DORDA

IT-S NOW

DORA - digital operational resilience for the financial sector

7 June 2024

Nino Tlapak

Partner and Co-Head of the Data Protection Team

- Focus: data protection, cybersecurity, IT-contracts with a focus on outsourcing and cloud contracts
- ILO Clients Choice Award for Blockchain 2023
- Recommended as Next Generation Partner in TMT and Data Privacy in the international legal directory "*Legal 500*" as well as Band 4 in "*Chambers Europe*"
- PrivacyConnect Co-Chair Vienna
- Lecturer for data protection law at master courses at the University of Vienna, FH Technikum Wien and FH Campus Wien as well as Vienna University for Business and Economics ("*Data Protection and New Technologies*") and Danube University Krems ("*Datenschutz und Privacy*")
- Regular speaker at relevant international conferences and meetings (IT Rechtstag; ITechLaw; Privacy Symposium; AlpinePrivacyDays etc)
- Member of "*it-law.at*" and "*Privacyofficers.at*"

Chambers
RANKED IN
Europe
2023
Nino Tlapak

Nino Tlapak

nino.tlapak@dorda.at

Agenda

1. General

- Background and regulatory framework
- Scope of application (definitions of financial entities, ICT services, ICT third-party service providers, etc.)

2. Details on DORA and contract design

- Governance & ICT risk management (risk management requirements, strategies and training)
- Contract design
- Digital operational resilience
- Reporting and information exchange

