Accurate Data Discovery, Automated Classification & Remediation

The EU General Data Protection Regulation: What We Know, Six Months In

Scott M. Giordano, Esq., CCEP/CCEP-I
VP, Data Protection, Spirion

Presenter

Scott M. Giordano, Esq., CCEP/CCEP-I, VP, Data Protection, Spirion

- Specializing in multinational/cross-border aspects of data protection
- ISO 17024 Certifications Advisory Board Member, International Association of Privacy Professionals
- Created and taught the first law school course on electronic evidence and -discovery
- Member of the California, the District of Columbia, and Washington state bar associations

Agenda

- First, the Bad News
- Then, the Good News
- Who Enforces the GDPR?
- Summary of the State of Information Security Requirements
- Case Study: Equifax
- Summary and Conclusions
- Bonus Case Study: Bupa Insurance

First, the Bad News

- Since May 25, no published audit guidelines from the European Data Protection Board (EDPB), nor is any on the horizon
- No guidelines from any of the 28 EU supervisory authorities
  - Industry-specific guidelines are being developed by the CNIL, the French supervisory authority
- That's it as of now

Then, the Good News

- The Equifax sanctions give us an excellent roadmap of what to do – and not to do
- Other authorities in the EU and elsewhere will be reading it

Who Enforces Data Protection Regulations?

- 28 EU member state supervisory authorities (ICO, CNIL)
- European Data Protection Board (the former Art. 29 Working Party + European Data Protection Supervisor) is the developer of guidelines, e.g., WP248.
- European Commission
  - Fine vs. Facebook in the WhatsApp matter: €110M
- European Court on Human Rights
  - Addresses violations of the European Convention on Human Rights
  - U.K. lost a privacy case on Sept 13 in connection with surveillance on citizens revealed by Edward Snowden
  - Has 90 days to appeal

What About Facebook and Cambridge Analytica?

- July, 2018, the UK Information Commissioner's Office (ICO) issued the following:
- "The ICO has issued Facebook with a Notice of Intent to issue a monetary penalty in the sum £500,000 for lack of transparency and security issues relating to the harvesting of data constituting."
- Aggregate IQ in Canada implicated but has rejected ICO jurisdiction
- Parent company SCL Elections Ltd. criminally charged with failing to comply with an ICO enforcement notice
- That's all we know

GDPR Complaints in (roughly) the first month

EU Member State	No. of Complaints	Span of Days
CZ	400	26
FR	426	24
GR	113	34
IE	386	32
NE	170	14
PL	756	37
RM	145	14
SL	102	25
UK	1,124	26

Source: IAPP, *Cataloging GDPR complaints since May 25*

GDPR Complaints by Max Schrems (NOYB.EU)

Company	Authority	Maximum Penalty	Complaint
Google (Android)	CNIL(France)	€ 3.7 Mrd	PDF
Instagram	DPA(Belgium)	€ 1.3 Mrd	PDF
WhatsApp	HmbBfDI(Hamburg)	€ 1.3 Mrd	PDF
Facebook	DSB (Austria)	€ 1.3 Mrd	PDF

What Does the GDPR Require?

Art. 5(1). Principles. Personal data shall be:

- processed in a manner that **ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, **using appropriate technical or organisational measures** ('integrity and confidentiality').

What Does the GDPR Require?

Art. 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,
    1. the **controller and the processor shall implement appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:

What Does the GDPR Require?

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

What Does the GDPR Require?

"Technical and organisational measures" cited 21 times in the GDPR, including Arts.:

- 24 Responsibility of the Controller
- 25 Data protection by design and by default
- 28 Processor (responsibilities)
- 30 Records of processing activities
- 34 Breach notification
- 83 Conditions (i.e., criteria) for imposing fines

Equifax

- Two parties: Equifax Inc. (U.S.), the data processor and Equifax Ltd. (UK), the data controller
- Lost control of approximately 15M records of UK data subjects containing personal data between May 13 – July 30, 2017; "EIV" and "GCS" datasets
- Name, DoB, address, CC #, UID, PW, secret question, some payment amounts
- U.S. and UK data mixed
- CVE 2017-5638 took advantage of the Apache Struts 2 web application framework
- Fined £500,000, per 55A of the U.K. Data Protection Act 1998, for the 2017 breach – the maximum allowed
- Under GDPR it would have been up to $120M
- FTC investigation under way

