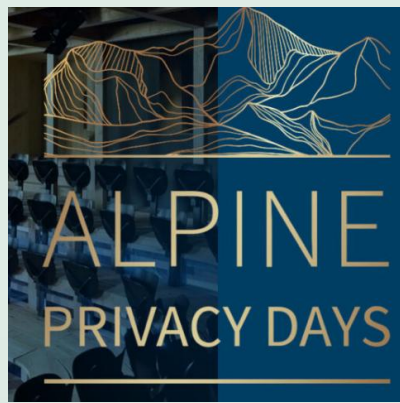




D O R D A

DORA, NIS & Cyberresilience

3 March 2025

Albin Buchmann / Nino Tlapak



Head of Legal, Erste Digital GmbH

Albin is the Head of Legal at Erste Digital, the central IT provider for Erste Group.

Erste Digital delivers innovative IT solutions to Erste Group banks across Austria and the CEE region.

With extensive experience in negotiating complex IT contracts, Albin specializes in Outsourcing, Cloud, and Data Protection.

Albin is a member of "it-law.at".

Albin Buchmann

albin.buchmann@erstegroup.com



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 2022-2025
- 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; APD etc)
- Member of "*it-law.at*" and "*Privacyofficers.at*"

Nino Tlapak

nino.tlapak@dorda.at

Agenda

1. General

- Background and regulatory framework in the EU
- Scope of application – DORA, NIS2

2. Practical insights on Cyberresilience in contract design

- Regulatory requirements
- Hot topics in contract design & negotiations

Background and regulatory framework

Why DORA, NIS2 etc?

- increase of cyberthreats and successful attacks
- DORA creates **regulatory framework** for digital operational resilience for the financial sector
- NIS2 broadens the scope of NIS to ensure network and information security (not only) as regards critical infrastructure
- response to increasing **digitalisation** - high dependency on ICT service providers
- timeline:
 - **DORA applicable since 17 January 2025**
 - **NIS2 applicable since 17 October 2024**
 - still not incorporated by all EU Member States

Interaction with EU / national legal acts

- National **DORA Enforcement Acts**
- DORA is lex specialis to **NIS II Directive** (EU) 2022/2555 for financial entities
- **Solvency II** (Directive 2009/138/EG)
- **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
- **EBA** Guidelines on outsourcing arrangements (EBA/GL/2019/02)
 - for financial institutions
 - even more comprehensive requirements on outsourcing contracts

DORA: Scope of application

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)
 - 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 entity's business activities
- ICT services also include providers of *hardware as a service* and hardware services (including technical support through software and firmware updates)
- Classic analogue telephone services are **excluded**: Public Switched Telephone Network (PSTN) services, landline services, Plain Old Telephone Service (POTS) or landline telephone services

Changes to the contractual landscape

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
 - dynamic references to websites of IT providers or other merely referenced documents are no longer permitted
 - place of **service provision** and **data storage**
 - obligation of ICT third-party service provider to notify intended changes in advance
 - provisions on **data protection**
 - access to data in the event of **insolvency** or similar circumstances
 - descriptions of the service level **agreement (SLA)**
 - including updates and revisions

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**
 - **termination rights** and related minimum notice periods in accordance with the expectations of the competent authorities
 - 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
 - notice periods and reporting obligations
 - notification of developments affecting the service provider's performance
 - ICT third-party service provider must implement and test emergency plans
 - collaboration and participation in threat-based penetration tests (**TLPT**) of the financial entity
 - exit scenarios and binding transition periods (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
 - **unrestricted** rights of access, inspection and audit by the financial entity, appointed third party and competent authority
 - **right to take copies** of relevant documentation on-site
 - the effective exercise is not limited by other contractual arrangements or 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 audit;
 - the obligation to provide details on the scope, procedures to be followed and frequency of such **inspections** and audits

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
 - i. do contracts also include critical or important functions?
 - ii. ICT third-party service providers based in a third country are involved?
 - iii. 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

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

THANK YOU FOR YOUR ATTENTION

D O R D A

Mag Nino Tlapak, LL.M.

T: +43 1 533 47 95 – 23

nino.tlapak@dorda.at



ERSTE Digital

Mag Albin Buchmann, LL.M.

T: +43 50 100 14511

albin.buchmann@erstegroup.com

Client Choice Award Lexology 2022-2025: Blockchain

TIER 1 Legal500 2007-2024: TMT

TIER 1 Legal500 2020-2024: Data Privacy & Data Protection

TIER 1 Legal500 2021-2024: Intellectual Property

BAND 1 Chambers Europe 2008-2024: TMT:IT

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at

The background of the image is a bright, modern office space. It features large floor-to-ceiling windows that offer a panoramic view of a city with historic architecture, including domes and classical buildings. In the foreground, there is a white, minimalist sofa and a low, rectangular glass coffee table. The overall atmosphere is clean, bright, and professional.

DORDA

We deliver clarity.