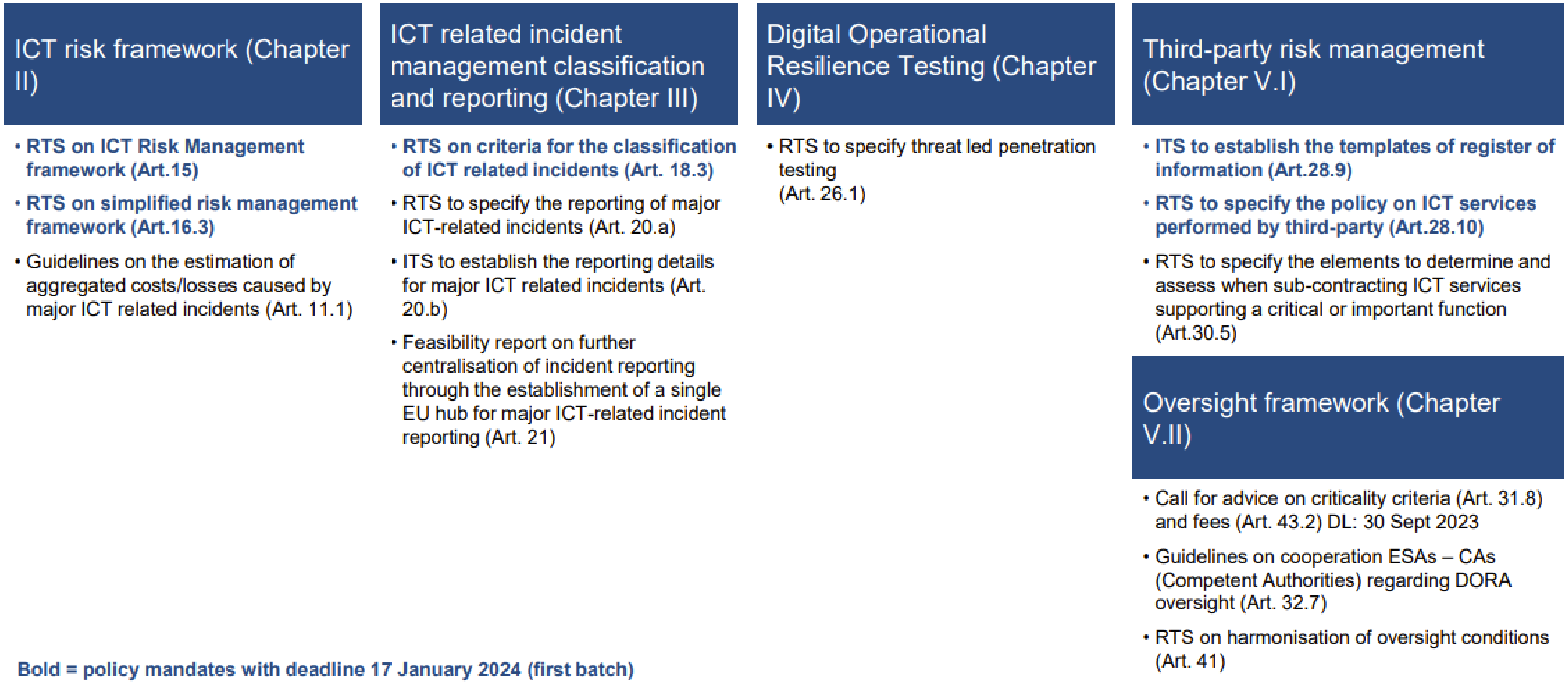
Background and regulatory framework

Why DORA?

- Reform following the **2008 financial crisis** mainly aimed at strengthening financial resilience of financial sector
- DORA creates **regulatory framework** for digital operational resilience
- Response to increasing **digitalisation** - high dependency on ICT service providers for provision of financial services
  - insurance intermediaries offering services oline operating with InsurTech
  - digital insurance underwriting
- DORA Timeline:
  - **Entered into force** on **17 January 2023**
  - **Applicable** from **17 January 2025**
    - 24 months implementation period provided
  - Possibly further guidance from ESAs and competent supervisory authorities such as FMA/ECB

Timeline DORA:
Overview of the RTS and ITS

- On 19 June 2023, ESA published first batch of drafts for RTS and ITS.
- On 8 December 2024, ESAs published the **second** batch of drafts for RTS and ITS.



ICT risk framework (Chapter II)

- **RTS on ICT Risk Management framework (Art.15)**
- **RTS on simplified risk management framework (Art.16.3)**
- Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1)

ICT related incident management classification and reporting (Chapter III)

- **RTS on criteria for the classification of ICT related incidents (Art. 18.3)**
- RTS to specify the reporting of major ICT-related incidents (Art. 20.a)
- ITS to establish the reporting details for major ICT related incidents (Art. 20.b)
- Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21)

Digital Operational Resilience Testing (Chapter IV)

- RTS to specify threat led penetration testing
(Art. 26.1)

Third-party risk management (Chapter V.I)

- **ITS to establish the templates of register of information (Art.28.9)**
- **RTS to specify the policy on ICT services performed by third-party (Art.28.10)**
- RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5)

Oversight framework (Chapter V.II)

- Call for advice on criticality criteria (Art. 31.8) and fees (Art. 43.2) DL: 30 Sept 2023
- Guidelines on cooperation ESAs – CAs (Competent Authorities) regarding DORA oversight (Art. 32.7)
- RTS on harmonisation of oversight conditions (Art. 41)

Bold = policy mandates with deadline 17 January 2024 (first batch)

Supervisory focus: Digital change

- The FMA's supervisory and audit priorities for 2024 and **preparatory work** for DORA:
    - FMA-internal competence centre for consistent cross-sector application of European regulations
    - Identification of critical ICT service providers
    - Further digitalisation of FMA: database for consumer complaints/ enquiries; Use of AI to analyse fund sector and capital market
    - Set up of organisational and technical requirements for incident reporting
    - Further development of test programmes
    - **FMA Cyber Security Toolbox** including **(i)** Cyber Maturity Level Assessment (measurement and evaluation of cyber resilience); **(ii)** Cloud Maturity Level Assessment (for insurance companies and pension funds for usage of cloud); **(iii)** Blackout Assessment; **(iv)** Assessment of mitigation measures for cyberattack scenarios selected by FMA; **(v)** Cyber Exercise: Simulation of a cyber attack in real time

