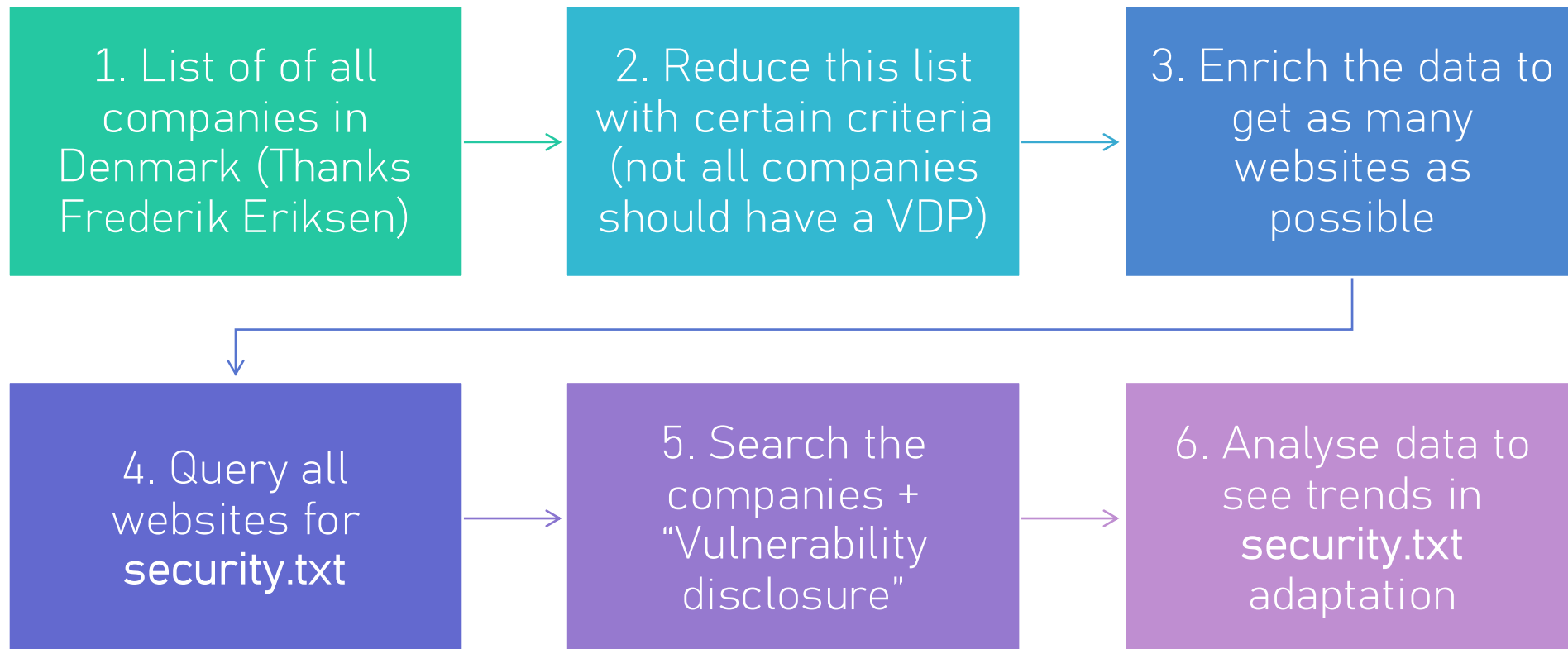
 [Contact IR](#)  [Download](#)

A close-up, artistic photograph of a person's hand pointing at a digital screen. The screen displays a line graph with a blue background and a red line that trends upwards from left to right. The line has several small, circular markers along its path. The lighting is dim, with the screen being the primary light source, creating a blue glow on the hand and the surrounding environment. The text 'Lets figure how how the digital Denmark is doing' is overlaid in white on the left side of the image.

Lets figure how
how the digital
Denmark is
doing



How to approach this



The starting point

```
(venv) emilhorning@EmilMac virksomhed_analyse % wc -l data/virksomheder_2.csv
578205 data/virksomheder_2.csv
```

Column Name	Data Type	Description
company_id	String	Unique identifier for the company
name	String	Official name of the company
email	String	Primary contact email address
webpage	String	Company website URL
short_description	String	Brief company type description (e.g., APS, A/S, FOR, FON)
industry_code	String	Danish industry classification code (DB93)
capital	Decimal	Registered capital amount
number_of_employees	Integer	Total number of employees

Reduction - Company types

APS	Anpartsselskab	337315	58.34
FFO	Frivillig forening	84656	14.64
PMV	Personligt ejet Mindre Virksomhed	40498	7.00
FOR	Forening	35678	6.17
A/S	Aktieselskab	29996	5.19
I/S	Interessentskab	17752	3.07
FON	Fonde og andre selvejende institutioner	7202	1.25
ØVR	Øvrige virksomhedsformer	4964	0.86
UDL	Anden udenlandsk virksomhed	4876	0.84
K/S	Kommanditselskab	3511	0.61
EUO	Enhed under oprettelse i Erhvervsstyrelsen	2039	0.35
KAS	Kommanditaktieselskab/Partnerselskab	1772	0.31
ANS	Andelsselskab (-forening)	1698	0.29
FKI	Folkekirkelige Institutioner	1682	0.29
EFO	Erhvervsdrivende fond	1312	0.23
FAS	Filial af udenlandsk aktieselskab, kommanditakties	595	0.10
ABA	Andelsselskab (-forening) med begrænset ansvar	494	0.09
FAP	Filial af udenlandsk anpartsselskab eller selskab	435	0.08
FMA	Forening med begrænset ansvar	375	0.06
SMA	Selskab med begrænset ansvar	350	0.06
STA	Statslig administrativ enhed	225	0.04
DØD	Dødsbo	213	0.04
FIV	Særlig finansiel virksomhed	167	0.03
GUS	Grønlandsk afdeling af udenlandsk selskab eller virksomhed	139	0.02
KOM	Primærkommune	100	0.02
PAR	Partrederi	82	0.01
UOP	Uoplyst virksomhedsform	17	0.00
FES	Filial af SE-selskab	17	0.00
FBA	Filial af udenlandsk virksomhed med begrænset ansv	11	0.00
SOV	Selvstændig offentlig virksomhed eller dattervirksomhed heraf	8	0.00

Reduction – Company industry codes

014920	Avl af pelsdyr mv.	871020	Institutionsophold med sygepleje i.a.n.
475300	Detailhandel med tæpper, vægbeklædning og gulvbelægning	581300	Udgivelse af ugeblade og magasiner
477610	Detailhandel med blomster og planter	015000	Blandet landbrugsdrift
603100	Nyhedsbureauers aktiviteter	515310	Engroshandel med træ, trælast og byggematerialer
477120	Detailhandel med baby- og børnetøj	932990	Drift af andre forlystelser og fritidsaktiviteter
662200	Forsikringsagenters og forsikringsmæglers aktiviteter	561110	Servering af mad i restauranter og caféer
104100	Fremstilling af olier og fedtstoffer	032100	Havbrug
791200	Rejsearrangørers aktiviteter	682040	Udlejning af erhvervsejendomme
682010	Udlejning af almennyttige boliger	243300	Koldbehandling
289500	Fremstilling af maskiner til produktion af papir og pap	873010	Drift af døgninstitutioner for personer med fysisk handicap
204200	Fremstilling af parfume, hårshampoo, tandpasta mv.	302000	Fremstilling af lokomotiver og andet rullende materiel til jernbaner
012200	Dyrkning af tropiske og subtropiske frugter	012500	Dyrkning af andre træfrugter, bær og nødder
920000	Lotteri- og andre spilleaktiviteter	131000	Forbehandling og spinding af tekstilfibre
279000	Fremstilling af andet elektrisk udstyr	321300	Fremstilling af bijouteri og lignende varer
461890	Agenturhandel med specialiseret varesortiment, bortset	641100	Centralbankers aktiviteter
106100	Fremstilling af mølleriprodukter	889120	Drift af vuggestuer
722200	Udvikling af kundespecifikt software og konsulentbistand	592000	Indspilning af lydoptagelser og udgivelse af musik
649910	Investering for egen regning	464420	Engroshandel med rengøringsmidler
952300	Reparation og vedligeholdelse af fodtøj og lædervarer	463100	Engroshandel med frugt og grøntsager
161200	Forarbejdning og færdigbearbejdning af træ	903910	Teknisk planlægning, levering, opsætning og betjening af udstyr til
841300	Administration af og bidrag til erhvervsfremme	476910	Detailhandel med musikinstrumenter
259100	Fremstilling af metaltønder og lignende beholdere	151200	Fremstilling af tasker, kufferter, sadelmagervarer mv., uanset mater
970000	Aktiviteter i husholdninger med ansat medhjælp	201200	Fremstilling af farvestoffer og pigmenter
012900	Dyrkning af andre flerårige afgrøder	711210	Rådgivende ingeniøraktiviteter inden for byggeri og anlægsarbejder

