NKF

Data Protection Webinar

Case Studies
19 April 2018

INTRODUCTION

Overview

1. GDPR Audit Approach
2. Consent
3. Dealing with Subject Access Requests („SAR“)
4. Data Privacy Impact Assessments („DPIA“)

Case Study: GDPR Audit

- Role: SC Ltd.'s CIO Fanny Worries is in charge of supervising that the provisions of the GDPR are complied with. Fanny Worries wants to be well-prepared, but is a bit clueless how she shall proceed.
- Company: SC (Supercompliant) Ltd. is a Swiss company producing electronic devices
- Customers: mostly big corporates in the ICT sector
- Global reach: 14,000 Employees and businesses around the world, HQ in Zug, Switzerland
- SC Direct: SC Ltd.'s customer online facing service used to order the electronic devices in Europe and Asia
- Outsourcing Project: SC Ltd. has completed an extensive outsourcing program and now has two centralised data hubs with customer and employee data in the Cloud
- Fraud Detection Program: SC Ltd. has implemented a fraud detection program monitoring the employees' use of the SC IT infrastructure

Case Study: GDPR Audit

- Significant project requires resources and support
  - Budget
  - Project management support
  - Business commitment
  - Senior executive champion
  - Steering Group

- Engage stakeholders at the beginning of the project:
  - Kick-off meeting about the substantive work on the project
  - Clear narrative
  - Manage expectations
  - Report progress

Case Study: GDPR Audit

- Gathering information and complete assessment:
  - Simplify
  - Relevance
  - Make individuals accountable
  - Make time

- Prioritization of Risks:
  - SC Ltd. is a large and complex organization – approach biggest risks first
  - Risk to the privacy of the individuals (employees and customers)
  - Risk to the business
  - Risk to the timelines

Case Study: GDPR Audit

- Remedy significant risks first and in parallel to the general GDPR audit
- SC Direct:
  - Review privacy and cookie notices
  - Review Terms & Conditions
  - Have a template data processing agreement available for customers
- Outsourcing Project
  - Cloud in the USA: Privacy shield? Standard Contractual Clauses?
  - Data Processing agreement with provider: conclude addendum in order to cover requirements of Art. 28 GDPR
- Fraud Detection Program:
  - Carry out a DPIA
  - Issue employee briefing and information

Case Study: GDPR Audit

- Third party suppliers:
  - Draw up a list of existing suppliers that process personal data for SC Ltd., identify the key providers
  - Carry out information security assessments
  - Conclude data processing agreements

- Information security and data export
  - Review information security standards for key products and internal processes
  - Put into place data breach response plan in order to meet the new 72 hour breach reporting obligation
  - Determine strategy for legitimising transfers of data outside the EU (BCR, SCC, Privacy Shield, etc.)

- Compliance:
  - GDPR is a compliance topic like e.g. anti-bribery, anti-money-laudering
  - Keep in mind that GDPR is for life not just for the 25th May

Case Study: Consent

- Role: DPO Jim Slim has data protection compliance lead
- Company: Global Services Ltd. with international SaaS business
- Workforce: 500 employees
- Current basis for employee data processing:
  - consent through employment contract
  - Purpose: paying salaries, training, development, monitoring and dealing with disciplinary matters
- Current basis for customer data processing and marketing:
  - Consent through accepting terms & conditions
  - Purpose: rendering services and sending marketing materials

Case Study: Consent (Employees)

- Employment contract consent for processing
  - Consent historically seen as “the” lawful ground for processing
  - Remains a lawful basis for processing under the GDPR, but it is tricky
  - Consent is not a “catch-all” basis for all processing

- Freely given
  - real choice and control
  - possibility to withdraw consent without detriment
  - not freely given where a clear power imbalance exists between the data subject and the data controller

Case Study: Consent (Employees)

- Article 29 working party:
  - *"deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees".*
  - Consent for employee data processing will be the exception not the rule.

