COPEBIT

aws


1100
010
0110
101
01010
1100
0100
1010
11001
0100
$
€
11
01
11
1101
010
11
1
110
0101
01
110010
00101
11010
110

COPEBIT

aws PARTNER Advanced Tier Services

- Public Sector
- Immersion Day
- Solution Provider
- Amazon RDS Delivery
- AWS CloudFormation Delivery
- Amazon EC2 for Windows Server Delivery

Webinar

Unboxing Cloud & Compliancy

21st August 2023

Agenda

- Welcome (Marco)
- The revised Data Protection Act (Clara-Ann Gordon)
- Q&A

Customers of copebit that have shown interest in revFADP

BERTSCHI

ELPRO

autoSense

ARI Appenzell Ausserrhoden Informatik

simpego

NIEDERER KRAFT FREY

COPEBIT

Cloud und Compliance

The revised Data Protection Act (revFADP) and the new Data Protection Ordinance (revFADP-O)

Clara-Ann Gordon

Zurich – 22 August 2023

Content

1. Introduction
2. Usage of Cloud and Data Protection
3. Overview of Changes to the revised Data Protection Act
4. In focus: TOMs
5. In focus: Obligation to Notify the FDPIC
6. Compliance Challenges
7. Step-by-Step Plan and Practical Implementation
8. Summary

Introduction

What is the Cloud?

- **Cloud definition:** Computer-based services that are made available via a network (e.g. internet) such as: software, storage capacities, development tools, network capacities, computer capacities etc.
- **Types**: Private, public, hybrid, community clouds, etc.
- **Service levels**: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (Saas), Business Process as a Service (BPaaS), Cybersecurity as a Service (CaaS), etc.
- **Contract structure:** GTC or individually negotiated contracts
- Data stored on **physical storage media (server)** usually owned by the Cloud Provider or a third party. In the case of a private cloud, the server may be owned by the customer.

Parties Involved

- **Cloud Provider:** e.g. AWS, Microsoft, Google, etc. is the contractor from a legal point of view
- **Cloud User:** is the customer of the cloud services offered by the Cloud Provider.
- **Service providers** around the cloud: e.g. copebit, who assist with selection, migration to the cloud, etc.
- **Regulatory authorities:** check compliance with laws when going to the cloud

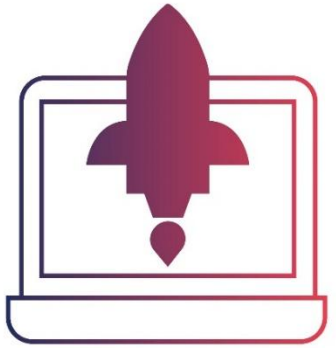
Usage of Cloud and Data Protection

When is the Usage of Cloud relevant under Data Protection Law?

- Relevant under data protection law Transfer of personal data to the cloud:
  - Office 365 tools for online collaboration between employees
  - Online management tools of e-mail addresses for newsletters or customer advisory services
  - Online CRM system
  - Uploading videos on streaming platforms
  - Uploading files to a remote server accessible via the Internet
- Use of cloud services is commissioned data processing ("outsourcing") from a data protection point of view.

Requirements for Outsourcing?

- The requirements for outsourcing are the following:
  - Contract in writing
  - Data may only be processed in the same manner as the person responsible would be allowed to do himself/herself
  - no legal or contractual secrecy obligations prohibit the transfer
  - Ensure data security (TOMs!)
  - Transfer of data processing to third parties only with consent



Relationship between Cloud Providers and Cloud Users

- Companies offering cloud services usually act as data processors of the Cloud User according to Art. 9 revFADP
- The Cloud User can be both a controller and a processor
  - Controller: Takes responsibility for ensuring that the Cloud Provider's data processing complies with data protection requirements
  - Processor: Cloud User must fulfil the requirements set by the controller
- Use of cloud services abroad
  - The Cloud User must check whether the disclosure abroad meets the legal requirements

Further Legal Issues?