Equifax – Timeline

- March 8, 2017: DHS US-CERT notifies Equifax of vulnerability in the Apache Struts 2 web application framework; Common Vulnerability Scoring System (CVSS) score: 10 (critical)
- March 9, 2017: Equifax Inc. notifies staff; consumer-facing portal not patched
- March 10, 2017: First "interaction using the vulnerability" takes places
- March 15, 2017: Equifax Inc. scans network looking for the vulnerability but misses it
- May 13 – July 30: Unauthorized access takes place
- July 29, 2017: Equifax Inc. discovers breach and takes portal offline
- August 2, 2017: Equifax Inc. engages Mandiant
- August 8, 2017: Equifax Inc. notifies the ICO of 15M records compromised
- September 7, 2018: Equifax Inc. notifies Equifax Ltd.

Equifax

UK Data Protection Act 1998 Data Processing Protection Principles (DDPAs): Personal information must:
Art. 1: be fairly and lawfully processed
Art. 2: be processed for limited purposes
Art. 3: be adequate, relevant and not excessive
Art. 5: not be kept for longer than is necessary
Art. 7: be secure
Art. 8: not be transferred to other countries without adequate protection

Equifax

DPA 1998: Personal information must:	GDPR:
Art. 1: be fairly and lawfully processed	Art. 5(1)(a)
Art. 2: be processed for limited purposes	Art. 5(1)(b)
Art. 3: be adequate, relevant and not excessive	Art. 5(1)(c)
Art. 4: be accurate and up to date	Art. 5(1)(d)
Art. 5: not be kept for longer than is necessary	Art. 5(1)(e)
Art. 6: be processed in line with the data subjects' rights	Arts. 13-22 ("Chapter III")
Art. 7: be secure	Art. 5(1)(e); Arts. 32, 24, 25, 28, 30, 34, 83
Art. 8: not be transferred to other countries without adequate protection	Arts. 45-49

Equifax – Security Failures

As regards DPP5 [Personal information must not be kept for longer than is necessary]:

- Upon the migration of EIV from the US to the UK …it was no longer necessary to keep any of the EIV dataset[.] Despite this, the, relevant EIV dataset was not deleted in full from the US environment and/or the migration process was inadequate in this respect.
- In respect of the GCS dataset stored on the US system, Equifax Ltd did not appear to be sufficiently aware of the purpose for which it was being processed until after the breach.
- Equifax Ltd failed to adequately follow up or check to ensure that all relevant UK data had been removed from the US environment or to have in place an adequate process to ensure this was done.

Equifax – Security Failures

As regards DPP7 [Personal information must be secure];

- Equifax Ltd did not undertake an adequate risk assessment(s) of the security arrangements put in place by Equifax Inc before transferring data to it and/or following the transfer.
- The Data Processing Agreement 2014 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) dated 23 October 2014 was inadequate in that it (i) failed to provide appropriate safeguards including but not limited to security requirements; and (ii) failed to incorporate the required standard contractual clauses.
- Agreement between Equifax Ltd and Equifax Inc stating:
- "Industry-leading technical and organisational security measurers**:** the data importer is a leading credit reference agency with market-leading positions in a number of territories worldwide. It deploys extensive technical and organisational security measures to achieve robust information security and management practices. The data importer will apply the full range of corporate policies and procedures to the personal data."

Equifax – Security Failures

As regards DPP8:

- (2) The Data Processing Agreement 2014 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor), was inadequate in that it failed to incorporate the required standard contractual clauses as a separate agreement and/or to provide appropriate safeguards for data transfers outside the EEA.
- (3) The Data Processing Agreement 2017 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) was inadequate in that it failed to provide appropriate safeguards for data transfers outside the EEA.
- It is the Commissioner's view that the aforesaid breaches of DPP7 and/or DPP8 also amount to a breach of DPP1, in that the relevant data was not being processed fairly and lawfully.

Equifax – Security Failures

The aforesaid failures in relation to the GCS dataset also amount to a breach of DPP1 in that the relevant data was not being processed **fairly** and lawfully and a breach of DPP2 in that the relevant data was not being processed for any **specified and lawful purpose** at the material time.

