Regulation of the Use of Cloud Computing by Public Authority in the Czech Republic

NÚKIB

National Cyber and Information Security Agency

24 September 2021

TLP: WHITE

Department of Regulation

What is cloud computing?

- The term does not come from academic world but business – inconsistent perception
- Typical features:
  - **Computing resources** = networks, servers, operating systems, software, repositories, applications, services
  - **Remote access** = Internet
  - **Self-service** = the other side controlled by computer = fast
  - **Expandable** = almost indefinitely as long as I have money
  - **Shared** = if I don't use it, someone else does, or we can use it together
- Also cloud computing services, cloud services, cloud
- ISO/IEC 17788
- NIST 800-145

CC Author: Julian Herzog, architecnologia.es

Reasons for cloud computing regulation

- The use of cloud services is growing rapidly in both private and public sectors.
- Cloud services can contribute to:
  - A more economical operation and
  - A safer operation of information systems (central management, surveillance, and updating).
- However, cloud services bring along new risks:
  - The location of data processing is often abroad and not known to the individual customers that use the cloud services;
  - The relevant aspects of the **legal system** of the third country must be considered – access of foreign bodies to data (GDPR, SD EU Schrems II);
  - Significant dependency on the provider and limited possibilities to verify them;
  - Difficult access for Czech “law enforcement” bodies to data about criminal activities;

Implementation of cloud computing regulation

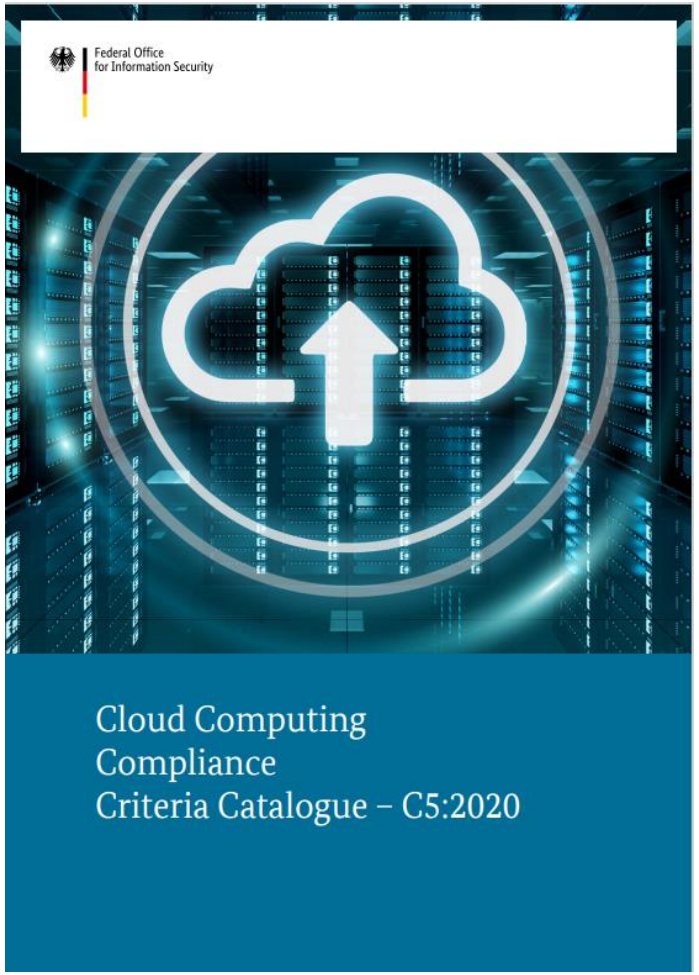
- Regulatory framework
  - Act No. 365/2000 Coll., On Public Authority Information Systems (ZoISVS)
  - Act No. 181/2014 Coll., On Cybersecurity (ACS)
- Main regulation since 1 August 2020 – a number of shortcomings – amendments required
- Amended by Act No. 261/2021 Coll., so-called DEPO, effective from **1 September 2021**.

