Privacy - GDPR a Year Later
June 25, 2019
Privacy- GDPR a Year Later

Today’s web conference is generously sponsored by:

Thales
https://www.thalesgroup.com/
Michael F. Angelo CRISC, CISSP has over 30 years of information assurance experience. Michael has served as a trusted security advisor and security architect with leading corporations and government entities. He has acted as a technical adviser in the development of US national and international export controls. Currently chairs the ISSA International Webinar committee. Amongst his accomplishments he is an ISSA Fellow, and is named on the ISSA Hall of FAME for his contributions to the security community. In addition, he currently holds 61 US Granted Patents. His current work encompasses certifications, SDL, Threat Modeling, AppSec / DevOPS, as well as and Software Supply Chain analysis. Michael is a veteran moderator and has appeared at numerous International conference and in a multitude of International Web Conferences.
Privacy - GDPR a Year Later

Speaker

Thomas Fischer, Security Advocate and Threat Researcher

Thomas has over 30 years of experience in the IT industry ranging from software development to infrastructure & network operations and architecture to settle in information security. He has an extensive security background covering roles from incident responder to security architect at fortune 500 companies, vendors and consulting organizations. He is currently security advocate and threat researcher focused on advising companies on understanding their data protection activities against malicious parties not just for external threats but also compliance instigated. Thomas is also an active participant in the InfoSec community not only as a member but also as director of Security BSides London, ISSA UK chapter board member and speaker at events like SANS DFIR EMEA, DeepSec, Shmoocon, and various BSides events.
One Year on…

Thomas Fischer
Year 1 of GDPR Decisions

- 31 countries DPA received reports
- 206,326 cases reported
  - Complaints: 94,622
  - Data breach related: 64,684
  - Others
- 63% of Cases closed, 37% ongoing
- 1% have been challenged
- Fines imposed 55,955,871 Euros
BDS issues 5280 EUR fine to sports café
- CCTV covering public areas (street, parking lot)

- Violated Article 5 (1)(a)/(c) for lawful, fair and transparent processing as well as data minimisation

- Reasons
  - No logs of video surveillance processing operations.
  - No deletion of personal image within 72 hours (no separate logs for processing of deletions)
  - No justification for an extended storage period
  - Inadequate signage about CCTV
Baden-Württemberg DPA issues 20,000 EUR fine to KNUDDELS

- Dating Chat App that suffered data breach
  - 300k login credentials compromised

- Stored cleartext passwords in violation of Article 32(1)(a)

- Minimal fine applied
  - Quick and accurate reporting to Supervisory Authority
  - Quickly (few weeks) implemented corrections

- DPA recognised KNUDDELS data breach response (pursuant to Article 83)
2019-01-21: CNIL (French DPA)

➢ CNIL issues EUR 50 Million fine to GOOGLE LLC
  ❑ Complaint based (NYOB, La Quadrature du Net)

  ❑ Lack of transparency, inadequate information, lack of valid consent

  ❑ Ad personalisation service when account is created in Android

  ❑ French DPA (CNIL) coordinated with Irish DPA (DPC)
    ✓ CNIL ruled to be competent to proceed
Polish DPA issues EUR 220,000

- Provides insight into interpretation of term “disproportionate effort” [Article 14(5)(b)]

- Company provider of digital business, marketing, and credit information

- Collected data on business entities from public sources (official business registry)

- Notified users where an email was available

- Did not notify anyone else claiming that it was too hard
Danish DPA issues DKK 1.2 million fine to TAXA4x35

- Audit by DPA on taxi service data anonymisation practices

- TAXA4x35 was anonymising customer name but not phone number

- Large amount of personal data stored without objective purpose
Danish DPA issues EUR 61,500 fine to MISTERTANGO UAB

- Investigation following possible data breach

- Personal data breach in payment systems *not reported* to DPA

- Collected *more* personal data *than necessary* and *longer than required*
  - Data store for 216 days instead 10 mins
  - Unable to demonstrate compliance (Article 5)