781 Different industry codes for all Danish companies

Reduction – Public institutions



– STA (Statslig administrativ enhed) – State administrative units



– REG (Region) – Regions



– KOM (Primærkommune) – Municipalities



– SOV (Selvstændig offentlig virksomhed) – Independent public companies



– In total: 337 companies

Reduction – Private companies



- – Must be **A/S** (Aktieselskab) OR **APS** (Anpartsselskab) in these industries:
- – 582100 | Publishing of computer games
- – 582900 | Other software publishing
- – 611000 | Provision of fixed, wireless and satellite telecommunications
- – 612000 | Resale of telecommunications and telecommunications brokerage activities
- – 619000 | Other telecommunications activities
- – 620200 | Information technology consultancy activities
- – 621000 | Computer programming
- – 622000 | Information technology consultancy activities and management of IT facilities
- – 629000 | Other IT service activities
- – 631000 | IT infrastructure, data processing, hosting and related activities
- – 631100 | Data processing, web hosting and related services
- – 639100 | Operation of Internet portals
- – 639200 | Other information activities

Reduction – General filtering

- Large Companies (ANY type)
 - Companies with >250 employees
 - Count:1,207 companies
- Top Companies by Capital (ANY type)
 - Top 3000 companies by reported capital
 - Count: 2,214 companies

Reduction – Other sources



Ask Claude / ChatGPT / Grok

"Give me a list of 1000 Danish companies that should have a VDP"



Berlingske top 1000

Top companies on revenue.
Take the list over the last many years
and

Reduction of the reductions

- Take all these companies, but exclude them if their name contains:
 - "fond" (fonds)
 - "holding" (holding companies)
 - "invest" (investment companies)



Total results after reductions:

Category	Count	~ % of Total
Public entities (STA, REG, KOM, SOV)	337	1.8%
Private IT companies (A/S or APS with IT codes)	14,859	79.8%
Companies with >250 employees	1,207	6.4%
Top 3000 by capital	1,710	9.1%
Companies suggested by LLM + Berlingske	504	2.7%
Total unique (with overlaps)	18,617	100%

Next task: Find their websites



Getting more websites from contact email

- Not all companies have their domain set in the dataset,
- but they have a contact email.
- We check if its a unique domain (not a service provider) then this is a good indicator

gmail.com, hotmail.com, hotmail.dk,
outlook.com, outlook.dk, live.dk, live.com,
mail.dk, me.com, yahoo.dk, yahoo.com
,icloud.com

4,866 → 8,873
~26 % → ~47 %

Getting more websites from .dk domains

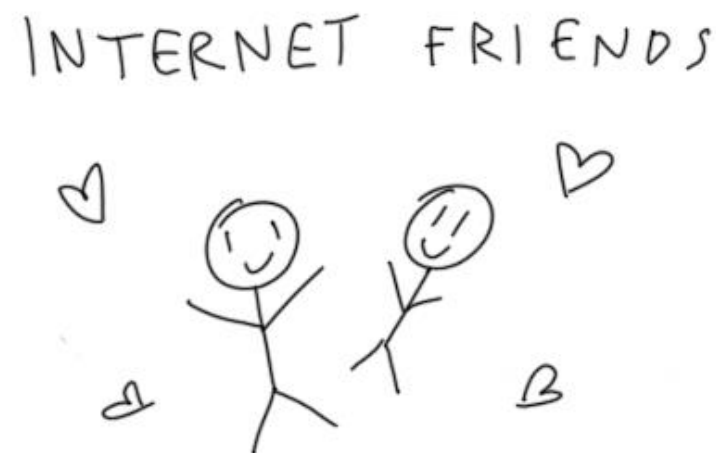
1. <https://wallnot.dk/dotdk/> contains a list of 1.212.913 .dk domains
2. Query the https:// webroot for all
3. Look for the words CVR
Check if there is a CVR number (8 numbers) in the vicinity (50 characters ahead)
4. Map this website to the company
5. (Potential errors, we live with them)



8,873 → 10,216
~47 % → ~54 %

Getting more websites from friends

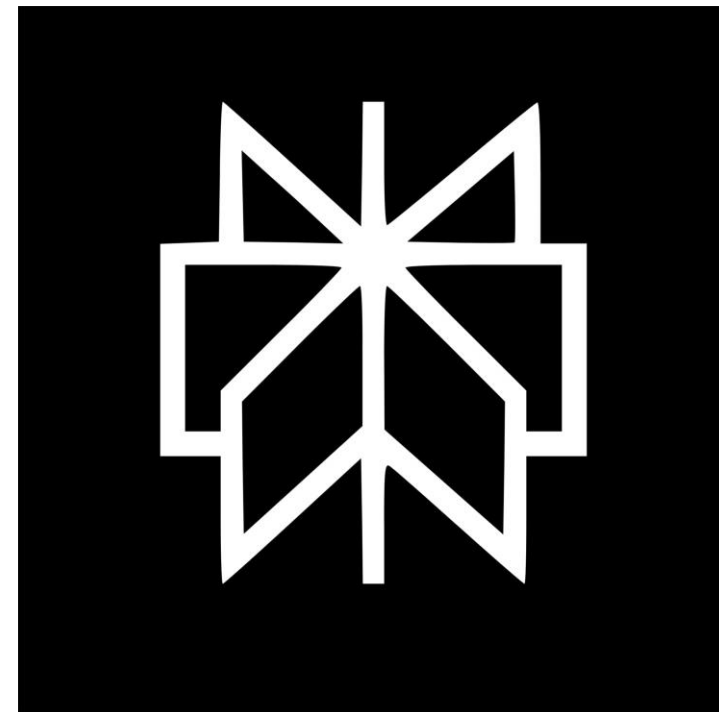
- Apparently cvr enrichment is something people fancy
- Got a list of CVR to website list from a friend: Tobias Evar Lauridsen from DC
 - Certificate transparency
 - Whois lookups
 - RDAP lookups
- Dansk Industri keeps a list of members with CVR and associated website



10,216 → 11,502
~54 % → ~61 %

Getting the last websites with perplexity

- Ask the LLM overlords to search for the last ones out
- *<COMPANY NAME> (ApS or A/S) website Denmark*
- Blindly trust what comes back.
- Filter off aggregators (Proff, Virk etc.)
- Left with a good website coverage!
- Perplexity was the best price: ~120 usd



11,502 → 18,103
~54 % → ~98 %

Landing on a final number of companies

- Remove companies that obviously don't have a website
- But include companies from previous research that has a security.txt
 - But not those who have one from a software provider
 - Like nextcloud or moodle

https://philipps.dk/well-known/security.txt https://rahbox.dk/well-known/security.txt https://rehm.dk/well-known/security.txt https://voresminder.dk/well-known/security.txt	Contact: https://hackerone.com/nextcloud Expires: 2023-04-30T23:00:00.000Z Acknowledgments: https://hackerone.com/nextcloud/thanks Acknowledgments: https://github.com/nextcloud/security-advisor Policy: https://hackerone.com/nextcloud Preferred-Languages: en
--	---

Cant use ❌

https://safepaynordic.dk/well-known/security.txt	Contact: mailto:administrator@safepaynordic.dk Expires: 2032-01-01T12:00:00Z
https://coolstuff.dk/well-known/security.txt	Contact: mailto:admin@coolstuff.com Expires: 2025-12-31T23:59:59.000Z Preferred-Languages: en, sv Canonical: https://www.coolstuff.se/well-known/security.txt

Can use ✅

Final Number: 18,355

Now we are left with this, these are the companies that SHOULD* have a VDP

- 18,355 companies with a domain
- Request `/security.txt` or `/.well-known/security.txt`
- Parse the results and verify it follows the standard
- Some sites give generic 404, so exclude those.