- In that connection, NÚKIB has issued two Decrees and is preparing a third one:
  - Decree No. 316/2021 Coll., on Certain Requirements for Registration in Cloud Computing Catalogue (so-called Entry Criteria)
  - Decree No. 315/2021 Coll., on Security Levels for the Use of Cloud Computing by Public Authorities (so-called Decree on Security Levels)

Basis for cloud computing regulation

- Summary Analytical Report on project Preparation of Creation of eGovernmentCloud (Government Resolution No. 749 of 14 November 2018)
- International standards C5, ISO 27001, 27017, and 27018
- Recommendations of the CNB (Czech National Bank) for the use of cloud by banks
- Comments of professional audience on the objective
- Outcome of negotiations with providers and public authorities

ISO 27017
International Organization for Standardization



Main points in cloud computing regulation

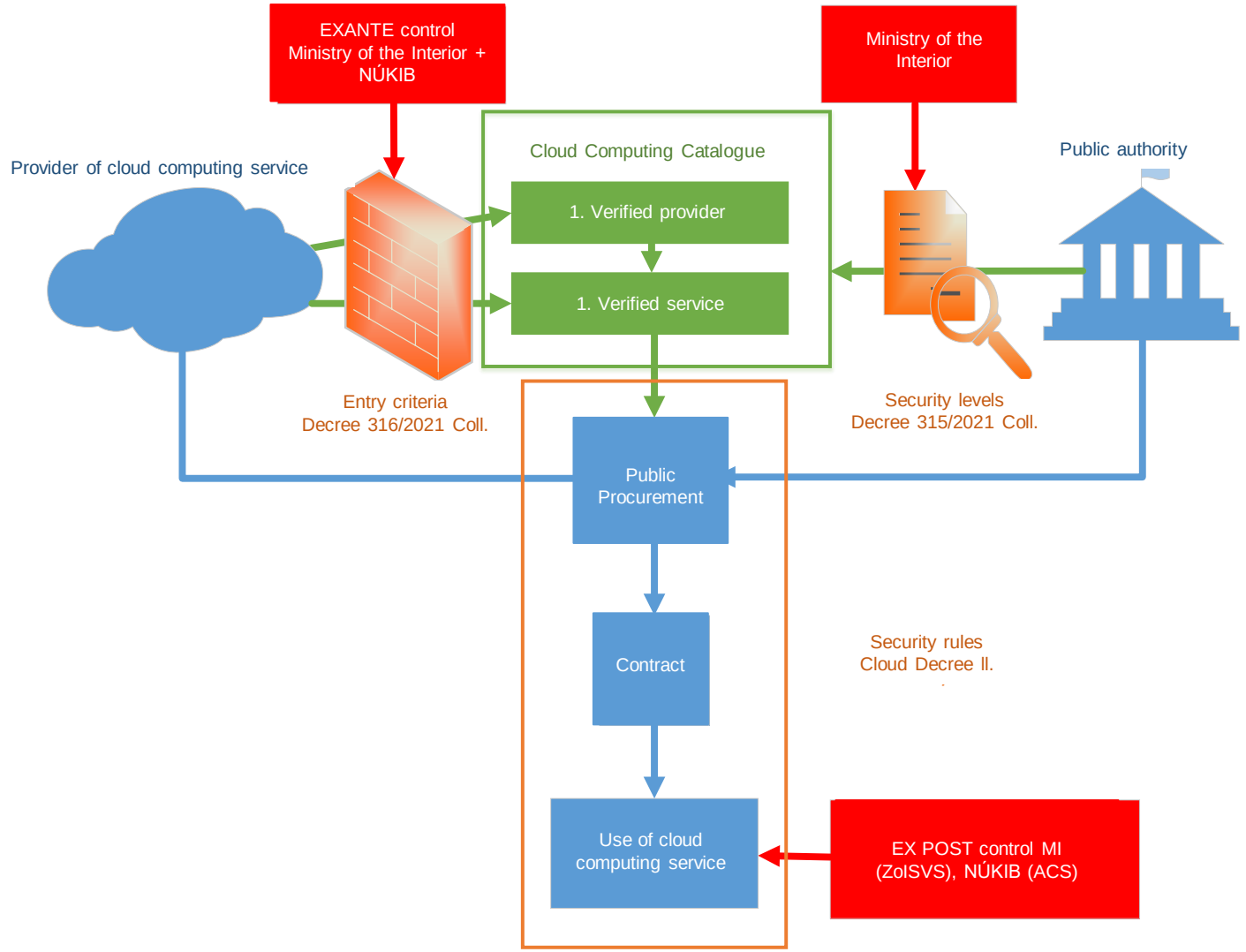
- TRUST
  - Verification of the cloud computing service **provider** with respect to public order, security, and respect for the rights of third parties
  - Requirements for a cloud computing service = ENTRY CRITERIA
  - Verification of providers and limited services – ex ante, capacities

- TRANSPARENCY
  - Requirements for information about data processing (where, why, how long), export outside the EU only in necessary cases

- RESPONSIBILITY
  - The public authority is still responsible for information security even in the event of using cloud services
  - Classification of the public authority information system = SECURITY LEVELS
  - Ensure the SECURITY RULES are observed

- A condition for public procurement for cloud computing service is that the security level of the offered cloud computing service ≥ the security level of the public authority information system (ZoISVS).

