yes® Signing Service

QES Regeln (IDP)

Version: 202010

Die vorliegenden Bedingungen gelten für die Erstellung einer qualifizierten elektronischen Signatur über yes® (die "**QES Regeln**").

§ 1 Geltungsbereich und Begriffsbestimmungen

1. Diese QES Regeln regeln die besondere Anforderungen an einen Identity Provider, die für eine ordnungsgemäße Funktionsweise von yes® im Rahmen des yes® Signing Services erfüllt sein müssen.

2. Neben diesen QES Regeln gelten die sonstigen Vereinbarungen zwischen den Parteien. Im Fall eines Widerspruchs gehen die Regelungen dieser QES Regeln den sonstigen Vereinbarungen vor.

§ 2 Definitionen und Interpretationen

In diesen QES Regeln gelten, soweit vorliegend nichts anderes vereinbart ist, die Definitionen aus eIDAS-VO[1] und den sonstigen Vereinbarungen zwischen den Parteien. Darüber hinaus gelten die folgenden Definitionen:

"GwG Identifizierungsmethode" ist eine Identifizierungsmethode nach Maßgabe dieser QES Regeln i.V.m. dem yes® Signing Service Solution Design, die auf GwG-konformen Daten basiert und für die durch eine akkreditierte Konformitätsbewertungsstelle die gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit zur Überprüfung der Identität von natürlichen Personen bei der Ausstellung von qualifizierten Zertifikaten bestätigt worden ist (siehe Art. 24 Abs. 1 lit. d eIDAS-VO).

"**Identity Provider**" oder "**IDP**" ist ein Kreditinstitut nach § 1 KWG[2] bzw. ein CRR Kreditinstitut, das direkt oder indirekt yes® Services bereitstellt und im Rahmen des yes® Signing Services Aufgaben einer Registrierungsstelle für die Zwecke des QTSP übernimmt.

"**Konformitätsbewertungsstelle**" ist die akkreditierte Konformitätsbewertungsstelle des jeweiligen QTSP.

"**QES Beteiligte**" sind der Identity Provider und der QTSP.

"**QTSP**", "**Qualified Trust Service Provider**" oder "**Vertrauensdiensteanbieter**" ist jeder an yes® teilnehmende qualifizierte Vertrauensdiensteanbieter.

"**Wesentlichen Fehler und Vorkommnisse**" sind jeder Vorfall, jede Sicherheitsverletzung oder jeder Integritätsverlust, die bzw. der sich auf die Leistungen nach diesen QES Regeln oder den dem yes® Signing Service zugrunde liegenden personenbezogenen Daten auswirken können. Insbesondere wird ein Fehler oder Vorkommnis als erheblich bezeichnet, wenn eines oder mehrere der folgenden Kriterien erfüllt sind:

- führt potentiell zu einer schwerwiegenden Störung oder Unterbrechung kritischer betriebsrelevanter Dienste;
- führt potentiell zur teilweisen oder vollständigen Unwirksamkeit primärer Sicherheitsmaßnahmen kritischer Systeme oder Dienste;
- führt potentiell zu versehentlichen oder absichtlichen unberechtigten Zugriffen oder Offenlegung von vertraulichen Informationen oder personenbezogenen Daten;

[1] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

[2] Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), das zuletzt durch Artikel 8 des Gesetzes vom 10. Juli 2018 (BGBl. I S. 1102) geändert worden ist.

- steht im Zusammenhang mit illegalen Aktivitäten und führt potentiell zu Schadensersatzansprüchen oder Untersuchungen durch Behörden;
- stellt potentiell einen aktiven Angriff auf einen yes® Partner, den QTSP oder yes.com dar;
- ist ein Angriff oder eine Störung von nicht unerheblichem Ausmaß, z.B. betrifft einen nicht unerheblichen Teil des betroffenen Unternehmens, einer Region oder der Kundenbasis;
- ist potentiell von öffentlichem Interesse;
- wird im Rahmen von internen Prozessen oder Vorgaben oder Verantwortlichen als Notfall oder Krise eingestuft;
- ist potentiell ein Advanced Persistent Threat (APT) oder eine zielgerichtete Attacke, bspw. durch einen Staat oder eine feindlich gesonnene Institution.

"**yes® Signing Service Solution Design**" sind die Technischen Anforderungen für den Identity Provider und den QTSP in Bezug auf die QES.