* I mean who am I to judge, there are regulators for that

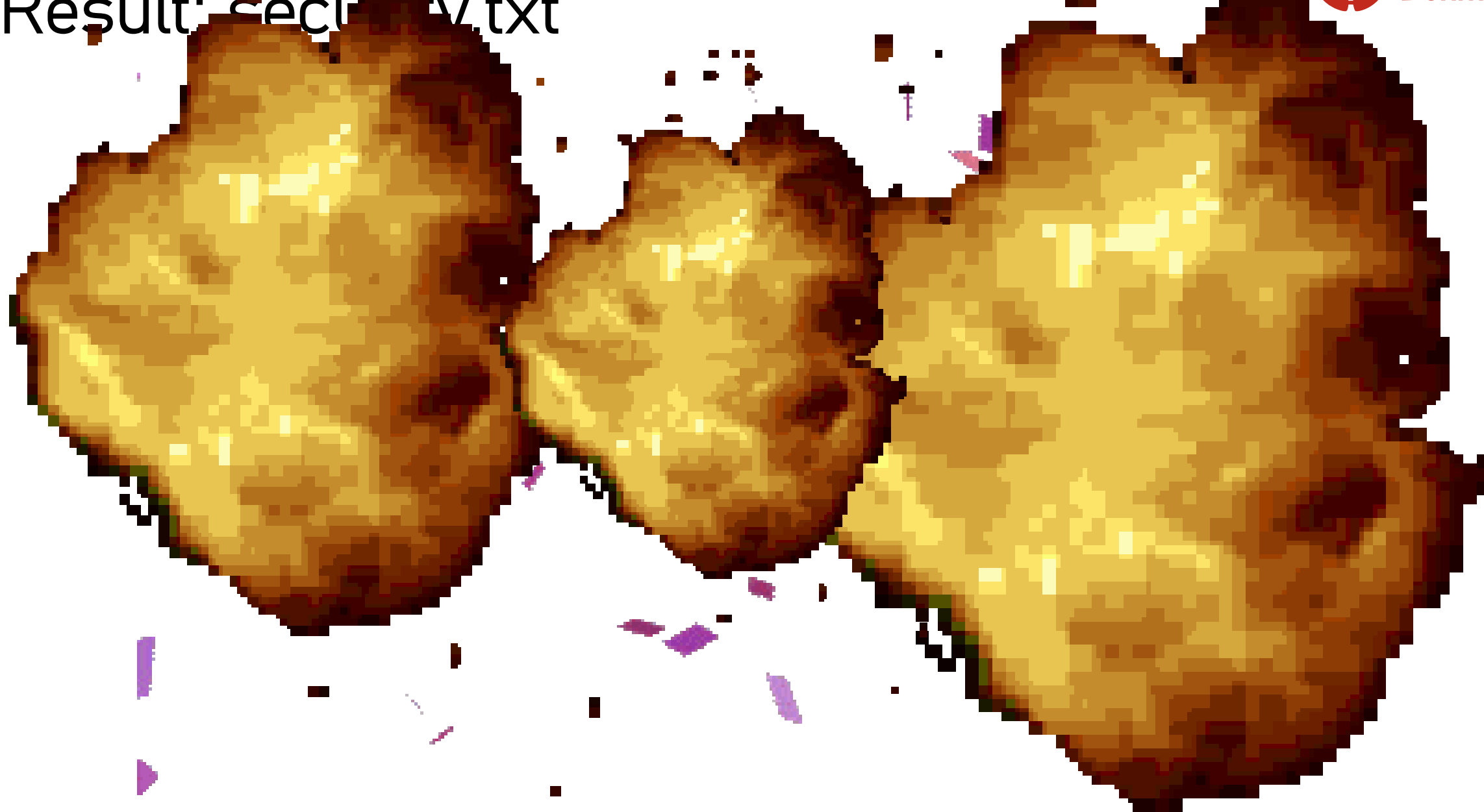
Result: security.txt



848 valid security.txt

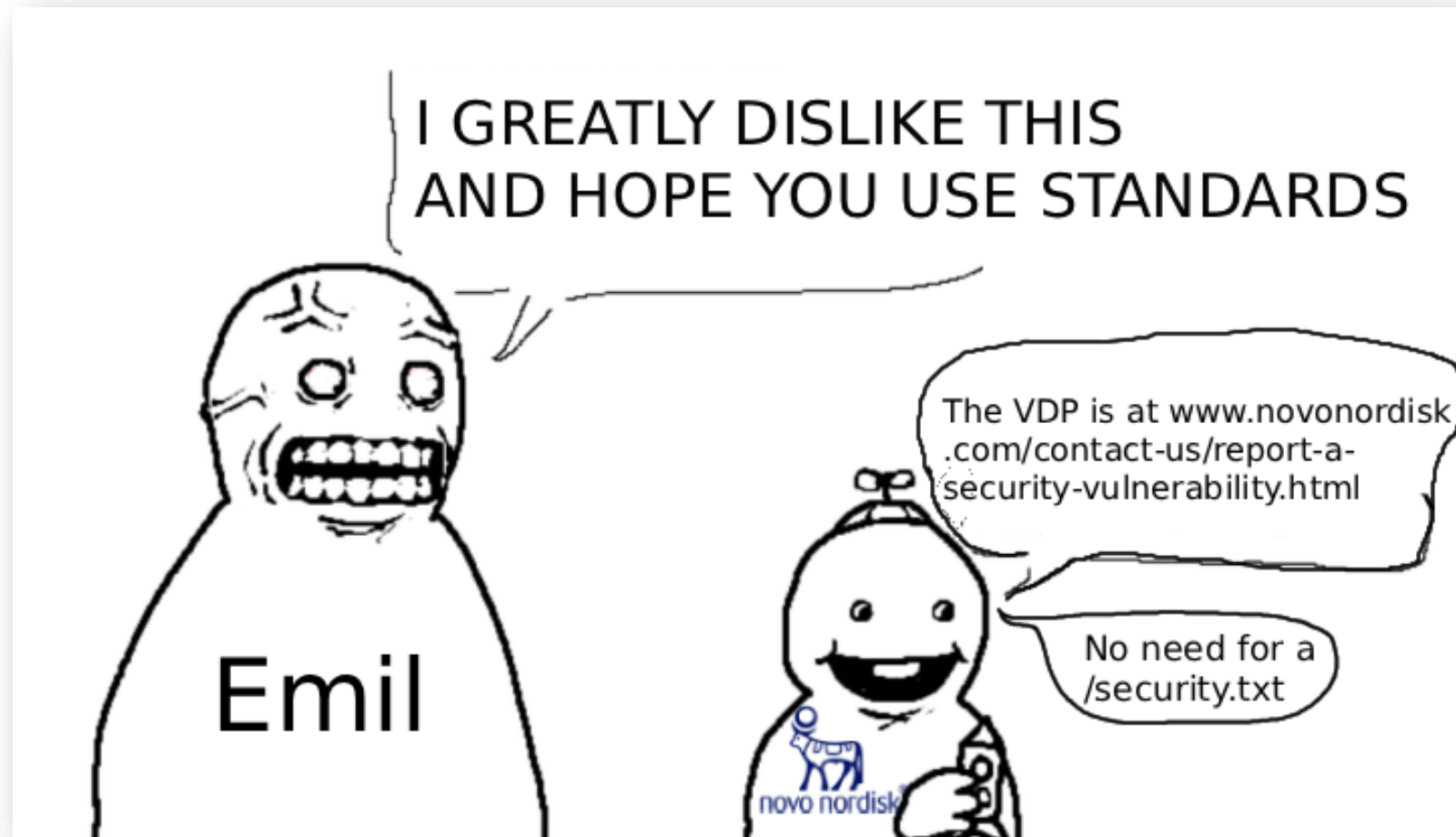


Result: security.txt



THE CATCH

- Some companies have a VDP
- That's great, that's fine, really cool
- But then they don't have a security.txt to reference to it