- Which personal data is stored in the cloud? Particularly worthy of protection? Personality profiles? Classified data?
- Which regulations are applicable to this data: Swiss and/or foreign data protection regulations, special legal confidentiality regulations?
- Are there any special regulatory requirements for the outsourcing of data processing (e.g. for insurance and banking data or public sector data)?
- Is data subject to special proof and archiving regulations (e.g. business records ordinance, social security law, VAT law)?
- etc.

Overview of new Provisions in the revised Data Protection Act

General provisions of the revFADP (I)

- The totally revised FADP applies from **1 September 2023** - no transitional period
- Scope of application: Is your company affected?

  Processing of personal data in Switzerland or outside Switzerland but with effect in Switzerland

  □ new: extraterritorial effect
- Protection goals: confidentiality, availability, integrity and traceability
- Protection needs analysis □ the higher the protection needs are, the stricter the requirements for the measures
- Recommended approach: **GAP analysis** between current state-of-the-art and target state

What are the most important Changes under the revFADP?

- **Extension of the information obligation** → now applies to every collection of personal data
- Personal data of legal entities are no longer protected
- The principles of "Privacy by Design" and "Privacy by Default" are introduced
- Genetic and biometric data are explicitly qualified as "sensitive personal data"
- High risk to personality / fundamental rights in the case of data processing? → DPIAs (Data Protection Impact Assessments) must be carried out
- Mandatory register of processing activities → **exception for SMEs** whose data processing involves only a low risk of infringing the personality of the data subjects
- Immediate **notification to the FDPIC** in case of a data breach
- "Profiling" was added to the new act (but it largely equals to the previous "personality profiles")

Fines

Considerably higher fines apply as of 1 September 2023:

- Ad personam fine of up to CHF 250,000
- Sanctioned offences: e.g. failure to name the country to which the personal data are disclosed abroad; violation of the right of access; violation of the obligation to ensure sufficient data security
- Criminal law provision: anyone who **intentionally** fails to comply with the minimum data security requirements is punished with a fine of up to CHF 250,000.

On focus: TOMs

TOMs – General Principles (I)

- General guideline (Art. 8 (1) and (2) revFADP): 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 revFADP-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 revFADP-O)
- Criteria for determination (Art. 1 para. 4 revFADP-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 revFADP).
- Under the GDPR, the same level of data protection is required with regard to TOMs

TOMs – Examples (I)

Goal	Measures acc. to Art. 3 revFADP-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 revFADP-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 revFADP-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

In focus: Obligation to Notify the FDPIC

Data Breach Notification (I)

- Cloud User notifies the FDPIC (and the Cloud Provider notifies the Cloud User) 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 revFADP)
- 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 revFADP)
- 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)

- Cloud User must document the violations
- The documentation must contain the facts related to the incidents, their effects and the measures taken (Art. 15 para. 4 revFADP-O)
- The documentation must be kept for at least two years from the date of notification (Art. 15 para. 4 revFADP-O)
  - The FDPIC has new a notification portal: https://databreach.edoeb.admin.ch/report

Reporting Obligations – Differences revFADP vs. GDPR

Notification	GDPR (Art. 33/34)	revFADP (Art. 24) / revFADP-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

Compliance challenges

Compliance Challenges re Usage of Cloud (I)

- Data security
  - Certifications confirm the compliance with the required data security
- Server location
  - Where is the data located? In Switzerland or abroad?
  - If server abroad then adequate level of data protection required
- Cloud Provider per se
  - Governmental data access? e.g. US Cloud Provider or its subsidiary

Compliance Challenges re Usage Cloud (II)

- Only limited possibilities for the data controller or Cloud User to customize the service or adapt the data processing accordingly
- Data protection by design and data protection by default according to Art. 7 revFADP

Obligations for the data controller to design the data processing technically and organizationally:

- Comply with data protection regulations
- Suitable default settings → The processing of personal data shall be limited to the necessary for the purpose
- Technical measures → e.g. fully encrypt or anonymize data before transferring it to the cloud