§ 3 yes® Signing Service Solution Design

In Bezug auf die Leistungen des Identity Providers im Rahmen der Erstellung der QES gilt das yes® Signing Service Solution Design. Der Identity Provider ist sich seiner Rolle gemäß dem yes® Signing Service Solution Design bewusst und versichert, die Anforderungen (inklusive rechtlicher, regulatorischer und technischer Art) an seine Rolle zu erfüllen.

§ 4 Besondere Leistungspflichten des Identity Providers

Identifizierung und Authentifizierung des Endnutzers

1. Die Identifizierung des Endnutzers durch den Identity Provider erfolgt gemäß der GwG Identifizierungsmethode durch Umsetzung dieser QES Regeln i.V.m. dem yes® Signing Service Solution Design.

2. Voraussetzung hierfür ist, dass der Identity Provider ein Kreditinstitut nach § 1 KWG bzw. ein CRR Kreditinstitut ist.

3. Die folgenden gesetzlichen bzw. regulatorischen Anforderungen finden dabei Anwendung:

    a) **Identifizierung gemäß GwG:** der Identity Provider identifiziert den Endnutzer (oder hat dies im Rahmen seiner Geschäftsbeziehung mit dem Endnutzer bereits getan) und teilt entsprechende Daten mit dem QTSP. Als Verpflichteter nach dem GwG verfügt der Identity Provider im Zusammenhang mit der Identifizierung über ein wirksames und angemessenes Risikomanagement zur Verhinderung von Geldwäsche und von Terrorismusfinanzierung (vgl. § 4 ff. GwG) und berücksichtigt die relevanten allgemeinen Sorgfaltspflichten (vgl. § 10 ff. GwG).

    b) **Erkennung von Risiken und Meldung von Vorfällen gemäß ZAG:** Im Rahmen der Identifizierung des Endnutzers hat der Identity Provider angemessene Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung der operationellen und der sicherheitsrelevanten Risiken im Zusammenhang mit den von ihm erbrachten Zahlungsdiensten eingerichtet, hält diese aufrecht und wendet diese an, inklusive wirksamer Verfahren für die Behandlung von Störungen im Betriebsablauf, auch zur Aufdeckung und Klassifizierung schwerer Betriebs- und Sicherheitsvorfälle (vgl. § 53 ZAG) sowie zur entsprechenden Meldung schwerwiegender Betriebs- und Sicherheitsvorfälle an die relevante Aufsicht (vgl. § 54 ZAG).

    c) **Starke Kundenauthentifizierung gemäß ZAG:** Die gemäß yes® Signing Service Solution Design im Rahmen des yes® Signing Services verlangte starke Kundenauthentifizierung erfolgt durch den Identity Provider entsprechend der Anforderungen des ZAG. Im Übrigen verfügt der Identity Provider über angemessene Sicherheitsvorkehrungen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale des Endnutzers zu schützen (vgl. § 55 ZAG).

d) **Geschäftsorganisation gemäß KWG:** Der Identity Provider verfügt über eine ordnungsgemäße Geschäftsorganisation, die die Einhaltung der vom Identity Provider zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet (vgl. § 25a KWG). Es wird abhängig von Art, Umfang, Komplexität und Risikogehalt einer Auslagerung von Aktivitäten und Prozessen auf ein anderes Unternehmen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind, angemessene Vorkehrungen treffen, um übermäßige zusätzliche Risiken zu vermeiden (vgl. § 25b KWG i.V.m. MaRisk und BAIT).

Empfangsbote des QTSP

4. Der Identity Provider übernimmt für den QTSP die direkte Kommunikation mit dem Endnutzer gemäß dem yes® Signing Service Solution Design. In diesem Zusammenhang wird der Identity Provider in Bezug auf das oder die zu unterzeichnende(n) Dokument(e) (i) dem Endnutzer die Datenschutzbestimmungen des QTSP anzeigen, um ihm die Möglichkeit zu deren Kenntnisnahme zugeben und (ii) von dem Endnutzer folgende Zustimmungen bzw. Auftragserteilungen einholen und an den QTSP weiterleiten (Empfangsbote des QTSP für die Willenserklärung des Endnutzers):

    a) Zustimmung zu den Geschäftsbedingungen des QTSP;

    b) Auftrag zur Erstellung der QES durch den QTSP;

    c) Auftrag zur Bereitstellung der QES durch den QTSP an die Relying Party.