Lets fix it

- Use Perplexity to help search for VDP links for companies
- This is expensive so we cannot do it on the remaining ~17.000 companies
- Analyze top 1500 companies on size (employees)
- Analyze top 1500 companies on capital
- Find vulnerability disclosure links and analyze them



Lets fix it

```
61
62 def process_company(company_name):
63     """
64     Process a single company: get Perplexity data see if they have responsible disclosure info
65     """
66     print(f"Processing: {company_name}")
67
68     model = "sonar-pro"
69     response_format = {
70         "type": "json_schema",
71         "json_schema": {"schema": AnswerFormat.model_json_schema()},
72     }
73
74     web_search_options = {
75         "search_context_size": "medium",
76         "user_location": {
77             "country": "DK"
78         }
79     }
80
81     messages = [
82         {"role": "system", "content": "The goal is to find links and research about danish companies' stances on vulnerability disclosure."},
83         {"role": "user", "content": f"""
84         You must perform research on Danish companies stances on vulnerability disclosure.
85         Search for this Danish Company: "{company_name}".
86         Please output a JSON object containing the following fields (you are allowed to provide empty strings if no information is found), the comment can MAXIMUM be 100 characters long:
87         company_website (only one), has_responsible_disclosure, responsible_disclosure_link, relevant_security_links, comment"""
88     ]
89
90
91     try:
92         client = OpenAI(api_key=YOUR_API_KEY, base_url="https://api.perplexity.ai")
```

Result: security.txt



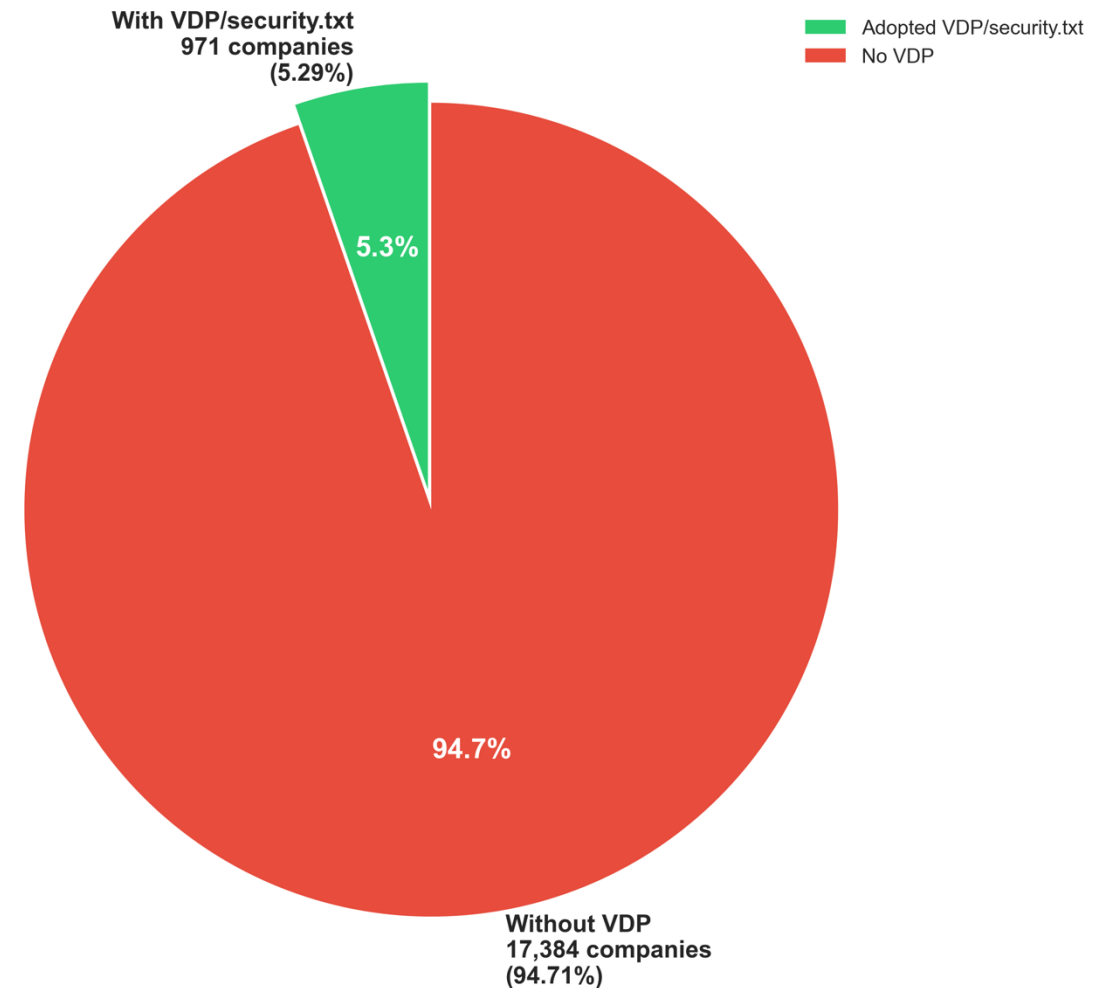
123 valid VDP



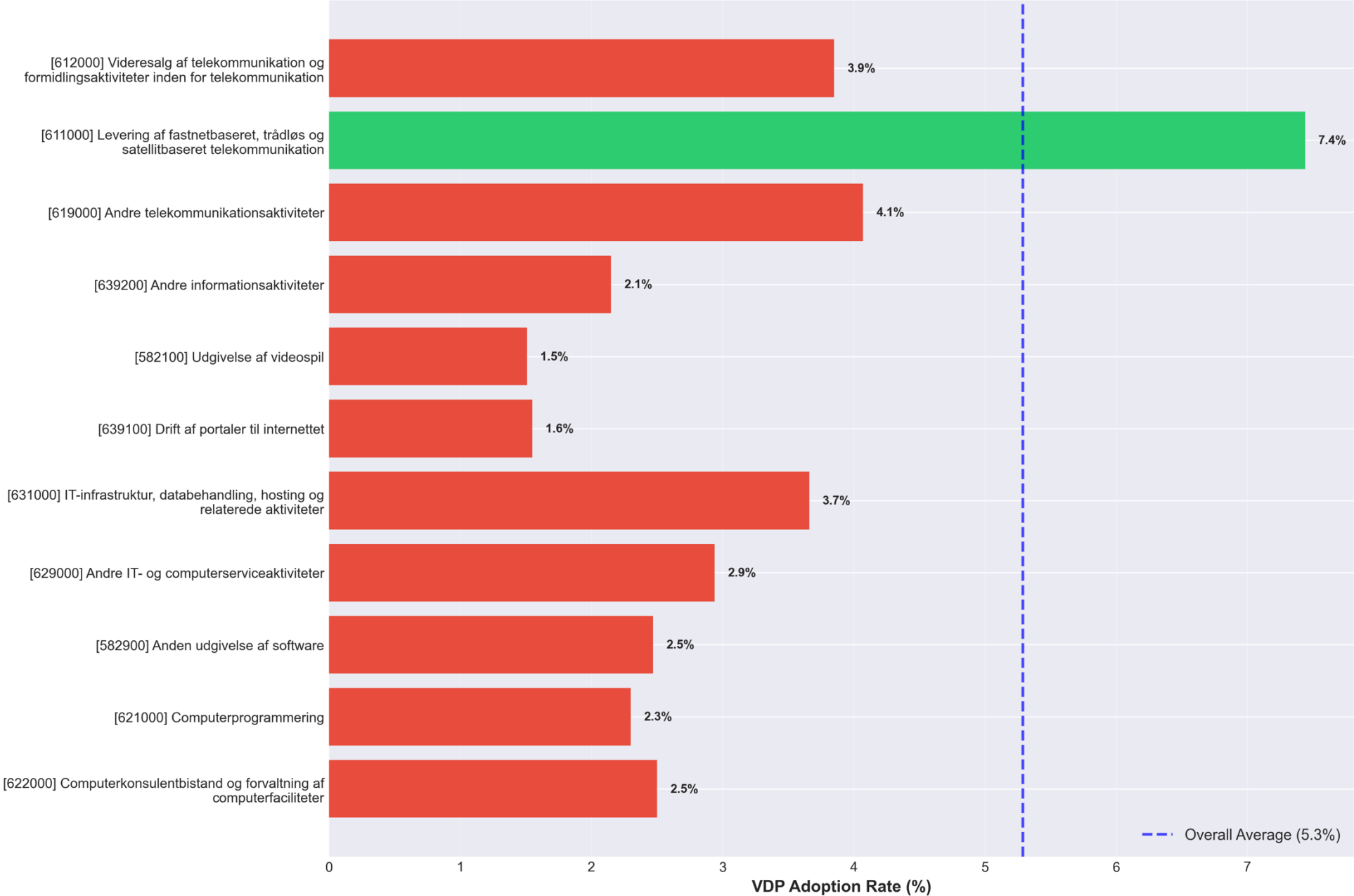
971 companies ~5% adoption

- Of companies that we filtered for specifically
- Naturally some of these companies may not need this
- Some of the companies may not be mature enough to have this
- But at the same time, I believe there are more than 971 companies in DK who are mature enough.