Step-by-Step Plan and Practical Implementation

Ten-step Plan for practical Implementation

Step 1: Draft or amend privacy policies

Step 2: Extended rights of data subjects

Step 3: Check data processing agreements (DPAs)

Step 4: Transfers of data abroad

Step 5: Draft or amend TOMs

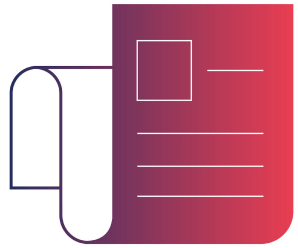
Step 6: Data breach notification

Step 7: Create a register of processing activities

Step 8: Data Protection Impact Assessment (DPIA)

Step 9: Automated decisions

Step 10: Create training and instruction documents



Step 1: Draft or amend Privacy Policies

- Privacy policies become mandatory under the revFADP
  - Information obligation is extended: applies to every collection of personal data
  - Privacy policy on own website, as an appendix to contracts etc.
- Minimum content determined by the revFADP:
  - identity and contact details of the controller
  - purpose of processing
  - categories of recipients
  - categories of collected and processed personal data
  - involved countries
  - transferring data to so-called unsafe third countries information on protective measures

 Important: Establish early on who is collecting which data within your company and for what purpose this facilitates the formulation of own privacy policies

Step 2: Extended Rights of Data Subjects

- Rights of data subjects:
  - **Right to information**: **significantly extended** □ duty to provide information whenever personal data is collected; if the data is not obtained from the data subject, the information must be provided subsequently (within one month at the latest) □ special right to information in the case of automated individual decisions
  - **Access rights**: analogous to current Art. 8 FADP □ information is generally to be provided free of charge within **30 days** □ create internal procedures and structures in order to be able to react more quickly to requests (data mapping and register of processing activities help)
  - **Right to rectification, deletion**: analogous to current law (Data Retention Policy helps)
  - **Right to data portability**: new □ release of personal data in a standard electronic format by the controller

□ **Important:** Setting up a contact point at an early stage that is responsible for inquiries from affected parties and can respond to these quickly

Step 3: Check Data Processing Agreements (DPAs)

- A DPA must be concluded if a company commissions another company to process personal data on its behalf (analogous to current Art. 10a FADP)
  - Ensuring that the data is only processed by the commissioned processor in the same way as the data controller would be permitted to do itself
  - Right to give instructions, right to control, support for FADP compliance
  - Ensuring data security appropriate careful selection of the commissioned data processor
- However, if the data is (also) processed by the company for its own purposes, then this company itself is responsible

  nevertheless one should conclude a DPA ("Controller to Controller")

Important: Check early on whether suitable contracts have already been signed with the service providers, whether these need to be amended or "new" DPAs (in the sense of a contract addendum) have to be concluded

Step 4: Transfers of Data abroad

- Is it recognised by the Federal Council that an equivalent level of data protection exists in the state in question (e.g. EU states)? if yes, unproblematic, but:
  - Duty to provide information is extended: applies to any data collection **provide information on country**
  - Provide privacy policy on own website etc. with link (e.g. to list of group companies)
- In the case of data transfers to so-called "unsafe" third countries without a comparable level of data protection, special precautions need to be taken
  - Federal Council determines which countries have an equivalent level of data protection
  - Maybe required: Transfer Impact Assessment (TIA)
  - In any case: implementation of guarantees to ensure data protection, e.g. by concluding the recognised EU standard contractual clauses (with Swiss addition)

 Important: In order to keep an overview of the data flows abroad, it would be useful to document all data transfers (data flow chart)

Step 5: Draft or amend TOMs

- Creation of a document listing all technical and organisational measures taken to ensure data protection and data integrity
- Creation based on input, in particular from IT, from data mapping
- Categories of measures: according to legal requirements (see revFADP-Ordinance)

Access control (*Zugriffskontrolle*)	Entrance control (*Zugangskontrolle*)
User control	Data carrier control
Storage control	Transport control
Recovery	Availability
Reliability	Data integrity
System security	Input control
Disclosure control	Elimination