Kommunikation mit dem Endnutzer

5. Der Identity Provider ist verantwortlich für jede Kommunikation mit dem Endnutzer im Zusammenhang mit dem yes® Signing Service, inklusive für jede notwendige Information von dem QTSP für den Endnutzer. Der Identity Provider erarbeitet - sofern erforderlich gemeinsam mit yes.com AG und/oder dem QTSP - einen Prozess für den Austausch relevanter Informationen für die Kommunikation mit dem Endnutzer. Dabei ist insbesondere sicherzustellen, dass der Identity Provider auf Verlangen von QTSP oder yes.com (Textform genügt) jede notwendige Information des QTSP an den Endnutzer im Zusammenhang mit dem yes® Signing Service innerhalb angemessener Frist und, soweit erforderlich, unmittelbar übermitteln wird.

Zusicherung des Identity Providers

6. In Ausführung seiner Tätigkeiten nach diesen QES Regeln sichert der Identity Provider dem QTSP zu, dass:

    a) der Endnutzer sich korrekt beim Identity Provider authentifiziert hat;

    b) der Identity Provider nur die Übermittlung solcher Daten und Informationen vom Endnutzer an den QTSP übernimmt, die der Endnutzer beauftragt hat;

    c) der Identity Provider im Falle einer Identifikation des Endnutzers mittels Video-Identifikation, sich nur solcher Videoident-Anbieter bedient, die die Anforderungen aus der eIDAS-VO nachweislich erfüllen, inkl. deren eingesetztes Verfahren gemäß der eIDAS-VO bestätigt ist. - Der Identity Provider wird auf Anforderung eine entsprechende Bestätigung bzw. einen Bericht der Konformitätsbewertungsstelle und/oder der jeweiligen Aufsichtsstelle vorgelegen;

    d) der Identity Provider ein System zur starken Kundenauthentifizierung basierend auf mindestens zwei Authentifizierungs-Faktoren aus verschiedenen Kategorien verwendet (vgl. § 55 ZAG, EU Richtlinie 2015/2366 sowie EU Richtlinie 2015/1502). Das Sicherheitsniveau des Systems zur Authentifizierung entspricht dem Sicherheitsniveau “substantiell” (vgl. die GwG Identifizierungsmethode).

§ 5 Besondere Leistungspflichten von yes.com

Voraussetzungen und Anforderungen des QTSP

1. Voraussetzung für die Teilnahme des QTSP an yes® ist, dass dieser als Vertrauensdiensteanbieter im Sinne der eIDAS-VO handeln darf und dem von der Aufsichtsstelle der entsprechenden Status verliehen worden ist.

2. yes.com wird alle relevanten Anforderungen des QTSP an die Rolle des Instituts im Zusammenhang mit dem yes® Signing Service bereitstellen.

Freischaltung von Identity Providern

3. yes.com wird einen Identity Provider für den yes® Signing Service freischalten, sobald und solange dieser die Anforderungen an seine Rolle im Zusammenhang mit dem yes® Signing Service akzeptiert und umsetzt, inklusive aller relevanten Anforderungen aus diesen QES Regeln und dem yes® Signing Service Solution Design.

4. Eine Freischaltung des Identity Providers erfolgt frühestens 48h (achtundvierzig Stunden) nach Inkrafttreten der vorliegenden QES Regeln und vollständiger technischer Integration.

Public Key Archive

5. yes.com betreibt ein Long-Term Public Key Archive gemäß dem yes® Signing Service Solution Design, welches Daten und Informationen bereitstellt über:

    a) die Tatsache, dass ein bestimmter Identity Provider zu einem bestimmten Zeitpunkt an yes® teilgenommen hat;

    b) den Link zwischen diesem Identity Provider und einem bestimmten Public Key.

§ 6 Verantwortlichkeit für Datenverarbeitung

1. Identity Provider und QTSP entscheiden zu jedem Zeitpunkt einzeln und unabhängig voneinander den Zweck und die Mittel jeglicher Verarbeitung personenbezogener Daten im Zusammenhang mit dem yes® Signing Service. Sie werden keine Zwecke oder Mittel gemeinsam bestimmen oder Daten für den jeweils anderen verarbeiten.

2. yes.com hat weder Einfluss noch Entscheidungsgewalt auf die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten eines Endnutzers durch den Identity Provider oder den QTSP im Zusammenhang mit dem yes® Signing Service, noch erhält yes.com solche personenbezogenen Daten im Zusammenhang mit dem yes® Signing Service.

