UBS

Policy für globale Leistungserbringer

Audit Policy

WARUM

Um uns die Informationen und die Übersicht zu verschaffen, die uns helfen, unseren rechtlichen und regulatorischen Pflichten nachzukommen und die Compliance sicherzustellen

WANN

Wenn Sie eine der folgenden Dienstleistungen / Produkte erbringen oder liefern:

1. ausgelagerte Dienstleistungen;
2. BCM-kritische Dienstleistungen / Produkte;
3. SOX-relevante Dienstleistungen / Produkte; oder
4. Produkte oder Dienstleistungen, die von einer für UBS zuständigen Aufsichtsbehörde reguliert werden.

WAS wissen WIE die Vorschriften einzuhalten sind

1. Umfang des Audits

- Sie müssen den Revisoren das Recht gewähren (oder dafür sorgen, dass Ihre Unterauftragnehmer den Revisoren das Recht gewähren) auf Zugang zu Ihren (oder Ihrer Agenten oder Unterauftragnehmer) Räumlichkeiten, Personal und relevanten Aufzeichnungen (einschliesslich Geräten, Systemen, Netzwerken, Informationen und Daten, die zur Erbringung der Dienstleistungen eingesetzt werden) insoweit dies vernünftigerweise erforderlich ist, um:
  - sämtliche regulatorischen Pflichten oder rechtlich durchsetzbaren Aufforderungen einer Aufsichtsbehörde zu erfüllen,
  - zu überprüfen, ob Sie die Bedingungen der Vereinbarung erfüllen (einschliesslich aller geltenden Policies) und ob Sie die Dienstleistungen gemäss den anwendbaren Gesetzen und Service Levels erbringen,
  - Unsere in Ihrem Besitz oder unter Ihrer Kontrolle befindlichen Bestände (einschliesslich geistiger Eigentumsrechte, UBS-Daten oder vertraulicher Informationen von UBS) sowie deren Integrität, Vertraulichkeit und Sicherheit zu inspizieren und
  - einen Betrugsverdacht oder wesentliche Rechnungslegungsfehler zu ermitteln.
- Sie müssen den Revisoren eine angemessene Zusammenarbeit und einen angemessenen Zugang im Rahmen des jeweiligen Audits gewähren.
- Die Revisoren haben unter anderem das Recht auf die Überprüfung von:
  - Dokumente oder Informationen, welche die Erbringung der Dienstleistungen dokumentieren
  - Ihre Risikomanagementprozesse
  - Ihre Informationssicherheit sowie Ihre physischen, technischen und administrativen Kontrollen
  - Ihre Notfallmassnahmen- und Business-Continuity-Pläne
  - Abhängigkeiten in Ihrer Lieferkette sowie operative Resilienz Ihrer Lieferkette
  - interne oder externe Revisionsberichte (z.B. ISO 27001, SOC 2 Typ II, PCI DSS) und Penetrationstestberichte, die von unabhängigen Stellen durchgeführt wurden (diese können bearbeitet werden, um unseren Zugang zu Ihren vertraulichen Informationen über andere Kunden zu beschränken),
  - falls zutreffend, Ihre Einhaltung der Policy für Unterauftragnehmer und die Einhaltung der Pflichten seitens des Unterauftragnehmers bezüglich untervergebener Dienstleistungen.
- Sie anerkennen, dass unsere regulierten Finanzdienstleistungskunden ebenfalls verpflichtet sein können, Sie nach Anwendbaren Gesetzen Audits zu unterziehen, und dass die Rechte in dieser Audit Policy auch für diese Kunden (oder für die für sie zuständigen Aufsichtsbehörden oder ernannten Revisoren) gelten.