Interaction with EU/national legal acts

- Ministerial draft of the **Austrian DORA Enforcement Act**
- DORA is lex specialis to **NIS II Directive** (EU) 2022/2555 for financial entities

The following European legal acts remain applicable alongside DORA:

- **Solvency II** (Directive 2009/138/EG)
- **Delegated Regulation (EU) 2015/35** supplementing Solvency II including risk management provisions and provisions on outsourcing
- **EIOPA** guidelines on outsourcing to **cloud providers** (EIOPA-BoS-20-002)
  - For insurance and reinsurance companies
  - Comprehensive requirements for outsourcing to cloud providers, such as embedding an governance, outsourcing strategy, due diligence audits, access and audit rights, data protection and binding contractual provisions, etc
- **EIOPA** Guidelines on security and governance in the area of **information and communication technology** (EIOPA-BoS-20/600)
  - For insurance and reinsurance companies
  - information on the management of ICT risks: Governance and strategy, information security, ICT operations management, ICT project and change management, testing of BCM plans, etc
- 01/2022 **FMA Guidelines** on Own Risk and Solvency Assessment (**ORSA**) stipulating that the risk management of insurance companies also has to cover ICT and digitalization risks

DORA: Scope of application

Scope of application DORA - Financial entities

20 types of financial entities

- listed in Art 2 lit a-t: e.g., insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries; credit institutions, etc
- Only very **few exceptions** (see following examples):
  - Auditors (evaluation in the next 3 years)
  - **Insurance intermediaries**, reinsurance intermediaries and ancillary insurance intermediaries qualifying as microenterprises or as small or medium-sized enterprises
  - **Insurance** and reinsurance undertakings as referred to in Art 4 Solvency II (exclusion due to size);
- Grades of financial entities:
  - **Micro-enterprises:** fewer than 10 employees and less than EUR 2 million annual turnover or balance sheet total,
  - **Small businesses**: 10 or more, but less than 50 employees and annual turnover or balance sheet total between EUR 2 and 10 million,
  - **Medium-sized companies**: fewer than 250 employees and annual turnover or balance sheet total below EUR 43 million

DORA Group application

Scope of DORA for financial groups (as defined by Accounting Directive)

- **Individual level**: Each financial entity bears full responsibility for compliance with its obligations under DORA at all times (see recital 64).
- **Group level**:
  - No group privilege (*Konzernprivileg*)
  - Intra-group provision of ICT services is subject to DORA (the control aspect may minimise risk) (recital 31)
  - ICT risks are monitored at individual and group level (recital 64)
  - Art 6 para 9 DORA: holistic strategy for the use of multiple ICT providers at group and entity level
  - Art 28 DORA: The management of ICT third party risk must take into account the potential impact on the continuity and availability of financial services and activities at individual and group level
  - Maintenance of an information register at entity and consolidated level

ICT third-party service providers

- **ICT third-party service provider** = a company that provides ICT services
- **Critical ICT third-party service providers** = ICT third-party service providers that have been categorised as critical (Art 31)
  - Survey of critical ICT third-party service providers at national and European level
  - Voluntary notification for such categorisation
  - delegated acts containing the criteria for categorisation
  - General criteria: systemic importance of the financial entities for which the ICT third-party service provider is active; degree of substitutability of the ICT third-party service provider; systemic impact in the event of failure of the ICT third-party service provider
  - Direct supervision by lead ESA
  - when located in third country: establishment of subsidiary in EU

Critical or important functions

- ICT services might serve "***critical or important functions***" of a financial entity
  - comparable to "*critical or important function*" as defined by Delegated Regulation 2015/35 (Art 274) and EIOPA guidelines on (cloud) outsourcing
  - it needs to be assessed if the disruption of this function
    - would materially impair the financial performance of a financial entity, or soundness or continuity of its services and activities, or
    - the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law

ICT services

- **ICT services** are

  (i) digital services and data services,

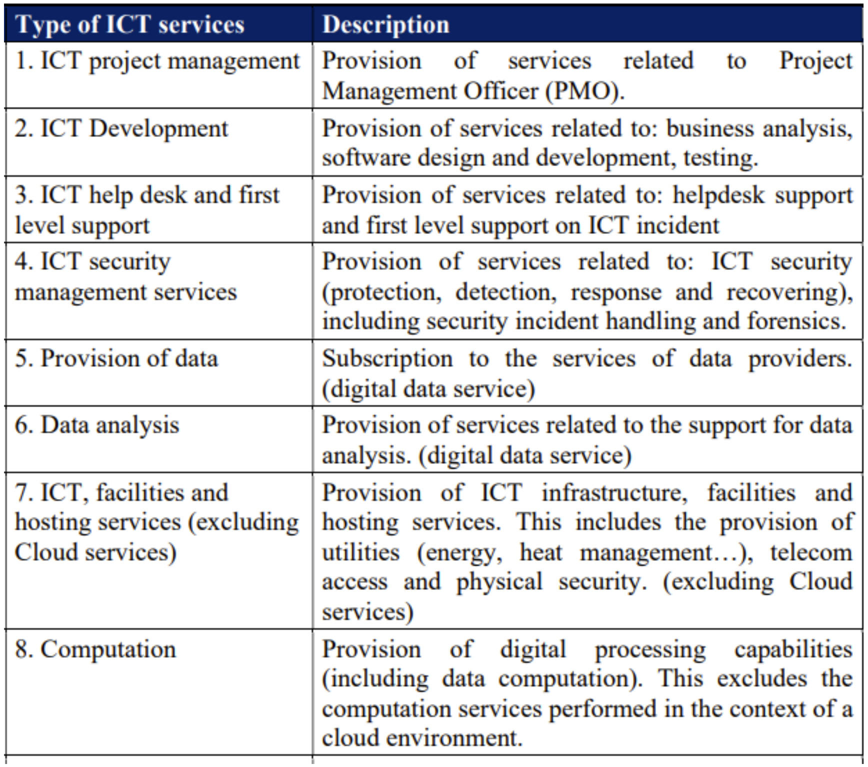
  (ii) provided through ICT systems to one or more internal or external users