- **Recommendation:** Create two TOMs documents, one for "external use" and one with more detailed information for internal use

Step 6: Data Breach Notification

- Data breach: breach of confidentiality, integrity or availability of personal data
  - E.g. wrong e-mail recipient, data loss, hacker attacks
- **Notification to the FDPIC** is only required if the data breach is likely to result in a high risk to the personality or fundamental rights of the data subject
  - Violation of the reporting obligation is not sanctioned
- Notification obligation applies to the data controller, but also to data processors
- Breach must be communicated to the data subject if necessary for his or her protection (e.g. in the case of a hacked password)

Important: Designate a responsible person and instruct employees to report the relevant incidents to it Data Breach Response Plan

Step 7: Create a Register of Processing Activities

- Keeping a register of processing activities becomes mandatory exception SMEs, if applicable
- All data processing must be listed in the register
  - No fixed or mandatory structure of the register
  - Enables an overall and structured overview of all data streams within the company
- Minimum content determined by the FADP:

  identity and contact details of the controller, purpose of processing, categories of data subjects and data processed, categories of recipients, storage period, countries involved, in the case of data transfers to so-called unsafe third countries: a description of the measures taken to ensure data protection

 Important: The register is a good basis for the creation of the privacy policy and other documents and may therefore also be the **first step** to take

Step 8: Data Protection Impact Assessment (DPIA)

- If the intended processing results in a high risk for the personality or the fundamental rights of the data subject, a DPIA must be carried out (e.g. installation of video camera)
  - Responsible person: self-assessment of the project
  - Content: description, analysis of the possible (also unintended) negative consequences for an affected person, measures taken to minimize or eliminate risk documentation
- If a project poses a high risk despite all the measures taken, the FDPIC (or the (independent) DPO) should be consulted

  Violation is not sanctioned

Important: Conduct the DPIA together with the respective department, because only this department knows the respective project in detail and the measures which could be taken

Step 9: Automated Decisions

- Definition: automated decisions means judgment calls with legal or significant other negative consequences that are made solely by a computer with respect to an individual person
  - Examples: automatic applicant selection or credit allocation (without "human review")
  - Permissible in principle, but the person concerned must be informed and, if requested be heard by a human being
- The protection does not apply if the person consented to the automation of the decision or if it is a contract in which an automated decision is made per se according to its characteristics (e.g. purchase in an online store)

 Important: Find out at an early stage to what extent and in which area automated decisions are applied in your company

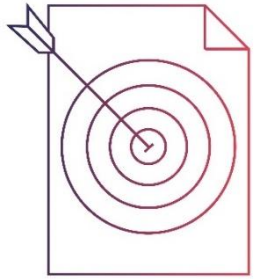
Step 10: Create Training and Instruction Documents

- Appropriate directives, work instructions and training are needed without these employees are not aware of the Do's and Dont's
  - In time adaptation or creation of internal directives
  - Samples and templates (e.g. for DPAs) should be created
  - Training should be provided so that employees know how to respond to requests for information, for example
  - Record training sessions so that there is documentation of compliance with the revFADP should any proceedings arise against the company in the future
- Clear internal processes and a point of contact for questions are also needed

Summary

Summary

- With regard to the use of the cloud, there are no significant changes under the revFADP
- However, Cloud Providers play a central role in complying with the cornerstones of data protection:
  - Ensure data security (TOMs are crucial!)
  - Cloud Providers also have reporting obligations for data breaches
- The main responsibility remains with the Cloud User
- Lack of a written contract is punishable by law
- Transparent and comprehensive information obligations of the Cloud User in relation to its end customers
- Server location is decisive - Is there a risk of state access?



Thank you for your attention! Questions?

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

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

COPEBIT

Closing

COPEBIT

aws


1100
010
0110
101
01010
1100
0100
1010
11001
0100
$
€
11
01
11
1101
010
11
1
110
0101
01
110010
00101
11010
110

COPEBIT

Thank you!