20. OSE Symposium am 31.01.2025 in München

Stephan Peters & Christian Weitzel

Deposix Software Escrow GmbH, München – www.deposix.de

DORA meets Escrow

Digitale Resilienz im Praxistest

DORA – hat das Boot nicht längst abgelegt?!

Worum ging es da noch gleich?

Neue gesetzliche Vorgabe der EU [Regulation (EU) 2022/2554]

- **Ziel:** Stärkung (Erhöhung Resilienz!) der IT-Sicherheit von Finanzinstituten in der EU
- Verordnung, unmittelbar geltend in allen EU-Staaten
- Betrifft direkt alle **3.600 Unternehmen im Finanzsektor** (D)
  - In der EU mehr als 20.000 Finanzunternehmen
  - Und indirekt über **10.000 IT-Dienstleister** allein in D (inklusive SUBs)
- **Vorbereitungsfrist** ist **abgelaufen**
  - Seit 17.1.2023 sollte sich jedes Finanzunternehmen auf die Umsetzung der DORA-Vorgaben vorbereiten
  - Ab 17.1.2025 müss(t)en alle Vorgaben implementiert sein
- **Fazit: Ist DORA also schon passé?**

Deposix digital escrow

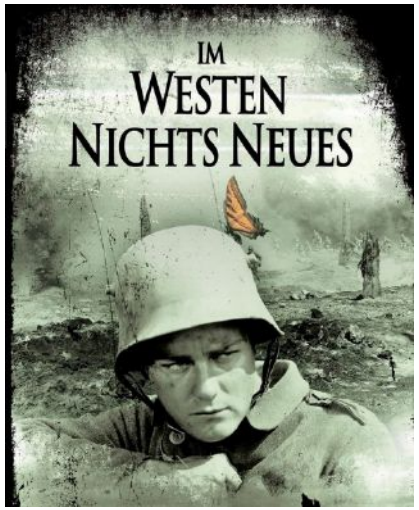
Jetzt schon passé?
Ein alter Hut also …?

Deposix
digital escrow

DORA – ist der Sturm längst vorbei?

Der Plan:

- Zwei Jahre gesetzliche Vorbereitungsfrist sollten ausreichen
- Verordnung ist am 17.1.2025 anwendbar geworden
- Nur Frist zur Einreichung des IKT-Informationsregisters bei der BaFin(1) verschoben auf 11. April
- Da kann es doch nichts Neues geben …



(1) BaFin = Bundesanstalt für Finanzdienstleistungsaufsicht

Deposix digital escrow

Kennen Sie diesen Herrn?

Grigori Alexandrowitsch Potjomkin
Feldmarschall und Liebhaber der Kaiserin Katharina der Großen

Laut Legenden Organisator der Potjomkinschen Dörfer, um blühende Landschaften vorzutäuschen

Deposix
digital escrow

Plan und Realität …

- Ernsthafter Beginn der Vorbereitung vielfach erst ab November
- Zum 17.1.2025 in großer Hast die wichtigsten Leitlinien erstellt und veröffentlicht (viel Papier, Potemkin‘sche Dörfer in den Finanzunternehmen)
- Implementierung des „Paperwork“ beginnt gerade
- IKT-Lieferanten werden erst jetzt richtig zur Verhandlung aufgefordert

=> Pulverrauch noch nicht entschwunden, die Schießerei beginnt erst

(1) BaFin = Bundesanstalt für Finanzdienstleistungsaufsicht

Deposix digital escrow

DORA – die stürmischen Zeiten stehen erst bevor

Überraschende Erkenntnisse (1/3)

Bei der Umsetzung in die Praxis

Neue Querschnittsfunktionen und mehr Personal benötigt:

- Unabhängige Kontrollfunktion – eigenständige Funktion aufgrund der **drei Verteidigungslinien**
- Einkauf, Risiko-Management und unabhängige Kontrollfunktion brauchen für die **vielen neuen Aufgaben** mehr Personal

  → Kann 5 bis 10 % Personalaufstockung in mittelgroßen Unternehmen erfordern

Liebgewonnene Bequemlichkeit muss aufgegeben werden:

- Corporate Risk Officer (CRO) kann nicht länger überwachen und Leitlinien setzen
  → muss seine Organisation in **operatives Risiko-Management** einbinden
- **Abläufe** bei rasch benötigter IT-Beschaffung viel **aufwendiger und langwieriger**

Deposix
digital escrow

Schlimmer geht immer!

