5 months into the regulation enforcement
How does the landscape look like

Tales from the trenches

Majority of penalties

1. Security and data breach (even for tiny companies)
2. Unappropriate marketing usage of personal data

Being Privacy-friendly is a significant selling point.

It shows your client that you are serious about their personal data and security.

SIGNAL OF TRUST and Accountability

25th of May deadline

only for big companies under the DPAs scrutiny

Authorities:

> *two years transition period for SMBs*

BUT:

- Only for new obligations
- Things that are different from previous privacy laws

Most likely risks for Software companies

Most of the fines related to Security

Security and proper data management becomes a liability

Think: Access Control, Data Lifecycle, overall security measures

Penalties mechanism:

Complaint filed to a DPA

Then

1. inquiry from the DPA,
2. recommendations issued,
3. other reprimand,
4. and if still not right -> fine.

Fines effective, proportionate and dissuasive

Examples of fines

security · data leaks · unauthorized marketing

CNIL

- Retail firm fined 100 000€ for negligence over processor actions follow-up
- Optician retail firm fined 250 000€ for violation of customers' personal data

ICO

- Heathrow Airport Limited fined £120,000 for serious failings in its data protection practices
- Firm fined £90,000 for nuisance emails about pre-paid funeral plans

Deadly sins

Consent campaign: you don’t have to do that

Either you have consent, or you don’t

Proof through ESP service

Bulk email addition
Do you have other legal ground than consent?

Consent not always the best legal base for processing

- Can you rely on other legal ground?

  contract, legal obligation, legitimate interest

- Document your choice
- Inform your users

Examples of legitimate interest:

- Mailing campaign to past customers
- Newsletter to subscribers of your service
- Newsletter after lead magnet

Conduct a balancing test

“Read my new privacy policy” campaign

not useful:

List of ‘we change this and that,’
User has no `diff`

useful:

- “this particular bit” has been replaced with “this other thing”.
- “You can contact us at such-and-such”

Provide information and reason why you need the data

It’s the law, BUT do not forget the WHY :

You want customers to trust you

What’s the landscape for tech companies

Who did nothing?

What’s the landscape for tech companies

Who did nothing?

Just started?

What's the landscape for tech companies

Who did nothing?

Just started?

50% complete/ still implementing?

What's the landscape for tech companies

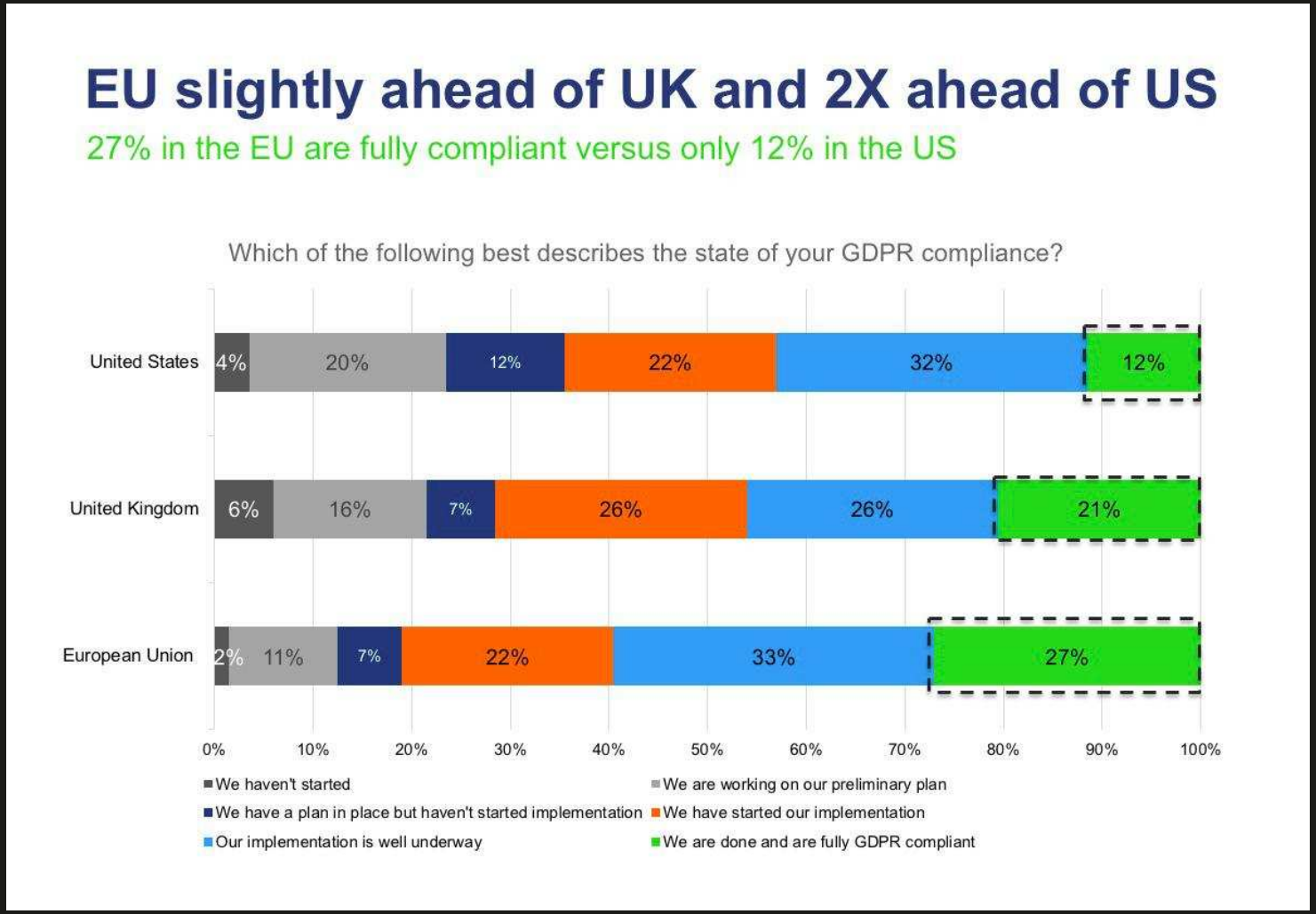
Who did nothing?