2. Durchführung von Revisionen

- Alle Audits werden gemäss den anerkannten nationalen und internationalen Revisionsstandards durchgeführt.
- Bei der Durchführung von Audits in Umgebungen mit mehreren Kunden ist uns bewusst, dass es zu beachten gilt, Risiken für die Umgebung anderer Kunden (z.B. Auswirkungen auf Service Levels, die Verfügbarkeit von Daten, Vertraulichkeitsaspekte) zu vermeiden oder zu vermindern. Diesbezüglich sind wir bestrebt, mit Ihnen zusammenzuarbeiten.
- Gegebenenfalls werden wir in Erwägung ziehen, gemeinsam mit Ihren anderen Kunden zusammengelegte Audits durchzuführen, um die Revisionsressourcen effizienter zu nutzen und die organisatorischen Auswirkungen für Sie und Ihre Kunden zu verringern.
- Bevor Besuche vor Ort oder physische Revisionen, Inspektionen oder Überwachungen stattfinden, werden wir oder die Revisoren Sie diesbezüglich benachrichtigen, es sei denn:
  - der Audit erfolgt aufgrund eines Notfalls oder einer Krisensituation, des Verdachts auf Betrug oder einer Sicherheitsverletzung,
  - der Audit wird von einer Aufsichtsbehörde gefordert oder ist erforderlich, um regulatorische Vorgaben zu erfüllen, und es ist nicht praktikabel oder unmöglich, Sie angemessen zu benachrichtigen,
  - die Benachrichtigung würde dazu führen, dass der Zweck des Audits vereitelt würde.
- Sie tragen Ihre eigenen Kosten und Aufwendungen, die durch einen Audit oder Inspektion entstehen; ebenso tragen wir unsere eigenen Kosten, es sei denn, es werden wesentliche Versäumnisse oder ein Verstoss identifiziert. In diesem Fall erstatten Sie uns unsere angemessenen Kosten und Auf-

wendungen, die aufgrund der Durchführung des Audits oder Inspektion entstanden sind (einschliesslich der Kosten für unsere Revisoren oder andere externe Berater).

3. Massnahmen zur Mängelbeseitigung

- Sollte bei einem Audit oder einer anderen Inspektion durch einen Revisor festgestellt werden, dass Sie oder ein Dritter in Ihrem Namen gegen die Anwendbaren Gesetze, eine Anordnung einer Aufsichtsbehörde oder die Bedingungen der Vereinbarung (einschliesslich der geltenden Policies) verstossen haben, müssen Sie unverzüglich alle erforderlichen Massnahmen für die Beseitigung dieses Zustands ergreifen
- Sie müssen alle anderen angemessenen Empfehlungen des Revisors innerhalb eines angemessenen Zeitrahmens oder gegebenenfalls innerhalb des von dem Revisor angegebenen Zeitrahmens umsetzen.

4. SOX-relevante Dienstleistungen / Produkte

- Wenn Sie SOX-relevante Dienstleistungen / Produkte erbringen oder liefern,
  - müssen Sie angemessene Kontrollen einrichten (oder einrichten lassen), einschliesslich Kontrollen in Bezug auf IT-Anwendungen, unterstützende Infrastruktur oder IT-Prozesse (z. B. Cloud Dienstleistungen, Rechenzentrum, Helpdesk). Diese Kontrollen und etwaige Kontrollmängel müssen in einem «SOC 1 Typ 2»-Bericht (oder einem gleichwertigen Bericht) gemeldet werden, wie in Abschnitt (i) unten beschrieben.
  - Sie müssen mindestens einmal jährlich und auf eigene Kosten eine Prüfung der Finanzberichterstattung gemäss den folgenden Standards durchführen (oder durchführen lassen):
    (i) dem Standard «SSAE No. 18 Systems and Organizational Service Organizational Controls (SOC1) Type 2» für Dienstleistungen / Produkte, die direkt oder indirekt für in den Vereinigten Staaten ansässige Empfänger innerhalb des UBS-Konzerns erbracht oder an diese geliefert werden, und
    (ii) den International Standards for Assurance Engagements (ISAE) No. 3402 für Dienstleistungen / Produkte, die direkt oder indirekt für alle anderen Empfänger innerhalb des UBS-Konzerns erbracht oder an diese geliefert werden,

  und die Ergebnisse dieser Prüfung(en) unverzüglich an UBS weiterleiten.

5. Fortbestand

- Diese Audit Policy bleibt nach Kündigung oder Ablauf der Vereinbarung weiterhin bestehen.