- Further points to note:
  - *"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*
  - Global Services Ltd. bundled different purposes for employee data processing under a single consent
  - Consent must be specific to the purpose

Case Study: Consent (Employees)

- Next steps
  - Global Services Ltd. needs to consider each of the purposes for which employee personal data is processed
  - Establish and document the lawful grounds relevant for each purpose
  - Create a separate employee privacy policy
  - Consider whether there are any exceptional cases where employee consent remains relevant
  - Review and refresh such consents to meet new GDPR consent requirements

Case Study: Consent (Customers)

- Global Services Ltd. customer data:
  - Consent must be specific and not bundled
  - Other grounds for certain purposes will be more relevant (and less tricky)
  - If the processing would still need to happen in the absence of consent, it is not the appropriate ground
  - Consent is not freely given, if performance of the service is conditional on consenting to something not necessary for the service (e.g. to marketing)
  - Marketing consents (where required) need to be granular to different channels and different group companies
  - Terms & Conditions must include all the information necessary for consent (where necessary)

Case Study: Consent (Customers)

- Next steps
  - Identify all the different purposes for processing customer personal data
  - Collect separate marketing (s) consents and split those consents across company and channels
  - Give information on the right to withdraw consent and how to do it
  - Review and update existing customer privacy notices to provide clear and transparent information on the processing and to ensure, where consent is relevant, that such consent is fully informed

Case Study: Dealing with SAR

- Role: an employee, Sally Smith, is confronted with the allegation that she is leaking confidential personal data of the company to competitors. An internal investigation is conducted. The allegations are not confirmed. Sally submits a SAR requesting to see the entire investigation file.
- Company: Nice Products Ltd. selling sports clothes
- Workforce: 200 employees

Case Study: Dealing with SAR

- Can Nice Products Ltd. avoid responding to Sally's request?
  - If a SAR is "manifestly unfounded or excessive", the company can charge a fee or refuse to respond, but in line with the emphasis on transparency and accountability
  - If disclosing it would "adversely affect the rights and freedoms of others" (guidance suggests that this could extend to intellectual property rights and trade secrets)
  - If Sally has made the SAR for the primary purposes of causing trouble and expense or is insisting on production of information with no conceivable value

How extensive does the search need to be?

- Similar to current requirements – searches must be proportionate, employers are not required to do things that would be unreasonable or disproportionate to the importance of providing subject access. This includes main servers, backed up data, deleted data and data held on other systems

Case Study: Dealing with SAR

What information is Sally entitled to see?

- Sally is only entitled to see her personal data:
  - sales figures, client data and unredacted statements from other employees is likely to include data which is not personal data, and may include data relating to other individuals
  - Non-personal information falls outside the scope
  - Data which relates to other individuals and does not relate in any way to Sally ("non-relevant personal data") falls outside the scope (Nice Products Ltd. may be able to redact, anonymise or pseudonymise)
  - If the personal data is also information relating to another individual, unless that individual has consented, consider whether it is reasonable to disclose it without consent.

Case Study: Dealing with SAR

- What about text messages?
  - As a general rule, text messages and other informal communications directly between devices (i.e. not using an external app) are likely to be discloseable, particularly where work devices are used. The IT Use Policies provide for guidance here as well
  - Employees have a right to privacy and may have an expectation of privacy based on staff handbooks, terms of use and other employer communications
  - Where such communications are made using personal devices, the employer is unlikely to be able to retrieve or force employees to provide such data (NB encrypted communications). Where such communications are made using work devices, is the employer a data controller or processor
- How quickly does Nice Products Ltd. need to respond to a SAR?
  - Nice Products Ltd. must respond within 1 month under the GDPR, and sanctions for potential breaches have been increased, so it will need to deal with Sally's request swiftly

Case Study: Dealing with SAR

- Can Nice Products Ltd. delete some of the more problematic data?
  - No. It is an offence under the GDPR for an employer or a person employed by the employer to alter or erase information with the intention of preventing disclosure, so staff must be made aware of this.
- Does Nice Products Ltd. still has to respond where it is using a data processor for its HR data?
  - Yes. It's the employer as a data controller who is responsible for complying with a SAR. If the employer uses a data processor, it must ensure it has contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to the employer or to the data processor.

