Downloaded from Blogs on 06.11.2026 17:18

Regulatory Blog

By PwC Deutschland | 04 November 2026

EBA Guidelines on the sound management of third-party risk regarding non-ICT services

Final report EBA/GL/2026/09

Downloaded from Blogs on 06.11.2026 17:18

Content

Vergleich TPR-Guidelines vs. Outsourcing-Guidelines 3

Vergleich TPR-Guidelines vs. Konsultationsentwurf 3

Nicht alle Fragen sind bereits beantwortet 4

Fazit 5

Wie PwC bei der Umsetzung unterstützt 5

Downloaded from Blogs on 06.11.2026 17:18

Die EBA hat am 18. September 2026 die ursprünglich bereits für April dieses Jahres angekündigte finale Fassung ihrer **Guidelines on the sound management of third-party risk („TPR-Guidelines“)** erlassen. Die TPR-Guidelines sollen an die Stelle der bislang geltenden **EBA Guidelines on outsourcing arrangements** vom 25. Februar 2019 („Outsourcing-Guidelines“) treten. Den finalen TPR-Guidelines ging ein Konsultationsentwurf vom 8. Juli 2025 („Konsultationsentwurf“) voraus, über den wir mit unserem Blogbeitrag **Next Level-Third Party Risk Management statt Outsourcing Governance** berichtet hatten.

Vergleich TPR-Guidelines vs. Outsourcing-Guidelines

Die TPR-Guidelines unterscheiden sich von den Outsourcing-Guidelines vor allem in folgenden Punkten:

- **Umfang des Regelungsgegenstands:**
  Die Outsourcing-Guidelines konzentrieren sich auf Auslagerungen. Die TPR-Guidelines erfassen dagegen grundsätzlich alle Third Party Arrangements (TPA), die wiederkehrende oder laufende externe Dienstleistungen betreffen, die eine Funktion des Instituts unterstützen. Auslagerung ist darin nur noch ein Teilbereich.
- **Fokus auf unterstützende Dienstleistungen:**
  In den Outsourcing-Guidelines stand die Frage im Vordergrund, ob aufgrund ihrer Risiken eine Leistung als Outsourcing einzustufen ist. Künftig ist nach den TPR-Guidelines die vorgelagerte Frage, ob externe Dienstleister (kritische oder wichtige) Funktionen unterstützen. Die Einstufung nach ihrer Funktion ist entscheidend für die weiteren Anforderungen an das TPA. Die Betrachtung des Risikos bzw. die Risikoanalyse erfolgt auf einer nachgelagerten Stufe.
- **Abgrenzung zu ICT und DORA:**
  Die Outsourcing-Guidelines umfassten auch IT- und Cloud-Auslagerungen. Den TPR-Guidelines unterfallen nur noch die Non-IKT Dienstleistungen, während für die IKT Dienstleistungen ausschließlich DORA anzuwenden ist. Bei Dienstleistungen, die mehrere Funktionen unterstützen und IKT Bestandteile besitzen, ist zu prüfen, ob der IKT Bestandteil materiell für die Erbringung der Leistung ist.
- **Ganzheitlicher Risikomanagementansatz:**
  Die Anforderungen zu Register, Risikoanalyse, Überwachung und Exit-Strategien bezogen sich nach den Outsourcing-Guidelines ausschließlich auf Outsourcing-Vereinbarungen. Die TPR-Guidelines betten diese Pflichten in ein breiteres Third-Party-Risk-Management-Framework ein, das sämtliche relevanten Abhängigkeiten von Drittparteien erfassen soll.
- **Erweiterte Anforderungen:**
  Die bereits in den Outsourcing-Guidelines enthaltenen Anforderungen an das Register, die Verträge, die Steuerung und Überwachung, das Notfallmanagement sowie die Beendigung werden in den TPR-Guidelines in abgestufter Form grundsätzlich auf alle TPAs ausgeweitet.

Vergleich TPR-Guidelines vs. Konsultationsentwurf

Downloaded from Blogs on 06.11.2026 17:18

Im Vergleich zum Konsultationsentwurf ergaben sich in der finalen Fassung der TPR-Guidelines noch folgende wesentlichen Änderungen:

- **Klarerer Fokus auf Non-ICT-Services**
  Im Konsultationsentwurf war bereits vorgesehen, dass ICT-Services wegen DORA grundsätzlich nicht in den Anwendungsbereich fallen. Der Titel und einige Formulierungen waren aber noch allgemeiner gehalten.
  In der finalen Fassung wird der Fokus deutlicher herausgestellt: Es geht um das Management von Drittparteienrisiken bei Non-ICT-Services. ICT-Drittparteienrisiken werden grundsätzlich durch DORA abgedeckt.
- **Stärkere Ausrichtung auf kritische oder wichtige Funktionen**
  Im Konsultationsentwurf wurden noch relativ breit alle Drittparteienvereinbarungen adressiert, auch wenn für kritische oder wichtige Funktionen strengere Anforderungen vorgesehen waren.
  In der finalen Fassung wurde stärker herausgestellt, dass es um wiederkehrende und laufende Unterstützungen einer Funktion geht und der Schwerpunkt auf Drittparteienvereinbarungen liegt, die kritische oder wichtige Funktionen unterstützen. Andere Drittparteienvereinbarungen bleiben zwar nicht völlig außen vor, sollen aber risikobasiert und proportional behandelt werden.
- **Mehr Proportionalität und weniger Belastung für weniger kritische Vereinbarungen**
  Im Konsultationsentwurf wirkten einige Anforderungen noch umfassender, insbesondere für die Dokumentation und Überprüfung aller bestehenden Drittparteienvereinbarungen.
  In der finalen Fassung wurde mehr Flexibilität eingeführt. Vor allem bei Drittparteienvereinbarungen, die keine kritischen oder wichtigen Funktionen unterstützen, können Review und Dokumentation stärker anlassbezogen erfolgen, insbesondere bei Verlängerung oder Erneuerung der Vereinbarung.
- **Flexiblerer Umgang mit dem Register**
  Im Konsultationsentwurf war ein Register für Drittparteienvereinbarungen vorgesehen, das an DORA angelehnt sein sollte. Die Anforderungen wirkten jedoch noch stärker wie ein eigenständiges zusätzliches Register für Non-ICT-Drittparteien.
  In der finalen Fassung wurde klargestellt, dass Finanzunternehmen mehr Flexibilität haben. Sie können das Register für Non-ICT-Services mit dem DORA-Register kombinieren oder ein separates, proportional ausgestaltetes Register führen, solange die Informationen konsistent bleiben.
- **Präzisere Regelungen zu Subcontracting und Lieferketten**
  Im Konsultationsentwurf wurden Subunternehmer bereits berücksichtigt, insbesondere bei kritischen oder wichtigen Funktionen. Die Formulierungen konnten aber so verstanden werden, dass sehr viele Subunternehmer in der Lieferkette erfasst werden müssten.
  In der finalen Fassung wurde die Regelung stärker an DORA angeglichen. Besonders relevant sind nun Subunternehmer, die die Erbringung von Services für kritische oder wichtige Funktionen tatsächlich wesentlich unterstützen bzw. „effectively underpin“.

Nicht alle Fragen sind bereits beantwortet

Downloaded from Blogs on 06.11.2026 17:18

Die vorgesehenen Veränderungen führen nicht zwangsläufig zu weniger Aufwand. Einzelne Registerangaben entfallen oder gelten nur für Dienstleistungen, die kritische oder wichtige Funktionen unterstützen. Andere Pflichten insbesondere im Vertragsmanagement werden auf alle Non-IKT Dienstleistungen erweitert und erfordern zusätzliche vertragliche Vereinbarungen.

Der Begriff „Third-Party Risk“ wirft Fragen zur Abgrenzung auf. Die Leitlinie regelt ausschließlich Nicht-IKT Dienstleistungen, währen der Begriff Third-Party Risk umfänglicher verstanden werden könnte.

Die strengsten Detailanforderungen konzentrieren sich auf Dienstleistungen für kritische oder wichtige Funktionen. Bei anderen einbezogenen Dienstleistungen wirft die neue Auslegung der Proportionalität Fragen auf, da auch sie beispielsweise weiterhin eine Leistungsüberwachung sicherstellen sollten.

Der konkrete Umsetzungszeitpunkt ist weiterhin offen. Solange das Anwendungsdatum nicht feststeht, bleibt auch unklar, wann die Übergangsfristen tatsächlich enden.

Fazit

Die neue Leitlinie verändert vor allem den Anwendungsbereich und die Verknüpfung bestehender Kontrollen. Die zentralen Aufgaben liegen in der vollständigen Erfassung relevanter Nicht-IKT-Dienstleistungen, ihrer Zuordnung zu kritischen oder wichtigen Funktionen und der Steuerung wichtiger Weiterverlagerungen. Institute können vorhandene Strukturen weiterverwenden, müssen diese jedoch gezielt erweitern und mit DORA verzahnen.

Wie PwC bei der Umsetzung unterstützt

Die neuen EBA-Leitlinien erfordern eine Überprüfung bestehender Auslagerungs- und DORA-Strukturen. Gleichzeitig stellen sich für viele Institute Fragen zur praktischen Umsetzung, zur Abgrenzung von DORA und zum tatsächlichen Anpassungsbedarf.

PwC unterstützt Institute dabei, die Auswirkungen der neuen Anforderungen zu bewerten und einen pragmatischen
Umsetzungsansatz zu entwickeln. Gemeinsam identifizieren wir Handlungsbedarfe, priorisieren erforderliche
Maßnahmen und begleiten die Umsetzung in bestehende Prozesse und Strukturen.

Unser Angebot: Von der ersten Betroffenheitsanalyse bis zur praktischen Umsetzung unterstützen wir Sie dabei, die neuen Anforderungen effizient und passgenau in Ihre bestehende Governance-, Auslagerungs- und DORA-Landschaft zu integrieren.

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie mehr unter “**Leistungen & Angebote**”.

Zu weiteren PwC Blogs

Downloaded from Blogs on 06.11.2026 17:18

Keywords

Bankenaufsicht (Europäische und Internationale Organisationen), Capital Requirements Regulation (CRR III), Digital Operational Resilience Act (DORA), Information and Communication Technology Risk (ICT), Outsourcing (Finanzdienstleistungsinstitute), Outsourcing (Kreditinstitute), Third-Party Risk

Contact



Martin Neisen

Frankfurt am Main

martin.neisen@pwc.com



Christoph Himmelmann

Frankfurt am Main

christoph.himmelmann@pwc.com