Deposix
digital escrow

Überraschende Erkenntnisse (2/3)

Bei der Umsetzung in die Praxis

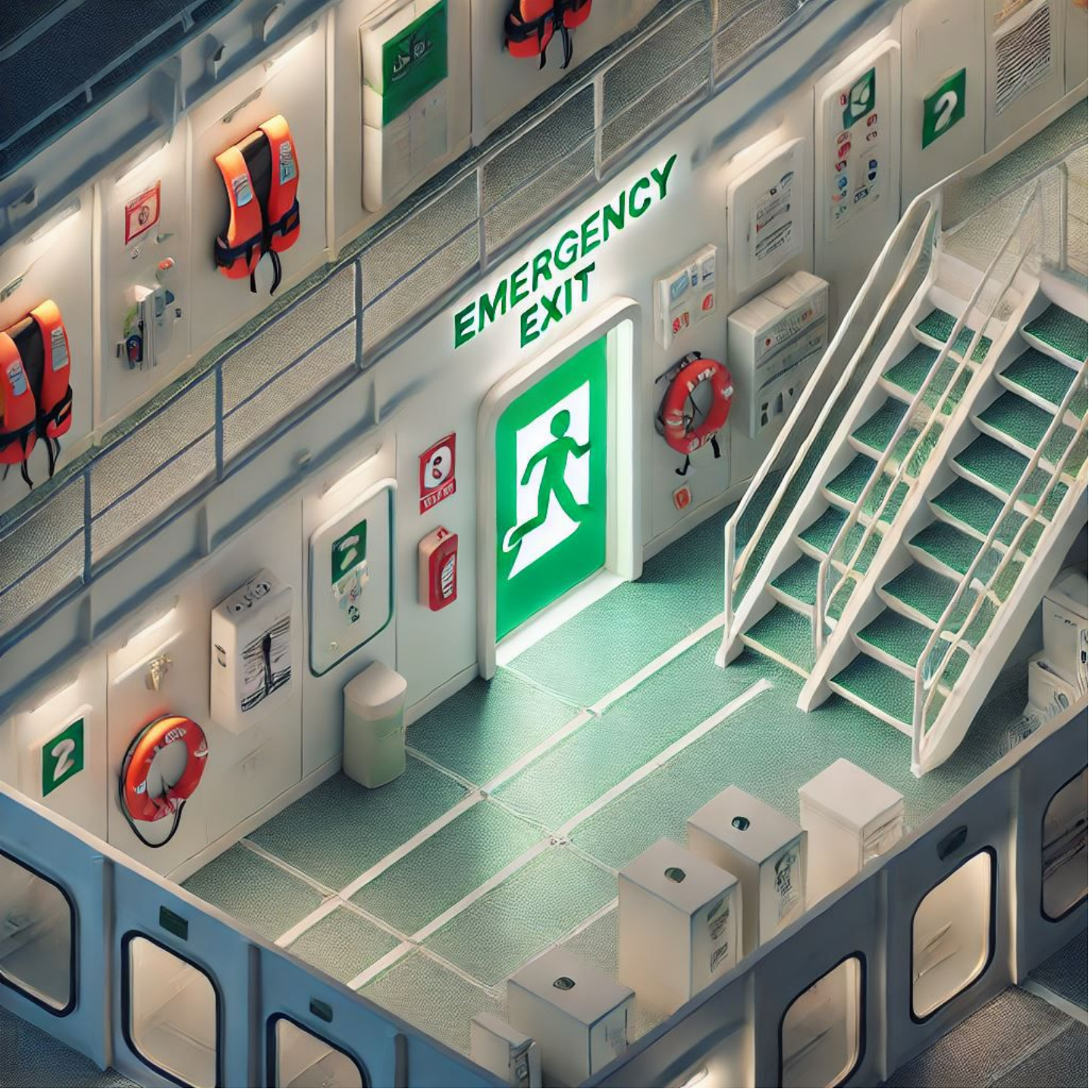
Lang vertraute Kompetenzordnungen werden komplett über den Haufen geworfen:

- **Risiko-Manager** braucht ein **Veto-Recht** gegenüber Einkauf und Fachbereich
- **Unabhängige Kontrollfunktion** braucht ein **höherrangiges Veto-Recht**
  => „Ja wie, der Fachbereich darf nicht entscheiden, wo er einkauft?!? Der Vorstand auch nicht?“

Datenflut beim IKT-Informationsregister:

- Unnütze Dry Run Exercise der EU (07-08/24), weil wirklich nur Trockenlauf mit wenigen Einträgen
- Bei vielen CIFs, TGs und Zweigstellen bis zu **vierstellige Zahl** an Funktionskennungen
- Bei großen Finanzinstituten **hunderttausende bis Millionen Zeilen** im Register
- Excel hoffnungslos überfordert, manche DORA-Tools auch
- Bei vielen Instituten noch nicht live getestet

Deposix
digital escrow



Und das richtig dicke Ende …

Deposix
digital escrow

Überraschende Erkenntnisse (3/3)

Bei der Umsetzung in die Praxis

Das dicke Ende kommt erst noch:

- Was schreibt man in den Notfallplan und die Ausstiegs-Strategie für AWS oder SAP?
- Wen benennt man als ernsthafte Alternative beim Ausfall von SAP oder Microsoft?

Schon jetzt ist klar: Umsetzung bei weitem komplexer und teurer als bei der DSGVO von 2016

- Die hatte auch zwei Jahre Vorbereitungsfrist bis zur Anwendbarkeit ab 2018
- Da waren die Firmen engagiert bei der Sache

Was befürchten
die Dienstleister?

Befürchtungen der IKT-Dienstleister

Oft berechtigt!

- Finanzinstitute werden im Windschatten zwingender DORA-Änderungen weitreichende oder inakzeptable Änderungen der Verträge „durchdrücken“. Beispiele aus DORA-Vertragsnachträgen:
  - Fristlose Kündigung mit einer „*Ausübungsfrist von mindestens drei Monaten*“
  - Pflicht zur Teilnahme an Resilienz-Schulungen auf eigene Kosten, wenn der Auftraggeber dies meint
- Rasche Ausstiegsmöglichkeit dank zwingender neuer Kündigungsklauseln
  - Wie bekommen wir das durch die Subunternehmer-Kette durchgereicht?
  - Wie können wir ein US-Unternehmen zur Anpassung laufender Verträge bewegen?
- Was bedeutet die Pflicht zur Aufnahme einer Aktualisierungsklausel in SLA?
  - Beispiel: „Die Parteien erörtern einmal pro Jahr, ob und inwiefern die Dienstleistungsgüte an aktuelle Bedarfe angepasst werden kann.“
  - Was ist, wenn der Dienstleister das nicht will oder kann?
  - Was ist mit der Vergütung?

Und was kommt nun?

Deposix
digital escrow

Prognose

Zu den mittelfristigen Auswirkungen von DORA

- Erhebliche **Umschichtungen** bei den IKT-Anbietern
- Hohe **Zusatzinvestitionen** mit steigenden Kosten in der Zulieferkette
  z.B. zweites Rechenzentrum für Hosting und SaaS-Anbieter
- **Kürzere** Vertragslaufzeiten
- **Weniger Rabatte** für Langfrist-Verträge
- ...

Deposix
digital escrow

Deposix
digital escrow

Träume sind Schäume …

Auch wenn es keiner zugeben will!

Excel als DORA-Tool

- In Einzelfällen über Tausend Zeilen im IKT-Register für einen einzelnen Vertrag
- Bei einer Änderung an diesem Vertrag sind Tausende Zeilen zu ändern

Wie wollen BaFIN und ESAs[(1)] mit der **Datenflut** umgehen, die sie anfordern?

- Konsistenzprüfung hat schon im Dry Run versagt und wurde abgeschaltet
- Welches Programm prüft Abermillionen an Datenzeilen auf Konzentrationsrisiken?

Notfallplan (binnen kurzer Zeit) und **Ausstiegsstrategien** für

- Cloud Computing
- Microsoft Office – bei Banken oft mit Kernbankensystem vernetzt
- SAP