Just started?

50% complete/ still implementing?

All done?

TrustArc Research Report, July 2018



source: [TrustArc report benchmarks]

The one thing essential

1. Document everything

2. Have everyone in your team trained about privacy

You want to make it everyone’s responsibility

What are the reasonable things to do?

Depends on the context

- Likely to lose a client if not privacy-friendly/ compliant
- Security issues / user not trusting service
- Advanced marketing techniques
- Handling sensitive data
- Running innovative service –users are at risk of privacy breach

Starter or Grown-up?

Starting = OK with privacy-friendly on the surface

Growing = implement the real stuff:

> Data mapping, privacy assessment, documents

Starting stage

Privacy policy and DPA

BUT have a plan for the future

Understanding privacy laws becomes vital

1. Be extra careful with security

Penalties can be brutal, even for small websites

- CNIL fined 25000€ a small website for transmitting personal data in URL
- banana.com, 25 person company. Only 31 CC data leaked
  Hit with stiff fines from the major credit card companies.

1. Be extra careful with security

Penalties can be brutal, even for small websites

- CNIL fined 25000€ a small website for transmitting personal data in URL
- banana.com, 25 person company. Only 31 CC data leaked
  Hit with stiff fines from the major credit card companies.

If you're a tech founder:

Security is baked into your product.

1. Be extra careful with security

Penalties can be brutal, even for small websites

- CNIL fined 25000€ a small website for transmitting personal data in URL
- banana.com, 25 person company. Only 31 CC data leaked
  Hit with stiff fines from the major credit card companies.

If you're a tech founder:

Security is baked into your product.

If you rely on hired out dev:

Check security policy

2. Cautious approach with:

- categories of data you are collecting

You don’t want to realize 2 years from now that you’re entirely off limit re GDPR
Health, Fintech, IoT, …

2. Cautious approach with:

- categories of data you are collecting

You don’t want to realize 2 years from now that you’re entirely off limit re GDPR
Health, Fintech, IoT, …

- picking a provider

  - know what it’s doing with the data you send
  - Cost of switching cloud service provider

Oops

Pick this provider for cool feature & because it's free tier

Then discover that he's selling your users' data

Do you want to inform your users about it?