Overview of the cloud computing regulatory framework - ZoISVS



Reqiurements on cloud computing providers - ZoISVS

Section 6m of the ZoISVS

Requirements on the cloud computing provider providing cloud computing to a public authority

- **(1)** A cloud computing provider providing cloud computing to a public authority may only be a person or another legal arrangement that is
- **a)** eligible to ensure a basic level of protection of confidentiality, integrity, and availability of information for the public authority,
- **B)** of integrity to the integrity extent required for a certified administrator of a certified electronic identification system,
- **c)** eligible to provide cloud computing to public authority with respect to public order, security, and respect for the rights of third parties.

Requirements on cloud computing - ZoISVS

Section 6n of the ZoISVS

Requirements for cloud computing used by a public authority

- A public authority may use and a cloud computing provider may provide to a public authority or a state provider of cloud computing such cloud computing that
- **a)** allows meeting the requirements of the information technology concept of the Czech Republic on public authority information systems,
- **b)** enables reaching at least the basic level of protection of confidentiality, integrity, and availability of information for a public authority,
- **c)** allows a public authority to follow security rules for public authority that use cloud computing services under the cybersecurity legislation,
- **d)** has the same or higher security level as the security level of the public authority information system or its part whose operation it shall ensure,

(…)

Requirements on public authority bodies - ACS

Section 4 paragpraph 5 of the ACS

Requirements on cloud computing used by a public authority

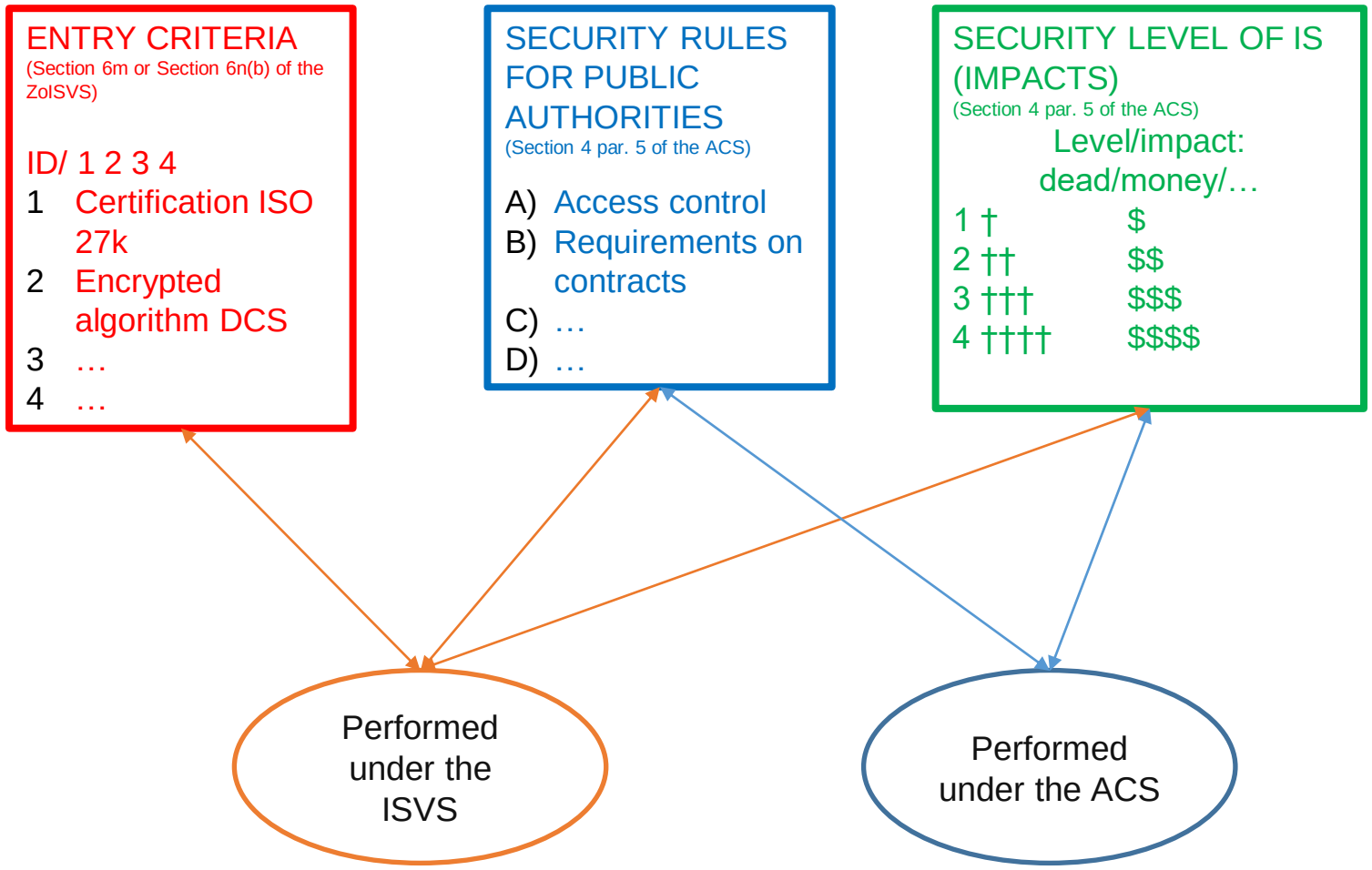
- Until 1 September 2021:

Bodies and persons mentioned in Section 3(c) through (g) which are public authority bodies are particularly obliged to ensure in the contract with a provider of cloud computing services that the security rules set by the Agency for provisions of cloud computing are adhered to, (…)

- Since 1 September 2021:

Before concluding contracts with cloud computing providers, public authority bodies are obliged to classify the enquired cloud computing within a security level with respect to the nature of the given information or communication in compliance with the implementing legislation and ensure that the security rules set by the Agency for provisions of cloud computing are adhered to (…)

Acts and three Decrees on cloud



The Three Cloud Decrees I.

1. Decree No. 316/2021 Coll., on Certain Requirements for Registration to Cloud Computing Catalogue

- EFFECTIVE SINCE 1 September 2021
- ‘Decree on Entry Criteria’
- A set of requirements that a provider of CC services must meet to be allowed to supply public authorities
- Cloud services are divided into 4 levels based on security requirements
- Individual suppliers must meet the entry requirements
- Compliance with the requirements is assessed by MI and NÚKIB = administrative proceeding

Strana 3770 Sbírka zákonů č. **316** / 2021 Částka 140

316

VYHLÁŠKA

ze dne 24. srpna 2021

o některých požadavcích pro zápis do katalogu cloud computingu

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2021 Sb., (dále jen „zákon“):

§ 1

Předmět úpravy

Tato vyhláška stanoví

a) požadavky na způsobilost poskytovatele cloud computingu (dále jen „poskytovatel“) zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona,

b) požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 6n písm. b) zákona,

c) seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona, doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2 zákona,

§ 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona.

§ 2

Základní pojmy

Pro účely této vyhlášky se rozumí

a) zákazníkem orgán veřejné správy využívající službu cloud computingu,

b) uživatelem ten, kdo službu cloud computingu prostřednictvím systému orgánu veřejné správy využívá nebo ji nastavuje,

c) zákaznickými daty všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu,

d) zákaznickým obsahem textová, zvuková, audiovizuální, obrazová nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům,

e) provozními údaji data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskytováním služby cloud computingu,

The Three Cloud Decrees II.

2. Decree No. 315/2021 Coll., on Security Levels for the Use of Cloud Computing by Public Authorities (Decree on Security Levels of Systems)

- EFFECTIVE SINCE 1 September 2021
- Categorising an information system or its part within security levels (SL)
- The security level determines the potential impact of a NIS incident
- Directory for assessment of the importance of public authorities systems and determination of requirements for their securing
- Applies to all public authorities
- There are 4 SLs: low, medium, high (= commercial provider), critical (= state owned provider)

Částka 139 Sbírka zákonů č. **315** / 2021 Strana 3763

315

VYHLÁŠKA

ze dne 24. srpna 2021

o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 205/2017 Sb., (dále jen „zákon"):