Equifax – Security Failures

As regards DPP1 [Personal information must be **fairly** and lawfully processed]:

- ….Equifax suggested that informing data subjects that their passwords would be stored in plaintext form would have created a security risk. The Commissioner's view is that **this type of processing activity was an inappropriate security risk**, particularly given the state of the art and costs of implementation as regards appropriate technical measures to protect personal data, the resources available to an organisation of Equifax's size, and the nature of the processing it undertook.
- Especially in the absence of any stated good reason, data subjects **could not have anticipated that the processing of their data would involve the storage of passwords in plaintext form**, in breach of the company's Cryptography Standard.
- Having not been provided with the relevant information, **any consent given by data subjects could not be regarded as being adequately specific and/or informed**, as required under the Directive.
- On that basis, the Commissioner's assessment is that any consent relied upon by Equifax was invalid in this context, thereby amounting to a contravention of DPP1 in that the data was not **fairly and lawfully processed.**

Equifax – Penalty Calculation

The Commissioner considers that this contravention was serious, in that:

1. Equifax Ltd contravened multiple data protection principles.
2. The **contravention entailed several systemic inadequacies in Equifax Ltd's technical and organisational measures** for the safeguarding of the relevant personal data. Cumulatively, this multi-faceted contravention was extremely serious
3. A number of the inadequacies related to significant measures needed for a robust data management system, as outlined above.
4. The multiple organisational inadequacies were particularly problematic in light of, inter alia, the nature of Equifax Ltd's business, the volume of personal data being processed, and the number of data subjects involved.
5. The Commissioner has not received a satisfactory explanation for those individual and cumulative inadequacies.
6. **At least a number of the inadequacies appear to have been in place for a long period of time** without being discovered or addressed.
7. The inadequacies put the personal data of millions of data subjects at risk.
8. The period of vulnerability for the affected UK data extended over an extended period of time and **the data breach was not detected promptly. It was not reported to the Commissioner until over two months after the event.**
9. In respect of the UK records that were compromised, there were and remain significant opportunities for misuse. The relevant personal data is liable to be useful to scammers and fraudsters.

Equifax – Penalty Calculation

The Commissioner has taken into account the following **mitigating** features of this case:

- The relevant data was, for the most part, not of itself highly sensitive in terms of its impact on data subjects' privacy;
- The affected data subjects, as well as Equifax Ltd, have been the victim of the malicious actions of third party individuals;
- Equifax Ltd proactively reported this matter to the Commissioner, promptly after learning about it from Equifax Inc, albeit a significant time after the actual data breach;
- Equifax Ltd deleted at least some of the data remaining in the US environment following migration of EIV to the UK;
- Equifax Ltd and Equifax Inc took steps to minimise potentially harmful consequences such as engaging specialist IT security experts to manage the data breach, offering free credit monitoring services to UK data subjects affected by the breach, and working with the relevant regulators in the US, Canada, and the UK; and
- Equifax Ltd and Equifax Inc have implemented certain measures to prevent the recurrence of such incidents, for example Equifax Inc has increased system scanning capability and is now storing passwords within a cryptographic hash value, whilst strengthened procedures are now in effect.

Equifax – Penalty Calculation

The Commissioner has also taken into account the following **aggravating** features of this case:

- The security breach impacted many more individuals than just the UK data subjects. 146 million data subjects' personal data was compromised and the data of millions more was put at risk;
- Those risks appear to have persisted for a prolonged period of time given the systemic inadequacies identified above;
- Some of the failures concern failures to identify / ensure appropriate security measures such as implementation of patches and the encryption of personal data and the appropriate securing of passwords;
- The data breach exploited a known vulnerability and therefore could potentially have been prevented. In particular, the security breach arose out of a failure to implement a patch to the affected system(s) which it failed to identify as vulnerable; and
- Equifax Ltd's contractual arrangements with Equifax Inc were inadequate in material respects.

What About Privacy Frameworks?

Generally Accepted Privacy Principles (GAPP) by AICPA/CICA:

- Management
- Notice
- Choice And Consent
- Collection
- Use, Retention, And Disposal
- Access
- Disclosure To Third Parties
- Security For Privacy
- Quality
- Monitoring And Enforcement

What About Privacy Frameworks?

