VISCHER

Whistleblowing, Monitoring & Profiling for Compliance

The (Swiss) Data Privacy Perspective

David Rosenthal
18. September 2020

Version 1.01

What are we talking about?

All are actual cases in Switzerland

- A multinational group implements a **whistleblowing scheme** globally for anonymously reporting misconduct
- An insurance company **monitors emails** for possible cases of fraud, data theft and other violations of company policy
- A software company suffers a **data breach** due to an employee inadvertedly making available client data on the Internet
- A bank continuously analyzes transaction and other data in order to identify and **predict fraud** and other misconduct
- A manufacturer **investigates** into red flags indicating potential bribery payments, and for this purpose collects and analyzes emails, files on personal devices, accounting data, CDRs, etc.

Is this legal?

- **Make** it legal!
- The basic data protection **principles** to keep in mind
  - Transparency
  - Proportionality
  - Purpose limitation, fairness and correctness
  - Justification (e.g., overriding interest, Swiss law)
  - Data subject rights (access, deletion) and due process
  - Transborder data flows only with appropriate safeguards
- Business and professional **secrecy obligations**
- **Art. 271** Swiss Penal Code when dealing with foreign states

Under the new DPA, you will have to do a Data Protection Impact Assessment (DPIA)

Will not materially change under the revised Data Protection Act (DPA)

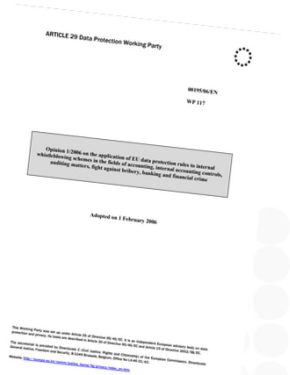
… unless you take automated decisions …

What is a DPIA?

Obligation also exists under the GDPR

- A **document** that shows that you have
  - Considered the possible **negative consequences** of your project
  - Taken the **steps necessary** to keep them at an acceptable level
- Focused on the processing of **personal data**, and needed only for potentially **delicate activities** in terms of data protection
- A DPIA contains
  - Description of the intended processing of personal data
  - Analysis under the DPA and of potential negative consequences
  - Measures taken or intended to counter these consequences
- No need to redo a DPIA for **similar processing activities**, but it should be updated approx. every three years or upon changes

Case 1: Whistleblowing Scheme


ARTICLE 29 Data Protection Working Party

00195/06/EN
WP 117

Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime

Adopted on 1 February 2006

- No predefined list of issues that may be reported, but they have to **relevant for work** → Art. 328b CO in case of personal data
  - **Anonymous** reports should not be endorsed, but are permitted
  - No promise of anonymity (as you may not be able to uphold it)
- Scheme should be governed in a **policy** regulating both the reporting and the handling/investigation of the reports
  - Employees will have to be **informed** and heard, but the current notification obligation (Art. 11a DPA) will go away in 2022
- Provider: Data processing **agreement** (plus EU model clauses)
  - The (local) employer must be the ultimate controller
- **Limit** circulation & record retention; mind professional **secrets**

https://bit.ly/35wSyG3

Case 2: Ongoing E-Mail-Monitoring

- Have a **policy** govern it, so that the employees understand what will happen with the e-mails they send and receive
  - Ask them to inform private contacts of the monitoring
- Limit to what is **really necessary**; have a DPIA explain so
- To the extent possible, let **only the computer** do the job
  - If an outgoing e-mail is blocked, inform employee instead of forwarding it automatically for human review
- Have it **trained** (which may include human review) properly and in a defined period of time which employees are aware of it
- You may **log** and **retain** suspicious e-mails, but access to identifiable data should be limited to cases of suspicion

Case 3: Data Breach

- If the data breach involves personal data (or business secrets), it is necessary to **understand the seriousness** of the situation
  - Data breaches may have to be notified to authorities and data subjects under various laws (revised DPA, FINMAG, GDPR)
- **Review of data** potentially disclosed is usually necessary
  - Such a review may involve private data carriers; in such cases, obtain consent from individuals for using private data carriers, which usually works
  - **Inform employees** by way of a policy of potential reviews
- Have data **forensically secured** and reviewed by an outside specialist, extracting only relevant data
  - Data to be tagged accordingly (sensitive own and 3rd party data)

Case 4: Fraud Detection

- Data protection applies where personal data is processed
  - Are individuals **identifiable** based on the data processed?
  - Profiling = automated interpretation of aspects of an individual
  - Employment law restricts **behavioral monitoring**, too
- **Inform** affected individuals (e.g., privacy policy, Intranet)
  - Relying on consent as a legal basis is usually no option
- Have a **DPIA** done, show need and effectiveness of detection
- **Proportionality** (and enforcing it) is usually the key
  - Data minimization? Pseudonymized data? Use of automated procedures (but beware of automated decision making)?
  - Limit and strictly regulate the use of any results

Case 5: Internal Investigation

https://bit.ly/2ZzZWMZ

- An employer in principle has the **right to review work related materials**, including personal e-mails
  - No consent required, but act only upon a **clear suspicion**
  - Do not lose time to preserve data (in doubt go broader)
- **Inform employees** as soon as possible
  - Generally (e.g., policy) and specifically (e.g., legal hold notice)
- Limit to what is **necessary**, (normally) exclude private data
  - Have an outside specialist do the review under clear instructions
  - Culling, use of search terms, technology assisted review (TAR)
  - Access from outside Europe only with additional safeguards
- Keep in mind: Data subjects have access and due process rights

Privacy does make your life a bit more difficult, but it will in general not prevent you from doing your job.

VISCHER

Thank you for your attention!

Questions: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com