[(1)] ESAs = European Supervisory Authorities

DORA meets Escrow – DOORA needs Escrow

Deposix
digital escrow

Herausforderungen in der konkreten Umsetzung

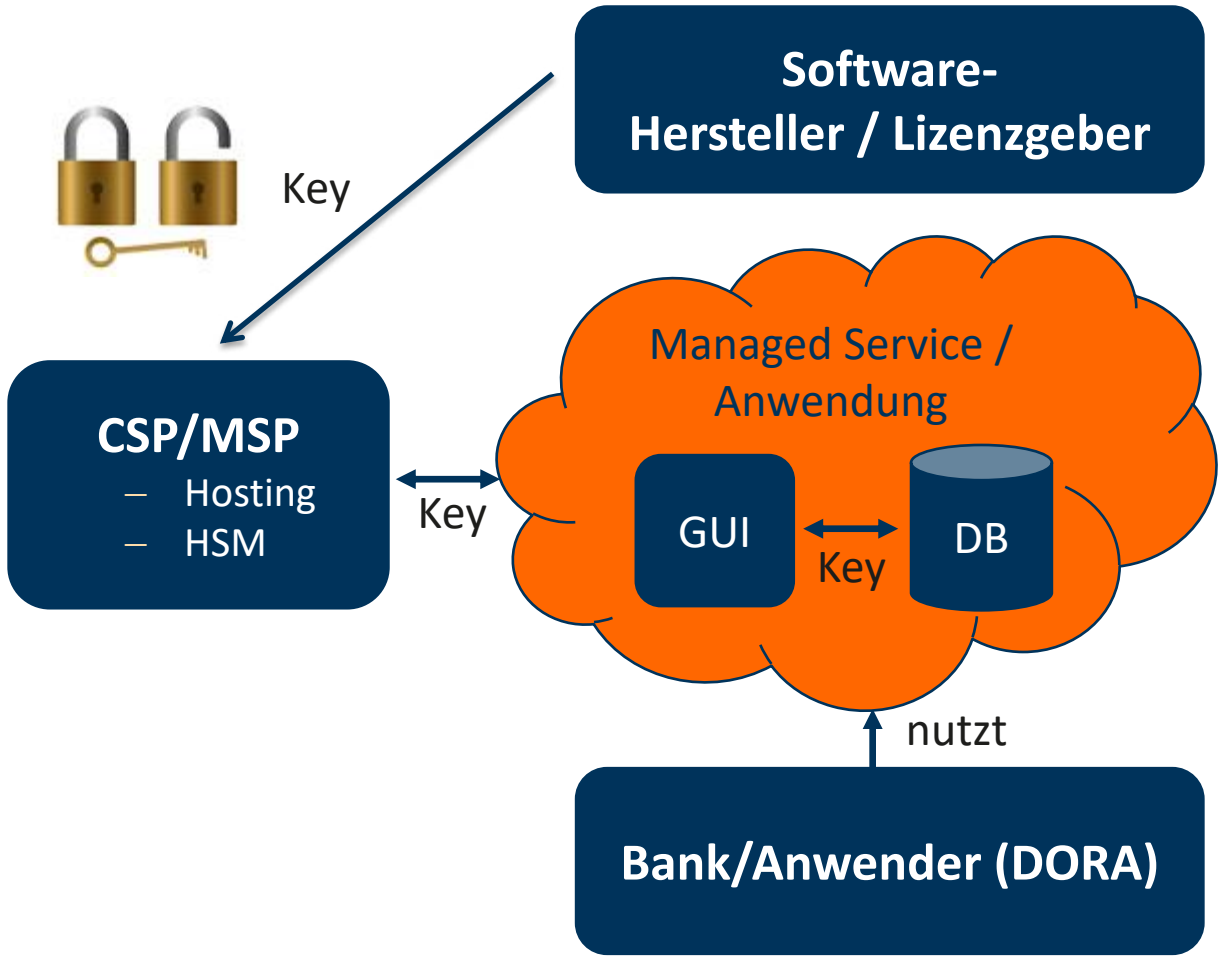
Wo erfordert DORA Escrow?

- Auf den ersten Blick nirgends
  - Im Verordnungstext ist Escrow nicht erwähnt
  - Mittelbar indes schon!

- DORA-Unternehmen müssen die kontinuierliche Funktion **kritischer und wichtiger Software sicherstellen**, *Art. 11 Abs. 2 lit. a) DORA*

- DORA-Unternehmen müssen bei Insolvenz oder Geschäftseinstellung eines Dienstleisters weiter **auf Daten zugreifen** können, *Art. 30 Abs. 2 lit. d) DORA*

Typischer Anwendungsfall: SaaS/Managed Service



© 2024 Deposix

Deposix
digital escrow

Lösungen für die konkrete Umsetzung

Was kann Escrow dennoch für DORA leisten?

- These: DORA ohne Escrow ist nicht möglich!