Spend 3 sprints integrating a privacy-friendly solution

Time to question where you want your customers' personal data stored

European equivalent of AWS = OVH

3. Give information to your customers.

Good guides by CNIL or ICO

> *Consider it marketing content*

3. Give information to your customers.

Good guides by CNIL or ICO

Consider it marketing content

4. Learn / train about GDPR & Privacy by design framework

3. Give information to your customers.

Good guides by CNIL or ICO

Consider it marketing content

4. Learn / train about GDPR & Privacy by design framework

5. 1-afternoon GDPR basics:

Google Analytics IP anonymization, checkbox for signup, cookie tool

3. Give information to your customers.

Good guides by CNIL or ICO

> *Consider it marketing content*

4. Learn / train about GDPR & Privacy by design framework

5. 1-afternoon GDPR basics:

Google Analytics IP anonymization, checkbox for signup, cookie tool

5. Processor?

Prepare a DPA

Growing stage

~ 100-200 users or lots of data

Must be a priority for Cx and head of business

Given the constraints it put into the company,
if you –as the boss– are not 100% behind, it's a death kiss

The Essentials steps

1. Pick someone to take charge of the project

2. Most likely also the point of contact for your company.

Probably no need for a DPO, but sometimes it’s a good signal

3. Train team –it is an obligation

including founders

- Everyone in the companies must take ownership of privacy matters
- Understand the Privacy By Design Framework
- Assess that you’re following the rules before building any new feature
- Do you need the data at all?

privacy by Design framework

Proactive, not reactive –preventive not remedial

Privacy as the default setting

Embed privacy into design

Keep it user-centric –Respect user privacy

End-to-end security

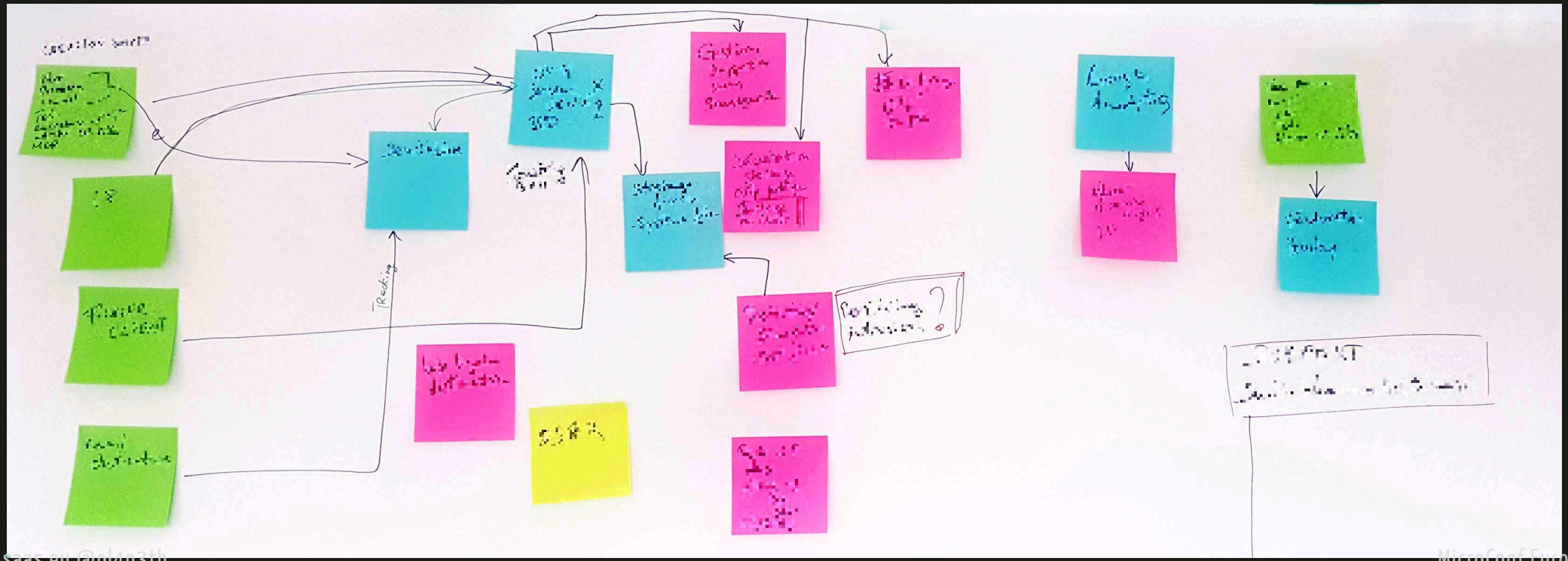
Keep it open –Maintain visibility & transparency