VDP/Security.txt Adoption in Danish Companies
(Total: 18,355 companies)



IT Industry VDP Adoption by Sector
(Green = Above Average, Red = Below Average)



Financial industry – Banks

- According to Wiki: 48 banks with more than 1 billion (milliard) in capital *
- 12 banks (~25%) have a VDP

Danske Bank

 JYSKE BANK

Sydbank

 SAXO
BANK

 Ringkjøbing
Landbobank

 SPAREKASSEN
SJÆLLAND-FYN

 DJURSLANDS BANK

 SKJERN BANK

 LUNAR

 Kreditbanken
- Sønderjyllands lokale bank

 Nordfyns Bank

 kompasbank

*https://da.wikipedia.org/wiki/Danske_pengeinstitutter_efter_st%C3%B8rrelse

The public sector

- Total government entities: 337
- 5 municipalities with VDP
- 1 region with VDP
- 4 state entities with VDP
- Lets see them!!!

Type	Description	Total	With VDP	Percentage
KOM	Kommuner (Municipalities)	100	5	5.00%
REG	Regioner (Regions)	5	1	20.00%
SOV	Selvejende (Self-Governing)	7	1	14.30%
STA	Staten (State Agencies)	225	3	1.3%
TOTAL	All Public Sector	337	10	2.97%

The public sector



AARHUS UNIVERSITET

Type: security.txt
Employees: 12799



Type: Security.txt + VDP
Employees: 5856

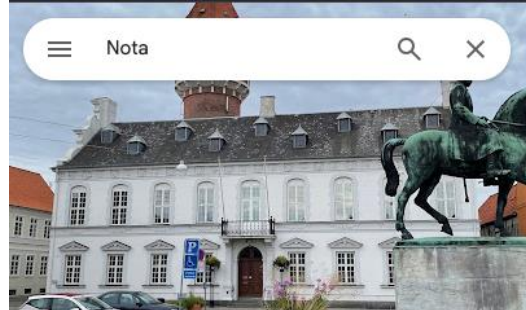


Type: Security.txt
Employees: 377



Type: Security.txt
Employees: 1*

Nota



Nota

4,1 ★★★★★ (19) ⓘ

Bibliotek · 📄

Oversigt

Anmeldelser

Om



Rutevejledning



Gem



I nærheden



Send til telefon



Del



Axeltorv 6, 4900 Nakskov



Lukker snart · 15.00 · Åbner 08.00 fre. ▾



nota.dk



39 13 46 00



R4JP+69 Nakskov



Ejer du denne virksomhed?