- DORA-Unternehmen müssen die kontinuierliche Funktion **kritischer und wichtiger Software** sicherstellen, *Art. 11 Abs. 2 lit. a) DORA*
  - **Das geht bei Ausfall des Herstellers nur mit Software Escrow.**
  - **Das geht je nach Verschlüsselung der Daten nur mit Key Escrow.**
  - **Das geht bei Verlust der Daten nur mit Daten Escrow.**

- DORA-Unternehmen müssen bei Insolvenz oder Geschäftseinstellung eines Dienstleisters weiter **auf Daten zugreifen** können, *Art. 30 Abs. 2 lit. d) DORA*
  - **Das geht bei SaaS letztlich nur mit SaaS Escrow.**

Deposix digital escrow

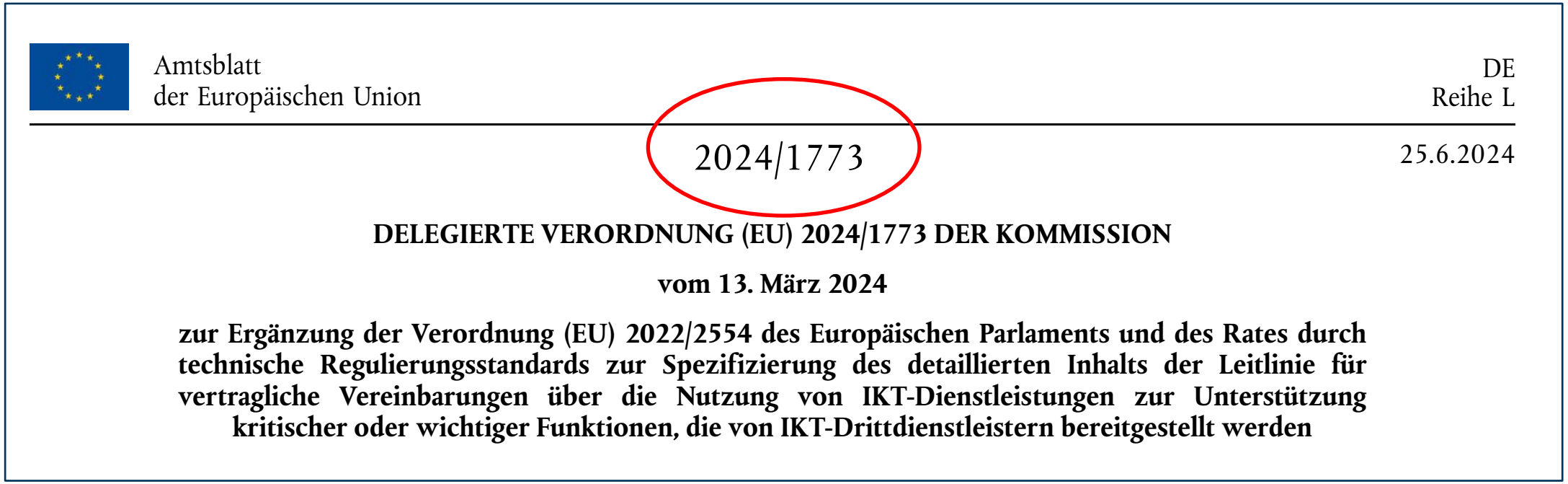
Ein Blick ins Detail…

Von DORA adressierte Risiken	Mitigation erfordert Escrow
Operationelle Risiken	Quellcodeprüfungen nach *Art. 25 Abs. 1 DORA*: • Wenn Hersteller Source Code nicht offenlegt, kann Prüfung nur über ein Escrow erfolgen.
Rechtliche Risiken	Vertragsvereinbarung zur Sicherstellung des Vertragsausstiegs ohne jede Betriebsunterbrechung, *Art. 28 Abs. 8 DORA*: Erfordert bei SaaS ein SaaS Escrow.
IKT-Risiken	Dto.
Reputationsrisiken	Wenn durch Betriebsunterbrechung Reputation gefährdet ist, muss diese mit Escrow verhindert werden.
Ausreichender Schutz vertraulicher oder personenbezogener Daten	Hohe Standards hinsichtlich gespeicherter Daten, *Art. 9 Abs. 2 DORA* • Erfordert bei Speicherung in der Cloud starke Verschlüsselung • Verschlüsselung nach FIPS 140-2 erfordert Speicherung der Schlüssel in HSMs • Technologische Resilienz erfordert dann Hinterlegung der Schlüssel beim Escrow
Unterbrechung der ständigen Verfügbarkeit von Daten	Vertragsvereinbarung zur Sicherstellung des Datenzugangs bei Insolvenz oder sonstigem Ausfall des IKT-Dienstleisters, *Art. 30 Abs. 2 lit. d) DORA*: • Erfordert bei HSM-Cloud-Verschlüsselung ein Key Escrow Technologische Resilienz nach *Art. 7 lit. (d) DORA*: • Lässt sich bei SaaS nur durch SaaS Escrow erzielen Vertragsvereinbarung zur Sicherstellung des Vertragsausstiegs ohne jede Betriebsunterbrechung, *Art. 28 Abs. 8 DORA*: • Erfordert bei SaaS ein SaaS Escrow. Wiederherstellung von IKT-Systemen und Daten mit minimaler Ausfallzeit, *Art. 12 Abs. 1 DORA* • Lässt sich bei SaaS nur durch SaaS Escrow erzielen • Lässt sich bei HSM-Cloud-Verschlüsselung nur mit Key Escrow erzielen

Deposix digital escrow

Wann muss der *Einkauf* zukünftig Escrow vorsehen?

Gesetzliche Vorgaben – unendlich detailliert



Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1773

25.6.2024

DELEGIERTE VERORDNUNG (EU) 2024/1773 DER KOMMISSION

vom 13. März 2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden

Deposix
digital escrow

Der Einkauf muss zukünftig Escrow *ex-ante* vorsehen

Klare Vorgaben für IKT-Einkaufsprozess

Der „Lebenszyklus“ von IKT-Einkaufsprozessen muss wie folgt gegliedert sein:

1. Governance
2. Planung
3. Entscheidungsfindung
4. Implementierung
5. Überwachung und Management
6. Ausstieg und Beendigung

Die Planung (2) erfordert eine ex-ante-Risikobewertung jedes avisierten IKT-Dienstleisters

- Ausfallrisiken mit Risikominderungsmaßnahmen, insbesondere für den Fall der Insolvenz, sind zu dokumentieren – Stichwort „Risk Mitigation in case of insolvency“
- Ausstiegsstrategie, Notfallplan und Beendigungsverfahren für jeden Vertrag sind zu dokumentieren

=> Ohne Escrow-Absicherungen dürfen viele IKT-Verträge in Zukunft gar nicht abgeschlossen werden!

Deposix digital escrow

What?

Digital Escrow: Bollwerk zum Schutz von IP

Classical Software Escrow (on-Prem)

IP Escrow

Data Escrow

SaaS Escrow

Cloud Escrow

Key Escrow

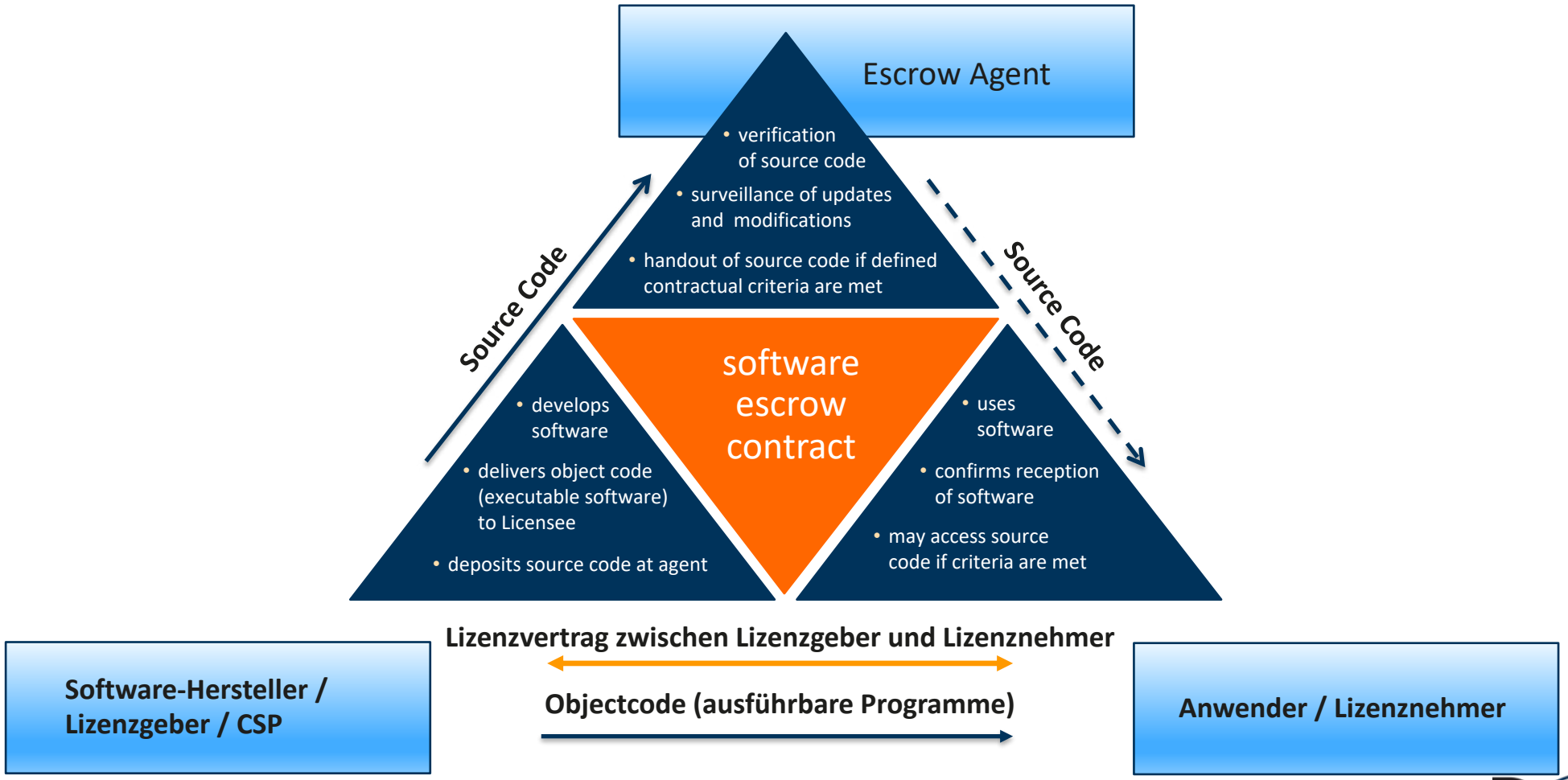
AI Escrow

HSM Key Escrow

© 2024 Deposix

Das klassische Escrow-Modell

3 Parteien



© 2024 Deposix

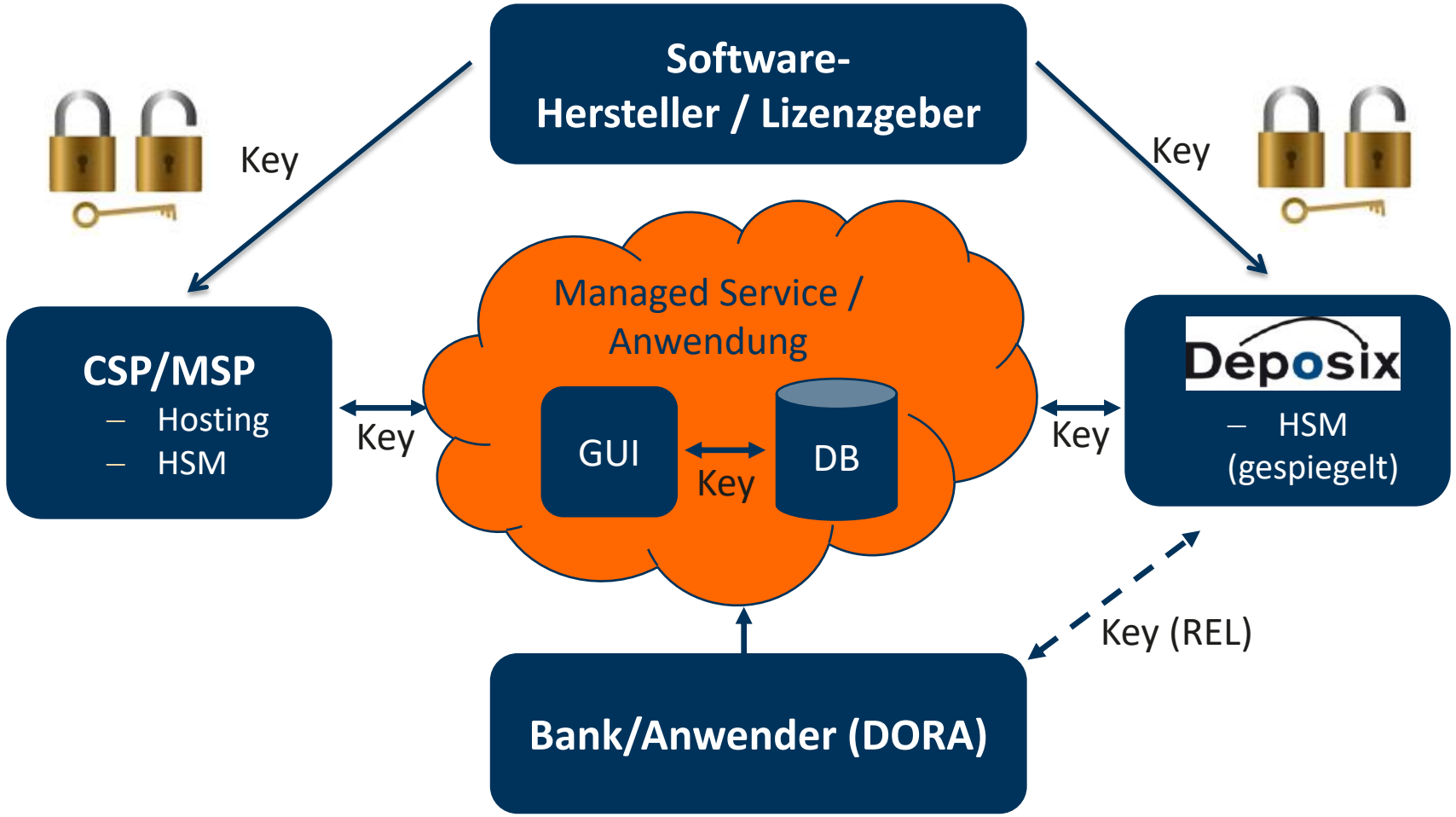
Deposix digital escrow

DORA Escrow-Modell

4 Parteien

Technischer Lösungsansatz für eine Cloud-Anwendung

DORA und SaaS: Was passiert bei Ausfall eines IKT-Dienstleisters?!
Hier: Verschlüsselung nach FIPS 140-2 Level 3



© 2024 Deposix

Deposix digital escrow

What?

Digital Escrow: Bollwerk zum Schutz von IP

*In **Grün**: Die unter DORA besonders relevanten Leistungen*

Classical Software Escrow (on-Prem)

IP Escrow

Data Escrow

SaaS Escrow

Cloud Escrow

Key Escrow

AI Escrow

HSM Key Escrow

© 2024 Deposix

The best is yet to come!

Unsere Hypothese: großer (Nachhol-)Bedarf für juristische Expertise

Key Take-Aways:

1. Finanzbranche *und IT-Branche* kommen nicht an DORA vorbei.
2. Im Kern: Identifizierung und Absicherung kritischer Software und Daten.
3. *Viele* DORA-Anforderungen können mit Escrow gelöst werden … *ohne* geht es nicht.
4. DORA = 62 Seiten (dt. Version), die es in sich haben. Der Sturm (die Arbeit) kommt erst noch.
5. Das Ziel der Digitalen Resilienz ist *und wird noch ein Akt! Der echte Praxistest steht noch aus - Bericht folgt in einem Jahr.*

Deposix digital escrow

Fazit:
DORA meets Escrow – DORA needs Escrow!

... mehr Berichte aus der Praxis dann beim
21. OSE Symposium am 30.01.26

Deposix
digital escrow

Vielen Dank!