  (iii) on an ongoing basis,

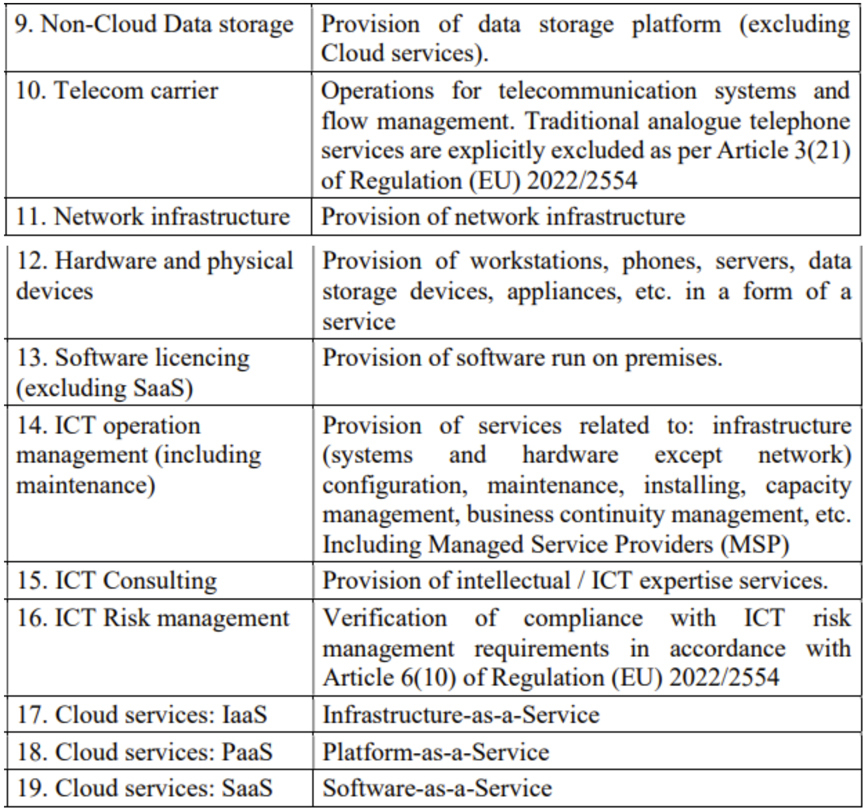
  (iv) including hardware as a service and hardware services, which also includes the provision of technical support via software or firmware updates by the hardware provider
- In conjunction with Art 28 para 1 lit a DORA (general principles), the ICT services must be related to the performance of the financial enitiy's business activities
- ICT services also include providers of *hardware as a service* and hardware services (including technical support through software and firmware updates)
- Traditional analogue telephone services are **excluded:** Public Switched Telephone Network (PSTN) services, landline services, Plain Old Telephone Service (POTS) or landline telephone services
- The categories of ICT services in the Final Report on ITS of the ESA on the Information Register, JC 2023 85 of 10 January 2024 (in particular Annex III) serve as a guide.

ICT Services - Categories

The ESA draft ITS for the template for the information register (Annex IV):



Type of ICT services	Description
1. ICT project management	Provision of services related to Project Management Officer (PMO).
2. ICT Development	Provision of services related to: business analysis, software design and development, testing.
3. ICT help desk and first level support	Provision of services related to: helpdesk support and first level support on ICT incident
4. ICT security management services	Provision of services related to: ICT security (protection, detection, response and recovering), including security incident handling and forensics.
5. Provision of data	Subscription to the services of data providers. (digital data service)
6. Data analysis	Provision of services related to the support for data analysis. (digital data service)
7. ICT, facilities and hosting services (excluding Cloud services)	Provision of ICT infrastructure, facilities and hosting services. This includes the provision of utilities (energy, heat management…), telecom access and physical security. (excluding Cloud services)
8. Computation	Provision of digital processing capabilities (including data computation). This excludes the computation services performed in the context of a cloud environment.



9. Non-Cloud Data storage	Provision of data storage platform (excluding Cloud services).
10. Telecom carrier	Operations for telecommunication systems and flow management. Traditional analogue telephone services are explicitly excluded as per Article 3(21) of Regulation (EU) 2022/2554
11. Network infrastructure	Provision of network infrastructure
12. Hardware and physical devices	Provision of workstations, phones, servers, data storage devices, appliances, etc. in a form of a service
13. Software licencing (excluding SaaS)	Provision of software run on premises.
14. ICT operation management (including maintenance)	Provision of services related to: infrastructure (systems and hardware except network) configuration, maintenance, installing, capacity management, business continuity management, etc. Including Managed Service Providers (MSP)
15. ICT Consulting	Provision of intellectual / ICT expertise services.
16. ICT Risk management	Verification of compliance with ICT risk management requirements in accordance with Article 6(10) of Regulation (EU) 2022/2554
17. Cloud services: IaaS	Infrastructure-as-a-Service
18. Cloud services: PaaS	Platform-as-a-Service
19. Cloud services: SaaS	Software-as-a-Service

No ICT services

There are following exceptions (if one is fulfilled, no ICT service):

- the service **does not provide digital services** and/or data services via ICT systems (including hardware services); or
- the service is purchased **once** (i.e. not recurring and not on an ongoing basis); or
- the service is **not** provided in connection with a **business activity** of the financial undertaking; or
- the service is a conventional analogue **telephone service** (e.g. landline services, conventional telephone services or landline telephone service).
- Examples:
  - Digital central heating (not including heating of server room);
  - Facility management (classic: cleaning, building management, building protection)

Governance & ICT risk management

DORA content

Governance & ICT risk management

- Responsibility of the management body
- Internal risk management with focus on ICT risks
- Monitoring of risks in connection with ICT third-party service providers
- Clear requirements for contractual agreements

Digital resilience

- General requirement to test (test intervals, test objects, etc.)
- Internal procedures and guidelines for testing
- Requirement to use of TLPT (Threat-Led Penetration Testing)

Reporting and exchange of information

- Reporting of ICT incidents
- Voluntary reporting of significant cyber threats
- Exchange of information on cyber threats between financial entities
- Documentation and reporting according to defined standards

ICT risk management framework

ICT risk management framework:

- Strategies for digital operational resilience;
- Guidelines and policies on availability, authenticity, integrity and confidentiality of data; and
- Procedures and ICT protocols and tools to ensure network security; appropriate security controls, access controls, monitoring systems
- Frequency of reviews:
  - at least annually, and
  - in the event of serious ICT-related incidents
  - in accordance with supervisory instructions or findings resulting from operational resilience tests or audits
  - regular internal audit review
- Responsibility for the implementation and management of ICT risks islies with **management**
- Regular **trainings** of staff and management required

Strategy for digital operational resilience

- As part of ICT risk management, a **strategy for digital operational resilience must be** developed, setting out how the ICT risk management framework will be implemented (including methods to address ICT risks and achieve specific ICT objectives)
- Art 6 para 8 DORA specifies the **content of the strategy**
  - Definition of the risk tolerance threshold for ICT risks and targets for information security,
  - Mechanisms for recognising ICT-related incidents,
  - the current status of digital operational resilience based on the number of reported serious ICT incidents, and
  - Demonstration of the effectiveness of preventive measures
- ICT strategy **goes further** than previous standards. It has to be established as an independent strategy or possibly as a sub-strategy to the general IT strategy
- Effectiveness of the implementation of the strategy must be **monitored on an ongoing basis**

Risk management of ICT third-party service providers

- Responsibility always lies with the **financial entity**
- **Pre-evaluation** of the ICT third-party service provider:
  - Suitability of the ICT third-party service provider
  - Fulfilment of the regulatory conditions for awarding contracts
  - Identification of all relevant risks and potential conflicts of interest
- Ongoing proactive control and monitoring
- Detailed internal overall **risk assessment**
- contractual agreements with ICT third-party service providers that comply with **appropriate** information security standards, only
- Stricter regulations for ICT services for critical or important functions
- **RTS/delegated regulation** on detailed content for a **guideline in** relation to contractual agreements with critical ICT services (published on 13 March 2024):
  - Governance requirements when using ICT services for critical/important functs;
  - Detailed requirements for ex-ante risk assessment and scope of due diligence of critical ICT service providers;

DORA-Compliance: Contracts

Before concluding contracts with ICT third-party service providers

Before concluding contracts with ICT third-party service providers, financial entities must (see Art 28 para 4 DORA):

a) Assess whether **critical or important function** are in scope;

b) Assess if **regulatory conditions** are met;

c) Identification and assessment of all relevant **risks** associated with the contractual arrangement, including the possibility that the contractual arrangement may contribute to increasing the ICT concentration risk;

d) fulfil due diligence on potential third-party ICT service providers and ensure that he is **suitable**;

e) Identification and assessment of conflicts of interest that may arise from the contractual agreement.