Din Maps-aktivitet



Tilføj en etiket

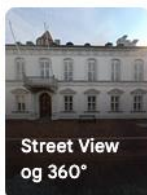


Foreslå en ændring

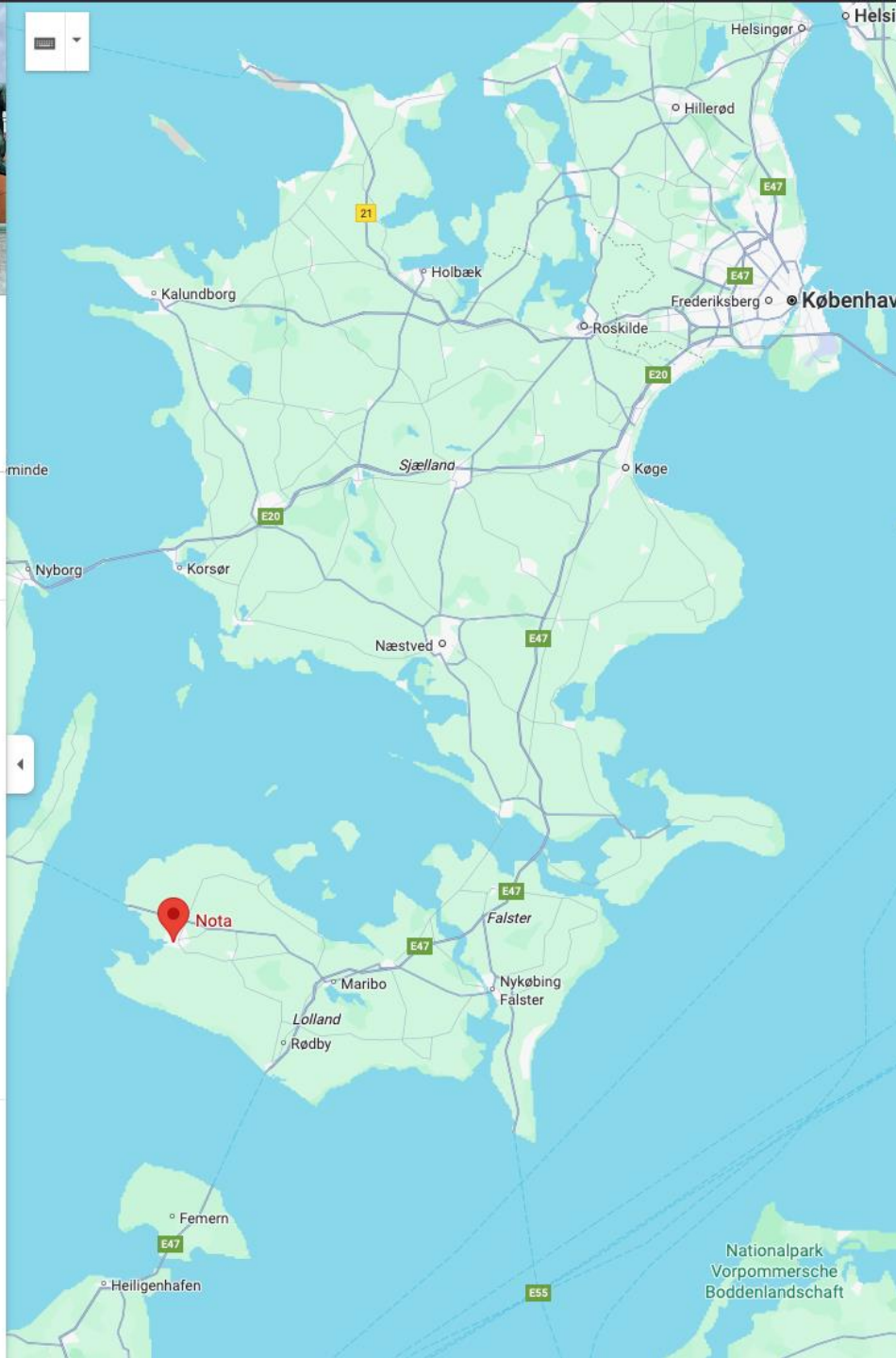
Billeder og videoer



Alle

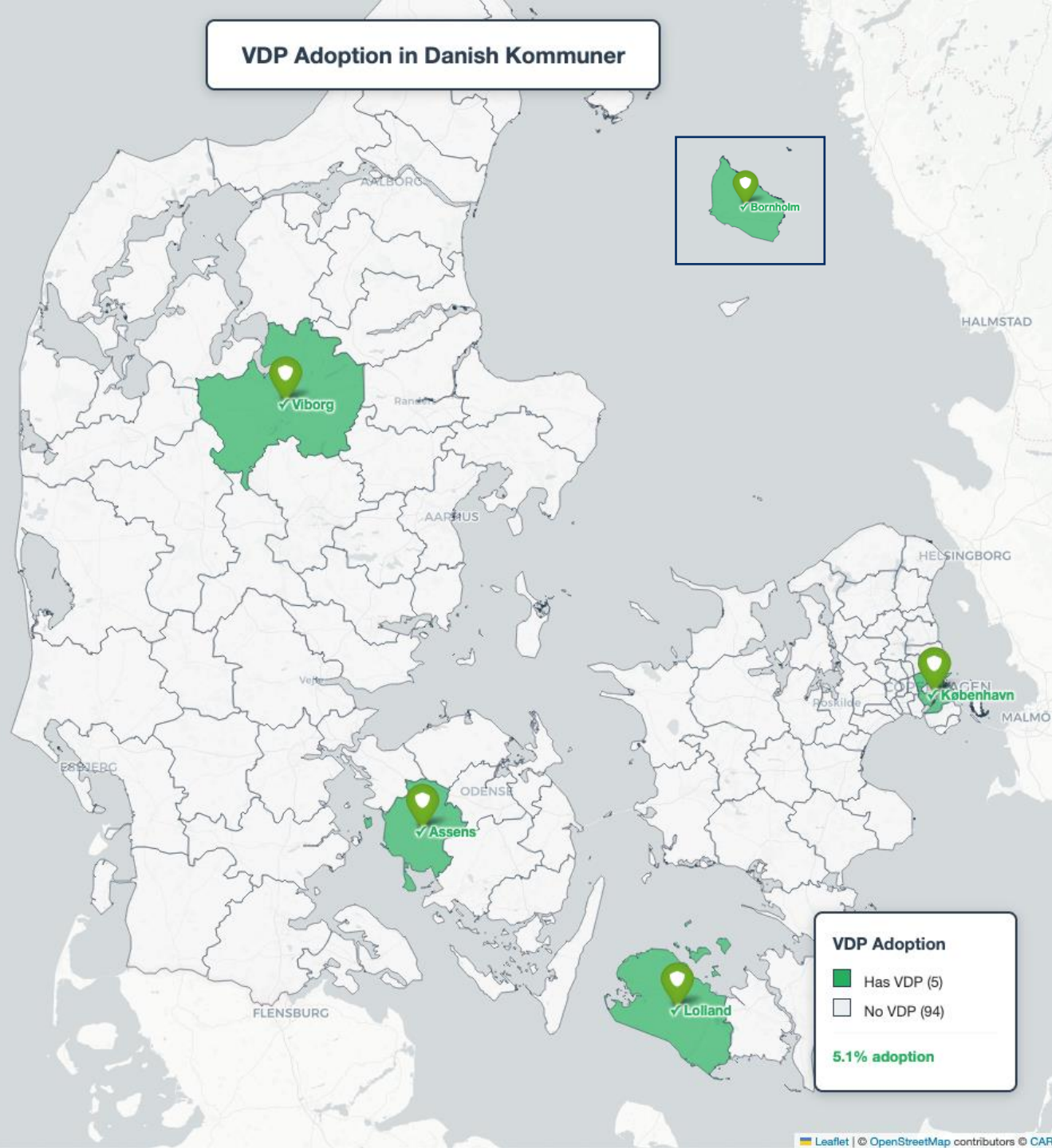


Street View
og 360°

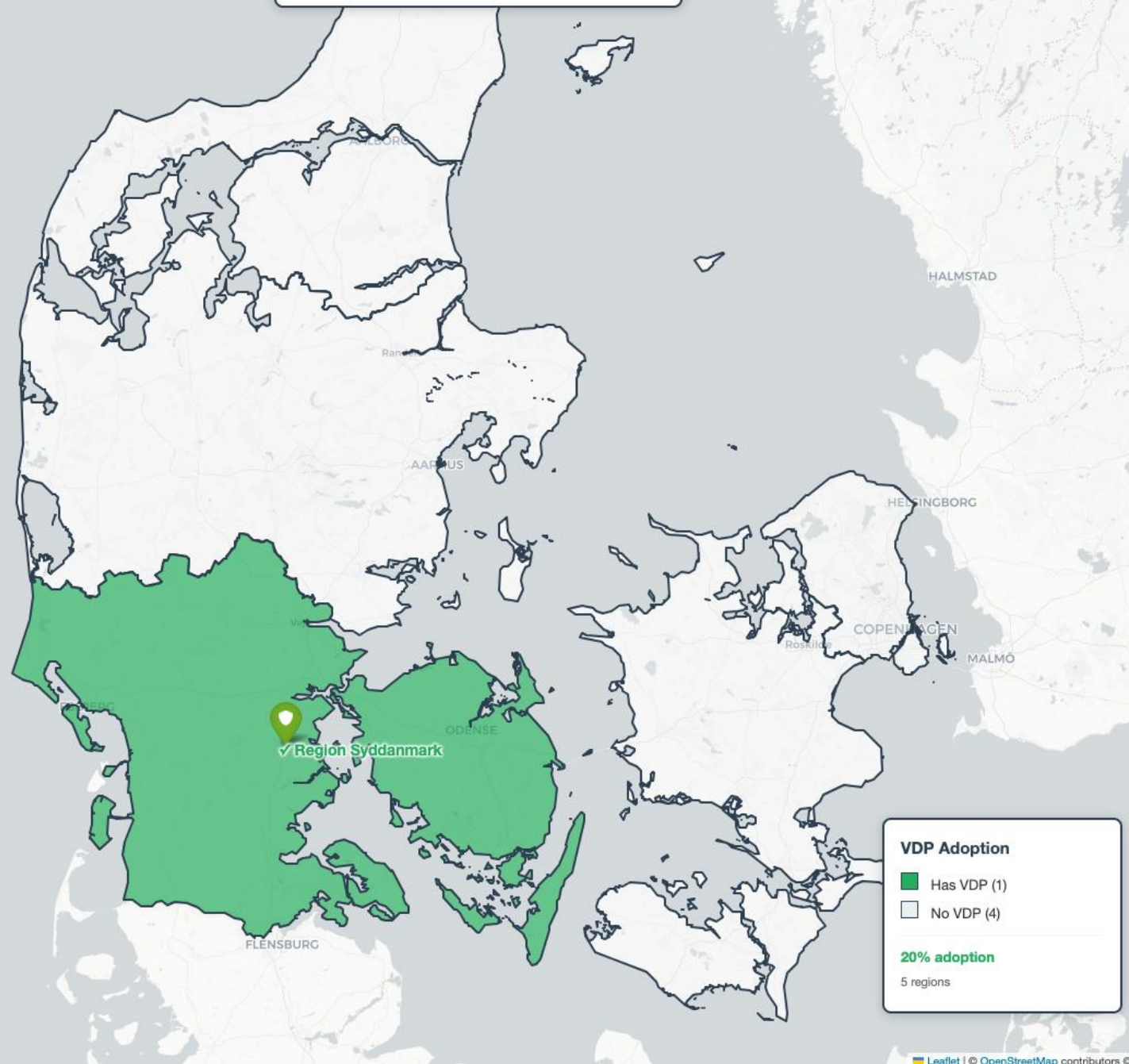




VDP Adoption in Danish Kommuner



VDP Adoption in Danish Regions



The universities



IT-UNIVERSITETET I KØBENHAVN



SDU 

The logo for SDU (Syddansk Universitet) includes the letters 'SDU' in a bold, black, sans-serif font, followed by a black icon of a branch with three leaves.

RUC

The logo for RUC (Roskilde Universitet) is the letters 'RUC' in a bold, black, sans-serif font.