Deposix Software Escrow GmbH
Innere Wiener Str. 11a, 81667 München
www.deposix.de
+49 (89) 189-1255-0

Christian Weitzel, Geschäftsführer
christian.weitzel@deposix.com

Stephan Peters, Gründer, Geschäftsführer
stephan.peters@deposix.com

Backup

Deposix
digital escrow

Kategorisierung der Komponenten von Digital Escrow auf Basis des Hinterlegungsgegenstandes

I. **Klassisches Software Escrow** (primärer Hinterlegungsgegenstand: Software Quellcode; hier mit zugeordnet: Quellcode von Embedded Software)
II. **Cloud Escrow** - auch SaaS, AaaS oder EaaS (primärer Hinterlegungsgegenstand: Software Quellcode)
III. **IP Escrow** (primärer Hinterlegungsgegenstand: allgemeines Know-how, Geschäftsgeheimnisse – *nicht* Software; beispielhaft Konstruktionsquelldaten wie Baupläne für Platinen, Material- und Stücklisten, Explosionszeichnungen, Angaben zu Zuliefererketten, Inhaltsstoffen für chemische Prozesse und Komponenten für Fertigungsanlagen und deren Konfiguration)
IV. **Key Escrow** (primärer Hinterlegungsgegenstand: kryptografische Schlüssel, Passwörter, manchmal Hashwerte)
V. **Data Escrow** (primärer Hinterlegungsgegenstand: große Datenmengen; Input oder Output oder Basis für statistische Auswertungen; strukturiert oder unstrukturiert)
VI. **KI Escrow** (primärer Hinterlegungsgegenstand: Quellcode und/oder Algorithmen der „leeren“ bzw. untrainierten KI Modelle bzw. Neuronalen Netzwerke, und dessen Trainingsdaten)

Zusätzlich: VII. True SaaS Escrow und VIII. HSM Key Escrow

© 2024 Deposix

Deposix digital escrow