NIEDERER KRAFT FREY

Data Security and Documentation

The new Data Protection Act Ordinance (revDPA-Ordinance)

Clara-Ann Gordon, Janine Reudt-Demont

Zurich – 18 January 2023

Content

1. Introduction
2. Certifications
3. TOMs
4. Logging
5. Data Retention
6. Processing Policy
7. Register of Processing Activities (ROPA)
8. Obligation to Notify the FDPIC

Introduction

General Provisions revDPA-Ordinance (I)

- The revDPA-Ordinance applies from **1 September 2023** – no transition period
- Scope: Is your company affected?

  Processing of personal data in Switzerland or outside Switzerland, but with effect in Switzerland (Art. 2 and 3 revDPA)

  → new: extra-territorial effect
- Protection goals (Art. 2 revDPA-O): confidentiality, availability, integrity and traceability
- Protection requirements analysis (Art. 1 revDPA-O): the more sensitive the personal data concerned, the stricter the requirements for the measures
- Recommended approach: **GAP analysis** between current and target status

General Provisions revDPA-Ordinance (II)

- General measures to ensure data security
  - Anonymization, pseudonymization and encryption of personal data
  - Procedures for identifying, assessing and evaluating risks and reviewing the appropriateness of the measures taken
  - Training and consulting
- Risk-based approach, i.e. no rigid minimum requirements, but rather the need for protection must be determined on a case-by-case basis and measures defined on the basis of risk

→ revDPA-Ordinance is similar in content, but less detailed than the GDPR (but technology-neutral)

Certifications

What are the Benefits of Certifications? (I)

- New / revised Ordinance on Data Protection Certifications ("**VDSZ**") – entry into force: 1 September 2023
- Certifications apply as follows: (Art. 13 para. 1 revDPA):
  - **Manufacturers** can certify their data processing systems or programs
  - **Controllers** and **processors** can certify their systems, products and services
- "Certification" means assessment by a recognized independent certification body
- VDSZ: contains provisions for the recognition of certification procedures with the aim of introducing a data protection quality mark

What are the Benefits of Certifications? (II)

Standards mentioned under the VDSZ to be considered for the audit of management systems:

- SN EN ISO 9001
- SN EN ISO/IEC 27001 and
- SN EN ISO/IEC 27701.

→ By means of certification, companies can, for example, prove that they comply with the principles of **privacy by design and default** and have an appropriate data protection management system in place

→ Possible advantage: The controller can **refrain from conducting a data protection impact assessment** (provided that the certification includes the processing which would have to be checked in the context of the DPIA)

TOMs

TOMs – General Principles (I)

- General guideline (Art. 8 (1) and (2) revDPA): The controller **and** the processor shall ensure data security appropriate to the risk by means of suitable technical **and** organizational measures. The measures must make it possible to **avoid** breaches of data security.
- Technical measures are measures that are implemented technically (e.g. password protection, access blockers or encryption)
- Organizational measures start with the human being (e.g. through a four-eyes principle, controls or training)

→ Technical measures tend to be considered stronger

- The measures must be reviewed over the entire processing period and adjusted if necessary (Art. 1 para. 5 revDPA-O). **The higher the risk, the more frequently a review is necessary.**
- The GDPR require a procedure for regular review.

TOMs – General Principles (II)

- Measures must correspond to the need for protection (cf. objectives Art. 2 revDPA-O)

- Criteria for determination (Art. 1 para. 4 revDPA-O):
  - State of the art (lit. a): it is sufficient to have measures that have already proven themselves;
  - Implementation costs (lit. b): "costs" is to be understood broadly and means (human, financial and time) resources

- Penal provision: anyone who intentionally fails to comply with the minimum data security requirements is liable to a fine of up to CHF 250,000 (Art. 61 lit. c revDPA).

- Under the GDPR, the same level of data protection is required with regard to TOMs

TOMs – Confidentiality

- **Access control («*Zugriffskontrolle*»)**: the access permissions and the type as well as the scope of access is determined
  - e.g. individual assignment of user rights, password query after inactivity
- **Admission control («*Zugangskontrolle*»)**: no access for unauthorized persons to the premises or facilities
  - e.g. permanently locked doors/windows, code locks on doors, security personnel
- **User control**: the data should not be used or shared in an unauthorized way
  - e.g. regular checks of authorizations (blocking in the event of personnel changes), "spyware" (insofar as permissible), virus protection/firewall

TOMs – Availability and Integrity (I)