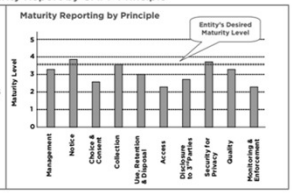
Privacy Maturity Model (PMM), also by AICPA/CICA

Figure 1 – Privacy Maturity Report by GAPP Principle

Figure 1 shows a sample graph that could be used to illustrate the maturity of the organization's privacy program by each of the 10 principles in GAPP.

The report also indicates the desired maturity level for the enterprise.

Reports like this are useful in providing management with an overview of the entity's privacy program and initiatives.



Summary and Conclusions

- No published audit guidelines from EDPB, nor is any on the horizon
- Security standards, guidelines, and frameworks such as ISO/IEC 27001/2, NIST 800-171, and CSC Top 20 can address Art. 32 and, indirectly, other articles that cite "technical and organizational" requirements
- GAPP can fill in some of the blanks
- Business partners (vendors, third parties, licensees, etc.) require vigorous policing

Summary and Conclusions

Organizations:

- Do not understand the nature of personal data
- Do not know where personal data lies in their organization's "information ecosystem"
- Do not know with whom data is being shared, inside or outside the organization
- Are not well prepared to legally share personal data
- Are not well prepared to address a data breach
- Are not able to focus team efforts to protect personal data

Thank you!

Scott M. Giordano

Scott.Giordano@Spirion.com

visit www.spirion.com

Resources

- U.S. Government Accountability Office, *DATA PROTECTION Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach (*GAO-18-559: Published: Aug 30, 2018. Publicly Released: Sep 7, 2018)
- GAPP: https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf
- PMM: https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

Bupa Insurance Services Ltd.

The Commissioner considers that the data controller knew or ought reasonably to have known that there was a risk that the contravention would (a) occur, and (b) be of a kind likely to cause substantial damage or substantial distress. She further considers that the data controller failed to take reasonable steps to prevent such a contravention, in that:

- Bupa Insurance Services Limited is a large, well-resourced and experienced data controller.
- The data controller was also aware of internal security risks to SWAN i.e. unauthorised use of customer data accessed through SWAN. The threat of a rogue employee is widely recognised in industry.
- The data controller should have been aware of the increasing prevalence of scams and attempted frauds…. The data controller should have assessed the technical and organisational measures pertaining to SWAN in light of those increased risks.
- The data controller had ample opportunity over a long period of time to implement appropriate technical and organizational measures … but it failed to do so. For example, it failed to take steps to prevent the large-scale accessing and exporting of the relevant personal data from SWAN.
- The data controller failed to undertake an adequate risk assessment of the use of SWAN[].
- The data controller failed to monitor its activity log (which was defective) in order to check for activity of concern, such as bulk extractions of data.

Bupa Insurance Services Ltd.

- Between Jan 6 – Mar 11, 2017, healthcare account data of 547k people exfiltrated by an insider and sold on the dark web
- Dark web advertisement stated:
- "DB [database] full of 500k+ Medically insured persons info from a well-known international blue chip Medical Insurance Company. Data lists122 countries with info per person consisting of Full name, Gender, DOB, Email Address plus Membership Details excluding CC Details."
- On June 17, 2017, Bupa began an investigation
- On July 12, 2017, Bupa notified customers
- In August of 2017, external review of data protection practices took place

Bupa Insurance Services Ltd.

- ICO levied a £175,000 fine under DPA 2018
- Violation of Article 7: Personal information must be secure

Bupa Insurance Services Ltd.

The Commissioner considers that this contravention was serious, in that:

- (1) The contravention comprised a number of material inadequacies in the data controller's technical and organisational measures for the safeguarding of the relevant personal data[].
- (2) The Commissioner has seen no satisfactory explanation for those inadequacies.
- (3) Those inadequacies were systemic, rather than arising from any specific incident or incidents.
- (4) Those systemic inadequacies appear to have been in place for a long period of time without being discovered or addressed.
- (5) Those inadequacies put the personal data of up to 1.5 million data subjects at risk.
- (6) …There [was] … a great number of opportunities for those inadequacies to be exploited and the relevant personal data to be misused.
- (7) Large volumes of personal data were accessed and could be exported swiftly by 20 PAT members, from the SWAN system to any device.