§ 7 Besondere Haftung zwischen Identity Provider und QTSP

1. In Bezug auf die Leistungspflichten nach diesen QES Regeln gewährt der Identity Provider dem QTSP jeweils einen direkten Haftungsanspruch nach Maßgabe des § 12 der yes® Regeln (hier sog. “Vertrag zugunsten Dritter” - denn gegenüber yes.com gewährt der QTSP auch dem Identity Provider einen direkten Haftungsanspruch). Wird zum Beispiel der QTSP erfolgreich für einen Schaden belangt, den jemand erleidet, der sich auf ein gültiges qualifiziertes Zertifikat verlassen hat, und ist dieser Schaden auf eine Verletzung des Identity Providers von Pflichten nach dieser QES Regeln zurückzuführen, haftet der Identity Provider dem QTSP direkt entsprechend der Maßstäbe des § 12 der yes® Regeln (vgl. auch Art. 13 eIDAS). Eine zusätzliche Inanspruchnahme durch yes.com ist insoweit ausgeschlossen.

2. Um das finanzielle Risiko angemessen bzw. tragfähig zu begrenzen, das dem QTSP und in der Konsequenz dem Identity Provider entstehen könnte, kann yes.com dafür sorgen, dass der QTSP die Nutzung der QES angemessen beschränkt und damit eine Haftung für Schäden aus einer darüber hinausgehenden Nutzung ausschließt (vgl. Art. 13 (2) eIDAS-VO). yes.com wird hierbei die Vorschläge des Identity Providers angemessen berücksichtigen.

§ 8 Koordination, Berichtspflichten und laufende Kontrolle

1. Die Interne Revision, der Geldwäschebeauftragte, der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte des Identity Providers wird in Bezug auf die Leistungen des Identity Providers nach § 4 (*Besondere Leistungspflichten des Identity Providers*) dieser QES Regeln (die "**Tätigkeit**") mit dem QTSP vertrauensvoll zusammenarbeiten und die erforderlichen Abstimmungen vornehmen. Die Interne Revision des QTSP hat das Recht, sich von der Einhaltung der relevanten Anforderungen regelmäßig zu überzeugen und darf nach vorheriger Absprache anlassbezogen eigene Ergänzungsprüfungen durchführen.

2. Darüber hinaus ist unverzüglich über alle Wesentlichen Fehler und Vorkommnisse beim Identity Provider mit Bezug zur Tätigkeit unverzüglich an den QTSP und soweit yes.com betroffen ist auch an yes.com berichten (Ad-Hoc-Bericht). Insbesondere ist dem QTSP unverzüglich nach Kenntnisnahme durch den Identity Provider über jede Sicherheitsverletzung, jeden Verstoß gegen Anforderungen aus dem GwG oder jeden Integritätsverlust beim Institut zu berichten, die bzw. der sich auf die Tätigkeit oder die darin vorhandenen personenbezogenen Daten auswirkt.

§ 9 Aufsicht durch die Aufsichtsstelle

1. Die relevante Aufsichtsstelle sowie die von dieser mit der Prüfung beauftragten Stellen und/oder Prüfer, inklusive der vom QTSP regelmäßig zur Prüfung ersuchten Konformitätsbewertungsstelle (vgl. Art. 20 ff. i.V.m Art. 17 ff. eIDAS-VO), haben ein jederzeitiges, vollumfängliches und ungehindertes Einsichts-, Informations- und Prüfungsrecht hinsichtlich der Tätigkeit; dies schließt die Anfertigung von Abschriften einschlägiger Unterlagen mit ein. Diesen Prüfern oder Stellen ist ein Zugang zu allen Dokumenten, Datenträgern und Systemen beim Identity Provider zu gewähren, die die Tätigkeit betreffen.

2. Außer im Fall von Anfragen durch Justizbehörden oder Aufsichtsbehörden, bestehen alle vorgenannten Rechte für einen Zeitraum von zwei Jahren nach Beendigung der Tätigkeit fort, beginnend mit dem Ablauf des Geschäftsjahres, in dem die vorliegenden QES Regeln nicht mehr Bestandteil der Kooperation zwischen dem jeweiligen yes® Partner und yes.com ist. Relevante Unterlagen müssen ebenso lange verfügbar bleiben.

3. Sofern sich der Identity Provider in Bezug auf die Tätigkeit Dritter bedient (z.B. eines technischen Dienstleisters), stellt der Identity Provider sicher, dass die Rechte aus dem vorliegenden Paragraphen auch gegenüber diesem Dritten gelten.