- **Data carrier control**: preventing unauthorized persons from reading, copying, modifying, moving, deleting or destroying data carriers; preventing personal data from being transferred to data carriers in an uncontrolled manner
  - e.g. encryption or destruction of data, secure storage of data media
- **Storage control**: make it impossible for unauthorized persons to access, view, modify or delete the contents of the data memory
  - e.g. differentiated access authorization for data, logging of accesses
- **Transport control**: designated recipient must receive data in its original form and no third party should be able to intercept the data without authorization
  - e.g. encryption, secure transport containers for physical transports

TOMs – Availability and Integrity (II)

- **Data Recovery**: ability to restore data availability and access after an incident
  - e.g. backup concept, backup and recovery systems (like RAID)

- **Reliability**: ensuring the stability of the systems; malfunction should be reported by the system itself; stored personal data should not be damaged by malfunction of the system
  - e.g. VPN tunnel, firewall, fire and smoke detection

- **System security**: process for updating systems or proactively remediating vulnerabilities
  - e.g. activation of available software and firmware updates

TOMs – Traceability

- **Input control**: it must be possible to check retrospectively which data was entered or changed at what time by which person
  - e.g. logging
- **Disclosure control**: identification of data recipients
  - e.g. logging
- **Detection / Prevention**: reactive measure to quickly detect and remedy data breaches and to mitigate or prevent negative consequences

TOMs – Examples (I)

Goal	Measures acc. to Art. 3 revDPA-O	Meaning	Practical example
Confidentiality	Access control	determine and restrict access permissions and the type and scope of access	individual assignment of user rights, password query after inactivity
	Admission control	no access to premises / facilities for unauthorized persons	doors/windows locked at all times, code locks on doors, security personnel, alarm system
	User control	the data shall not be used or disclosed in an unauthorized manner	regular checks of authorizations (blocking in the event of personnel changes), "spyware" (insofar as permissible), virus protection/firewall, VPN

TOMs – Examples (II)

Goal	Measures acc. to Art. 3 revDPA-O	Meaning	Practical example
Availability & Integrity	Data medium control	prevent unauthorized persons from reading, copying, modifying, moving, deleting or destroying data carriers; prevent personal data from being transferred to data carriers in an uncontrolled manner	encryption or destruction of data, secure storage of data carriers, locking of USB data carriers
	Memory control	prevent unauthorized persons from accessing, viewing, modifying and deleting the contents of the data storage device	differentiated access authorizations for data, logging of accesses
	Transport control	designated recipient receives data in its original form; unauthorized third parties cannot intercept data	encryption, secure transport containers for physical transports
	Recovery	possibility of restoring the availability of data and access to data after an incident	redundant data storage and backup concept, backup and recovery systems (such as RAID)
	Data integrity	ensuring the stability of the systems; malfunction should be reported by the system itself; stored personal data should not be damaged by malfunction of the system	VPN tunnel, firewall, fire and smoke detection
	System security	process for updating systems or proactively remediating vulnerabilities	automatic activation of available software and firmware updates

TOMs – Examples (III)

Goal	Measures acc. to Art. 3 revDPA-O	Meaning	Practical example
Traceability	Input control	it must be possible to check retrospectively which data was entered or changed at which time by which person	Logging
	Disclosure control	identification of data recipient	logging
	Detection and elimination	reactive measure to quickly detect and remedy data breaches and to mitigate or prevent negative consequences	(AI-)software

Logging

Logging (I)

— Logging (Art. 4 revDPA-O) must take place if

- — personal data requiring special protection is processed on a large scale by automated means; **or**
- — high-risk profiling is performed, **and**
- — preventive measures do not ensure data protection

→ in particular, if it cannot otherwise be determined retrospectively whether the data were processed for the purposes for which they were obtained or disclosed

— Logging must provide information about:

- — the **identity** of the person who performed the processing;
- — the **type** of processing;
- — the **date** and **time** of processing; and
- — if applicable, the **identity of the recipient** of the data

Logging (II)

— Logs must be stored separately for **at least one year**

→ Access: only for bodies and persons responsible for verifying the application of data protection rules or for preserving or restoring the data and use only for this purpose

— Classic preventive data security measure

— Operations covered: storing, modifying, reading, disclosing, deleting and destroying data

→ Logging is similarly regulated as under the GDPR, but Swiss law does **not** provide for **general accountability**

Data Retention

Data Retention – General

To the extent that records contain personal data within the meaning of the DPA, such records may not be kept (at least not in a form that permits identification of the data subjects) for longer than is **necessary** to achieve the purposes for which the personal data were collected, unless the data subject has given his or her consent

→ Development of deletion rules and a deletion concept

Procedure:

— **Data mapping**: categories of data that are processed and that are archived

— Clarification of the essential **retention periods** (a mixture of retention obligations and statutes of limitations)

— Configuration of applications for **automatic deletion**

Data Retention – Deadlines

- Accounting in general: the books of account and the respective vouchers as well as the annual report and the audit report must be kept for ten years (Art. 958f CO; details in "GeBüV")
- Obligation to keep records of blood and blood products for 30 years (Art. 40 TPA)
- Personnel files, directories and other documents must be kept for at least five years after expiry of their validity (Art. 46 "ArG" in conjunction with Art. 73 "ArgV 1")
- NEW: Logs (according to Art. 4 revDPA-O) must be kept for at least one year separately from the system in which the personal data are processed (see TOMs explanations); data protection impact assessments must be kept for at least 2 years after the end of the data processing (Art. 14 revDPA-O)

Data Retention – Examples (I)

Document type	Retention period	Storage type
Company General		
– Foundation documents – Statutes – Partnership agreements	lifetime of the company	paper
– Minutes and resolutions of the shareholders' meeting, board of directors' meetings, committee meetings, EC resolutions, annual reports	10 years	paper
– Annual reports and audit reports	10 years	paper (written and signed)
Accounting		
– Balance sheet and income statement/financial statements	10 years	paper and signed
– Books of account (excl. balance sheet and income statement), namely: – Journal, general ledger and inventories – All auxiliary ledgers (e.g. accounts payable, accounts receivable, inventory accounting)		

Data Retention – Examples (II)

Document type	Retention period	Storage type
Accounting		
– Accounting records, namely: – Bank and postal receipts – Account and deposit statements – Delivery bills – Payroll – Invoices and receipts – Expense reports – Payment transaction documents – Cash receipts – Accounting journals – Tax directories	10 years	paper/electronic
– Business correspondence (if this business correspondence is the only existing accounting document for the business transaction in question): – Incoming and outgoing business letters – Business emails	10 years	paper/electronic
– Intellectual property rights documents (e.g. trademark registration certificates)	at least for the duration of the protection	paper/electronic
– Documents related to real estate	20 years	paper /electronic
– Insurance policies	at least for the duration of the insurance	paper/electronic
– Contracts of any kind including contract negotiations	10-15 years	paper (if the original is in paper form)

Data Retention – Examples (III)

Document type	Retention period	Storage type
Taxes		
– General tax documents	10 years	paper/electronic
– Documents related to real estate taxes	20 years	paper/electronic
– Contracts –	10 years from the last of the following events: termination, expiration, or fulfillment, if necessary for the full maintenance of an entity's accounts and records.	paper/electronic
– Business relevant documents	no specific retention period, but 10 years if needed to fully understand a company's books and records; at least for the duration of the mandate	paper/electronic
– Permits – Licenses – Certificates	no specific retention period, but 10 years if needed to fully understand a company's books and records	paper/electronic
– Non-disclosure and non-competition agreements (if the non-competition or confidentiality clause is subject to a penalty)	10 years; at least 10 years if needed to fully understand the accounting and records of a company; start of the retention period: termination of the agreement.	
– Correspondence	no specific retention period; At least 10 years if necessary for a full understanding of a company's books and records.	

Data Retention – Examples (IV)

Document type	Retention period	Storage type
Employment relationship		
– Documents with information proving the proper enforcement of the Swiss Labor Code – Documents on social security issues	5 years after the end of employment	paper/electronic
– Recruitment documents	no specific retention period (as long as necessary)	paper/electronic
– Personal data of employees in network systems, computer systems, communications equipment used by employees, access controls, and other internal management/administrations	1 year from the creation of the recordings (video recordings within 24 hours)	electronic
Anti-Money Laundering		
– Anti-money laundering records	10 years from termination of the business relationship or conclusion of the transaction	paper/electronic

Processing Policy

Processing Policy – General

- Regulations for automated processing must be drawn up if (Art. 5 para. 1 revDPA-O):
  - personal data requiring special protection is processed on a large scale (lit. a); or
  - profiling with high risk is carried out (lit. b)
- The obligation to have a Processing Policy in place is incumbent on the controller **and** its processor
- The Processing Policy must in particular contain information on the internal organization, the data processing and control procedure and the measures to ensure data security (Art. 5 para. 2 revDPA-O)
- The Processing Policy must be updated regularly (Art. 5 para. 3 revDPA-O)