§ 1

Předmět úpravy

Tato vyhláška stanoví bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci podle § 6 písm. e) zákona.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) poptávaným cloud computingem informační nebo komunikační systém jako celek nebo jeho část, které mohou být provozovány pomocí cloud computingu a které je orgán veřejné moci povinen zařadit do bezpečnostní úrovně,

b) částí informačního nebo komunikačního systému taková část tohoto systému, která je jednoznačně oddělitelná, zabezpečuje cílevědomou a systematickou informační činnost[1]), může být provozována pomocí cloud computingu a je definována z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti,

c) oblastí dopadu vymezená oblast, v rámci které může mít dopad kybernetického bezpečnostního incidentu na poptávaný cloud computing vliv na bezpečnost a zdraví lidí, ochranu osobních údajů, trestněprávní řízení, veřejný pořádek, mezinárodní vztahy, řízení a provoz, důvěryhodnost, finanční model nebo zajišťování služeb,

d) úrovní dopadu nízká, střední, vysoká nebo kritická hodnota, která odpovídá dopadu kybernetického bezpečnostního incidentu na poptávaný cloud computing v každé oblasti dopadu.

§ 3

Bezpečnostní úrovně

Bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci vyjadřuje možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou nízká, střední, vysoká nebo kritická.

§ 4

Zařazení poptávaného cloud computingu do bezpečnostní úrovně

(1) Zařazení poptávaného cloud computingu do bezpečnostní úrovně provede orgán veřejné moci podle přílohy k této vyhlášce. Orgán veřejné moci zhodnotí naplnění úrovně dopadu, které je poptávaný cloud computing schopen dosáhnout v rámci každé oblasti dopadu. Úroveň dopadu je v rámci každé oblasti dopadu dána nejhorším možným dopadem kybernetického bezpečnostního incidentu.

(2) Při zjišťování nejhoršího možného dopadu kybernetického bezpečnostního incidentu zohlední orgán veřejné moci možné narušení důvěrnosti, integrity a dostupnosti poptávaného cloud computingu a povahu informačního nebo komunikačního systému, který je poptávaným cloud computingem, jako celku. V případě, že je poptávaným cloud computingem pouze určitá část informačního nebo komunikačního systému, zohlední také vztah této části k bezpečnostní úrovni informačního nebo komunikačního systému jako celku.

(3) Bezpečnostní úroveň pro využívání poptá-

[1]) § 2 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

The Three Cloud Decrees III.

3. Decree on Security Rules

- In preparation – assumed to be issued in Q2/2022
- Relevant security measures will be set for each of the security levels (1-4)
- Affects all public authority bodies
- Close to the DCS as for its content; builds on the German C5 standard
- Will contain both mandatory and optional security rules – about 250 rules in total (46 mandatory)
- An entity will implement mandatory measures and consider the appropriateness of the optional ones
- Securing options:
  - Declarations of providers
  - Certification of providers – ISO 27001, ISO 27017, ISO 27018, C5, SOC 2® Type 2, ISO 20000 or ISO 22301
  - Contractual obligation of the provider

Temporary provisions

- **Act No. 12/2020 Coll. Section 17** (amended by Act No. 261/2021 Coll.)
  - Since 1 August 2020, a public authority (PA) must register the cloud computing (CC) it uses in the CC catalogue
  - PA was using as of 1 August 2020 = it can continue to use the CC for another 41 months (1 January 2024)
- **Act No. 261/2021 Coll., Article LXXXI**
  - PA was using CC or concluded a (framework) contract before 1 September 2021 = it can continue to use the CC until 31 December 2023
  - CC in the catalogue before 1 September 2021/Registered under conditions valid before 1 September 2021 = the CC may be used until 31 December 2023
  - PA started to use the CC between 1 September 2021 and 31 January 2022 = it can continue to use the CC until 31 December 2022

Note: if the given CC meets the current requirements – it is registered in the catalogue and meets the requirements of the Cloud Decrees – it may be used without a time limit

Relation of cloud regulations in the Czech Republic to the EUCS

- Following the implementation of the EUCS and settling some reservations, the national regulation can be adapted to the EUCS:
  - Adjustment of ENTRY CRITERIA
    - Possibility to table EUCS certificate + additional requirements for the place of data processing and verification of the cloud service provider
  - Adjustment of SECURITY RULES
    - Harmonisation of the wording of security rules with the requirements for cloud service providers of the EUCS + requirements exclusively relating to public authority bodies

Cloud Decrees - where to find information

- Decrees, including justification:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
- FAQ:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/
- Cloud Computing Catalogue – registered offers and enquiries:
  - https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3d%3d
- Offer registration forms
  - Click through the NÚKIB's website: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/
- Services permanently saving data outside the EU – NÚKIB's Notice Board - https://www.nukib.cz/cs/uredni-deska/

Any questions?

Turn to us on

regulace@nukib.cz