- Improper *disclosure* as data publicly available for 2 days (Article 5 & 32)

- *Failure* to report breach (Article 33)
CNPD issues 400,000 EUR fine to a Hospital
- Audit found *Unauthorised Access* to Patient Data
  - False profiles/accounts
  - Unrestricted access to all patient files

- CNPD ruled that Hospital was responsible for ensuring IT Systems were secured properly

- CNPD used the GDPR principles
Lessons to be Taken

➢ No particular section of GDPR is immune

➢ Data minimisation

➢ Failure to disclose

➢ Unauthorised access

➢ Failures in securing personal data processing
NEW: The ICO has issued two enforcement notices to the Metropolitan Police Service (MPS) over their SARs backlog, ordering them to answer all SARs by September 2019. The MPS currently has over 1000 SARs waiting to be answered.
SARs - Subject Access Requests

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Right related to automated decision making including profiling
Procedures

➢ Are you covering all request avenues?
  ❑ Email
  ❑ Phone
  ❑ Written
  ❑ Online forms

➢ Must be of charge
  ❑ Except when unfounded

➢ Data must be provided within 1 month of request
  ❑ May request extension if complex (max. 3 months)
Common Mistakes

➢ Asking for too much proof of identity

➢ Not providing the right information
  ❑ Reason why you need the data
  ❑ Categories
  ❑ 3rd parties who have access
  ❑ Highlight important data subject rights
  ❑ Confirm if data is being used for “automated decision making”

➢ Not responding
To: dpa@xxxx
From: Thomas@myemailaccount
Subject: Data Subject Access Request

To the Data Protection Officer

This is a subject access request under Article 15 of the GDPR (General Data Protection Regulation for the EU).

I am the owner of this email address which I have been notified was leaked in a recent data breach at your company. I therefore require the following information:
- The source from which you acquired my personal data and at what data it was acquired
- The purpose(s) and lawful basis under which your company was/is processing my personal data
- The names of all Data Controller and Data Processor recipients to which you have disclosed my personal data
- Copies of the information which constitutes my personal data which you were/are processing

I would like to remind you that you are required to provide this information within 30 calendar days.

No further verification is needed as this request is being sent from the email account which you have on file for me and are/were processing.
Tabletop It!

➢ **purpose** of a **tabletop exercise** is to evaluate an organization’s **preparedness**

➢ Run test SARs for each scenario

➢ Make sure you include a breach scenario

➢ Walk through the whole process
Don’t Forget

➢ Backup systems

➢ Legacy Applications and Data

➢ How you deliver the data

➢ 3rd Parties
Cost of a SAR

GBP 10,000 $\rightarrow$ GBP 100,000

Per Data Subject/Request
QUESTIONS?
Lisa M. Angelo is a cyber liability attorney. She works with companies of all sizes and advises clients on data privacy, cyber insurance disputes, data breach response, technology contracts, intellectual property, and other matters related to technology and cyber law.

Lisa is recognized as a Privacy Law Specialist by the International Association of Privacy Professionals. She has two internationally-recognized certifications in privacy: a Certified Information Privacy Manager and a Certified Information Privacy Professional.

Lisa is an elected council member for the State Bar of Texas Computer & Technology Section. She is the Vice-Chair of the State Bar Business Law Section’s General Practice Committee and serves on the Blockchain Committee dealing with blockchain’s application in regulated industries. Lisa is also a member of the FBI’s InfraGard Houston Chapter which is in an initiative for the private and public sectors to share information about cyber risk. Recognized for her professional achievements, Lisa was named a Texas Super Lawyers’ 2019 Rising Star. She is licensed to practice law in Texas and Colorado having earned a Juris Doctorate from South Texas College of Law and a bachelor’s in psychology from The University of Texas at Austin.
ISSA International Webinar

Privacy- GDPR a Year Later

June 25, 2019
I’m a lawyer, but...