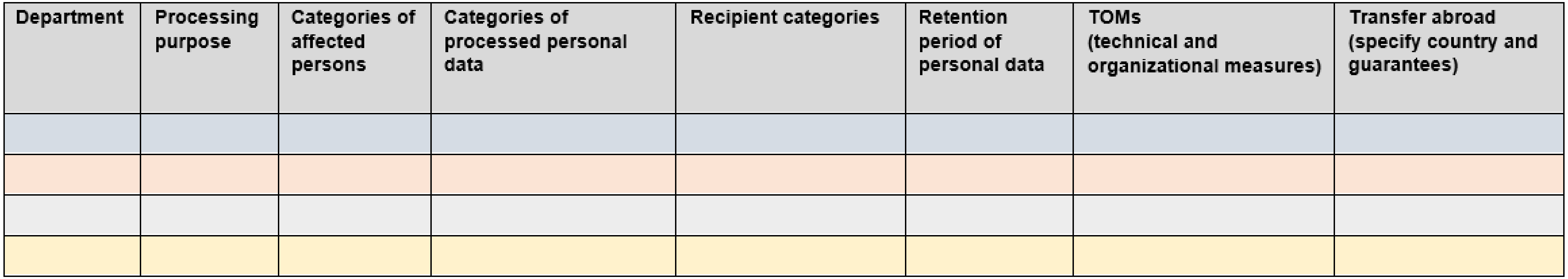
Processing Policy – Content

- The internal organization must be described – this includes a description of the architecture and functioning of the systems
- It should be recorded which data processing procedures are carried out
- The procedure for exercising the data subject's rights of access, information, disclosure and transfer of data (data portability) must be described
- The control procedures described must make it possible to determine the access authorizations, the type and scope of access
- Finally, it must also include the TOMs to ensure adequate data security

Register of Processing Activities (ROPA)

ROPA

- New requirement (Art. 12 revDPA): controllers **and** processors must each keep a register of their processing activities
- Exception (Art. 24 revDPA-O): Companies with **less than 250 employees**
- Counter-exception: a register of processing activities must be kept in any case if (Art. 24 revDPA-O):
  - personal data requiring special protection are processed on a large scale (lit. a); or
  - profiling with high risk is carried out (lit. b)



Department	Processing purpose	Categories of affected persons	Categories of processed personal data	Recipient categories	Retention period of personal data	TOMs (technical and organizational measures)	Transfer abroad (specify country and guarantees)

Obligation to Notify the FDPIC

Data Breach Notification (I)

- The controller notifies the FDPIC (and the processor notifies the controller) as soon as possible of a breach of data security that is likely to result in a high risk to the personality or fundamental rights of the data subject (Art. 24 para. 1 and 3 revDPA)

- A breach of data security occurs when personal data is unintentionally or unlawfully lost, deleted, destroyed or altered, or disclosed or made accessible to unauthorized persons (Art. 5 lit. h revDPA)

- With regard to the high risk, a case-by-case assessment is made
  - If a severe adverse outcome is at least likely or a moderate adverse outcome is very likely, the risk is high
  - Methodology of risk calculation = probability of occurrence x extent of damage

Data Breach Notification (II)

- The responsible person must document the violations
- The documentation must contain the facts related to the incidents, their effects and the measures taken (Art. 15 para. 4 revDPA-O)
- The documentation must be kept for at least two years from the date of notification (Art. 15 para. 4 revDPA-O)
- The FDPIC is currently working on the development of a web-based reporting interface, probably in the form of an **interactive form**

Reporting Obligations – Differences revDPA vs. GDPR

Notification	GDPR (Art. 33/34)	revDPA (Art. 24) / revDPA-O (Art. 15)
Data protection authority	- immediately and if possible within 72 hours - except if no risk is expected	- as soon as possible - if expected high risk
Person concerned	- immediately - if expected high risk	- if necessary for the protection of the data subject's rights - if requested by the FDPIC
Sanction for omission	- fines of up to EUR 10 million or 2% of the worldwide annual turnover	N/A

Our Newsletters on the revDPA

Checklist NKF on the revised DPA:

https://www.nkf.ch/app/uploads/2022/10/en-nkf-client-news-revised-federal-act-on-data-protection-02122020.pdf

Newsletter NKF on Specific Amendments and Measures under the revised DPA:

https://www.nkf.ch/app/uploads/2022/10/en-client-news-specific-amendments-and-measures-under-the-revised-fdpa-final.pdf

Thank you for your attention! Questions?

Clara-Ann Gordon
clara-ann.gordon@nkf.ch
D +41 58 800 84 26

Janine Reudt-Demont
janine.reudt-demont@nkf.ch
D +41 58 800 83 95

NKF

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