Retain full functionality –positive sum, not zero-sum

4. Map your data

Mandatory: ICO, CNIL, other DPAs says “do it.”
Good avenue to assess your risks

Easiest: data mapping workshop



Assess your risks

Derive from data mapping

- Security
- Sensitive data
- Lack of information, inaccessible information to users & customers
- Documents missing (LIA, DPA, Record of processing activities)
- New categories of processing (AI, profiling, IoT,...)

Some exemples:

- Support team uses Slack, and put personal data in it
- Logging for debug and improvement:

5. Information & privacy notice

Easy to be checked on by a DPA

Forms and data collection

Write your privacy policy as if it is content marketing

Reviewed by professionals

6. Tech stack Review

Code · Providers · Security

Vest providers, libraries, frameworks, plugins, API, …

- Document requirements for privacy
- Review and Sign DPAs with your providers
- Enforce security and password policy for the whole team

Password: **n°1 cause of data breach**

Encourage pass phrase with caps, numbers, and special character

Proper data management

- Data lifecycle
  `cron` job to check for stale data, to-delete date and erase it from all storages

Deleted data = data gone

- Files in versionning
- Data used in test & staging

7. Handling of data breach

Recommended ways:

- Encrypted at rest and in transfer
- Pseudonymization (data still under GDPR)
- Anonymization (this is hard)

Plan beforehand

Processor?

Process to notify customers

8. Record of Processing Activities

- Mandatory, the first thing a DPA will ask for
- Document Central to operations
- Comprehensive view of critical data & what we do with it.

Customize it to serve Business Purposes

Templates at ico.org.uk and cnil.fr

9. Data Subject Access Request

Requests are far and few

Do the minimum to handle it.
Write manual procedures.

Except if you *know* that people will ask for it

Advanced marketing practice?

Need consent for cookies

Check requirement if

- Ads,
- Facebook retargeting,
- Profiling

be prepared for e-privacy

what DPOs says

Efty work but worth it

It's the direction of history

Our company's image is at stake

Privacy is for Everyone in the company

Am I handling personal data?

If yes, is this thing I'm planning to do
–new feature, support task, marketing–
aligned with privacy requirement?

Business growth means more pro-active on security and privacy

GDPR offers you a framework of thinking

Security/ privacy is a shared concern in the teams

Biggest time sink

1. Documents

Privacy Policy, DPA, Terms of Service

Back and forth trips between the company and legal team

2. Data mapping and Record of Processing Activities

Privacy is an ongoing process

Have a plan to maintain compliance

- You won’t do everything in one go.
- Long-term commitment.
- Best achievers: users/customers focused
- Others laws in the making

Review your process every 6 months

Earmark a sprint for GDPR

- Better information notice when collecting data
- automate erasure of stale/obsolete data
- Better security

ICO survey

most UK citizens still don't trust organisations with their data

- 34% have trust and confidence in companies using their personal information (21% in 2017)
  15% only for social media companies
- 33% would get advice and/or information from the ICO
- 78% felt that if a company/organisation that they used was affected by a data breach and their information was lost or stolen, the company holding the data should be held responsible.
- 51% of people are concerned about automated decision making.

DPOs' STORIES

"I want to sign a DPA"

You are a **controller**, you received this email:

> *Give us a DPA to sign*

As a **controller**:

> Signing a Term of Service is a contract

DPA is a contract between a **processor and a controller**
Because a processor can only process data on written instructions of the controller

Data Subject Access Request or “letter from hell”

Copy/paste from article 15.

A request can be filled through any channel

Support should handle request in any form:
phone call, email or form submission

Latest news

1. Japan and EU agreed to a data transfer agreement
2. Other laws/regulations in the making
   India, Ca
3. E-privacy directive is on its way
4. EBDP not content with Privacy Shield

   Privacy and Civil Liberties Oversight Board revived

   Ombudsperson appointed

Thanks :)

Photo credit: Wavy1 on Visualhunt / CC BY-NC-SA