The universities

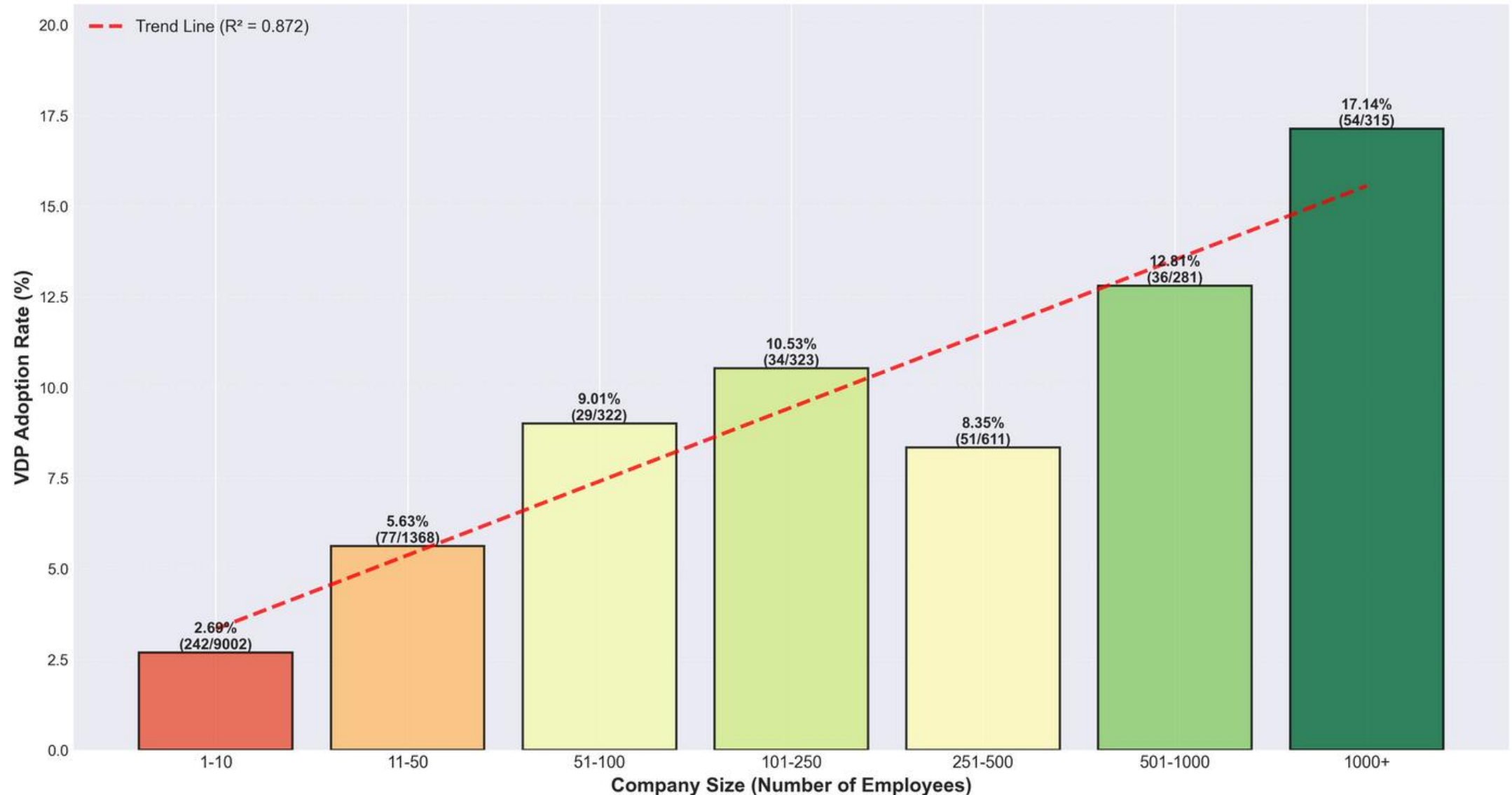
1/8



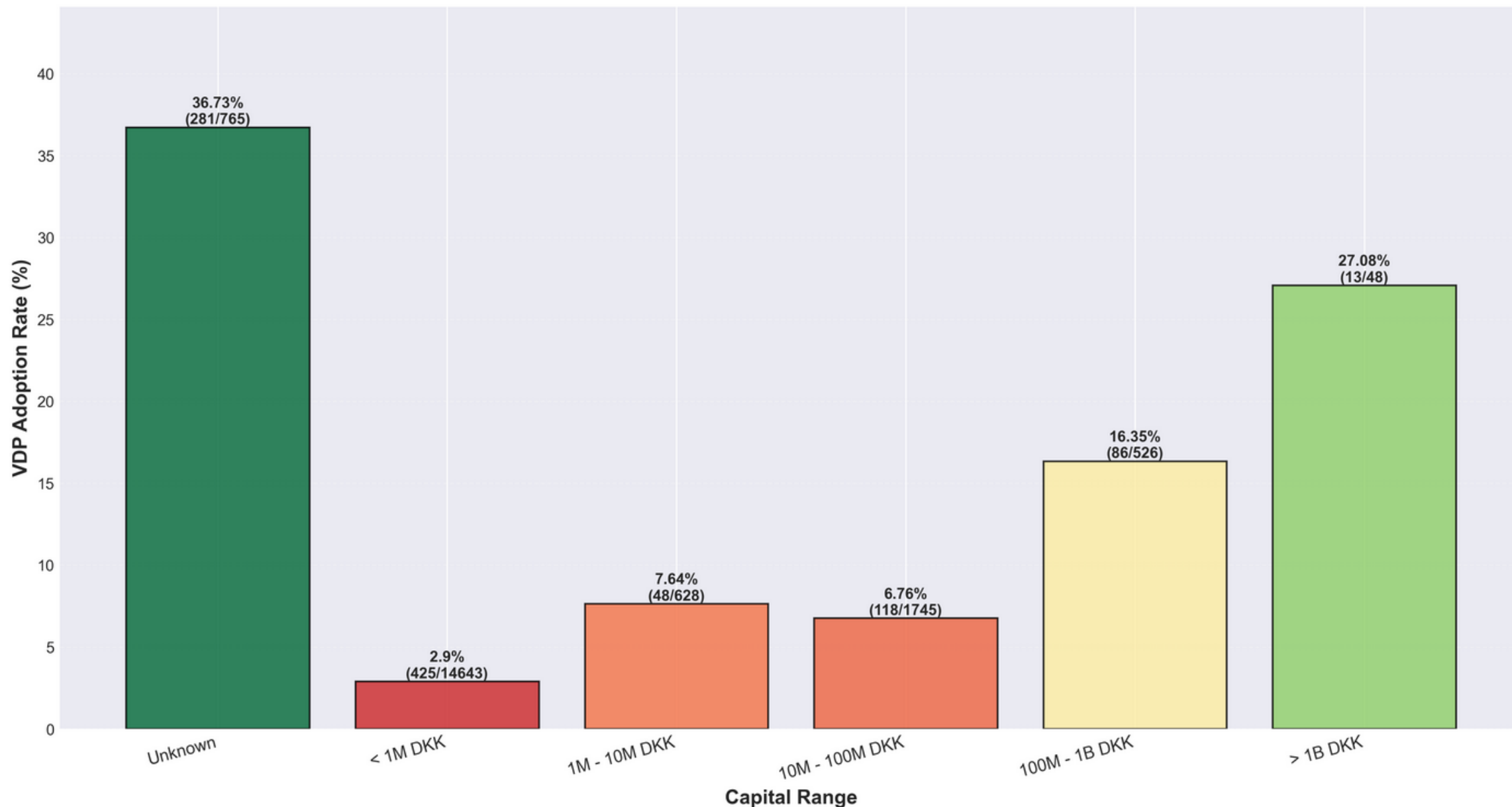
IT-UNIVERSITETET I KØBENHAVN



Size of company correlates with VDP adption



Capital of company correlates with VDP adption



How about bug bounty 🤖💰

Not very utilized, mostly large companies or international companies

- Visma
- Queue-It
- Too Good To Go
- DBA/Bilbasen/Bilinfo (Via Vend)
- SumUp
- WithSecure
- CM.Com Danmark
- Six Danmark
- Palantir Technologies Danmark
- BitDefender
- Spotify Danmark
- Toyota Danmark