Contracts in the light of DORA (1)

- Clear requirements for contractual agreements (if there are **no** critical or important functions):
  - **written** document and complete description of services (incl. regulation on the admissibility of subcontracting; see also no 37 lit a, e EIOPA GL); dynamic references to websites of IT providers or other merely referenced documents being not attached to the contract are no longer permitted
  - Place of **service provision** and **data storage;** obligation of ICT third-party service provider to notify intended changes in advance (no 37 lit f EIOPA GL)
  - Regulations on **data protection** (no 37 lit g EIOPA GL)
  - Access to data in the event of **insolvency** or similar circumstances (no 37 lit n EIOPA GL)
  - Descriptions of the service level **agreement** (**SLA**) including updates and revisions (no 37 lit i EIOPA GL)

Contracts in the light of DORA (2)

- Clear requirements for contractual agreements (if there are **no** critical or important functions):
  - Mandatory support in the event of an **ICT incident** (without additional costs or predetermined costs)
  - Cooperation with the **authorities** (supervisory and resolution authorities; see no 37 lit m EIOPA GL)
  - **Termination rights** and related minimum notice periods in accordance with the expectations of the competent authorities (unclear which expectations – so far no guidance from the supervisory authorities; see no 37 lit b EIOPA GL); for list of termination rights see Art 28 para 7 DORA
  - Conditions for participation in internal **trainings** of financial entities by employees of the ICT third-party service provider

Contracts in the light of DORA (3)

- Additional contractual requirements for the support of **critical** or **important functions:**
  - Detailed description of the service level agreement (SLA, see no 37 lit i EIOPA GL)
  - Notice periods and reporting obligations (e.g., notification of developments affecting the service provider's performance; see no 37 lit b, j EIOPA GL)
  - ICT third-party service provider must implement and test emergency plans (see no 37 lit l EIOPA GL)
  - Collaboration and participation in threat-based penetration tests (**TLPT**) of the financial entity
  - Exit scenarios and binding transition periods (see also Art 28 para 8 DORA)

Contracts in the light of DORA (4)

- Additional contractual requirements for support of **critical** or **important functions:**
  - Comprehensive **monitoring rights** of the financial undertaking (no 37 lit h and m EIOPA GL):
    - **unrestricted** rights of access, inspection and audit by the financial entity or appointed third party, and by competent authority. Right to take copies of relevant documentation on-site if they critical to the operations of ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;
    - the right to agree on **alternative assurance levels** if other clients' rights are affected;
    - the obligation of the ICT third-party service provider to **fully cooperate** during the onsite inspections and audits performed by competent authorities, Lead Overseer, financial entity or an appointed third party; and
    - the obligation to provide details on the scope, procedures to be followed and frequency of such **inspections** and audits

Other contractual components – EIOPA guidelines

- The following requirements for outsourcing of critical or important functions of **EIOPA** guidelines on cloud outsourcing **go beyond** DORA:
  - the date on which agreement begins and, if applicable, ends (lit b);
  - the court jurisdiction and the governing law of the agreement (lit c);
  - the parties' financial obligations (lit d);
  - Information on whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested (lit k)

To Dos regarding contracts

We recommend following **first To Dos**:

1. Creation of a complete **list** of existing contracts (ATTENTION: DORA also applies to old contracts!)
2. **Identification** of which contracts actually fall under DORA
3. **Check** whether
   1. do contracts also include critical or important functions?
   2. ICT third-party service providers based in a third country are involved?
   3. there are also critical ICT third-party service providers among the contractual partners?
4. **Gap analysis** of current contracts for conformity with DORA (in particular Art 30 - essential contractual provisions)
5. **Implementation** and adaptation of contracts

New contracts currently being concluded should already contain new DORA requirements

Information register

- All contracts for ICT services must be recorded in an **information register** (on individual and consolidated level)
- The information register must be **kept up to date** (incl. audit trail)
- Information may be removed from information register at the earliest 5 years after termination of contract
- **Annual** report to the competent supervisory authority on the number and type of new ICT contracts and type of ICT service
- The competent supervisory authority must be informed **promptly** of any **planned contractual agreement** on use of ICT services to support critical or important functions and in the event that a function has become critical or important.
- The ESAs have published draft ITS for **standard templates** for the information register