The materials and information provided in this presentation are for informational purposes only and should not be considered legal advice.

Please consult an attorney if you seek legal advice.
One year of GDPR by the numbers

Data protection complaints: > 144,376
Data breach notifications: > 89,271
Reports of personal data breach to ICO: > 14,000
Data protection concerns from public to ICO: > 41,000 & 2017/2018 was only about 21,000
Registered DPOs: > 500,000
Fines: > $63 mil ($56 mil euros)

Sources:
Focus of enforcement authorities

- Data breaches
  - Systemic failures
  - Inconsistent compliance with established policies & procedures
- Lack of transparency
- Lack of consent
- No valid legal basis (or too vague)
- Data breach notifications
- Data subject access requests
  - Result of GDPR awareness
  - From employees & consumers
Trends in GDPR violations

Ongoing infringements > one-offs

Mitigating factors
- Pro-active approach
- Supporting documentation
- Cooperation

But also....
- Class action lawsuits after a data breach
US businesses & GDPR

- Business subject to GDPR
- Business “subject” to GDPR
- Third Party Vendors
- Expanding business to EU
Business Activities

- Data-Mapping (privacy v. security)
- Data Processing Agreements
- Third Party/Vendor relationship management
- Policies & Procedures
- Privacy Notices
- Privacy Impact Assessments
- Incident Response
- Training (awareness, procedures, table-tops)
GDPR-Style

- Federal Trade Commission Complaints
- State Data Privacy Laws
- State Breach Notifications Law
Federal Trade Commission Complaints

<table>
<thead>
<tr>
<th>Deceptive</th>
<th>Unfair Acts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Misrepresentations</td>
<td></td>
</tr>
<tr>
<td>• <em>Reasonable steps to secure</em> data</td>
<td></td>
</tr>
</tbody>
</table>
| Marketing lingo  
  Press release  
  Social media post  
  Privacy notice |
| • Failing to provide *reasonable security* to prevent unauthorized access to PI |
“Unreasonable security” according to FTC Complaints

▷ Failing to take reasonable, low-cost measures that could have helped prevent a breach

▷ Consequences of FTC complaint:
  - Mandated cybersecurity program
  - Third party audits
  - Prohibit specific activity
  - Other record reporting requirements
  - Fines up to about $43,000 per violation of mandated program

Take-away: Data breach not required for legal liability; failure to take proactive measures can cost money (fines, mandates, reputation).
GDPR // US

Issues commonly addressed

- Protect certain categories of data
- Obligations for collecting/processing data
- Notice required in event of a breach
- Secure disposal of data
- Consent to share data
- Transparency in handling of data
- Security controls
- Documenting cyber incidents
- Consumer rights (delete, rectify, private right of action)
Shift in thinking about data privacy

- Privacy is important > privacy for embarrassing/shameful activity
- Departure from “nothing to hide”
- Proactive > reactive
  - Promote proactive behavior
  - Don’t just wait for a data breach
- Non-technical businesses included in the conversation
- Goal: protect data > make money off of fines
- Self-reporting > hiding behind excuses/privilege
- Data privacy is normal part of doing business
The Good News

Opportunity for innovation

Opportunity to set the narrative
Sources


- https://edpb.europa.eu/our-work-tools/consistency-findings_en
Jason is a global award-winning cyber security expert and chief technology officer for Thales’ data protection solutions. He is a former ethical hacker with 20 years’ experience in the information security industry and has created technologies to keep organizations one step ahead of evolving cyber threats, including the world’s leading cloud-based authentication platform. He is also deeply interested in reducing and researching the risk of password theft, and is globally known for exposing a large number of major password vulnerabilities. You might even find him popping up on the BBC and CNBC, and reading his regular contributions to publications such as the Financial Times, The Guardian and Time.