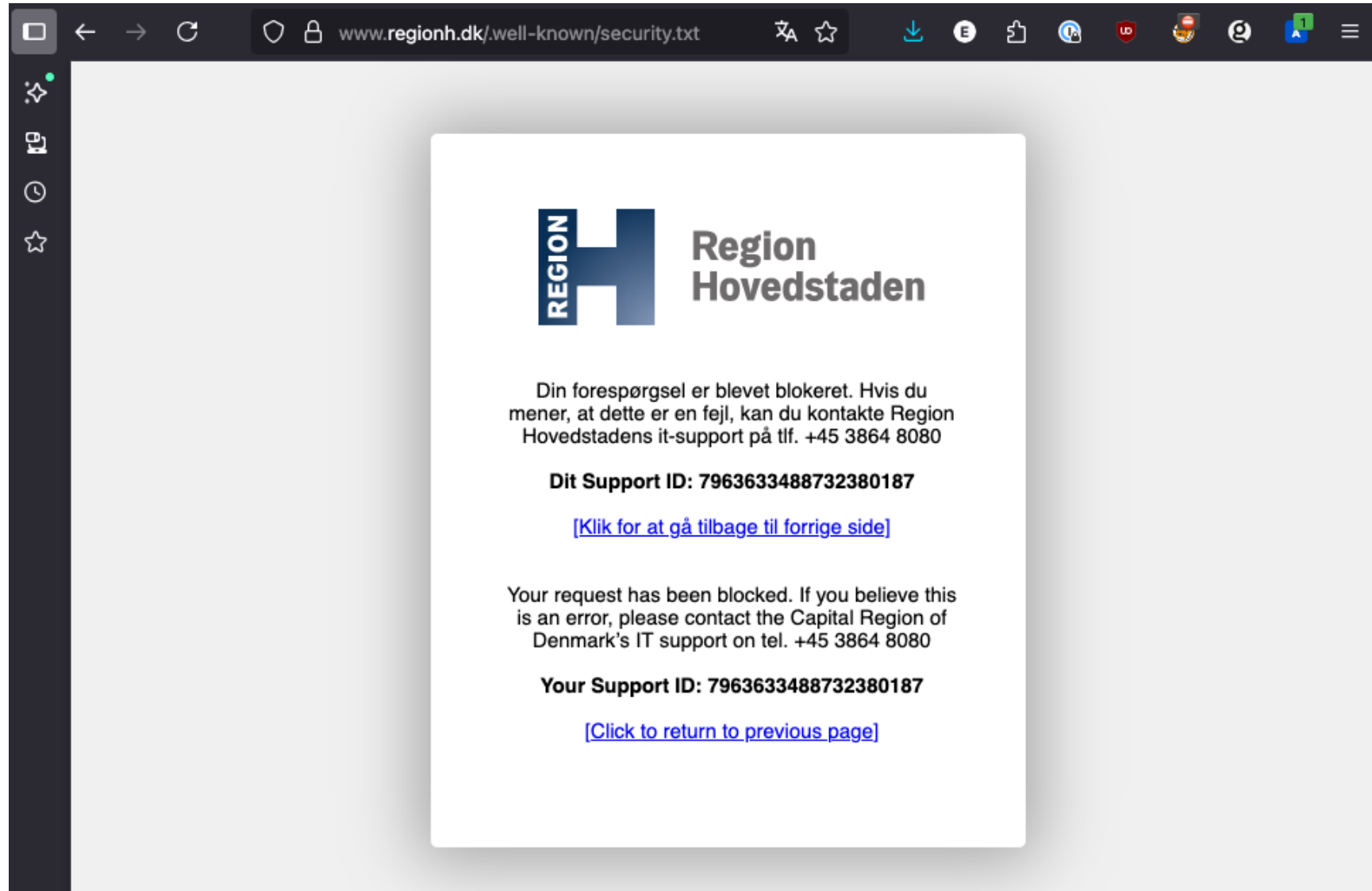


Lets end on a high note with some funny findings



Funny findings 1

REGION H BLOCKING
REQUESTS FOR
SECURITY.TXT



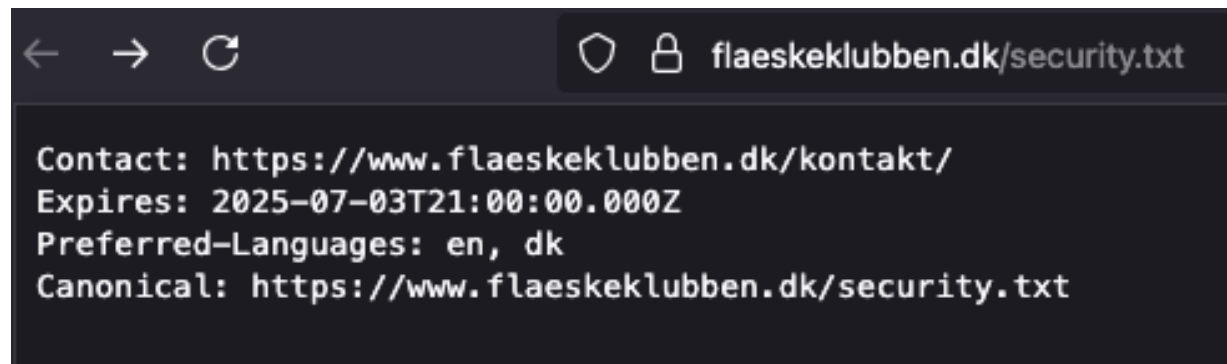
Contact: mailto:security@aboutyou.com
Expires: 2026-11-01T00:00:00.000Z
Preferred-Languages: en, de
Hiring: <https://corporate.aboutyou.de/en/departments/tech#jobs>



So F***ing Special

Funny findings 3

150 mænd spiser sig gennem 200 kilo stegt flæsk



Funny findings 4



Yasmin hviler sig



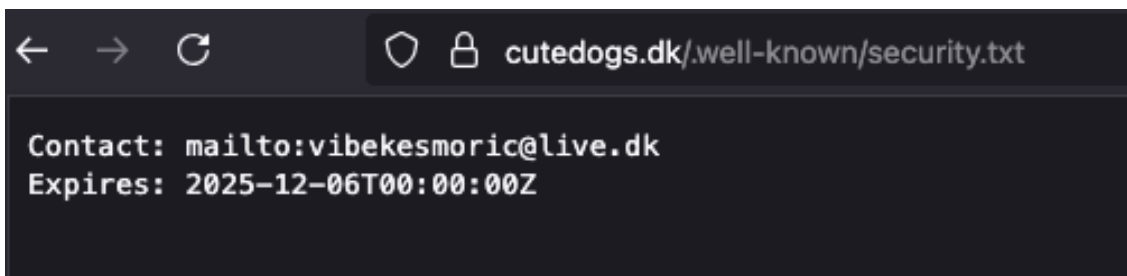
Sultne munde mættes



Aika



Abby



Funny findings 5:

Death by *beg bounty hunters*

```
← → ↻  powerhosting.dk/.well-known/security.txt

Contact: mailto:abuse@powerhosting.dk
Expires: 2099-02-01T07:00:00.000Z
Preferred-Languages: en, dk
Canonical: https://powerhosting.dk/.well-known/security.txt
#
# Please do not spam us with trivial X-frame By-Pass "vulnerabilities"
# -It is a waste of both yours and ours time! Cheers!
```

Funny findings 5:

Death by *beg bounty hunters*

Issue detail:-

The web server contains a robots.txt file.

Issue background:-

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation:-

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

We have found more bugs/vulnerability in your website. Kindly clarify if there is any payout if we disclose them to you?

We understand but my team worked very hard to find these bugs in your website. We have found more. If you can pay us small token of appreciation 100-150\$ we will submit all of our reports.

So what can you do now?

- Figure out if your organization has a security.txt
- If not, then create one:
<https://securitytxt.org/>
- Figure out if you should have a vulnerability disclosure policy
- Figure out your internal process when a security researcher inevitably contacts you
- Consider if you want to incentivize ethical hackers to find bugs in your systems for bounties
 - In that case, lets talk.

securitytxt.org

Step 1

Create a text file called `security.txt` under the `.well-known` directory of your project.

Recent changes to the specification

The date format for Expires has changed to ISO 8601. An example of the new format is `Expires: 2021-12-31T18:37:07.000Z`.

Contact Required

A link or e-mail address for people to contact you about security issues. Remember to include "https://" for URLs, and "mailto:" for e-mails. See [the full description of Contact](#)

Add another alternative

Expires Required Only 1 allowed

The date and time when the content of the security.txt file should be considered stale (so security researchers should then not trust it). Make sure you update this value periodically and keep your file under review. See [the full description of Expires](#)

Add another alternative

Encryption Optional

A link to a key which security researchers should use to securely talk to you. Remember to include "https://". See [the full description of Encryption](#)

Add another alternative



Emil Hørning

Fremmer Bugbounty i 🇩🇰 med Defend
Denmark | OSCP, OSCE3

