The GDPR compliance journey at Skroutz

Apollon Oikonomopoulos
`apollon@skroutz.gr`

ENISA - Security of Personal Data Processing
8/10/2018, Athens — GR

Skroutz – who we are and what we do

What we do: product search & price comparison engine

- 2.9k e-shops
- 4M SKUs indexed
- 7M visits/month
- 850k visits/day

Who we are:

- Founded in 2005
- 187 employees
- ∼ 500 servers (physical & virtual)

Before GDPR: security by design, security in depth

- Part of every new service design
- Data access on need-to-know basis
- Extensive use of crypto for authentication, integrity and confidentiality
- Security measures implemented rigorously, deployed through automated means for consistency

Before GDPR: privacy & PD processing

- Mostly ”anonymous” (i.e. non-logged-in) service
- Limited use of cookies for billing/accounting/traffic monitoring purposes
- SSL-enabled for quite a while
  - Included in HTTPS-Everywhere since 2012
  - HTTPS-only since 2017
- Opt-out newsletter for account holders (sent roughly once per year)
- Fine-grained opt-out controls for notifications
  - price drops in watched products
  - shop and product review reminders
  - smart cart activity
- Concise, plain-language control descriptions
- Respect users’ privacy, never initiate communication unilaterally
- Terms of Use laying out *some* privacy rules

Identifying what we needed to do

- <250 employees, however we facilitate 7M users monthly
  - Probably *not* occasional processing, not exempt from Article 30
- Record processing activities and affected parties
- Update our internal policies
- New public Privacy Policy in plain language
- Determine lawful bases for processing
- LIA & PIA templates and when to use them

Identifying what we needed to do

- <250 employees, however we facilitate 7M users monthly
  - Probably *not* occasional processing, not exempt from Article 30
- Record processing activities and affected parties
- Update our internal policies
- New public Privacy Policy in plain language
- Determine lawful bases for processing
- LIA & PIA templates and when to use them

Most importantly

Embed privacy and data protection in our day-to-day processes, from design to development to operations.

Compliance: first steps

- Dedicated small team (2 people), running compliance as a project
- Specific deliverables
  - Privacy Policy
  - Updated internal policies
- Key decisions: Consent vs Legitimate Interest + Right to Object
- Seek external review where possible
- Disseminate information throughout the company
- Embed PIA and LIA templates in our work management system
- Aid teams in conducting their first PIAs
  - Privacy audits in *retrospect* for existing systems leading to changes

Compliance: first steps

- Dedicated small team (2 people), running compliance as a project
- Specific deliverables
  - Privacy Policy
  - Updated internal policies
- Key decisions: Consent vs Legitimate Interest + Right to Object
- Seek external review where possible
- Disseminate information throughout the company
- Embed PIA and LIA templates in our work management system
- Aid teams in conducting their first PIAs
  - Privacy audits in *retrospect* for existing systems leading to changes

Overall a strenuous 3-month effort amidst a very busy period

Compliance: technical actions taken

- Notified registered users about ToS/PP update
  - … leading to a stream of account deletion requests
- Removed or masked PD from systems where they were not strictly necessary
- Removed third-party Javascript that was not strictly necessary and had possible privacy implications (e.g. social network ”like” buttons)

Persistent changes

- All departments have PD processing awareness
  - Concerns raised in every tier, not only by department heads
  - It is clear that mainstream media also helped raise general awareness – although the information provided was not always accurate
- Development teams have been conducting PIAs

Continuing challenges

- Human resources are scarce; experts even more so
- Need to bridge the gap between legal & tech
- Compliance requires shifting of resources, conflicting with business needs
- Training and awareness, new channels to monitor
- Privacy *by design* across the board

Thank you!

skroutz