Digital operational resilience & Reporting

Digital operational resilience

- Digital operational resilience (ability to establish, maintain and verify its **operational integrity** and **reliability** through and despite use of ICT services), has to be ensured primarily by following measures:
  - Continuous planning and execution of tests
  - Physical safety checks, interviews, questionnaires
  - Several levels: Management systems, processes, technical implementation
  - Vulnerability management process
- In order to identify weaknesses, deficiencies and and to implement corrective measures immediately, financial entities (except micro-enterprises) must define **test programmes as** part of ICT risk management
- This programme should include a range of assessments, tests, methods, procedures and tools
- A **risk-based approach must be** applied
- financial entities need procedures and guidelines to prioritise, classify and resolve issues that have arisen during testing

Testing

- financial entities (other than micro-enterprises) shall ensure that appropriate testing is carried out at least **annually** on all ICT systems and applications that support **critical** or **important functions.**

Basic Testing	For all financial entities

- The following test procedures can be used for testing ICT tools and systems:
  - Vulnerability assessment and scans,
  - Open source analyses, network security assessments,
  - Gap analyses, physical security checks,
  - Questionnaires and scans of software solutions, source code checks where feasible,
  - Scenario-based tests, compatibility tests, performance tests, end-to-end tests and penetration tests

Extended tests	for financial entities selected by national authorities

- Tests at least **every 3 years** (frequency can be adjusted by the national supervisory authority depending on the risk profile of the financial entity)
- Testing must be carried out by independent, **internal** or **external** partners (significant credit institutions can only use external testers); **pooled tests**

Reporting and information exchange

- Introduction and implementation of a management process for monitoring and logging ICT-related incidents
- Types of incidents (among others):
  - **ICT-related incident:** Unplanned event compromising security of ICT systems that has detrimental impact on availability, authenticity, integrity or confidentiality of data or on services provided by financial organisation
  - Other types such as payment-related opertational incident, cyberattack, cyber threat
- **Voluntary exchange of information** on cyber threats between financial entities
- RTS/Delegated Regulation in relation to the **reporting** of ICT incidents (reporting thresholds, criteria for categorising incidents):
  - Number of customers (10%, at least 100,000), financial counterparties (30%) and transactions affected (10% of the daily average transaction volume)
  - Reputational impact: the financial entity must answer yes/no questions from the RTS/Delegated Regulation (e.g. the incident was covered in the media)
  - Geographical scope: significant impact on two or more jurisdictions
  - Data loss: various criteria such as data becoming unusable, unauthorised access to data, altered data, impact on the trustworthiness of the data

Contact us

Dr Axel Anderl, LL.M.

Managing Partner

IT/IP, Data Protection

axel.anderl@dorda.at

+43 1 533 47 95 - 23

Mag Nino Tlapak, LL.M.

Partner

IT-, Data Protection and Cybersecurity

nino.tlapak@dorda.at

+43 1 533 47 95 – 23

The Legal 500 (2024)
Axel Anderl (TMT)
Hall of Fame

The Legal 500 (2024)
TMT
Tier 1

The Legal 500 (2024)
Data Privacy & Data Protection
Tier 1

Trend Anwaltsranking (2024)
Axel Anderl
Data Protection , IP and Media
Top 1 overall ranking

DORDA

Managing IP (2024)
Austrian Copyright Firm of the Year

Austria Firm of the Year

Talent Management – Firm of the Year

Women in Business Law Awards Europe 2023

equalitA
DAS GÜTESIEGEL FÜR INNERBETRIEBLICHE FRAUENFÖRDERUNG

Client Choice winner
IT & Internet

Client Choice Awards 2024

Who`s Who Legal (2024)
Axel Anderl (Data Privacy & Protection)
Thought Leader Global Elite

Chambers Europe (2024)
TMT:IT
Band 1

DORDA

We deliver clarity.