Case Study: Dealing with SAR

- How to react if the employee files a complaint?
  - It is important to respond promptly, investigate the complaint appropriately and document both the investigation and your response to Sally in these circumstances
  - Nice Products Ltd. should use this as an opportunity to review the processes, searches, search criteria and any other key aspects of the initial response, and consider whether Sally has grounds for complaint
  - Communications to Sally should be in writing, in case she decides to take matters to court.

Case Study: DPIA

- Role: DPO of a global company in the financial services sector
- Context: Global implementation of bribery detection tool to track employees' e-mail and telephone communications
- Purpose of the tool: assessment of employees‘ compliance with the anti-bribery guidelines
- Functionalities of the tool:
  - Monitoring of employee communications including emails and conference and video calls over the company’s network on a permanent basis (including communications received or sent via business and personal devices)
  - Where unusual activities are detected, the tool will automatically create records and keep copies of the activity with the full details of the communications and the personal details of the employee. The information will not be filtered in any way.

Case Study: DPIA

- Action taken so far:
  - The employees have not been informed about the tool
  - No security assessment of the tool/on the individual contractors has been completed
- Meeting DPO/HR Director: Is there anything we should do before implementing the tool?

Case Study: DPIA

- Each company should have its own DPIA guidance:
  - assessment checklist
  - the criteria and methodology to implement it
  - who to involve and/or consult,
  - official guidance from the relevant supervisory authority
  - matrix which helps you mitigate the privacy risks to an acceptable level
- When does DPIA have to be carried out?
  - Warning signals
  - Activities which may result in "high risk“
  - Automated processing of personal data is conducted to profile, make predictions or take measures/decisions based on information about individuals

Case Study: DPIA

- sensitive/special categories of personal data, such as race/ethnic origin, religious belief, genetic data, biometric data or information regarding criminal convictions, are processed on a large scale; and
- systematic monitoring of a publicly accessibly area on a large scale

- Application
  - Wide scope
  - Type of activities carried out
  - Employees not informed

- Assessment
  - Privacy risk checklist: factors to take into account
  - Decision to decide to complete the DPIA
    - Do not underestimate the involvement required
    - Buy-in and support from relevant stakeholders

Case Study: DPIA

- Carry out the DPIA
  - Identify the processing activities and data flows and analyze risk
    - Set out the data flows and data processing involved clearly
    - Risk level assignment
  - Involve the right stakeholders
    - Key stakeholders involved at the outset of the DPIA lifecycle
    - Consultation: allow people to highlight privacy risks based on their own areas of interest and expertise
    - External support

Case Study: DPIA

- Mitigating measures
  - Aim
  - Suggested risk mitigation measures
    - clarify and reduce the scope of tool
    - exempt personal communications from the monitoring
    - monitoring should not occur on an automated basis: introduce human intervention
    - prevent the use of the information for performance evaluation purposes
    - Apply a data retention policy so that data is not retained indefinitely
    - restrict monitoring to limited periods of time
    - inform employees about the existence of the tool, why the business needs it and how it will be used

Case Study: DPIA

- Further points to consider:
  - Obligation to consult with the supervisory authority
  - Local rules of supervisory authorities vs global implementation
  - Trade unions
  - Privacy rights come first.

NKF Data Protection Practice

Niederer Kraft Frey advises on all areas of data protection across all sectors:

- Implementing national and international data protection policies and structures
- GDPR audits and implementation
- Data protection and data security in transactions
- Worldwide roll out of contracts
  - Employee data protection (e.g. implementation of HR database)
  - Assessment of new processes and IT systems (e.g. HR or CRM systems)
  - Advising companies in audits of regulatory authorities and in potential disclosure or summary proceedings
- Authorization / Notification
  - International data protection requirements (SCC, BCR, Privacy Shield, etc.)
  - Advising on the introduction of new products and services

THANK YOU!

Your contacts

Clara-Ann Gordon
Partner
clara-ann.gordon@nkf.ch

Phone +41 58 800 80 00
Fax +41 58 800 80 80
Web http://www.nkf.ch

Victor Stancescu
Associate
victor.stancescu@nkf.ch

Phone +41 58 800 80 00
Fax +41 58 800 80 80
Web http://www.nkf.ch

Niederer Kraft Frey AG Bahnhofstrasse 53 CH-8001 Zürich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch