

## आधार (अधिप्रमाणन और ऑफलाइन सत्यापन) विनियम, 2021<sup>1</sup>

[23.10.2023 को अद्यतन किया गया]

आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 यथा संशोधित आधार एवं अन्य विधियां (संशोधन) अधिनियम 2019 (2019 की संख्या 14) की उप धारा 54 धारा (1) की उप धारा (2) के उप खंड (क) (खक) (गक) (गख) (च) (चक) (चख) एवं (ब) और उप खंड (1) के तहत प्रदत्त शक्तियों का प्रयोग करते हुए तथा आधार (अधिप्रमाणन) विनियम, 2016 के अधिक्रमण में, उक्त अधिक्रमण से पूर्व किए गए या किए जाने वाले कार्यों को छोड़कर, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा निम्नलिखित विनियम बनाती है:-

### अध्याय - 1

#### प्रारंभिक

#### 1. संक्षिप्त नाम और प्रारंभ:-

- (1) इन विनियमों को आधार (अधिप्रमाणन और ऑफलाइन सत्यापन) विनियम, 2021 कहा जाएगा।
- (2) ये विनियम सरकारी राजपत्र में इनके प्रकाशन की तिथि से लागू होंगे।

#### 2. परिभाषाएं:-

- (1) जब तक कि संदर्भ में अन्यथा अपेक्षित न हो, इन विनियमों में,-

- (क) **“अधिनियम”** से अभिप्राय आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 से है;
- (कक) **‘आधार नंबर’** से अभिप्राय आधार अधिनियम की धारा 3 की उप-धारा (3) के अधीन किसी व्यक्ति को जारी पहचान संख्या से है, और इसमें उस धारा की उप-धारा (4) के अधीन सृजित कोई वैकल्पिक वर्चुअल पहचान भी शामिल है,
- <sup>2</sup>[(कख) **“आधार पत्र”** का अभिप्राय किसी निवासी के आधार नंबर को संसूचित करने वाले दस्तावेज़ से है;]
- (ख) **“आधार नंबर धारक”** का अभिप्राय कोई व्यक्ति, जिसे अधिनियम के अंतर्गत आधार नंबर जारी किया गया है, से है;
- (खक) **‘आधार नंबर कैप्चर सर्विस टोकन या एएनसीएस टोकन’** से तात्पर्य अधिप्रमाणन प्रक्रिया को पूर्ण करने के लिए प्राधिकरण द्वारा आधार नंबर के लिए दी गई कूटबद्ध संख्या से है। एएनसीएस टोकन प्राधिकरण द्वारा यथा निर्धारित अल्प अवधि के लिए वैध होगा।
- (खख) **‘आधार कागज रहित ऑफलाइन ई-केवाईसी’** से तात्पर्य प्राधिकरण द्वारा जारी डिजिटल रूप से हस्ताक्षरित दस्तावेज से है, जिसमें आधार नंबर के अंतिम चार अंक, जनसांख्यिकीय संबंधी सूचना जैसे नाम, पता, लिंग और जन्म तिथि तथा आधार नंबर धारक की फोटो आदि अंतर्निहित है।

<sup>1</sup> भारत के राजपत्र, असाधारण, भाग III, खंड 4, संख्या 542 दिनांक 9.11.2021 में अधिसूचना संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2021 का संख्या 2), दिनांक 8.11.2021 द्वारा प्रकाशित और बाद में संशोधन अधिसूचनाओं संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2022 का संख्या 1), दिनांक 4.2.2022, संख्या एच क्यू-13011/2/2021/अधि.-II (2023 का संख्या 1), दिनांक 24.2.2023 (प्रभावी दिनांक 27.2.2023 से), और संख्या एच क्यू-13073/1/2020-अधि.-II (ई), दिनांक 29.9.2023 (दिनांक 3.10.2023 से प्रभावी)

<sup>2</sup> अधिसूचना संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2022 का संख्या 1), दिनांक 4.2.2022 द्वारा प्रविष्ट।

- (खग) **‘आधार सुरक्षित क्यूआर कोड’** से तात्पर्य प्राधिकरण द्वारा सृजित त्वरित प्रतिक्रिया कोड से है, जिसमें डिजिटल रूप से हस्ताक्षरित डेटा जैसे आधार नंबर के अंतिम चार अंक, जनसांख्यिकीय संबंधी सूचना जैसे नाम, पता, लिंग तथा जन्म तिथि और आधार नंबर धारक की फोटो आदि अंतर्निहित है।
- <sup>3</sup>(खघ) **“आधार पीवीसी कार्ड”** का अभिप्राय एक पोलिविनाइल क्लोराइड कार्ड (पीवीसी) से है, जो निर्धारित शुल्क के भुगतान पर प्राधिकरण द्वारा जारी किया जाता है, जिसमें आधार नंबर, जनसांख्यिकीय जानकारी और आधार नंबर धारक की फोटो के साथ आधार सुरक्षित क्यूआर कोड मुद्रित होता है और जो कागज-आधारित आधार पत्र के समतुल्य है।
- (ग) **“अधिप्रमाणन”** का अभिप्राय, ऐसी प्रक्रिया से है, जिसके द्वारा किसी व्यक्ति की जनसांख्यिकीय सूचना अथवा बायोमेट्रिक सूचना आधार नंबर सहित उसके सत्यापन के लिए ‘केन्द्रीय पहचान डेटा रिपोजिटरी’ के पास जमा की जाती है और ऐसा रिपोजिटरी उसकी यथार्थता अथवा कमी को उपलब्ध सूचनाओं के आधार पर सत्यापित करता है;
- (घ) **‘अधिप्रमाणन सुविधा’** का अभिप्राय प्राधिकरण द्वारा प्रदत्त ऐसी सुविधा से है, जिसके अंतर्गत, हां/ना प्रतिक्रिया या ई-केवाईसी डेटा, यथा लागू, को उपलब्ध कराने के द्वारा अधिप्रमाणन प्रक्रिया के जरिए किसी आधार नंबर धारक की जनसांख्यिकीय सूचना या बायोमेट्रिक जानकारी के साथ आधार नंबर का अधिप्रमाणन किया जाता है।
- (च) **“अधिप्रमाणन अभिलेख”** का अभिप्राय अधिप्रमाणन के समय तथा अनुरोधकर्ता संस्था की पहचान एवं उससे सम्बद्ध प्राधिकरण द्वारा उपलब्ध कराये गए प्रत्युत्तर के अभिलेख से है;
- (छ) **“अधिप्रमाणन सेवा एजेंसी”** अथवा **“एएसए”** का अभिप्राय, ऐसी लाइसेंस प्राप्त संस्था से होगा, जो प्राधिकरण द्वारा उपलब्ध कराई गयी अधिप्रमाणन सुविधा का उपयोग करते हुए अधिप्रमाणन के निष्पादन के संबंध में अनुरोधकर्ता संस्था को समर्थ बनाने के लिए सुरक्षित नेटवर्क संयोजन एवं सम्बद्ध सेवाएं सुनिश्चित करने के लिए आवश्यक अवसंरचना उपलब्ध करा रही है;
- (ज) **“अधिप्रमाणन प्रयोक्ता एजेंसी”** अथवा **“एयूए”** का अभिप्राय उस अनुरोधकर्ता संस्था से है, जो प्राधिकरण द्वारा उपलब्ध कराई गयी हां/ना अधिप्रमाणन सुविधा का उपयोग करती है;
- (झ) **“प्राधिकरण”** का अभिप्राय अधिनियम की धारा 11 की उप-धारा (1) के तहत स्थापित भारतीय विशिष्ट पहचान प्राधिकरण से है;
- (ट) **“केन्द्रीय पहचान डेटा रिपोजिटरी”** अथवा **“सीआईडीआर”** का अभिप्राय एक या अधिक स्थानों पर केन्द्रीकृत डेटाबेस से है, जिसमें आधार नंबर धारक को जारी आधार नंबर के साथ ऐसे व्यक्तियों की जनसांख्यिकीय तथा बायोमेट्रिक सूचना और तत्संबंधी अन्य संबद्ध सूचना अंतर्निहित है;
- (टक) **‘बालक’** का अभिप्राय उस व्यक्ति से है जिसने 18 वर्ष की आयु पूर्ण नहीं की है।
- <sup>4</sup>(टख) **“डिजिटल हस्ताक्षर”** का अभिप्राय सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 2 की उप-धारा (1) के खंड (द) में यथा परिभाषित डिजिटल हस्ताक्षर से है;

<sup>3</sup> अधिसूचना संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2022 का संख्या 1), दिनांक 4.2.2022 द्वारा प्रविष्ट।

<sup>4</sup> अधिसूचना संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2022 का संख्या 1), दिनांक 4.2.2022 द्वारा प्रविष्ट।

- <sup>5</sup>(टग) **“ई-आधार”** का अभिप्राय पासवर्ड से सुरक्षित आधार पत्र की इलेक्ट्रॉनिक प्रति से है, जो प्राधिकरण द्वारा डिजिटल रूप से हस्ताक्षरित है और इसे आधिकारिक वेबसाइट या प्राधिकरण के मोबाइल एप्लिकेशन से डाऊनलोड किया जा सकता है;
- (ठ) **“ई-केवाईसी अधिप्रमाणन सुविधा”** का अभिप्राय एक ऐसी अधिप्रमाणन सुविधा से है, जिसमें अनुरोधकर्ता संस्था के जरिए आधार नंबर धारक की सहमति से बायोमेट्रिक सूचना तथा/अथवा ओटीपी एवं आधार नंबर को सुरक्षित रूप से जमा किया जाता है, जिसका मिलान सीआईडीआर में उपलब्ध डेटा से किया जाता है, और जिस पर प्राधिकरण, अधिप्रमाणन संव्यवहार से संबंधित अन्य तकनीकी विवरण के साथ डिजिटल रूप से हस्ताक्षरित प्रतिकृता युक्त ई-केवाईसी डेटा प्रदान करता है;
- (ड) **“ई-केवाईसी डेटा”** का अभिप्राय किसी आधार नंबर धारक की पूर्ण अथवा सीमित जनसांख्यिकीय सूचना तथा/अथवा फोटोग्राफ से है। ई-केवाईसी डेटा में पूर्ण अथवा मास्क आधार नंबर अंतर्निहित हो सकता है;
- (ढ) **“ई-केवाईसी प्रयोक्ता एजेंसी”** अथवा **“केयूए”** का अभिप्राय उस अनुरोधकर्ता संस्था से है, जो एयूए होने के अतिरिक्त प्राधिकरण द्वारा प्रदान की गयी ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग करती है;
- <sup>6</sup>(ढक) **“एमआधार”** का अभिप्राय प्राधिकरण द्वारा विकसित आधिकारिक मोबाइल एप्लिकेशन से है जो आधार नंबर धारकों को सीआईडीआर के साथ पंजीकृत अपने आधार विवरण को साथ रखने के लिए एक इंटरफ़ेस प्रदान करता है, जिसमें अन्य बातों के साथ-साथ जनसांख्यिकीय जानकारी और आधार नंबर धारक की फोटो के साथ आधार नंबर शामिल है;
- (ण) **“लाइसेंस कुंजी”** से अभिप्राय, प्राधिकरण द्वारा निर्धारित प्रक्रिया के अनुसार अनुरोधकर्ता संस्था द्वारा सृजित कुंजी से है;
- (णक) **‘ऑफलाइन सत्यापन’** का अभिप्राय ऐसे ऑफलाइन विधियों, जैसा विनियमों द्वारा यथा विनिर्दिष्ट हो, के द्वारा अधिप्रमाणन के बिना ‘आधार नंबर धारक’ की पहचान सत्यापन करने की प्रक्रिया से है।
- (णख) **‘ऑफलाइन सत्यापन चाहने वाली संस्था’** का अभिप्राय ऐसी संस्था से है, जो किसी आधार नंबर धारक का ऑफलाइन सत्यापन करना चाहती है;
- (णग) **‘ऑफलाइन आधार डेटा’** का तात्पर्य ऑफलाइन आधार सत्यापन से संबंधित डेटा से है, जिसमें भंडारण से पूर्व आधार नंबरों की मास्किंग की आवश्यकता सहित समय समय पर प्राधिकरण द्वारा यथा विनिर्दिष्ट विशेषताएं शामिल हैं;
- (त) **“पीआईडी ब्लॉक”** का अभिप्राय व्यक्तिगत पहचान डेटा घटक से है, जिसके अन्तर्गत अधिप्रमाणन के दौरान आधार नंबर धारक से संग्रहीत आवश्यक जनसांख्यिकीय तथा/अथवा बायोमेट्रिक और/या ओटीपी शामिल है;
- (तक) **‘पंजीकृत उपकरण’** से तात्पर्य ऐसे बायोमेट्रिक उपकरणों से है जो प्राधिकरण में पंजीकृत हों।

<sup>5</sup> अधिसूचना संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2022 का संख्या 1), दिनांक 4.2.2022 द्वारा प्रविष्ट।

<sup>6</sup> अधिसूचना संख्या के-11020/240/2021/अधि./ भा.वि.प.प्रा.(2022 का संख्या 1), दिनांक 4.2.2022 द्वारा प्रविष्ट।

- (थ) **“अनुरोधकर्ता संस्था”** का अभिप्राय ऐसी एजेंसी या व्यक्ति से है, जो किसी व्यक्ति के आधार नंबर, और जनसांख्यिकीय सूचना या बायोमेट्रिक सूचना केंद्रीय पहचान डेटा रिपोजिटरी को अधिप्रमाणन हेतु प्रस्तुत करता है;
- (थक) **‘सब-एयूए’** का तात्पर्य ऐसी अनुरोधकर्ता संस्था से है, जो विद्यमान एयूए के जरिए प्राधिकरण द्वारा उपलब्ध कराई गई हां/नहीं अधिप्रमाणन सुविधा का उपयोग कर रही है;
- (थख) **‘सब-केयूए’** का तात्पर्य ऐसी अनुरोधकर्ता संस्था से है, जो विद्यमान केयूए के जरिए प्राधिकरण द्वारा उपलब्ध कराई गई ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग कर रही है;
- (थग) **‘यूआईडी टोकन’** का तात्पर्य प्राधिकरण द्वारा सृजित 72 अंकों के अक्षरांकीय क्रम से है, जो आधार नंबर से मैप किया हुआ और किसी अनुरोधकर्ता संस्था के लिए विशिष्ट होता है;
- (थघ) **‘वर्चुअल पहचानकर्ता’** का तात्पर्य अन्तर-परिवर्तनीय 16 अंकीय यादृच्छिक संख्या से है, जो आधार नंबर धारक के आधार नंबर से मैप होती है, और
- (द) **“हां/ना अधिप्रमाणन”** का अभिप्राय एक प्रकार की अधिप्रमाणन सुविधा से है, जिसमें किसी अनुरोधकर्ता संस्था के जरिए आधार नंबर धारक की सहमति द्वारा पहचान संबंधी सूचना एवं आधार नंबर को सुरक्षित रूप से प्रस्तुत किया जाता है और तत्पश्चात उसका मिलान सीआईडीआर में उपलब्ध डेटा से किया जाता है, तथा प्राधिकरण अधिप्रमाणन संव्यवहार से संबंधित अन्य तकनीकी विवरण साथ डिजिटल रूप से हस्ताक्षरित प्रतिक्रिया से युक्त “हां” या “ना” वाले प्रत्युत्तर, पहचान संबंधी सूचना के बिना, प्रदान करता है।
- (2) इन विनियमों में उपयोग किए गए शब्द एवं अभिव्यक्तियां, जिन्हें इन विनियमों में परिभाषित नहीं किया गया है, का वही अर्थ होगा जो कि अधिनियम अथवा उसके तहत बनाए गए नियमों और अन्य विनियमों अथवा सूचना प्रौद्योगिकी अधिनियम, 2000 में परिभाषित किया गया है।

## अध्याय - 2

### आधार अधिप्रमाणन तंत्र

#### 3. अधिप्रमाणन सुविधाओं के प्रकार: -

प्राधिकरण द्वारा दो प्रकार की अधिप्रमाणन सुविधाएं उपलब्ध करायी जाएंगी, नामतः-

- (i) **हां/ना अधिप्रमाणन सुविधा**, जिसका निष्पादन विनियम 4(2) में विनिर्दिष्ट किसी भी माध्यम से किया जा सकता है; तथा
- (ii) **ई-केवाईसी अधिप्रमाणन सुविधा**, जिसका निष्पादन केवल विनियम 4(2) में विनिर्दिष्ट ओटीपी तथा/अथवा बायोमेट्रिक अधिप्रमाणन के जरिए ही किया जा सकता है।

#### 3क. ऑफलाइन सत्यापन के प्रकार:-

1. प्राधिकरण द्वारा निम्नलिखित प्रकार की ऑफलाइन सत्यापन सुविधाएं उपलब्ध कराई जाएंगी, नामतः-

- (i) क्यू आर कोड सत्यापन,
- (ii) आधार कागज रहित ऑफलाइन ई-केवाईसी सत्यापन,
- (iii) ई-आधार सत्यापन,
- (iv) ऑफलाइन कागज आधारित सत्यापन, और
- (v) समय-समय पर प्राधिकरण द्वारा लागू किसी भी अन्य प्रकार का ऑफलाइन सत्यापन।

उपर्युक्त ऑफलाइन सत्यापन किसी संस्था द्वारा समय-समय पर प्राधिकरण द्वारा दिए गए विनिर्देशों के अनुसार किया जा सकता है।

2. प्राधिकरण वेबसाइट, मोबाईल ऐप्लीकेशन या अन्य माध्यमों द्वारा क्यूआर कोड, ई-आधार या आधार कागज रहित ऑफलाइन ई-केवाईसी को डाउनलोड करने हेतु विभिन्न सुविधाएं उपलब्ध कराएगा।

#### 4. अधिप्रमाणन के माध्यम:-

- (1) इन विनियमों के अनुसार तथा प्राधिकरण द्वारा निर्धारित विनिर्देशों के अनुरूप इलेक्ट्रॉनिक रूप में किसी अनुरोधकर्ता संस्था द्वारा प्रेषित किसी अनुरोध को ही प्राधिकरण द्वारा अधिप्रमाणन अनुरोध के रूप में स्वीकार किया जाएगा।
- (2) अधिप्रमाणन को निम्नलिखित माध्यमों द्वारा निष्पादित किया जा सकता है:
  - (क) **जनसांख्यिकीय अधिप्रमाणन:** आधार नंबर धारक से प्राप्त आधार नंबर धारक की जनसांख्यिकीय सूचना और आधार नंबर का मिलान, सीआईडीआर में उपलब्ध आधार नंबर धारक की जनसांख्यिकीय सूचना के साथ किया जाता है।
  - (ख) **वन-टाइम पिन आधारित अधिप्रमाणन:** सीमित समय की वैधता वाले वन टाइम पिन (ओटीपी) को, प्राधिकरण में पंजीकृत अथवा अन्य उपयुक्त साधनों द्वारा सृजित, आधार नंबर धारक के मोबाइल नंबर तथा/अथवा ई-मेल पते पर भेजा जाता है। अधिप्रमाणन के दौरान आधार नंबर धारक इस ओटीपी को अपने आधार नंबर के साथ उपलब्ध करायेगा, जिसका मिलान प्राधिकरण द्वारा सृजित ओटीपी से किया जाएगा।
  - (ग) **बायोमेट्रिक आधारित अधिप्रमाणन:** आधार नंबर धारक द्वारा जमा किया गया आधार नंबर तथा बायोमेट्रिक सूचना का मिलान, सीआईडीआर में संचित आधार नंबर धारक की बायोमेट्रिक सूचना से किया जाता है। यह फिंगरप्रिंट आधारित अथवा पुतली आधारित अधिप्रमाणन अथवा अन्य बायोमेट्रिक पद्धतियों पर आधारित हो सकती है, जो सीआईडीआर में संचित बायोमेट्रिक सूचना के आधार पर होती है।
  - (घ) **बहु-कारक अधिप्रमाणन:** उपर्युक्त विधियों के दो अथवा दो से अधिक संयोजन का उपयोग अधिप्रमाणन के लिए किया जा सकता है।
- (3) कोई अनुरोधकर्ता संस्था अपनी आवश्यकता के अनुसार किसी विशेष सेवा अथवा व्यावसायिक कार्य के लिए उप-विनियम (2) में विनिर्दिष्ट माध्यमों से, वृहत्तर सुरक्षा के लिए, बहु-कारक अधिप्रमाणन सहित, अधिप्रमाणन का उपयुक्त माध्यम चुन सकती है।

#### 4क.वर्चुअल पहचान संख्या (वीआई डी)

- (1) प्राधिकरण अधिप्रमाणन के प्रयोजनार्थ आधार नंबर से जुड़ी हुई एक वैकल्पिक पहचान संख्या (वीआईडी) उपलब्ध कराएगा।
- (2) आधार नंबर धारक अपनी वीआईडी को यूआईडीएआई की वेबसाइट, एसएमएस, मोबाईल ऐप्लीकेशन, ई-आधार डाउनलोड और समय-समय पर प्राधिकरण द्वारा उपलब्ध कराए गए किसी अन्य माध्यम से सृजित कर सकते हैं या उसे पुनः प्राप्त कर सकते हैं।
- (3) ऑनलाइन अधिप्रमाणन या ई-केवाईसी के लिए आधार नंबर धारक, आधार नंबर के स्थान पर वीआईडी का प्रयोग कर सकते हैं।

- (4) कोई भी संस्था अपने सिस्टम में वर्चुअल आईडी को संचित नहीं करेगी।

## 5. आधार नंबर धारक के लिए सूचना :-

- (1) अधिप्रमाणन या ऑफलाइन सत्यापन के समय, क्रमशः अनुरोधकर्ता संस्था या ऑफलाइन सत्यापन मांगकर्ता संस्था (ओवीएसई) आधार नंबर धारक को या बालक के मामले में उसके पिता या माता अथवा संरक्षक, को निम्नलिखित सूचनाएं प्रदान करेगी :-
- (क) सूचना की प्रकृति, जिसे अधिप्रमाणन पर प्राधिकरण द्वारा अनुरोधकर्ता संस्था के साथ साझा किया जाएगा;
- (ख) उपयोग जिसके लिए अधिप्रमाणन या ऑफलाइन सत्यापन के दौरान प्राप्त सूचना का उपयोग किया जा सकता है;
- (ग) पहचान प्रस्तुत करने के विकल्प और व्यवहार्य माध्यम तथा निवासी द्वारा अधिप्रमाणन या ऑफलाइन सत्यापन के लिए इंकार करने या असमर्थ होने की स्थिति में, किसी सेवा से वंचित नहीं किया जाएगा।
- (2) अनुरोधकर्ता संस्था यह सुनिश्चित करेगी कि ऊपर उप-विनियम (1) में संदर्भित सूचना स्थानीय भाषा में भी आधार नंबर धारक को उपलब्ध करायी जायेगी।
- (3) अनुरोधकर्ता संस्था या ओवीएसई यह सुनिश्चित करेगी कि निवासी द्वारा अधिप्रमाणन या ऑफलाइन सत्यापन करने से इंकार करने में असमर्थ होने पर निवासी को किसी भी सेवा से वंचित नहीं किया जाएगा बशर्ते कि उपर्युक्त उप विनियम (1) (ग) के अंतर्गत अनुरोधकर्ता संस्था द्वारा सुझाए गए व्यवहार्य वैकल्पिक माध्यम से निवासी अपनी पहचान सिद्ध करने में समर्थ हो।

## 6. आधार नंबर धारक की सहमति:-

- (1) विनियम 5 के तहत सूचना प्रदान करने के बाद, अनुरोधकर्ता संस्था या ऑफलाइन सत्यापन की मांगकर्ता संस्था (ओवीएसई) अधिप्रमाणन या सत्यापन के लिए आधार नंबर धारक या बालक के मामले में उसके पिता या माता अथवा संरक्षक की सहमति प्राप्त करेगी।
- (2) अनुरोधकर्ता संस्था या ओवीएसई उपर्युक्त उप विनियम (1) में संदर्भित सहमति भौतिक रूप से अथवा विशेषकर इलेक्ट्रॉनिक प्रारूप में प्राप्त करेगी और इस उद्देश्य के लिए प्राधिकरण द्वारा विनिर्दिष्ट तरीके अथवा प्रारूप में प्राप्त सहमति के लॉग अथवा अभिलेख रखेगी।

## 7. अनुरोधकर्ता संस्था द्वारा बायामेट्रिक सूचना ग्रहण करना:-

- (1) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा निर्धारित प्रक्रियाओं और विनिर्देशों के अनुसार प्रमाणित बायामेट्रिक उपकरणों के उपयोग द्वारा आधार नंबर धारक की बायामेट्रिक सूचना को अभिग्रहण करेगी।
- (1क) अधिप्रमाणन के लिए प्रयोग किए जाने वाले सभी बायोमेट्रिक्स उपकरण प्राधिकरण द्वारा समय-समय पर विनिर्दिष्ट मानकों के अंतर्गत पंजीकृत उपकरण होंगे।
- (1ख) सभी बायोमेट्रिक्स उपकरण अनुरोधकर्ता संस्था के सर्वर पर पंजीकृत किए जाएंगे।
- (2) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा निर्धारित विनिर्देशों के अनुरूप बायामेट्रिक डेटा को अभिग्रहण करते समय उसे आवश्यक रूप से कूटबद्ध एवं सुरक्षित करेगी।
- (3) बायामेट्रिक सूचना अभिग्रहण करने में इष्टतम परिणाम हेतु अनुरोधकर्ता संस्था इस उद्देश्य के लिए प्राधिकरण द्वारा समय-समय पर यथा विनिर्दिष्ट प्रक्रियाओं को अपनाएगी।

## 8. अधिप्रमाणन में प्रयुक्त उपकरण, क्लाइंट एप्लीकेशन्स आदि:-

- (1) अधिप्रमाणन के लिए प्रयुक्त समस्त यन्त्र एवं उपकरण इस प्रयोजनार्थ प्राधिकरण द्वारा समय-समय पर जारी विनिर्देशों के अनुसार आवश्यक रूप प्रमाणित किये जाएंगे।
- (2) अधिप्रमाणन के प्रयोजनार्थ अनुरोधकर्ता संस्था द्वारा प्रयोग में लाये जाने वाले क्लाइंट एप्लीकेशन्स अर्थात् सॉफ्टवेयर इस उद्देश्य के लिए समय-समय पर प्राधिकरण द्वारा निर्धारित मानक एपीआई और विनिर्देशों के अनुरूप होंगे।

## 9. अधिप्रमाणन अनुरोध भेजने की प्रक्रिया:-

- (1) अनुरोधकर्ता संस्था द्वारा प्रदान आधार नम्बर अथवा कोई अन्य पहचानकर्ता, जो आधार नंबर और आधार नंबर धारक से आवश्यक जनसांख्यिकीय तथा/अथवा बायोमेट्रिक सूचना और/या ओटीपी से मैप है, के संग्रहण के पश्चात् प्राधिकरण द्वारा निर्धारित विनिर्देशों के अनुसार क्लाइंट एप्लीकेशन तुरन्त किसी हस्तांतरण से पूर्व इन इनपुट पैरामीटरों को पीआईडी ब्लॉक में पैकेज और कूटबद्ध करेगा, और इस प्रयोजनार्थ प्राधिकरण द्वारा यथा निर्धारित सुरक्षा प्रोटोकॉल के उपयोग द्वारा उसे अनुरोधकर्ता संस्था के सर्वर के पास भेज देगा।
- (2) विधिमान्यकरण के उपरान्त, अनुरोधकर्ता संस्था का सर्वर प्राधिकरण द्वारा निर्धारित विनिर्देशों के अनुसार अधिप्रमाणन सेवा एजेंसी के सर्वर के माध्यम से अधिप्रमाणन अनुरोध को सीआईडीआर को भेज देगा। अधिप्रमाणन अनुरोध को अनुरोधकर्ता संस्था तथा/अथवा अधिप्रमाणन सेवा एजेंसी द्वारा, उनके पारस्परिक समझौते के अनुसार, डिजिटल रूप से हस्ताक्षरित होगा।
- (3) अधिप्रमाणन अनुरोध के माध्यम के आधार पर, सीआईडीआर अपने पास संचित डेटा के समक्ष इनपुट पैरामीटर का विधिमान्य करेगा और डिजिटल रूप से हस्ताक्षरित 'हां' या 'ना' अधिप्रमाणन प्रत्युत्तर, अथवा कूटबद्ध ई-केवाईसी डेटा सहित डिजिटल रूप से हस्ताक्षरित ई-केवाईसी, जैसी स्थिति हो, को अधिप्रमाणन संव्यवहार से सम्बद्ध अन्य तकनीकी विवरण के साथ वापस करेगा।
- (4) अधिप्रमाणन की सभी विधियों में, आधार नंबर अनिवार्य है और इसे उपर्युक्त उप-विनियम (1) में विनिर्दिष्ट इनपुट पैरामीटरों के साथ इस प्रकार जमा किया जाता है कि अधिप्रमाणन सदैव 1: 1 के मिलान के अनुसार रहे।
- (5) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि प्राधिकरण द्वारा निर्धारित विनिर्देशों एवं प्रक्रियाओं के अनुसार अधिप्रमाणन उपकरण द्वारा अभिग्रहण करते समय पीआईडी ब्लॉक का एन्क्रिप्शन होता रहे।

## 10. आधार नंबर धारक को अधिप्रमाणन या ऑफलाइन सत्यापन की अधिसूचना/अभिस्वीकृति:-

- (1) किसी भी अधिप्रमाणन के संबंध में अनुरोधकर्ता संस्था द्वारा आधार नंबर धारक को ई-मेल और/या एसएमएस और/या अन्य डिजिटल माध्यमों से और/या लिखित अभिस्वीकृति के आधार पर अधिप्रमाणन के प्रत्येक अनुरोध के सफल या असफल होने की अधिसूचना प्रदान की जाएगी। ऐसी अधिसूचना/अभिस्वीकृति में, जैसा मामला हो, अनुरोधकर्ता संस्था का नाम, तिथि, अधिप्रमाणन का समय, अधिप्रमाणन प्रत्युत्तर कोड, आधार नंबर के अंतिम 4 अंक और अधिप्रमाणन का उद्देश्य दिया जाएगा।
- (2) किसी भी ऑफलाइन सत्यापन के लिए आधार नंबर धारक को ओवीएसवी द्वारा ई-मेल और/या एसएमएस और/या अन्य डिजिटल माध्यमों से और/या लिखित अभिस्वीकृति के आधार पर प्रत्येक ऑफलाइन सत्यापन अनुरोध के सफल या असफल होने की अधिसूचना प्रदान की जाएगी।

(3) अधिप्रमाणन के असफल हो जाने के मामलों में, अनुरोधकर्ता संस्था निवासी को स्पष्ट एवं सहज भाषा में अधिप्रमाणन के असफल होने के कारणों जैसे स्थगित/रद्द आधार या बायोमेट्रिक्स/आधार लॉकिंग की सूचना प्रदान करेगी।

#### 11. बायोमेट्रिक लॉकिंग:-

- (1) प्राधिकरण आधार नंबर धारक को उसके बायोमेट्रिक को स्थायी तौर पर लॉक करने तथा आवश्यकतानुसार बायोमेट्रिक अधिप्रमाणन हेतु अस्थायी तौर पर अनलॉक करने की सुविधा दे सकता है।
- (2) ऐसे लॉक किए गए बायोमेट्रिक अभिलेख के समक्ष समस्त बायोमेट्रिक अधिप्रमाणन एक उचित प्रत्युत्तर कोड सहित “नहीं” विकल्प के साथ असफल होंगे।
- (3) आधार नंबर धारक को अधिप्रमाणन हेतु अपने बायोमेट्रिक को अस्थायी तौर पर अनलॉक करने की अनुमति दी जाएगी और ऐसी अस्थायी अनलॉकिंग, प्राधिकरण द्वारा निर्दिष्ट समयावधि के पश्चात अथवा अधिप्रमाणन संव्यवहार की पूर्णता तक, जो भी पहले हो, जारी नहीं रहेगी।
- (4) प्राधिकरण आधार नंबर धारक के लिए किसी भी समय ऐसे स्थायी लॉकिंग को सुरक्षित तरीके से समाप्त करने का प्रावधान करेगा।

#### 11क आधार लॉकिंग:-

- (1) प्राधिकरण आधार नंबर धारक को अपने आधार नंबर को लॉक करने तथा अधिप्रमाणन के लिए आवश्यक होने पर अनलॉक करने की सुविधा प्रदान करेगा।
- (2) ऐसे लॉक किए गए आधार नंबर के समक्ष किए गए सभी अधिप्रमाणन अनुरोधों का उत्तर ‘नहीं’ होगा और साथ ही उपयुक्त प्रतिक्रिया कोड दिया जाएगा।
- (3) आधार लॉक होने पर प्राधिकरण निवासी को वर्चुअल आईडी या अन्य माध्यमों से अधिप्रमाणन की अनुमति प्रदान करेगा।

### अध्याय - 3

#### अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की नियुक्ति

#### 12. अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की नियुक्ति :-

- <sup>7</sup>[(1) किसी अधिप्रमाणन सुविधा के उपयोग के लिए अनुरोधकर्ता संस्था के रूप में नियुक्ति चाहने वाली एजेंसी या अन्य व्यक्ति नियुक्ति के लिए प्राधिकरण को ऐसे प्रपत्र में आवेदन करेगा जैसा कि प्राधिकरण द्वारा ऐसी एजेंसी या व्यक्ति के द्वारा उसे किए गए अनुरोध पर उपलब्ध कराया जाए :

परंतु यह कि ऐसी एजेंसी या व्यक्ति अनुरोधकर्ता संस्था के रूप में नियुक्ति होने पर, केवल ऐसे प्रयोजन के लिए अधिप्रमाणन करेगी जैसे कि-

(क) उप-धारा (4) के तहत अनुज्ञात की गई है या वह अधिनियम की धारा 4 की उप-धारा (7) में संदर्भित किसी भी विधि के अंतर्गत अपेक्षित है; या

---

<sup>7</sup> विनियम 12 (1) को अधिसूचना संख्या एच क्यू-13073/1/2020/अधि.-II (अ), दिनांक 29.9.2023 (दिनांक 3.10.2023 से प्रभावी) द्वारा प्रतिस्थापित किया गया, प्रतिस्थापन से पहले विनियम 12(1), इस प्रकार था:

“(1) प्राधिकरण द्वारा प्रावधानित अधिप्रमाणन सुविधाओं के उपयोग के लिए अनुरोधकर्ता संस्था बनने की इच्छुक एजेंसियां, प्राधिकरण द्वारा इस उद्देश्य हेतु समय समय पर विनिर्दिष्ट प्रक्रिया अनुसार अनुरोधकर्ता संस्था के रूप में नियुक्ति हेतु आवेदन करेंगी, बशर्त की प्रमाणीकरण सेवाओं की आवश्यकता जिन उद्देश्यों हेतु हो, वो अधिनियम की धारा 4 (4) (b) (i) अथवा 4 (4) (b) (ii) अथवा 4 (7) अथवा 7 के प्रावधानों के तहत अनुमत हों।”

(ख) अधिनियम की धारा 7 के तहत केंद्र सरकार या राज्य सरकार द्वारा अपेक्षित है।]

- (1क) अनुरोधकर्ता संस्था तथा एएसए समय-समय पर प्राधिकरण द्वारा यथा विनिर्दिष्ट तकनीकी एवं सुरक्षा मानदंडों को पूरा करेंगी।
- <sup>8</sup>[(2) किसी अधिप्रमाणन सुविधा के उपयोग के लिए एएसए के रूप में नियुक्ति चाहने वाली संस्था नियुक्ति के लिए प्राधिकरण को ऐसे प्रपत्र में आवेदन करेगी जैसा कि प्राधिकरण द्वारा ऐसी संस्था के द्वारा उसे किए गए अनुरोध पर उपलब्ध कराया जाए।
- (2क) एएमए के रूप में नियुक्ति चाहने वाली संस्था अनुसूची क में विनिर्दिष्ट मानदंडों की पूर्ति करेगी।]
- (3) प्राधिकरण ऐसी आवेदक संस्था अथवा अधिप्रमाणन सेवा एजेंसियों, जैसी भी स्थिति हो, की गतिविधियों से सम्बद्ध मामलों के संबंध में आवेदक से अन्य सूचना अथवा स्पष्टीकरण का उल्लेख करने के लिए कह सकता है, जिसे आवेदन पर विचार करने और निपटान करने के लिए प्राधिकरण द्वारा विचारार्थ लिया जा सकता है।
- (4) आवेदक, प्राधिकरण द्वारा इस संबंध में यथा विनिर्दिष्ट समय के अन्दर, प्राधिकरण की संतुष्टि के अनुरूप ऐसी सूचना तथा स्पष्टीकरण को प्रस्तुत करेगा।
- (5) आवेदन पर विचार करते समय, आवेदक द्वारा प्रस्तुत की गयी सूचना और उसकी पात्रता को प्राधिकरण दस्तावेजों, अवसरचना एवं तकनीकी सपोर्ट, जिन्हें आवेदक के पास होना आवश्यक है, के प्रत्यक्ष सत्यापन द्वारा स्थापित कर सकता है।
- (6) आवेदक द्वारा प्रस्तुत किये गए आवेदन, दस्तावेजों तथा उसकी पात्रता के सत्यापन के पश्चात प्राधिकरण:
- (क) अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी के आवेदन, जो भी स्थिति हो, को अनमोदित कर सकता है; तथा
- (ख) संस्था अथवा एजेंसी के साथ प्राधिकरण की अधिप्रमाणन सुविधा के अनुरोधकर्ता संस्थाओं द्वारा उपयोग के लिए, या एएसए द्वारा सेवाओं के प्रावधान हेतु, दायित्वों के गैर-निष्पादन की स्थिति में क्षतियों तथा हतोत्साहन सहित, निबंधन एवं शर्तों को शामिल करते हुए उपयुक्त अनुबंध कर सकती है।
- (7) प्राधिकरण, समय-समय पर संस्थाओं द्वारा उनकी नियुक्ति के दौरान उनके द्वारा देय शुल्क एवं प्रभार सहित आवेदन शुल्क, वार्षिक सदस्यता शुल्क तथा वैयक्तिक अधिप्रमाणन संव्यवहार के लिए शुल्क निर्धारित कर सकता है।
- (8) प्राधिकरण समय-समय पर ऐसी अनुरोधकर्ता संस्थाओं को नियत करेगा जिन्हें आधार नंबर या मास्क किए गए आधार नंबर के संचयन की अनुमति होगी।
- (9) प्राधिकरण समय-समय पर, विशेष अनुरोधकर्ता संस्थाओं को ई-केवाईसी प्रतिक्रिया के रूप में उपलब्ध डेटा फ़ील्ड के सम्बंध में निर्णय लेगा।

---

<sup>8</sup> विनियम 12 (1) को अधिसूचना संख्या एच क्यू-13073/1/2020/अधि.-II (अ), दिनांक 29.9.2023 (दिनांक 3.10.2023 से प्रभावी) द्वारा प्रतिस्थापित किया गया, प्रतिस्थापन से पहले विनियम 12(1), इस प्रकार था:

“(2) अधिप्रमाणन सेवा एजेंसियों के रूप में नियुक्ति चाहने वाली संस्थाएं इस उद्देश्य के लिए प्राधिकरण द्वारा यथा विनिर्दिष्ट प्रक्रिया के अनुरूप नियुक्ति के लिए आवेदन करेंगी। केवल अनुसूची ‘क’ के मानदंडों को पूरा करने वाली संस्थाएं ही आवेदन करने की पात्र होंगी। प्राधिकरण आदेश द्वारा समय-समय पर अनुसूची ‘क’ में संशोधन कर सकता है, ताकि पात्रता मानदंड को संशोधित किया जा सके।”

- (10) प्राधिकरण समय-समय पर यह निर्धारित करेगा कि अनुरोधकर्ता संस्था को अधिप्रमाणन हेतु आधार नंबर या वर्चुअल आईडी या यूआईडी टोकन या एएनसीएस या किसी अन्य पहचान माध्यम की अनुमति प्रदान की जा सकती है।

**13. प्रक्रिया, जहां नियुक्ति के लिए आवेदन अनुमोदित नहीं है:-**

- (1) यदि, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी, जैसी स्थिति हो, की नियुक्ति के लिए आवेदन प्राधिकरण द्वारा विनिर्दिष्ट अपेक्षाओं को सन्तुष्ट नहीं करने पर प्राधिकरण आवेदन निरस्त कर सकता है।
- (2) आवेदन निरस्त करने के प्राधिकरण के निर्णय की सूचना आवेदक को इस निर्णय के तीस दिनों के अंदर लिखित रूप में दे दी जाएगी, जिसमें उसके आवेदन को निरस्त करने के कारणों का उल्लेख किया जाएगा।
- (3) कोई भी आवेदक जो प्राधिकरण के निर्णय से असन्तुष्ट है, इस सूचना की प्राप्ति की तिथि के तीस दिनों के अंदर निर्णय पर पुनर्विचार करने के लिए प्राधिकरण के पास आवेदन कर सकता है।
- (4) प्राधिकरण, आवेदक द्वारा भेजे गये आवेदन पर पुनर्विचार करेगा और इससे संबंधित निर्णय को यथाशीघ्र आवेदक को लिखित रूप में सूचित करेगा।

**14. अनुरोधकर्ता संस्थाओं की भूमिका तथा उत्तरदायित्व:-**

- (1) अनुरोधकर्ता संस्था को निम्नलिखित कार्य एवं उत्तरदायित्वों का निर्वहन करना होगा:
- (क) अधिप्रमाणन से संबंधित स्वयं के तंत्र, प्रक्रियाओं, अवसंरचना, तकनीक, सुरक्षा आदि सहित आवश्यक प्रचालनों का संस्थापन एवं अनुरक्षण करना;
- (ख) अधिप्रमाणन अनुरोधों को भेजने के लिए प्राधिकरण द्वारा अनुमोदित एएसए के माध्यम से सीआईडीआर के साथ नेटवर्क कनेक्टिविटी सुनिश्चित करना;
- (ग) यह सुनिश्चित करना कि अधिप्रमाणन अनुरोधों को भेजने के लिए प्रयुक्त अधिप्रमाणन उपकरणों तथा सीआईडीआर के मध्य नेटवर्क कनेक्टिविटी इस उद्देश्य के लिए प्राधिकरण द्वारा निर्धारित मानकों एवं विशिष्टियों के अनुरूप है;
- (गक) यह सुनिश्चित करना कि निवासी द्वारा अधिप्रमाणन अनुरोध के लिए उपलब्ध कराए गए आधार नंबर /वर्चुअल आई डी/एएनसीएस टोकन को उपकरण ऑपरेटर द्वारा अपने पास या उपकरण के अंदर या एयूए सर्वर में न रख लिया जाए।
- (गख) यह सुनिश्चित करना कि वर्चुअल आईडी का प्रयोग करते हुए अधिप्रमाणन के प्रावधान को उपलब्ध कराया जाए।
- (घ) केवल उन्हीं यन्त्रों, उपकरण, अथवा सॉफ्टवेयर का उपयोग करना जो आवश्यक रूप से प्राधिकरण द्वारा पंजीकृत या अनुमोदित अथवा प्रमाणित या प्राधिकरण द्वारा विनिर्दिष्ट हैं और इस उद्देश्य हेतु प्राधिकरण द्वारा निर्धारित मानकों और विनिर्देशों के अनुरूप हैं;
- (च) इस संबंध में प्राधिकरण द्वारा समय-समय पर जारी एवं सूचित नियमों एवं शर्तों, मानकों, निर्देशों तथा विनिर्देशों के लिए अपने यंत्रों तथा उपकरणों के प्रचालन की आवधिक आधार पर निगरानी करना;
- (छ) यह सुनिश्चित करना कि अधिप्रमाणन कार्यों के निष्पादन, तथा आवश्यक तंत्रों, अवसंरचना एवं प्रक्रियाओं के अनुरक्षण के लिए उसके द्वारा नियुक्त कर्मचारियों के पास ऐसे कार्यों के निष्पादन की अपेक्षित योग्यता है;

- (ज) एएसए, जिसके साथ उसका समझौता हुआ है, के विषय में प्राधिकरण को सूचित रखना;
- (जक) किसी तृतीय पक्ष संस्था को सब-एयूए/सब-केयूए के रूप में नियुक्त करने से पूर्व प्राधिकरण से अनुमित प्राप्त करना।
- (झ) यह सुनिश्चित करना कि उसके प्रचालन तथा तंत्र प्राधिकरण के मानकों तथा विनिर्देशों के अनुरूप हैं, जिसे सुनिश्चित करने के लिए किसी प्रतिष्ठित निकाय द्वारा प्रमाणित सूचना पद्धति लेखापरीक्षक द्वारा वार्षिक आधार पर लेखापरीक्षा करवाई गयी है और अनुरोध किए जाने पर लेखापरीक्षा रिपोर्ट प्राधिकरण के साथ साझा करनी होगी;
- (ट) निवासियों को अधिप्रमाणन सेवाओं के निर्बाध प्रावधान सुनिश्चित करने के लिए अपवाद संचलन क्रियाविधि तथा बैक-अप पहचान अधिप्रमाणन क्रियाविधि कार्यान्वित करना;
- (ठ) अधिप्रमाणन से सम्बद्ध धोखाधड़ी अथवा विवाद सम्बन्धी किसी जांच की स्थिति में वह प्राधिकरण, अथवा इसके द्वारा नियुक्त या प्राधिकृत किसी एजेंसी अथवा किसी अन्य प्राधिकृत जांच एजेंसी का पूर्ण सहयोग करेगी और अपने परिसर, अभिलेख, कार्मिक तथा किसी अन्य संसाधन या सूचना तक उनकी पहुंच बनाने का प्रावधान करेगी। इसके साथ-साथ किसी भी आधार डेटा से संबंधित धोखाधड़ी के संबंध में जन सामान्य को सूचना प्रदान करने के लिए प्राधिकरण का सहयोग करेगी, ताकि आधार नंबर धारक यह तय कर सके कि कहीं वे किसी धोखाधड़ी का शिकार तो नहीं हो गए हैं और वे निवारक कार्रवाई कर सकें।
- (ड) अनुरोधकर्ता संस्था द्वारा अपनी आधार अधिप्रमाणन प्रणाली को स्थानीय अधिप्रमाणन प्रणाली के साथ एकीकृत करने की इच्छा रखने की स्थिति में, ऐसे प्रक्रिकरण को समय-समय पर प्राधिकरण द्वारा जारी मानकों तथा विनिर्देशों के अनुरूप निष्पादित करना होगा;
- (ढ) वे प्राधिकरण को अपने नेटवर्क के भीतर आधार संबंधी सूचना अथवा तंत्र के आधार फ्रेमवर्क अथवा किसी अन्य समझौते से सम्बद्ध किसी सूचना अथवा तंत्र के किसी दुरुपयोग के विषय में सूचित करेगी; यदि अनुरोधकर्ता संस्था धोखाधड़ी की शिकार है अथवा उसे आधार प्रमाणीकरण से संबंधित धोखाधड़ी जांच प्रणाली के माध्यम से किसी धोखाधड़ी की जानकारी प्राप्त होती है, वे उस धोखाधड़ी से संबंधित समस्त जानकारी प्राधिकरण को साझा करेंगी। वे उस धोखाधड़ी से संबंधित समस्त जानकारी बिना अनावश्यक विलम्ब के प्राधिकरण को और प्रभावित आधार नंबर धारक को साझा करेंगी।
- (ण) वे अधिप्रमाणन प्रचालनों तथा परिणामों के लिए उत्तरदायी होंगी, भले ही अपने प्रचालनों को तीसरे पक्षों के साथ उप-अनुबन्धित किया हो। अनुरोधकर्ता संस्था यह सुनिश्चित करने के लिए भी उत्तरदायी होगी कि ऐसे तीसरे पक्ष की संस्थाओं के अधिप्रमाणन से सम्बन्धित प्रचालन प्राधिकरण के मानकों एवं विनिर्देशों के अनुरूप हैं और उनकी अनुमोदित स्वतन्त्र लेखापरीक्षा एजेंसियों द्वारा नियमित लेखापरीक्षा करवाई गयी है;
- (णक) ऐसे ग्राहकों के साथ, अपने ग्राहकों को अधिप्रमाणन सेवाएं उपलब्ध कराने के लिए अधिप्रमाणन प्रभारों हेतु सहमत हो सकती है और फिलहाल प्राधिकरण का इस संबंध में कोई नियंत्रण नहीं होगा; किन्तु भविष्य में इस संबंध में प्राधिकरण को एक भिन्न क्रियाविधि निर्धारित करने का अधिकार सुरक्षित होगा;
- (णख) भौतिक रूप से प्राप्त की गई आधार नंबर या आधार पत्रों की फोटो प्रतियों को अनुरोधकर्ता संस्था द्वारा संचित करने से पूर्व आधार नंबर के पहले 8 अंकों को छुपाते हुए मास्क किया जाएगा।

- (त) वे प्रत्येक समय प्राधिकरण द्वारा प्रदान की कई अधिप्रमाणन सुविधाओं के उपयोग के प्रयोजनार्थ प्राधिकरण द्वारा जारी अनुबन्धित शर्तों एवं समस्त नियमों, विनियमों, नीतियों, नियमावलियों, प्रक्रियाओं, विनिर्देशों, मानकों तथा निर्देशों का पालन करेंगी।
- (थ) प्राधिकरण से विशेष अनुमति प्राप्त करेंगी और प्राधिकरण के साथ उपयुक्त अनुबंध पर हस्ताक्षर करेंगी, यदि गैर -अधिप्रमाणन उद्देश्यों के लिए आधार नंबर का संचयन अपेक्षित है। आधार नंबर को प्राधिकरण द्वारा समय समय पर यथा विनिर्दिष्ट सुरक्षित तरीके से संचित करना होगा।
- (द) अधिप्रमाणन में प्रयोग किए जाने वाले डेटा की प्रकृति, दुरुपयोग के क्षेत्र और ऐसे दुरुपयोगों या धोखाधड़ी से बचाव के कदम उठाने के लिए आधार नंबर धारकों की जानकारी के लिए प्राधिकरण द्वारा चलाए जाने वाले किसी भी व्यापक जागरूकता कार्यक्रम में प्राधिकरण को पूर्ण सहयोग प्रदान करेंगी।

#### 14क. ऑफलाइन सत्यापन मांगकर्ता संस्थाओं के दायित्व:-

(1) ओवीएसई के निम्नलिखित दायित्व होंगे:-

- (क) आधार अधिनियम और उसके अन्तर्गत बनाए गए विनियमों एवं संबंधित नीतियों, मैनुअल, प्रक्रियाओं, विनिर्देशों, मानक एवं प्राधिकरण द्वारा जारी निर्देशों का अनुपालन सुनिश्चित करना।
- (ख) किसी भी व्यक्ति विशेष के आधार नंबर या बायोमेट्रिक सूचना को किसी भी उद्देश्य के लिए एकत्र, उपयोग एवं संचित नहीं किया जाएगा तथा ऑफलाइन आधार डेटा को अधिनियम एवं उसके अन्तर्गत निर्मित विनियमों के अन्यत्र किसी अन्य संस्था को साझा नहीं किया जाएगा।
- (ग) आधार डेटा से संबंधित धोखाधड़ी या विवाद की जांच के मामलों में संस्था प्राधिकरण को या उनके द्वारा नियुक्त अथवा प्राधिकृत किसी एजेन्सी को या किसी अन्य प्राधिकृत जांच एजेन्सी को पूर्ण सहयोग प्रदान करेगी और उन्हें अपने परिसर, रिकार्ड, कार्मिकों एवं अन्य किसी संगत संसाधन या सूचना तक पहुंच प्रदान करेगी। इसके साथ साथ आधार डेटा से संबंधित धोखाधड़ी के संबंध में जन सामान्य के लिए सूचना जारी करने में प्राधिकरण की सहायता करेगी ताकि आधार नंबर धारक यह सुनिश्चित कर सके कि कहीं वह धोखाधड़ी का शिकार तो नहीं हो गया है और साथ ही उपचारी कार्रवाई सुनिश्चित कर सके।
- (घ) किसी भी सूचना के दुरुपयोग या आधार फ्रेमवर्क से संबंधित प्रणाली या आधार संबंधित सूचना के दुरुपयोग का पता लगने पर प्राधिकरण को बिना किसी अनावश्यक विलम्ब के और हर हालत में 72 घंटे के अंदर सूचित करना होगा। यदि ओवीएसई धोखाधड़ी से पीड़ित है या ऑफलाइन सत्यापन से संबंधित धोखाधड़ी विश्लेषण प्रणाली के माध्यम से किसी धोखाधड़ी के तरीके की पहचान होती है तो वह धोखाधड़ी से संबंधित सभी आवश्यक सूचना को प्राधिकरण के साथ साझा करेगी और बिना किसी विलंब के आधार नंबर धारक को भी सूचित करेगी।
- (च) ऑफलाइन सत्यापन प्रचालन और परिणामों के लिए उत्तरदायी होगी चाहे अपने प्रचालन के कुछ भाग को तृतीय पार्टी को उप-अनुबंधित कर दिया हो। इसके अलावा ओवीएसई यह भी सुनिश्चित करेगी कि पार्टी को दिए गए ऑफलाइन सत्यापन से संबंधित प्रचालनों में उक्त संस्थाएं प्राधिकरण के मानकों एवं विनिर्देशों का अनुपालन सुनिश्चित करेगी।
- (छ) ऑफलाइन सत्यापन में प्रयोग की जा रही डेटा की प्रकृति, दुरुपयोग की गुंजाइश और ऐसे दुरुपयोगों या धोखाधड़ी से बचाव के लिए कदम के संबंध में आधार नंबर धारकों को जागरूक करने के लिए प्राधिकरण द्वारा चलाए जाने वाले व्यापक जागरूकता कार्यक्रमों में प्राधिकरण को पूरा सहयोग देना।

## 15. हां/ना अधिप्रमाणन सुविधा का उपयोग:-

- (1) अनुरोधकर्ता संस्था, अपने निजी उपयोग अथवा अन्य एजेंसियों की ओर से किसी आधार नंबर धारक की पहचान के सत्यापन के लिए प्राधिकरण की हां/ना अधिप्रमाणन सुविधा का उपयोग कर सकती है।
- (2) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा स्थापित पोर्टल या अन्य किसी तंत्र के माध्यम से किसी अन्य एजेंसी अथवा संस्था को, प्रत्येक ऐसी संस्था के लिए एक अलग से लाइसेंस कुंजी के सृजन तथा सहभागिता करने के द्वारा कथित संस्था को हां/ना अधिप्रमाणन निष्पादन के लिए अनुमति दे सकती है। सन्देह के निराकरण के लिए, यह स्पष्ट किया जाता है कि लाइसेंस कुंजी की ऐसी सहभागिता की अनुमति केवल हां/ना अधिप्रमाणन के निष्पादन के लिए ही है और ई-केवाईसी अधिप्रमाणन की स्थिति में निषिद्ध है।
- (3) ऐसी एजेंसी अथवा संस्था:
  - (क) किसी उद्देश्य के लिए किसी अन्य व्यक्ति अथवा संस्था के साथ लाइसेंस कुंजी साझा नहीं करेगी; तथा
  - (ख) आधार नंबर धारक की व्यक्तिगत सूचना, डेटा सुरक्षा एवं अनुरोधकर्ता संस्था के लिए प्रयोज्य अन्य प्रासंगिक उत्तरदायित्वों से सम्बद्ध समस्त दायित्वों का अनुपालन करेगी
- (3क) आधार अनुप्रमाणन के लिए एयूए/केयूए/सब-एयूए/सब-केयूए अपने क्लाइंट ऐप्लीकेशन का प्रयोग करेंगी, जिसे अनुरोधकर्ता संस्था द्वारा डिजिटल रूप में हस्ताक्षरित किया जाएगा।
- (4) यह सुनिश्चित करना अनुरोधकर्ता संस्था का उत्तरदायित्व होगा कि कोई संस्था अथवा एजेंसी जिसके साथ उसने लाइसेंस कुंजी सहभाजित की है, प्राधिकरण के अधिनियम के प्रावधानों, विनियमों, प्रक्रियाओं, मानकों, दिशानिर्देशों, विनिर्देशों तथा प्रोटोकॉल के उपबन्धों का अनुपालन करे, जो अनुरोधकर्ता संस्था पर लागू हैं।
- (5) अनुरोधकर्ता संस्था, प्राधिकरण के विनियमों, प्रक्रियाओं, मानकों, दिशानिर्देशों तथा प्रोटोकॉल के अनुपालन के लिए उस संस्था या एजेंसी के साथ संयुक्त तथा पृथक् रूप से उत्तरदायी होगी, जिसके साथ लाइसेंस कुंजी को साझा किया गया है।

## 16. ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग:-

- (1) केयूए अपने स्वयं के उद्देश्यों के लिए आधार नंबर धारक का ई-केवाईसी डेटा प्राप्त करने के लिए प्राधिकरण द्वारा प्रदत्त ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग कर सकता है।
- (2) सब-केयूए के साथ ई-केवाईसी डेटा साझा करने के लिए केयूए प्राधिकरण से विशेष अनुमति के लिए आवेदन प्रस्तुत करेगी और आधार नंबर धारक की विशिष्ट सहमति के साथ ऐसे डेटा समय-समय पर प्राधिकरण द्वारा जारी दिशानिर्देशों के अनुसार कूटबद्ध रूप में साझा किए जाएंगे।
- (3) जिस सब-केयूए के साथ केयूए ने आधार नंबर धारक के ई-केवाईसी डेटा साझा किए हैं वह इन्हें किसी अन्य संस्था या एजेंसी के साथ आगे साझा नहीं करेगी।
- (4) आधार नंबर धारक किसी भी समय केयूए/सब-केयूए को अपने ई-केवाईसी डेटा को संचित करने के लिए दी गई सहमति को वापस ले सकता है। सहमति वापस लेने के उपरान्त केयूए/सब-केयूए सत्यापन के आधार पर ई-केवाईसी डेटा को समाप्त कर देगा तथा इसकी पावती आधार नंबर धारक को उपलब्ध कराई जाएगी।
- (5) उप-विनियम (3) में उल्लिखित भावी सहभागिता के प्रतिबंध के अतिरिक्त, आधार नंबर धारक व्यक्तिगत सूचना से सम्बन्धित अन्य समस्त दायित्व, अनुरोधकर्ता संस्थाओं के लिए लागू डेटा सुरक्षा एवं अन्य सम्बन्धित

उत्तरदायित्व उन सब केयूए के लिए भी लागू होंगे, जिनके साथ विनियम 16 के अनुरूप ई-केवाईसी डेटा साझा किया जा चुका है।

- (6) केयूए ऐसे सभी संव्यवहारों का प्राधिकरण द्वारा विनिर्दिष्ट समयावधि के लिए एक लेखापरीक्षणीय संलेख अनुरक्षित करेगा, जहां डेटा अन्य सब-केयूए के साथ साझा किया गया है।

#### **16क ऑफलाइन सत्यापन सुविधा का उपयोग:-**

- (1) आधार नंबर धारक के ऑफलाइन आधार डेटा को प्राप्त करने के लिए प्राधिकरण द्वारा उपलब्ध कराई गई ऑफलाइन सत्यापन सुविधा का उपयोग ओवीएसई द्वारा केवल उन उद्देश्यों के लिए किया जाए जिन्हें सत्यापन के समय आधार नंबर धारक को निर्दिष्ट कर दिया गया हो।
- (2) किसी अन्य संस्था या व्यक्ति की ओर से कोई संस्था ऑफलाइन सत्यापन नहीं करेगी।
- (3) ओवीएसई ऑफलाइन सत्यापन के समय आधार नंबर धारक से प्राप्त आधार डेटा को आधार नंबर धारक की सहमति से, समय-समय पर प्राधिकरण द्वारा जारी दिशानिदेशों के अनुसार सुरक्षित रूप से संचयित करेगी।
- (4) आधार नंबर धारक किसी भी समय ओवीएसई को अपने ऑफलाइन आधार डेटा को संचित करने के लिए दी गई सहमति को वापिस ले सकता है। सहमति वापिस लेने की स्थिति में ओवीएसई सत्यापित किए जा सकने वाले रूप में ऑफलाइन आधार डेटा को समाप्त कर देगी और इसकी पावती आधार नंबर धारक को उपलब्ध कराई जाएगी।
- (5) चूक या अतिक्रमण या विधि में परिवर्तन या किसी अन्य कारण से, जो प्राधिकरण को संगत लगता है तो वह ओवीएसई को ऑफलाइन सत्यापन सेवाओं के उपयोग को समाप्त करने के निर्देश दे सकती है।

#### **9[16ख. आधार नंबर के स्वैच्छिक उपयोग का ढंग:-**

(1) आधार नंबर धारक, अधिनियम कि धारा 4 कि उप-धारा (3) के अनुसार, आधार पत्र (या उसकी प्रति) अथवा मुद्रित ई-आधार या आधार पीवीसी सहित भौतिक रूप में आधार नंबर का स्वेच्छा से ऑफलाइन सत्यापन के लिए अपनी पहचान को स्थापित करने के लिए किसी वैध प्रयोजन हेतु उपयोग कर सकता है तथा ऑफलाइन सत्यापन मांगकर्ता संस्था (ओवीएसई) डिजिटल रूप से हस्ताक्षरित आधार सुरक्षित क्यूआर कोड द्वारा आधार पत्र या मुद्रित ई-आधार अथवा आधार पीवीसी कार्ड पर मुद्रित विवरण को सत्यापित करेगी।

(2) आधार नंबर धारक, अधिनियम कि धारा 4 कि उप-धारा (3) के अनुसार, ऑफलाइन सत्यापन के द्वारा अपनी पहचान स्थापित करने के लिए किसी वैध प्रयोजन हेतु ई-आधार या आधार कागजरहित ऑफलाइन ई-केवाईसी (एक्सएमएल) अथवा एमआधार सहित, इलेक्ट्रॉनिक रूप में आधार नंबर का स्वेच्छा से उपयोग कर सकता है तथा ऑफलाइन सत्यापन मांगकर्ता संस्था (ओवीएसई) डिजिटल रूप से हस्ताक्षर को सत्यापित करेगी।

(3) आधार नंबर धारक, अधिनियम की धारा 4 की उप-धारा (3) के अनुसार, अधिकृत अनुरोधकर्ता संस्था के माध्यम से हाँ/नहीं या ई-केवाईसी अधिप्रमाणन सुविधा के द्वारा अपनी पहचान स्थापित करने के लिए किसी वैध प्रयोजन हेतु प्रमाणीकरण के जरिए इलेक्ट्रॉनिक रूप में आधार नंबर का उपयोग कर सकता है।

**16ग. आधार नंबर धारक की पहचान के प्रमाण के रूप में आधार नंबर को स्वीकार करने की शर्तें:**

(1) कोई भी ऑफ़लाइन सत्यापन मांगकर्ता संस्था, आधार नंबर को भौतिक या इलेक्ट्रॉनिक रूप में (प्रमाणीकरण के बिना), किसी वैध उद्देश्य के लिए पहचान के प्रमाण के रूप में, आधार पत्र पर आधार सुरक्षित क्यूआर कोड या ई-आधार अथवा एमआधार या आधार कागजरहित ऑफ़लाइन ई-केवाईसी (एक्सएमएल), जैसा भी मामला हो, में प्रदान किए गए प्राधिकरण के डिजिटल हस्ताक्षर के पूर्व सत्यापन बिना स्वीकार नहीं करेगी।

(2) कोई भी अनुरोधकर्ता संस्था आधार नंबर को, आधार नंबर धारक की पहचान के प्रमाण के रूप में इलेक्ट्रॉनिक रूप में प्रमाणीकरण के माध्यम से तब तक स्वीकार नहीं करेगी, जब तक कि यह एक वैध उद्देश्य के लिए न हो, जो अधिनियम के संबंधित उपबंधों के अनुरूप हो और आधार नंबर धारक की संसूचित सहमति के साथ तथा इन आधार (अधिप्रमाणन और ऑफ़लाइन सत्यापन) विनियम, 2021 में यथा उपबंधित ढंग में हो।]

**17. अनुरोधकर्ता संस्था द्वारा पहचान सूचना के उपयोग से सम्बंधित दायित्व:-**

(1) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि:

- (क) आधार नंबर धारक से संगृहीत कोर बायोमेट्रिक सूचना को किसी भी उद्देश्य के लिए संचित, साझा अथवा प्रकाशित नहीं किया गया है, और उसके पास कोर बायोमेट्रिक मुख्य बायोमेट्रिक सूचना की कोई प्रति शेष नहीं है;
- (ख) संगृहीत कोर बायोमेट्रिक सूचना को कूटबद्ध पीआईडी ब्लॉक के सृजन के बिना किसी नेटवर्क पर संप्रेषित नहीं किया गया है, जिसे प्राधिकरण द्वारा निर्धारित विशिष्टियों तथा प्रक्रियाओं के अनुरूप संप्रेषित किया जा सकता है;
- (ग) कूटबद्ध पीआईडी ब्लॉक संचित नहीं किया गया है, जब तक कि यह बफरकृत अधिप्रमाणन के लिए है, जहां इसे अल्प समयावधि के लिए अधिप्रमाणन उपकरण पर अस्थायी तौर पर रखा जा सकता है, और संप्रेषण के पश्चात इसे समाप्त कर दिया गया है;
- (घ) अधिप्रमाणन के दौरान, प्राप्त पहचान सूचना केवल अधिप्रमाणन के समय आधार नंबर धारक के लिए विनिर्दिष्ट उद्देश्य के लिए प्रयुक्त की गयी है, और जिस आधार नंबर धारक से यह सूचना सम्बंधित है, उसकी पूर्व सहमति लिए बिना आगे प्रकट नहीं की जाएगी;
- (च) अधिप्रमाणन के दौरान संगृहीत आधार नंबर धारक की पहचान सूचना तथा अधिप्रमाणन प्रक्रिया के दौरान सृजित कोई अन्य सूचना को एक्सेस, उपयोग एवं प्रकटन के सम्बंध में सुरक्षित रखा गया है जिसकी अधिनियम तथा इसके विनियम के अधीन अनुमति नहीं है।
- (छ) अधिप्रमाणन अनुरोध के डिजिटल रूप में हस्ताक्षर के लिए प्रयुक्त प्राइवेट कुंजी तथा लाइसेंस कुंजी को सुरक्षित रखा गया है और एक्सेस नियन्त्रित है; तथा
- (ज) अपनी प्रणालियों में आधार-आधारित पहचान सूचना से सम्बंधित डेटा संचयन तथा डेटा संरक्षण के सम्बन्ध में समस्त प्रासंगिक कानून एवं विनियम, जो उनके एजेंट (यदि लागू हो) के तथा अधिप्रमाणन उपकरण के विषय में हैं, अनुपालन किया गया है।

**18. अनुरोधकर्ता संस्था द्वारा लॉग का रखरखाव:-**

(1) अनुरोधकर्ता संस्था को अपने द्वारा अधिप्रमाणित किए गए कार्य के संबंध में नीचे सूचीबद्ध विवरण सहित कार्य लॉग का रखरखाव करना होगा:-

- (क) आधार नंबर, वर्चुअल आईडी, एएनसीएस टोकन या यूआईडी टोकन के अतिरिक्त अधिप्रमाणन अनुरोध के लिए विनिर्दिष्ट पैरामीटर प्रस्तुत करना।
  - (ख) मामले के अनुसार पूर्ण आधार नंबर या मास्क आधार सहित अधिप्रमाणन प्रक्रिया के रूप में प्राप्त विनिर्दिष्ट पैरामीटर।
  - (ग) अधिप्रमाणन के समय आधार नंबर धारक या बालक के मामले में उसके माता या पिता अथवा अभिभावक को किया गया सूचना प्रकटीकरण अभिलेख का उद्देश्य।
  - (ड.) अधिप्रमाणन के लिए आधार नंबर धारक या बालक के मामले में माता-पिता अथवा अभिभावक की सहमति का अभिलेख, परन्तु, किसी भी स्थिति में पीआईडी सूचना को अपने पास नहीं रखेगा।
- (2) अनुरोधकर्ता संस्था द्वारा अधिप्रमाणन कार्य के लॉग का रखरखाव 2 (दो) वर्ष की अवधि के लिए किया जाएगा तथा इस दौरान आधार नंबर धारक को इस संबंध में निर्धारित प्रक्रिया के अनुसार ऐसे लॉग को एक्सेस करने का अधिकार प्राप्त होगा।
  - (3) उप विनियम (2) में विनिर्दिष्ट अवधि की समाप्ति के पश्चात, लॉग को 5 वर्ष की अवधि अथवा विधि अनुसार अथवा संस्था का संचालन करने वाले विनियमों के अनुसार अपेक्षित वर्षों के लिए, इनमें से जो भी बाद में हो, पुरालेख के तौर पर रखा जाएगा सिवाय ऐसे अभिलेखों के जिन्हें उक्त अवधि की समाप्ति के बाद किसी न्यायालय के आदेश जो न्यूनतम उच्च न्यायालय के न्यायाधीश द्वारा दिया गया हो या किसी बकाया विवाद के लंबित रहने तक सुरक्षित रखना अपेक्षित होगा।
  - (4) अनुरोधकर्ता संस्था द्वारा संबंधित आधार नंबर धारक से प्राप्त अनुरोध पर अथवा शिकायत के निपटान तथा विवादों के समाधान के लिए अथवा न्यायालय के आदेश जो न्यूनतम न्यायालय के न्यायाधीश द्वारा दिया गया हो, के अतिरिक्त किसी भी अन्य व्यक्ति के साथ अधिप्रमाणन लॉग को साझा नहीं किया जाएगा। इस उप विनियम में उल्लिखित उद्देश्य के अलावा किसी अन्य उद्देश्य के लिए अधिप्रमाणन लॉग का प्रयोग नहीं किया जाएगा।
  - (5) अनुरोधकर्ता संस्था द्वारा लॉग के संचयन के संबंध में सूचना प्रौद्योगिकी अधिनियम, 2000 तथा भारतीय साक्ष्य अधिनियम, 1872 सहित, किंतु उन तक सीमित नहीं, सभी संबंधित विधियों, नियमों तथा विनियमों का पालन किया जाएगा।
  - (6) इस विनियम में विनिर्दिष्ट अधिप्रमाणन लॉग से संबंधित दायित्व इन विनियमों के अनुसार संस्था की नियुक्ति निरस्त करने के बावजूद भी मान्य रहेंगे।

## 19. अधिप्रमाणन सेवा एजेंसियों की भूमिका, उत्तरदायित्व एवं आचार संहिता:-

अधिप्रमाणन सेवा एजेंसी के क्रियाकलाप तथा दायित्व निम्नानुसार होंगे: -

- (क) अनुरोधकर्ता संस्था द्वारा अधिप्रमाणन अनुरोध हस्तांतरित करने के लिए केन्द्रीय पहचान डेटा रिपोजिटरी (सीआईडीआर) के साथ प्राधिकरण द्वारा इस उद्देश्य हेतु विनिर्दिष्ट विधि के अनुसार सुरक्षित कनेक्टिविटी उपलब्ध करवाना;
- (ख) सीआईडीआर को प्रेषित करने से पूर्व अधिप्रमाणन डेटा पैकेट से संबंधित मूलभूत अनुपालन एवं पूर्णतः जांच से संबंधित अनुपालन करना;
- (ग) सीआईडीआर से प्रतिक्रिया प्राप्त होने पर अनुरोध करने वाली अनुरोधकर्ता संस्था को किए गए कार्य के परिणाम संप्रेषित करना;

- (घ) केवल प्राधिकरण द्वारा अनुमोदित अनुरोधकर्ता संस्थाओं के साथ कार्य करना तथा इसका निष्पादन कर रही अनुरोधकर्ता संस्थाओं की सूची की जानकारी प्राधिकरण को देना;
- (च) अनुरोधकर्ता संस्था के साथ किए गए अनुबंधों की प्रत्येक संबंधित जानकारी प्राधिकरण को सूचित करना;
- (छ) यह सुनिश्चित करना कि अधिप्रमाणन कार्य तथा आवश्यक तंत्र, अवसंरचना, प्रक्रियाओं इत्यादि के रखरखाव के लिए नियुक्त व्यक्ति को अपेक्षित योग्यता प्राप्त हैं;
- (ज) प्रचालनों की लेखापरीक्षा किसी मान्यताप्राप्त निकाय द्वारा प्रमाणित सूचना प्रणाली लेखापरीक्षकों द्वारा वार्षिक आधार पर की जाए तथा इस संबंध में समय-समय पर प्राधिकरण द्वारा जारी नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों एवं विनिर्देशनों के अनुपालन की प्रमाणित लेखापरीक्षा रिपोर्ट प्राधिकरण को उपलब्ध करवाना सुनिश्चित करना;
- (झ) यह सुनिश्चित करना की तंत्र, प्रक्रियाएं, उपकरण, सॉफ्टवेयर एवं बायोमेट्रिक अवसंरचना, सुरक्षा तथा अन्य संबंधित घटकों सहित सभी अवसंरचनाएं और प्रचालन इस उद्देश्य के लिए प्राधिकरण द्वारा विनिर्दिष्ट मानकों एवं विनिर्देशनों के अनुरूप हैं;
- (ट) नेटवर्क तथा अन्य सूचना प्रौद्योगिकी अवसंरचना, प्रक्रियाओं, कार्यविधियों इत्यादि के संबंध में प्राधिकरण द्वारा जारी निदेशों, विनिर्देशनों आदि का हमेशा अनुपालन करना;
- (ठ) सभी संबंधित कानून तथा विनियमों, विशेषकर डाटा सुरक्षा तथा डेटा प्रबंधन का अनुपालन करना;
- (ड) अधिप्रमाणन सेवा एजेंसियों द्वारा किसी अनुरोधकर्ता संस्था को अनुबंध के अंतर्गत प्रदान की गई अन्य मूल्यवर्धित सेवाएं आधार अधिप्रमाणन प्रक्रिया का भाग नहीं होगी;
- (ढ) अधिप्रमाणन सेवा एजेंसी के द्वारा उप-अनुबंध के अंतर्गत अपने प्रचालन का कुछ भाग अन्य संस्थाओं को दिए जाने के मामले में भी, अधिप्रमाणन से संबंधित सभी प्रचालनों के लिए प्राधिकरण के प्रति उत्तरदायित्व अधिप्रमाणन सेवा एजेंसी का होगा;
- (ण) अधिप्रमाणन से सम्बद्ध धोखेबाजी अथवा विवाद से संबंधित मामले की जांच के लिए अधिप्रमाणन सेवा एजेंसी द्वारा प्राधिकरण (अथवा उसकी एजेंसी) तथा/अथवा अन्य प्राधिकृत जाच एजेंसी को अपने परिसर, अभिलेख, सिस्टम, कर्मियों, अवसंरचना, अन्य किसी संबंधित संसाधन अथवा सूचना तथा अन्य अधिप्रमाणन प्रचालनों से संबंधित अन्य संबंधित पहलू तक एक्सेस उपलब्ध कराने सहित पूर्ण सहयोग प्रदान किया जाएगा;
- (त) किसी अनुरोधकर्ता संस्था को अधिप्रमाणन प्रभारों पर सेवाएं प्रदान करने की सहमति दी जा सकेगी तथा, ऐसी अनुरोधकर्ता संस्था पर, प्राधिकरण का इस मामले में सामयिक तौर पर कोई हस्तक्षेप नहीं होगा, तथापि, ऐसे मामले में प्राधिकरण के पास भविष्य में किसी भिन्न व्यवस्था के निर्धारण करने का अधिकार सुरक्षित होगा;
- (थ) प्राधिकरण द्वारा जारी प्रत्येक संविदागत शर्तों तथा सभी नियमों, विनियमों, नीतियों, मैनअलों, प्रक्रियाओं, विशिष्टताओं, मानकों तथा निदेशों का सदैव पूर्णतः पालन किया जाएगा।

## 20. अधिप्रमाणन सेवा एजेंसियों द्वारा लॉग का रखरखाव:-

- (1) अधिप्रमाणन सेवा एजेंसी अपने द्वारा निष्पादित अधिप्रमाणन कार्यों के लॉग का रखरखाव किया जाएगा, जिसमें निम्नलिखित स्वयंवरार का ब्योरा शामिल होगा, नामतः:-
  - (क) अनुरोधकर्ता संस्था की पहचान;

(ख) प्रस्तुत अधिप्रमाणन अनुरोध के मानदंड; तथा

(ग) अधिप्रमाणन प्रतिक्रिया के रूप में प्राप्त मानदंड:

बशर्ते कि जहां लागू होगा, वहां आधार नंबर, वर्चुअल आईडी, यूआईडी टोकन, एएनसीएस टोकन, पीआईडी सूचना, उपकरण पहचान संबंधी डेटा और ई-केवाईसी प्रतिक्रिया डेटा का प्रतिधारण नहीं किया जाएगा।

- (2) अधिप्रमाणन सेवा एजेंसी द्वारा अधिप्रमाणन कार्य के लॉग का रखरखाव 2 (दो) वर्ष की अवधि के लिए किया जाएगा तथा इस दौरान प्राधिकरण तथा/अथवा अनुरोधकर्ता संस्था द्वारा शिकायत निवारण, विवाद निपटान तथा लेखापरीक्षा कार्यों के लिए इन विनियमों में विनिर्दिष्ट प्रक्रिया के अनुसार ऐसे अभिलेख के प्रयोग की मांग की जा सकेगी। इस उप विनियम में उल्लिखित उद्देश्यों के अन्यत्र किसी अन्य उद्देश्य के लिए अधिप्रमाणन अभिलेख का प्रयोग नहीं किया जाएगा।
- (3) उप विनियम (2) में विनिर्दिष्ट अवधि की समाप्ति के पश्चात, लॉग को 5 वर्ष की अवधि अथवा विधि अनुसार अथवा संस्था का संचलन करने वाले विनियमों के अनुसार अपेक्षित वर्षों के लिए सुरक्षित रखा जाएगा तथा 5 वर्ष की अवधि की समाप्ति के उपरान्त, इनमें से जो भी बाद में हो, पुरालेख के तौर पर रखा जाएगा तथा उक्त अवधि की समाप्ति के पश्चात, किसी न्यायालय जो उच्च न्यायालय के न्यायाधीश से निम्न नहीं होगा अथवा किसी बकाया विवाद के लिए अपेक्षित लॉग के अलावा अन्य अभिलेखों को हटा लिया जाएगा।
- (4) अधिप्रमाणन सेवा एजेंसी द्वारा लॉग के संचयन के संबंध में सूचना प्रौद्योगिकी अधिनियम, 2000 सहित सभी संबंधित विधियों का पालन किया जाएगा।
- (5) इस विनियम में विनिर्दिष्ट अधिप्रमाणन लॉग से संबंधित दायित्व इन विनियमों के अनुसार नियुक्ति निरस्त होने के बावजूद भी मान्य रहेंगे।

## **20क. ऑफलाइन सत्यापन मांगकर्ता संस्था द्वारा लॉग का वैकल्पिक अनुरक्षण:-**

- (1) ऑफलाइन सत्यापन मांगकर्ता संस्था निवासी की सहमति से अपने द्वारा स्साधित सत्यापन संव्यवहारों, यदि ओवीएसई आवश्यक समझे, के ऐसे लॉग का रखरखाव कर सकती है, जिनमें निम्नलिखित संव्यवहार का विवरण अंतर्निहित हो, नामत:-
  - क. निवासी द्वारा साझा किया गया ऑफलाइन आधार डेटा की उपयुक्त रूप से सुरक्षा करना;
  - ख. निवासी द्वारा सत्यापन के द्वारा साझा किए गए मोबाईल नम्बर, ई-मेल आई डी, फोटो आदि सहित कोई अन्य डाटा;
  - ग. ओवीएसई और निवासी के बीच स्थानीय सत्यापन संबंधी कार्रवाई का लॉग;
  - घ. आधार नंबर धारक को भेजे गए ऑफलाइन सत्यापन से संबंधित अधिसूचना का ब्योरा।

किन्तु किसी भी स्थिति में आधार नंबर धारक के आधार नंबर और वर्चुअल आईडी को संचित नहीं किया जाएगा।

- (2) ओवीएसई संबंधित आधार नंबर धारक के अतिरिक्त किसी भी व्यक्ति के साथ लॉग को साझा नहीं करेगी। शिकायत निवारण या विवाद सुलझाने के लिए अधिनियम के उपबंधों के अनुरूप कार्य किया जाएगा। उप विनियम में वर्णित उद्देश्य के अतिरिक्त सत्यापन लॉग का उपयोग किसी भी कार्य के लिए नहीं किया जाएगा।

## **21. अनुरोधकर्ता संस्थाओं, अधिप्रमाणन सेवा एजेंसियों और ऑफलाइन सत्यापन मांगकर्ता संस्थाओं की लेखापरीक्षा:-**

- (1) यह सुनिश्चित करना कि संस्थाएं प्राधिकरण द्वारा जारी अधिनियम, नियमों, विनियमों, नीतियों, प्रक्रियाओं, दिशानिर्देशों के अनुरूप कार्य कर रही हैं, प्राधिकरण सब-एयूए तथा सब-केयूए, अधिप्रमाणन सेवा एजेंसियों तथा

ऑफलाइन सत्यापन मांगकर्ता संस्थाओं सहित अनुरोधकर्ता संस्थाओं का प्रचालन, अवसंरचना, प्रणालियों और प्रक्रियाओं की लेखापरीक्षा स्वयं करेगी या प्राधिकरण द्वारा नियुक्त लेखापरीक्षा एजेंसी के माध्यम से करायेगी।

- (2) प्राधिकरण स्वयं अथवा प्राधिकरण द्वारा नियुक्त लेखापरीक्षा के माध्यम से उप-विनियम (1) में संदर्भित संस्थाओं के प्रचालनों तथा प्रणाली की लेखापरीक्षा कर सकता है। ऐसी लेखापरीक्षा की बारम्बारता, समय एवं प्रक्रिया समय-समय पर प्राधिकरण द्वारा अधिसूचित की जाएगी।
- (3) लेखापरीक्षा की जाने वाली संस्था द्वारा प्राधिकरण अथवा प्राधिकरण द्वारा अनुमोदित तथा/अथवा प्राधिकरण द्वारा नियुक्त एजेंसी को लेखापरीक्षा प्रक्रिया के दौरान पूर्ण सहयोग प्रदान किया जाएगा तथा प्राधिकरण अथवा प्राधिकरण द्वारा अनुमोदित तथा/या नियुक्त एजेंसी को अपनी प्रक्रिया, अभिलेखों तथा प्राधिकरण से प्राप्त सेवाओं से संबंधित सूचना के लिए पूर्ण एक्सेस प्रदान की जाएगी। लेखापरीक्षा की लागत का वहन संबंधित संस्था द्वारा किया जाएगा।
- (4) प्राधिकरण द्वारा किसी प्रकार की त्रुटि की शिनाख्त किए जाने पर प्राधिकरण संबंधित संस्था से आवश्यक स्पष्टीकरण तथा/अथवा इसके क्रियाकलापों से संबंधित सूचना प्रस्तुत करने के लिए कहा जा सकेगा तथा ऐसी संस्था से ऐसी त्रुटि के निवारण अथवा इन विनियमों में विनिर्दिष्ट कार्रवाई करने की अपेक्षा की जा सकेगी।
- (5) खंड (4) की किसी बात के होते हुए भी और अधिनियम के अन्तर्गत उठाए गए किसी कदम पर प्रतिकूल प्रभाव डाले बिना, प्राधिकरण लेखापरीक्षा के आधार पर पाई गई कमियों पर विनियम 25(1क) के अंतर्गत कार्रवाई कर सकता है।

## 22. डाटा सुरक्षा:-

- (1) अनुरोधकर्ता संस्था तथा अधिप्रमाणन सेवा एजेंसी/ओवीएसई द्वारा आधार अधिप्रमाणन अनुरोध कार्यो एवं क्रमशः सीआईडीआर/ऑफलाइन सत्यापन की रूटिंग के लिए डेटा केंद्र के अन्दर स्थित या भारत में स्थित क्लाउड स्टोरेज केन्द्रों में अपने सर्वर का उपयोग किया जाएगा।
- (1क) भारत की क्षेत्रीय सीमाओं से बाहर स्थित संस्थाओं से अधिप्रमाणन अनुरोध स्वीकार नहीं किए जाएंगे। भारत से बाहर के अधिप्रमाणन अनुरोधों को स्वीकार करने के लिए अनुरोधकर्ता संस्था प्राधिकरण से विशेष अनुमति प्राप्त करेगी।
- (2) अधिप्रमाणन सेवा एजेंसी प्राधिकरण के डाटा केंद्र के साथ इस उद्देश्य से प्राधिकरण द्वारा निर्दिष्ट प्रक्रिया तथा सुरक्षा कार्यविधियों के अनुसार दोहरी रेडन्डेंट, सुरक्षित लीड लाइनें अथवा एमपीएलएस कनेक्टिविटी की स्थापना करेगी।
- (3) अनुरोधकर्ता संस्था अधिप्रमाणन सेवा एक्सेस के लिए केवल प्राधिकरण द्वारा उपलब्ध कराई गई अधिप्रमाणन की सुविधा का उपयोग प्राधिकरण द्वारा विनिर्दिष्ट उद्देश्य के लिए एसए के सुरक्षित नेटवर्क के माध्यम से किया जाएगा।
- (4) अनुरोधकर्ता संस्था, अधिप्रमाणन सेवा एजेंसियाँ तथा ओवीएसई प्राधिकरण द्वारा समय-समय पर जारी सभी विनियमों, सूचना, सुरक्षा नीतियों, प्रक्रियाओं, मानकों, विनिर्देशों तथा दिशानिर्देशों का अनुपालन करेंगी।

## 23. अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी द्वारा अधिप्रमाणन सुविधा की पहुंच को छोड़ना:-

- (1) प्राधिकरण द्वारा प्रदान की गई अधिप्रमाणन सुविधा के लिए प्रदान की गई पहुंच को छोड़ने की इच्छा, इन विनियमों के अंतर्गत नियुक्त की गई है, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी ऐसे सरडेर के लिए अपना आवेदन प्राधिकरण को प्रस्तुत कर सकती हैं।

- (2) इन विनियमों के अंतर्गत सरेंडर के लिए प्राप्त अनुरोध का निपटान करते समय प्राधिकरण द्वारा अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी से आपेक्षा की जाती है, कि वह निम्नलिखित सहित सेवाओं को निर्वाध रूप से रोकने या समाप्त करने के लिए किसी भी आवश्यक मामले में प्राधिकरण को संतुष्ट करेगा:-
- (क) अधिप्रमाणन अभिलेख के रखरखाव तथा परिरक्षण के लिए अनुरोधकर्ता संस्था द्वारा की गई व्यवस्था तथा इन विनियमों एवं प्रक्रियाओं के अनुसार इस उद्देश्य से प्राधिकरण द्वारा विनिर्दिष्ट अन्य दस्तावेज;
  - (ख) अनुरोधकर्ता संस्था द्वारा संबंधित आधार नंबर धारक से अनुरोध प्राप्त होने पर उपलब्ध कराने हेतु अधिप्रमाणन अभिलेख के रखरखाव की व्यवस्था;
  - (ग) शिकायतों के निपटान, यदि कोई हों, का अभिलेख;
  - (घ) प्राधिकरण के साथ किया गया लेखा निपटान, यदि कोई हो;
  - (च) अधिप्रमाणन सेवा एजेंसी द्वारा सरेंडर किए जाने के मामले में, अधिप्रमाणन सेवा एजेंसी को अपनी पहुंच छोड़ने से पूर्व अपनी सम्बद्ध अनुरोधकर्ता संस्थाओं को अन्य अधिप्रमाणन सेवा एजेंसियों के प्रचालन में जाने के लिए पर्याप्त समय देना सुनिश्चित करेगी।

#### 24. इन विनियमों के लागू होने से पूर्व नियुक्त की गई एजेंसियां:-

- (1) इन विनियमों के अंतर्गत, इन विनियमों के लागू होने से पूर्व नियुक्त की गई अधिप्रमाणन उपयोक्ता एजेंसी (एयूए) अथवा ई-केवाईसी उपयोक्ता एजेंसी (केयूए) को अनुरोधकर्ता संस्था तथा अधिप्रमाणन सेवा एजेंसी (एएसए) अथवा ई-केवाईसी सेवा एजेंसी (केएसए) को अधिप्रमाणन सेवा एजेंसी माना जाएगा तथा ऐसी एजेंसियों एवं योजना आयोग, भारत सरकार के दिनांक 28 जनवरी, 2009 की अधिसूचना संख्या ए-43011/02/2009-प्रशासन-1 के अधीन स्थापित भारतीय विशिष्ट पहचान प्राधिकरण अथवा ऐसे प्राधिकरण के किसी अधिकारी के मध्य अधिनियम के अंतर्गत किए गए सभी अनुबंध प्राधिकरण द्वारा जारी अधिनियम के उपबंधों, इनके विनियमों तथा अन्य विनियमों, नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों तथा विनिर्देशनों के साथ असंगत न होने की सीमा तक प्रभावी रहेंगे।
- (2) उप-विनियम (1) में उल्लिखित होने के बावजूद भी उप-विनियम (1) में संदर्भित किसी मान्यताप्राप्त अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी से अधिनियम के प्रावधानों, इन विनियमों, प्राधिकरण द्वारा निर्मित अन्य विनियमों तथा प्राधिकरण द्वारा जारी नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों तथा विनिर्देशनों का अनपुलन करने की अनिवार्यता होगी।
- (3) उप-विनियम (1) में संदर्भित किसी एजेंसी द्वारा इन विनियमों में निर्दिष्ट अधिप्रमाणन सेवाओं से विलग होने की अपेक्षा की स्थिति में वह अपने प्रत्यय पत्र एवं अपने क्रियाकलापों की तुरंत समाप्ति के लिए आवेदन प्रस्तुत कर सकती है:  
  
बशर्ते कि ऐसे मामले में सेवाएं समाप्त करने पर एजेंसी अथवा प्राधिकरण को किसी मुआवजे का भुगतान नहीं किया जाएगा।
- (4) उप-विनियम (3) के अधीन सेवाएं समाप्त किए जाने की स्थिति में संबंधित संस्था से विनियम 23(3) उल्लिखित कार्य समापन अपेक्षाओं का पालन करने की अनिवार्यता होगी।

#### 25. चूक की स्थिति में देयताएं एवं कार्रवाई:-

- (1) इस अधिनियम के अंतर्गत नियुक्त किसी संस्था अथवा अधिप्रमाणन सेवा एजेंसी यदि:-

- (क) प्राधिकरण द्वारा समय-समय पर जारी किन्हीं प्रक्रियाओं, कार्यविधियों, मानकों, विनिर्देशनों अथवा निदेशों का अनुपालन नहीं करती है;
- (ख) अधिनियम तथा इन विनियमों के दायित्वों का उल्लंघन करती है;
- (ग) आधार अधिप्रमाणन सुविधाओं का प्रयोग, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी की नियुक्ति के लिए दिए गए आवेदन में की गई निर्दिष्टि के अलावा किन्हीं अन्य उद्देश्यों के लिए करती है;
- (घ) इन विनियमों के उद्देश्यों से प्राधिकरण द्वारा अपेक्षित किसी सूचना को प्रस्तुत नहीं कर पाती है; अथवा
- (च) प्राधिकरण द्वारा किसी निरीक्षण अथवा जांच अथवा पूछताछ अथवा लेखापरीक्षा के दौरान सहयोग नहीं करती है,

तो प्राधिकरण द्वारा, इस अधिनियम के अध्याधीन की जाने वाली किसी अन्य कार्रवाई के प्रति किसी प्रतिकूलता के बिना, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी के विरुद्ध अधिनियम के उपबंधों, उससे संबंधित नियमों एवं विनियमों का उल्लंघन करने पर ऐसी संस्था अथवा एजेंसी के क्रियाकलापों को समाप्त करने सहित दंडात्मक कार्रवाई के उपाय अथवा ऐसे अन्य उपाय किए जा सकेंगे, जिनके संबंध में ऐसी संस्था तथा प्राधिकरण के मध्य किए गए अनुबंध में विशिष्ट व्यवस्था की गई हो।

बशर्ते कि आधार अधिप्रमाणन से संबंधित सेवाओं तथा प्रचालनों की समाप्ति से पूर्व ऐसी संस्था अथवा एजेंसी को सनुर्वाई का अवसर प्रदान किया जाएगा।

**(1क)** जब कोई ऑफलाइन सत्यापन मांगकर्ता संस्था :-

- क. प्राधिकरण द्वारा समय-समय पर जारी प्रक्रिया, कार्यविधि, मानकों, विनिर्देशनों या निदेशों के अनुपालन में असफल होती है, अधिनियम और इन विनियमों के अधीन दायित्वों का उल्लंघन में पाया जाता है।
- ख. विनिर्दिष्ट कार्यों के अलावा किन्हीं अन्य कार्यों के लिए यदि आधार ऑफलाइन सत्यापन सुविधा का उपयोग किया जाता है।
- ग. इन विनियमों के अन्तर्गत प्राधिकरण द्वारा अपेक्षित सूचना को उपलब्ध कराने में असफल रहने पर, या
- घ. प्राधिकरण द्वारा कराए गए किसी निरीक्षण या जांच या पूछताछ या लेखा परीक्षा में सहयोग देने में असफल रहने पर।

प्राधिकरण, अधिनियम के अन्तर्गत की जाने वाली किसी अन्य कार्रवाई पर प्रभाव डाले बिना और किसी आपराधिक कार्रवाई सहित, जिसे प्राधिकरण सही समझे, अधिनियम, नियमों और विनियमों के उपबंधों का उल्लंघन करने के लिए ऑफलाइन सत्यापन मांगकर्ता संस्था पर हतोत्साहन लगाने के लिए कदम उठा सकता है।

बशर्ते कि कार्रवाई करने से पूर्व संस्था या एजेंसी को सुने जाने का अवसर प्रदान किया जाएगा।

- (2) उप विनियम (1) में संदर्भित ऐसी कोई भी कार्रवाई किसी भी संस्था या सब-एयूए या सब-केयूए के विरुद्ध भी की जा सकती है।

- (3) प्राधिकरण द्वारा सेवाएं समाप्त किए जाने पर अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी द्वारा आधार नाम तथा लोगो का प्रयोग, किसी भी स्वरूप तथा उद्देश्य, कारण चाहे कुछ भी हो, से नहीं किया जा सकेगा तथा उसे विनियम 23(2) में सचीबद्ध घटकों सहित समापन के आवश्यक घटकों के प्रति प्राधिकरण को संतुष्ट करना होगा।

#### **अध्याय-4**

#### **अधिप्रमाणन संव्यवहार डेटा और अधिप्रमाणन अभिलेख**

#### **26. अधिप्रमाणन संव्यवहार डेटा का संचयन एवं रखरखाव:-**

- (1) प्राधिकरण द्वारा निम्नलिखित सूचना से युक्त अधिप्रमाणन संव्यवहार डेटा का संचयन एवं रखरखाव किया जायेगा :-
- (क) पीआईडी ब्लॉक सहित प्राप्त अधिप्रमाणन अनुरोध डेटा
- (ख) प्रेषित अधिप्रमाणन प्रतिक्रिया डेटा
- (ग) आवश्यकतानुसार कोई अधिप्रमाणन सर्वर साईड संरूपण

बशर्ते कि प्राधिकरण द्वारा किसी भी मामले में अधिप्रमाणन के उद्देश्य या किसी कार्य सम्पादन के लिए कोई मेटा डाटा (प्रोसेस मेटा डाटा को छोड़कर) का भंडारण नहीं किया जाएगा।

#### **27. संचयन की अवधि:**

- (1) प्राधिकरण द्वारा अधिप्रमाणन संव्यवहार डेटा का 6 माह की अवधि के लिए किया जाएगा। परिपत्र के रूप में सामूहिक और बिना नाम के अधिप्रमाणन कार्य संपादन डेटा को अनुसंधान कार्यों के लिए पुरालेख करने और उनके मूल्यांकन के संबंध में प्राधिकरण द्वारा प्रक्रिया निर्धारित की जा सकती है।
- (2) उप विनियम (1) में विनिर्दिष्ट 6 माह की अवधि की समाप्ति के पश्चात अधिप्रमाणन संव्यवहार डेटा को हटाया जाएगा। किन्तु न्यूनतम उच्च न्यायालय के न्यायाधीश स्तर के किसी न्यायालय के आदेश पर या लंबित विवाद से संबंधित होने पर अधिप्रमाणन संव्यवहार डेटा को बरकरार रखा जाएगा।

#### **28. आधार नंबर धारक द्वारा एक्सेस:-**

- (1) आधार नंबर धारक को अभिलेखों का पुरालेख किए जाने से पूर्व अनुरक्षण किए जाने की अवधि के दौरान, विहित शर्तों तथा प्राधिकरण द्वारा निर्धारित शुल्क का भुगतान करने पर प्राधिकरण के सम्मुख आवेदन प्रस्तुत करके अपने अधिप्रमाणन अभिलेख को एक्सेस करने का अधिकार प्राप्त होगा।
- (2) इन विनियमों में निर्दिष्ट के अनुसार, पुरालेख से पूर्व अनुरक्षण की अवधि के दौरान, आधार नंबर धारकों को अपने डिजिटली हस्ताक्षरित सत्यापित अभिलेख की प्राप्ति के लिए प्राधिकरण द्वारा ऑनलाइन पोर्टल अथवा मोबाइल एप्लीकेशन अथवा अभिहित संपर्क केन्द्रों की सुविधा उपलब्ध करवाई जा सकती है।
- (3) प्राधिकरण, बायामेट्रिक अथवा ओटीपी अधिप्रमाणन के उपरांत निर्धारित शुल्क के भुगतान तथा प्रक्रियाओं के अनुसार आधार नंबर धारकों को डिजिटल रूप से हस्ताक्षरित ई-केवाईसी डाटा उपलब्ध करवा सकता है।

(4) सत्यापित अभिलेख तथा ई-केवाईसी डाटा को किसी व्यक्ति अथवा संस्था के साथ साझा नहीं किया जा सकेगा:-

(क) आधार नंबर धारक जिनसे विनिर्दिष्ट अधिप्रमाणन प्रक्रिया के अनुसार अभिलेख या ई-केवाईसी डेटा संबंधित है, के अलावा किसी अन्य के साथ। आधार नंबर धारक द्वारा अपने डिजिटल रूप से हस्ताक्षरित सत्यापित अभिलेख तथा ई-केवाईसी डाटा को अन्य संस्थाओं के साथ साझा किया जा सकेगा, जो आगे किसी अन्य संस्था के साथ आधार नंबर धारक से प्रत्येक बार अनुमति प्राप्त किए बिना साझा नहीं करेंगे।

(ख) अधिनियम में किए गए उपबंधों के अन्यत्र।

## अध्याय - 5

### विविध

#### 29. निरसन एवं व्यावृत्ति:-

- (1) भारत सरकार के योजना आयोग के दिनांक 28 जनवरी, 2009 की अधिसूचना संख्या ए-43011/02/2009-प्रशासन-1 के माध्यम से स्थापित भारतीय विशिष्ट पहचान प्राधिकरण अथवा प्राधिकरण की स्थापना से पूर्व ऐसे प्राधिकार प्राप्त किसी अधिकारी अथवा अधिनियम के तहत द्वारा जारी सभी कार्यपद्धति, आदेश, प्रक्रियाएं, मानक तथा नीतियां अथवा हस्ताक्षर किए सभी समझौता ज्ञापन, करार अथवा सविदाएं उस सीमा तक लागू रहेंगी, जब तक कि वे अधिनियम के उपबंधों तथा इनके तहत तैयार किए गए अधिनियम अथवा विनियम के तहत असंगत सिद्ध न हो जाएं।
- (2) आधार (अधिप्रमाणन) विनियम 2016 के निरसन होते हुए भी, उक्त विनियम के तहत किए गए कार्यों या उक्त विनियमों के अन्तर्गत की गई कार्रवाई को पूर्ण हुआ माना जाएगा या उन्हें इन विनियमों के तदन्तर प्रावधानों के अन्तर्गत लिया जाएगा।

#### 30. स्पष्टीकरण तथा दिशानिर्देशों को जारी करने की शक्ति तथा कठिनाईयों का निराकरण:-

इन विनियमों के अनुप्रयोग अथवा निर्वचन से संबंधित मामलों को स्पष्ट करने अथवा इन विनियमों के कार्यान्वयन में किन्हीं कठिनाईयों का निराकरण करने के लिए, प्राधिकरण के पास परिपत्र के रूप में स्पष्टीकरण तथा दिशानिर्देशों जारी करने की शक्ति होगी, जिनका प्रभाव विनियम के समान होगा।

#### 31. नीतियां जारी करने, दस्तावेजों के प्रसंस्करण आदि की शक्तियां:-

प्राधिकरण इन विनियमों से असंगत ऐसी नीतियों, आदेशों, प्रक्रियाओं, मानकों, विनिर्देशों या अन्य दस्तावेजों को जारी कर सकता है जिन्हें इन विनियमों के अन्तर्गत निर्दिष्ट करना अपेक्षित हो या इन विनियमों को प्रभावी बनाने के लिए उक्त प्रावधान आवश्यक हों।

#### <sup>10</sup>[32. प्रत्यायोजित शक्ति या कृत्य से संबंधित कार्य या बात करना:-

- (1) कोई भी कार्य या बात जो इन विनियमों के तहत प्राधिकरण द्वारा की जानी है या की जा सकती है, वह प्राधिकरण के किसी ऐसे सदस्य या अधिकारी या किसी अन्य व्यक्ति द्वारा भी की जा सकेगी जिसे प्राधिकरण ने अधिनियम की धारा 51 के अंतर्गत लिखित रूप में सामान्य या विशेष आदेश द्वारा संबंधित शक्ति या कृत्य प्रत्यायोजित किया है।

<sup>10</sup> अधिसूचना संख्या एच क्यू-13073/1/2020/अधि.-II (अ), दिनांक 29.9.2023 (दिनांक 3.10.2023 से प्रभावी) द्वारा प्रविष्ट किया गया।

- (2) प्राधिकरण यह अवधारित कर सकता है कि उप-विनियम (1) के अंतर्गत किसी सदस्य, अधिकारी या अन्य व्यक्ति द्वारा किया गया कोई कार्य या बात उत्त उप-विनियम में यथा संदर्भित प्रत्यायोजित शक्ति या कृत्य संबंधित है या नहीं।]

<sup>11</sup>[\*\*\*]

<sup>12</sup>[अनुसूची - क]

**अनुरोधकर्ता संस्थाओं की नियुक्ति के लिए पात्रता मापदंड**

**[विनियम 12(2क) देखें]**

1. एएसए के रूप में अपॉइंटमेंट की मांगकर्ता संस्थाओं को निम्नानुसार वर्गीकृत किया गया है:

क्रम संख्या	संगठन श्रेणी
श्रेणी 1	केंद्र सरकार या राज्य सरकार का मंत्रालय या विभाग या केंद्र सरकार या राज्य सरकार के स्वामित्व या नियंत्रणाधीन उपक्रम
श्रेणी 2	केंद्रीय या राज्य अधिनियम के अंतर्गत गठित कोई प्राधिकरण
श्रेणी 3	प्राधिकरण की राय में राष्ट्रीय महत्व की कोई अन्य संस्था
श्रेणी 4	कंपनी अधिनियम, 2013 (2013 का 18) के तहत भारत में रजिस्ट्रीकृत कंपनी
श्रेणी 5	एयूए या केयूए

2. एएसए के रूप में नियुक्ति के संबंध में संस्थाओं के लिए तकनीकी और वित्तीय मापदंड इस प्रकार हैं:-

श्रेणी	वित्तीय अपेक्षाएं	तकनीकी अपेक्षाएं
श्रेणी 1, 2 और 3	—	—
श्रेणी 4	पिछले तीन वित्तीय वर्षों के लिए लेखापरीक्षित वित्तीय विवरणों के अनुसार वार्षिक टर्नओवर न्यूनतम 100 करोड़ रुपये	दूरसंचार सेवा प्रदाता (एक्सेस सेवाओं के लिए प्राधिकार प्राप्त यूनिफाइड लाइसेंस का धारक या यूनिफाइड एक्सेस सर्विसेज लाइसेंस का धारक, जिसे भारतीय टेलीग्राफ अधिनियम, 1885 (1885 का 13) की धारा 4 के तहत लाइसेंस प्रदान किया गया है), जिसके पास भारत में न्यूनतम 100 मल्टीप्रोटोकॉल लेवल

<sup>11</sup> अधिसूचना संख्या एच क्यू-13011/2/2021/अधि.-II (2023 का संख्या 1), दिनांक 24.2.2023 (प्रभावी दिनांक 27.2.2023 से) के माध्यम से "अनुसूची क" को हटा दिया गया और अधिसूचना संख्या एच क्यू-13011/2/2021/अधि.-II (2023 का संख्या 1), दिनांक 24.2.2023 (प्रभावी दिनांक 27.2.2023) से "अनुसूची ख" को "अनुसूची क" द्वारा प्रतिस्थापित किया गया।

<sup>12</sup> "अनुसूची क" को अधिसूचना संख्या एच क्यू-13073/1/2020-अधि.-II (ई), दिनांक 29.9.2023 (प्रभावी दिनांक 3.10.2023) द्वारा प्रतिस्थापित किया गया।

		<p>स्विचिंग (एमपीएलएम) पॉइंट्स ऑफ प्रेजेंस (पीओपी) हैं।</p> <p>या</p> <p>नेटवर्क सेवा प्रदाता या सिस्टम इंटीग्रेटर, जिसके पास डेटा ट्रांसमिशन के लिए अखिल भारतीय स्तर पर नेटवर्क कनेक्टिविटी है और जिसके पास भारत में न्यूनतम 100 एमपीएलएस पीओपी हैं।</p>
<b>श्रेणी 5</b>	_____	<p>ऐसे अधिप्रमाणन संव्यवहार मानदंड जैसे कि प्राधिकरण द्वारा समय-समय पर अवधारित किए जाएं, की पूर्ति करने वाला एयूए या केयूए।</p>

# THE AADHAAR (AUTHENTICATION AND OFFLINE VERIFICATION) REGULATIONS, 2021<sup>1</sup>

*[Updated as on 23.10.2023]*

*In exercise of the powers conferred by sub-section (1), and sub-clauses (a), (ba), (ca), (cb), (f), (fa), (fb) and (w) of sub-section (2) of Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 as amended vide the Aadhaar and Other Laws (Amendment) Act, 2019 (No. 14 of 2019) and in supersession of the Aadhaar (Authentication) Regulations, 2016 except as respects things done or omitted to be done before such supersession, the Unique Identification Authority of India, hereby makes the following regulations, namely:—*

## CHAPTER I PRELIMINARY

**1. Short title and commencement.**—(1) These regulations may be called the Aadhaar (Authentication and Offline Verification) Regulations, 2021.

(2) These regulations shall come into force on the date of their publication in the Official Gazette.

**2. Definitions.**—(1) In these regulations, unless the context otherwise requires,—

(a) “Act” means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016;

(aa) “Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3 of Aadhaar Act, and includes any alternative virtual identity generated under sub-section (4) of that section;

<sup>2</sup>[(ab) “Aadhaar Letter” means a document for conveying the Aadhaar number to a resident;]

(b) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;

(ba) “Aadhaar Number Capture Service Token or ANCS Token” means an encrypted number generated for an Aadhaar number by the Authority for completion of an authentication transaction. ANCS Token shall be valid for a short period of time as prescribed by the Authority;

(bb) “Aadhaar Paperless Offline e-KYC” means a digitally signed document generated by the Authority containing last 4 digits of Aadhaar number, demographic data like

---

<sup>1</sup> Published in the Gazette of India, Extraordinary, Part III, Section 4, No. 542, dated 9.11.2021, *vide* notification No.K-11020/240/2021/Auth/UIDAI (No. 2 of 2021), dated 8.11.2021, and subsequently amended *vide* notification No. K-11020/240/2021/Auth/UIDAI (No. 1 of 2022), dated 4.2.2022 (w.e.f. 4.2.2022), No. HQ-13011/240/2021-AUTH-II (No. 01 of 2023) dated 24.2.2023 (w.e.f. 27.2.2023) and No. HQ-13073/1/2020-AUTH.II (E), dated 29.9.2023 (w.e.f. 3.10.2023).

<sup>2</sup>Ins. by notification No.K-11020/240/2021/Auth/UIDAI (No. 1 of 2022), dated 4.2.2022 (w.e.f. 4.2.2022).

name, address, gender, and date of birth, and photograph of the Aadhaar number holder etc.;

(bc) “Aadhaar Secure QR Code” means a quick response code generated by the Authority which contains digitally signed data like last 4 digits of Aadhaar number, demographic data like name, address, gender, and date of birth, and photograph of the Aadhaar number holder etc.;

<sup>3</sup>[(bd) “Aadhaar PVC Card” means a Polyvinyl Chloride Card (PVC), issued by the Authority upon payment of prescribed charges, which has Aadhaar number, demographic information and photograph of an Aadhaar number holder printed on it along with Aadhaar Secure QR code and is equivalent to paper-based Aadhaar Letter;]

(c) “Authentication” means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

(d) “Authentication facility” means the facility provided by the Authority for authenticating the Aadhaar number along with demographic information or biometric information of an Aadhaar number holder through the process of authentication, by providing a Yes/ No response or e-KYC data, as applicable;

(e) “Authentication record” means the record of the time of authentication and identity of the requesting entity and the response provided by the Authority thereto;

(f) “Authentication Service Agency” or “ASA” shall mean a licensed entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority;

(g) “Authentication User Agency” or “AUA” means a requesting entity that uses the Yes/ No authentication facility provided by the Authority;

(h) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;

(i) “Central Identities Data Repository” or “CIDR” means a centralised database in one or more locations containing Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

(ia) “child” means a person who has not completed eighteen years of age;

<sup>4</sup>[(ib) “Digital signature” means digital signature as defined in clause (p) of sub-section (1) of Section 2 of the Information Technology Act, 2000 (21 of 2000);

---

<sup>3</sup>Ins. by notification No.K-11020/240/2021/Auth/UIDAI (No. 1 of 2022), dated 4.2.2022 (w.e.f. 4.2.2022).

<sup>4</sup>Ins. by notification No.K-11020/240/2021/Auth/UIDAI (No. 1 of 2022), dated 4.2.2022 (w.e.f. 4.2.2022).

- (ic) “e-Aadhaar” means a password protected electronic copy of Aadhaar letter, which is digitally signed by the Authority and can be downloaded from the official website or mobile application of the Authority;]
- (j) “e-KYC authentication facility” means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction;
- (k) “e-KYC data” means full or limited demographic information and/or photograph of an Aadhaar number holder. The e-KYC data may contain full or masked Aadhaar number;
- (l) “e-KYC User Agency” or “KUA” shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority;
- <sup>5</sup>[(la) “mAadhaar” means the official mobile application developed by the Authority to provide an interface to Aadhaar Number holders to carry their Aadhaar details as registered with CIDR which inter alia includes Aadhaar number along with demographic information and photograph of the Aadhaar number holder;]
- (m) “License Key” is the key generated by a requesting entity as per the process laid down by the Authority;
- (ma) “Offline Verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;
- (mb) “Offline Verification Seeking Entity” or “OVSE” means any entity desirous of undertaking offline verification of an Aadhaar number holder;
- (mc) “Offline Aadhaar Data” means the data relating to offline Aadhaar verification, having characteristics as specified by the Authority from time to time including the requirement of masking Aadhaar numbers before storing;
- (n) “PID Block” means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication;
- (na) “Registered Devices” means biometric devices that are registered with the Authority;
- (o) “Requesting entity” means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication;

---

<sup>5</sup>Ins. by notification No.K-11020/240/2021/Auth/UIDAI (No. 1 of 2022), dated 4.2.2022 (w.e.f. 4.2.2022).

- (oa) “Sub-AUA” means a requesting entity that uses the Yes/ No authentication facility provided by the Authority through an existing AUA;
- (ob) “Sub-KUA” means a requesting entity that uses e-KYC authentication facility provided by the Authority through an existing KUA;
- (oc) “UID Token” means a 72-character alphanumeric string generated by the Authority mapped to the Aadhaar number and specific to a requesting entity;
- (od) “Virtual Identifier” means an interchangeable 16-digit random number mapped with the Aadhaar number of the Aadhaar number holder; and
- (p) “Yes/No authentication facility” means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing “Yes” or “No”, along with other technical details related to the authentication transaction, but no identity information.

(2) Words and expressions used and not defined in these regulations shall have the meaning assigned thereto under the Act or under the rules or regulations made there under or under the Information Technology Act 2000.

## ***CHAPTER II***

### **AADHAAR AUTHENTICATION FRAMEWORK**

**3. Types of Authentication Facilities.** —There shall be two types of authentication facilities provided by the Authority, namely-

- (i) Yes/No authentication facility, which may be carried out using any of the modes specified in regulation 4(2); and
- (ii) e-KYC authentication facility, which may be carried out only using OTP and/ or biometric authentication modes as specified in regulation 4(2).

**3A. Types of Offline Verification.**—1. There shall be following types of Offline Verification services provided by the Authority, namely-

- (i) QR Code verification,
- (ii) Aadhaar Paperless Offline e-KYC verification,
- (iii) e-Aadhaar verification,
- (iv) Offline Paper based verification, and
- (v) Any other type of Offline verification introduced by the Authority from time to time.

Offline Verification as above may be carried out by the entity as per the specifications given by the Authority from time to time.

2. The Authority shall provide various means to download QR Code, e-Aadhaar or Aadhaar Paperless Offline e-KYC through website, mobile application or other means.

**4. Modes of Authentication.**—(1) An authentication request shall be entertained by the Authority only upon a request sent by a requesting entity electronically in accordance with these regulations and conforming to the specifications laid down by the Authority.

(2) Authentication may be carried out through the following modes:

- (a) **Demographic authentication:** The Aadhaar number and demographic information of the Aadhaar number holder obtained from the Aadhaar number holder is matched with the demographic information of the Aadhaar number holder in the CIDR.
- (b) **One-time pin based authentication:** A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.
- (c) **Biometric-based authentication:** The Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.
- (d) **Multi-factor authentication:** A combination of two or more of the above modes may be used for authentication.

(3) A requesting entity may choose suitable mode(s) of authentication from the modes specified in sub26 regulation (2) for a particular service or business function as per its requirement, including multiple factor authentication for enhancing security.

**4A. Virtual Identity number (VID).**—(1) Authority shall provide an alternate identification number mapped with Aadhaar number for the purpose of authentication.

(2) Aadhaar number holder may generate or retrieve his/her VID through UIDAI website, SMS, mobile application, eAadhaar download and any other means as provided by Authority from time to time.

(3) The Aadhaar number holder may use VID in lieu of Aadhaar number for online authentication or e-KYC.

(4) No entity shall store Virtual ID in its system.

**5. Information to the Aadhaar number holder.**—(1) At the time of authentication or Offline Verification, a requesting entity or Offline Verification Seeking Entity (OVSE) respectively shall inform the Aadhaar number holder or in case of a child, inform the parent or guardian, of the following details: -

- (a) the nature of information that will be shared by the Authority upon authentication with the requesting entity;

- (b) the uses to which the information received during authentication or offline verification may be put; and
- (c) alternate and viable means of submission of identification and that no service to the resident will be denied for refusing to, or being unable to, undergo authentication or offline verification.

(2) A requesting entity shall ensure that the information referred to in sub-regulation (1) above is provided to the Aadhaar number holder in local language as well.

(3) A requesting entity or OVSE shall ensure that the no service is denied to any resident for refusing to or being unable to undergo authentication or offline verification provided that the resident is able to identify himself through a viable alternative means as suggested by the requesting entity under sub-regulation (1) (c) above.

**6. Consent of the Aadhaar number holder.**—(1) After communicating the information in accordance with Regulation 5, a requesting entity or Offline Verification Seeking Entity (OVSE) shall obtain the consent of the Aadhaar number holder or in case of a child, the consent of the parent or guardian of the child for the authentication or verification.

(2) A requesting entity or OVSE shall obtain the consent referred to in sub-regulation (1) above in physical or preferably in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.

**7. Capturing of biometric information by requesting entity.**—(1) A requesting entity shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by the Authority.

(1a) All biometric devices used for authentication shall be Registered Devices as per the standards specified by the Authority from time to time.

(1b) All the biometric devices shall be registered with the server of the requesting entity.

(2) A requesting entity shall necessarily encrypt and secure the biometric data at the time of capture as per the specifications laid down by the Authority.

(3) For optimum results in capturing of biometric information, a requesting entity shall adopt the processes as may be specified by the Authority from time to time for this purpose.

**8. Devices, client applications, etc. used in authentication.**—(1) All devices and equipment used for authentication shall be certified as required and as per the specifications issued, by the Authority from time to time for this purpose.

(2) The client applications i.e. software used by requesting entity for the purpose of authentication, shall conform to the standard APIs and specifications laid down by the Authority from time to time for this purpose.

**9. Process of sending authentication requests.**—(1) After collecting the Aadhaar number or any other identifier provided by the requesting entity which is mapped to Aadhaar number and necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application shall immediately package and encrypt these input

parameters into PID block before any transmission, as per the specifications laid down by the Authority, and shall send it to server of the requesting entity using secure protocols as may be laid down by the Authority for this purpose.

(2) After validation, the server of a requesting entity shall pass the authentication request to the CIDR, through the server of the Authentication Service Agency as per the specifications laid down by the Authority. The authentication request shall be digitally signed by the requesting entity and/or by the Authentication Service Agency, as per the mutual agreement between them.

(3) Based on the mode of authentication request, the CIDR shall validate the input parameters against the data stored therein and return a digitally signed Yes or No authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data, as the case may be, along with other technical details related to the authentication transaction.

(4) In all modes of authentication, the Aadhaar number is mandatory and is submitted along with the input parameters specified in sub-regulation (1) above such that authentication is always reduced to a 1:1 match.

(5) A requesting entity shall ensure that encryption of PID Block takes place at the time of capture on the authentication device as per the processes and specifications laid down by the Authority.

**10. Notification/Acknowledgement of authentication or offline verification to Aadhaar number holder.**—(1) The Aadhaar number holder shall be notified by the requesting entity about any authentication, through email and/or SMS and/or other digital means and/or paper based acknowledgement about success or failure of authentication on each request. Such notification/acknowledgement shall include requesting entity's name, date and time of authentication, auth response code, last 4 digits of Aadhaar number and purpose of authentication, as the case may be.

(2) The Aadhaar number holder shall be notified by the OVSE about any offline verification, through email and/or SMS and/or other digital means and/or paper based acknowledgement about success or failure of offline verification on each request.

(3) In case of authentication failure the requesting entity should, in clear and precise language, inform the resident about the reasons of authentication failure such as Suspended/Cancelled Aadhaar or Biometric/Aadhaar Locking.

**11. Biometric locking.**—(1) The Authority may enable an Aadhaar number holder to permanently lock his biometrics and temporarily unlock it when needed for biometric authentication.

(2) All biometric authentication against any such locked biometric records shall fail with a “No” answer with an appropriate response code.

(3) An Aadhaar number holder shall be allowed to temporarily unlock his biometrics for authentication, and such temporary unlocking shall not continue beyond the time period specified by the Authority or till completion of the authentication transaction, whichever is earlier.

(4) The Authority may make provisions for Aadhaar number holders to remove such permanent locks at any point in a secure manner.

**11A. Aadhaar locking.**—(1) The Authority shall enable an Aadhaar number holder to lock his/her Aadhaar number and unlock it when needed for authentication.

(2) All authentication requests using Aadhaar number against any such locked Aadhaar number shall result with a “No” answer with an appropriate response code.

(3) In case of a locked Aadhaar, the Authority will allow the resident to authenticate using Virtual ID or other means.

### **CHAPTER III**

#### **APPOINTMENT OF REQUESTING ENTITIES AND AUTHENTICATION SERVICE AGENCIES**

**12. Appointment of Requesting Entities and Authentication Service Agencies.**—<sup>6</sup>[(1) An agency or other person seeking appointment as a requesting entity for use of an Authentication facility shall apply to the Authority for appointment, in such form as the Authority may provide upon request made to it by such agency or person:

Provided that such agency or person, on appointment as requesting entity, shall perform authentication only for such purpose as is—

- (a) allowed under sub-section (4) or required under any law as referred to in sub-section (7) of section 4 of the Act; or
- (b) required by the Central Government or a State Government under section 7 of the Act.]

(1A) Requesting entity and ASA shall meet technical and security criteria as specified by the Authority from time to time.

<sup>7</sup>[(2) An entity seeking appointment as an ASA for use of an Authentication facility shall apply to the Authority for appointment, in such form as the Authority may provide upon request made to it by such entity.

(2A) The entity seeking appointment as ASA shall fulfil the criteria specified in Schedule A.]

---

<sup>6</sup>Substituted *vide* notification No. HQ-13073/1/2020-AUTH.II(E), dated 29.9.2023 for regulation 12(1) (w.e.f. 3.10.2023). Regulation 12(1), before substitution, stood as under:

“(1) Agencies seeking to become requesting entities to use the authentication facility provided by the Authority shall apply for appointment as requesting entities in accordance with the procedure as may be specified by the Authority for this purpose from time to time provided that the purpose, for which authentication services are required, is permitted under the provisions of Sections 4(4) (b) (i) or 4(4) (b) (ii) or 4(7) or 7 of the Act.”

<sup>7</sup>Subs. *vide* notification No. HQ-13073/1/2020-AUTH.II(E), dated 29.9.2023 (w.e.f. 3.10.2023), for regulation 12(2). Regulation 12(2), before substitution, stood as under:

“(2) Entities seeking appointment as Authentication Service Agencies shall apply for appointment to the Authority in accordance with the procedure as may be specified by the Authority for this purpose. Only those entities that fulfill the criteria laid down in [Schedule A] are eligible to apply. The Authority may by order, amend [Schedule A] from time to time so as to modify the eligibility criteria.”

(3) The Authority may require the applicant to furnish further information or clarifications, regarding matters relevant to the activity of such a requesting entity or Authentication Service Agencies, as the case may be, which may otherwise be considered necessary by the Authority, to consider and dispose of the application.

(4) The applicant shall furnish such information and clarification to the satisfaction of the Authority, within the time as may be specified in this regard by the Authority.

(5) While considering the application, the information furnished by the applicant and its eligibility, the Authority may verify the information through physical verification of documents, infrastructure, and technological support which the applicant is required to have.

(6) After verification of the application, documents, information furnished by the applicant and its eligibility, the Authority may:

- a. approve the application for requesting entity or Authentication Service Agency, as the case may be; and
- b. enter into appropriate agreements with the entity or agency incorporating the terms and conditions for use by requesting entities of the Authority's authentication facility, or provision of services by ASAs, including damages and disincentives for non-performance of obligations.

(7) The Authority may from time to time, determine the fees and charges payable by entities during their appointment, including application fees, annual subscription fees and fees for individual authentication transactions.

(8) The Authority may from time to time, determine requesting entities which may be allowed to store Aadhaar number or masked Aadhaar number.

(9) The Authority may from time to time, determine the data fields to be provided as part of e-KYC response to particular requesting entities.

(10) The Authority may from time to time, determine if requesting entities will be allowed to perform authentication using Aadhaar number or Virtual ID or UID Token or ANCS or any other identifier.

**13. Procedure where application for appointment is not approved.**—(1) In the event an application for appointment of requesting entity, Authentication Service Agency, as the case may be, does not satisfy the requirements specified by the Authority, the Authority may reject the application.

(2) The decision of the Authority to reject the application shall be communicated to the applicant in writing within thirty days of such decision, stating therein the grounds on which the application has been rejected.

(3) Any applicant, aggrieved by the decision of the Authority, may apply to the Authority, within a period of thirty days from the date of receipt of such intimation for reconsideration of its decision.

(4) The Authority shall reconsider an application made by the applicant and communicate its decision thereon, as soon as possible in writing.

**14. Roles and responsibilities of requesting entities.**—(1) A requesting entity shall have the following functions and obligations:

- (a) establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication;
- (b) establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests;
- (c) ensure that the network connectivity between authentication devices and the CIDR, used for sending authentication requests is in compliance with the standards and specifications laid down by the Authority for this purpose;
- (ca) ensure that the Aadhaar number/Virtual ID/ANCS Token provided by the resident for authentication request shall not be retained by the device operator or within the device or at the AUA server(s);
- (cb) ensure that the provision of authentication using Virtual ID is provided;
- (d) employ only those devices, equipment, or software, which are duly registered with or approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose;
- (e) monitor the operations of its devices and equipment, on a periodic basis, for compliance with the terms and conditions, standards, directions, and specifications, issued and communicated by the Authority, in this regard, from time to time,
- (f) ensure that persons employed by it for performing authentication functions, and for maintaining necessary systems, infrastructure and processes, possess requisite qualifications for undertaking such works.
- (g) keep the Authority informed of the ASAs with whom it has entered into agreements;
- (ga) obtain approval from the Authority before appointing any third party entity as Sub-AUA/Sub-KUA.
- (h) ensure that its operations and systems are audited by information systems auditor certified by a recognised body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;
- (i) implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to the residents;
- (j) in case of any investigation involving authentication related fraud(s) or dispute(s), it shall extend full cooperation to the Authority, or any agency appointed or authorised by it or any other authorised investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resources or information as well to assist the Authority in disseminating information

to the general public about any Aadhaar data related fraud to enable Aadhaar number holders to evaluate whether they were victims of the fraud and take remedial action;

- (k) in the event the requesting entity seeks to integrate its Aadhaar authentication system with its local authentication system, such integration shall be carried out in compliance with standards and specifications issued by the Authority from time to time;
- (l) shall inform the Authority of any misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within their network. If the requesting entity is a victim of fraud or identifies a fraud pattern through its fraud analytics system related to Aadhaar authentication, it shall share all necessary details of the fraud with the Authority as well as to affected Aadhaar number holders without undue delay;
- (m) shall be responsible for the authentication operations and results, even if it sub-contracts parts of its operations to third parties. The requesting entity is also responsible for ensuring that the authentication related operations of such third party entities comply with Authority standards and specifications and that they are regularly audited by approved independent audit agencies;
- (ma) may agree upon the authentication charges for providing authentication services to its customer, with such customer, and the Authority shall have no say in this respect, for the time being; however, the Authority's right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;
- (mb) Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters shall be masked by the requesting entity by redacting the first 8 digits of the Aadhaar number before storing the physical copies.
- (n) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority, for the purposes of using the authentication facilities provided by the Authority.
- (o) shall take specific permission of the Authority and sign appropriate agreement with the Authority, if requiring storage of Aadhaar number for non-authentication purposes. Aadhaar number shall be stored in a secure manner as specified by the Authority from time to time
- (p) extend full co-operation to the Authority for any mass awareness programmes that the Authority may undertake to sensitize Aadhaar number holders about the nature of data being used in authentication, the scope of misuse as well as steps to protect against such misuse or fraud.

**14A. Obligations of Offline Verification Seeking Entities.**—(1) An OVSE shall have the following obligations: -

- (a) ensure compliance of Aadhaar Act and Regulations framed thereunder as well as relevant policies, manuals, procedures, specifications, standards, and directions issued by the Authority;
- (b) shall not collect, use or store Aadhaar number or biometric information of any individual for any purpose or share offline Aadhaar data with any other entity except in accordance with the Act and Regulations framed thereunder;
- (c) in case of any investigation involving Aadhaar data related fraud(s) or dispute(s), it shall extend full cooperation to the Authority, or any agency appointed or authorised by it or any other authorised investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resources or information as well to assist the Authority in disseminating information to the general public about any Aadhaar data related fraud to enable Aadhaar number holders to evaluate whether they were victims of the fraud and take remedial action;
- (d) shall inform the Authority, without undue delay and in no case beyond 72 hours after having knowledge of misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information. If the OVSE is a victim of fraud or identifies a fraud pattern through its fraud analytics system related to Offline Verification, it shall share all necessary details of the fraud with the Authority as well as to affected Aadhaar number holders without undue delay;
- (e) shall be responsible for the Offline Verification operations and results, even if it sub-contracts parts of its operations to third parties. Further, the OVSE is responsible for ensuring that the Offline Verification related operations of such third-party entities comply with the Authority standards and specifications;
- (f) extend full co-operation to the Authority for any mass awareness programmes that the Authority may undertake to sensitize Aadhaar number holders about the nature of data being used in offline verification, the scope of misuse as well as steps to protect against such misuse or fraud.

**15. Use of Yes/ No authentication facility.**—(1) A requesting entity may use Yes/ No authentication facility provided by the Authority for verifying the identity of an Aadhaar number holder for its own use or on behalf of other agencies.

(2) A requesting entity may permit any other agency or entity to perform Yes/ No authentication by generating and sharing a separate license key for every such entity through the portal or any other mechanism provided by the Authority to the said requesting entity. For the avoidance of doubt, it is clarified that such sharing of license key is only permissible for performing Yes/ No authentication, and is prohibited in case of e-KYC authentication.

(3) Such agency or entity:

- a. shall not further share the license key with any other person or entity for any purpose; and

- b. shall comply with all obligations relating to personal information of the Aadhaar number holder, data security and other relevant responsibilities that are applicable to requesting entities.

(3A) AUAs/KUAs/Sub-AUAs/Sub-KUAs shall use their client application for Aadhaar authentication which shall be digitally signed by the requesting entity.

(4) It shall be the responsibility of the requesting entity to ensure that any entity or agency with which it has shared a license key, complies with the provisions of the Act, regulations, processes, standards, guidelines, specifications and protocols of the Authority that are applicable to the requesting entity.

(5) The requesting entity shall be jointly and severally liable, along with the entity or agency with which it has shared a license key, for non-compliance with the regulations, processes, standards, guidelines and protocols of the Authority.

**16. Use of e-KYC authentication facility.**—(1) A KUA may use the e-KYC authentication facility provided by the Authority for obtaining the e-KYC data of the Aadhaar number holder for its own purposes.

(2) A KUA shall obtain specific permission from the Authority by submitting an application for sharing of e-KYC data with Sub-KUA and such data may be shared in encrypted form as per the guidelines issued by the Authority from time to time, with specific consent of Aadhaar number holder.

(3) The Sub-KUA with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall not share it further with any other entity or agency.

(4) The Aadhaar number holder may, at any time, revoke consent given to a KUA/Sub-KUA for storing his e-KYC data, and upon such revocation, the KUA/Sub-KUA shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.

(5) In addition to the restriction on further sharing contained in sub-regulation (3), all other obligations relating to the personal information of the Aadhaar number holder, data security and other relevant responsibilities applicable to requesting entities, shall also apply to the Sub-KUA with whom e-KYC data has been shared in accordance with this regulation 16.

(6) The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with Sub- KUAs, for a period specified by the Authority.

**16A. Use of Offline Verification facility.**—(1) An OVSE may use the Offline Verification facility provided by the Authority for obtaining the offline Aadhaar data of the Aadhaar number holder only for the purpose specified to the Aadhaar number holder at the time of verification.

(2) No entity shall perform Offline Verification on behalf of another entity or person.

(3) An OVSE may store, with consent of the Aadhaar number holder, offline Aadhaar data of the Aadhaar number holder, received upon Offline Verification, securely as per the guidelines issued by the Authority from time to time.

(4) The Aadhaar number holder may, at any time, revoke consent given to an OVSE for storing his/her offline Aadhaar data, and upon such revocation, the OVSE shall delete the offline Aadhaar data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.

(5) The Authority in cases of default or breach or change in law or any other circumstance as may be deemed appropriate by it, may direct the OVSE to discontinue the use of Offline Verification services.

<sup>8</sup>[**16B. Manner of voluntary use of Aadhaar number.**—(1) An Aadhaar number holder may, in accordance with sub-section (3) of section 4 of the Act, voluntarily use the Aadhaar number in physical form, including Aadhaar letter (or copy thereof) or printed e-Aadhaar or Aadhaar PVC Card for a lawful purpose for establishing his identity by way of offline verification and the OVSE shall verify the printed details on Aadhaar letter or printed e-Aadhaar or Aadhaar PVC card with digitally signed Aadhaar Secure QR code<sup>12</sup>.

(2) An Aadhaar number holder may, in accordance with sub-section (3) of section 4 of the Act, voluntarily use the Aadhaar number in electronic form, including e-Aadhaar or Aadhaar Paperless Offline e-KYC (XML) or m-Aadhaar for a lawful purpose for establishing his identity by way of offline verification and the Offline Verification Seeking Entity shall verify the digital signature.

(3) An Aadhaar number holder may, in accordance with sub-section (3) of section 4 of the Act, voluntarily use the Aadhaar number in electronic form by way of authentication for a lawful purpose for establishing his identity by way of Yes/No or eKYC authentication facility through an authorized requesting entity.

**16C. Conditions for accepting an Aadhaar number as proof of identity of the Aadhaar number holder.**—(1) No Offline Verification Seeking Entity shall accept Aadhaar number, in physical or electronic form (without authentication), as a proof of identity for a lawful purpose, without first verifying the digital signature of the Authority as provided in the Aadhaar secure QR Code on Aadhaar Letter or e-Aadhaar or m-Aadhaar or Aadhaar Paperless Offline e-KYC (XML), as the case may be.

(2) No requesting entity shall accept Aadhaar number as a proof of identity of the Aadhaar number holder, in electronic form by way of authentication, unless it is for a lawful purpose which is in conformity with the relevant provisions of the Act and only with the informed consent of the Aadhaar number holder and in a manner as provided in these Aadhaar (Authentication and Offline Verification) Regulations, 2021.]

**17. Obligations relating to use of identity information by requesting entity.**—(1) A requesting entity shall ensure that:

---

<sup>8</sup> Ins. by notification No. K-11020/240/2021/Auth/UIDAI (No. 1 of 2022), dated 4.2.2022 (w.e.f. 4.2.2022).

- (a) the core biometric information collected from the Aadhaar number holder is not stored, shared or published for any purpose whatsoever, and no copy of the core biometric information is retained with it;
- (b) the core biometric information collected is not transmitted over a network without creation of encrypted PID block which can then be transmitted in accordance with specifications and processes laid down by the Authority.
- (c) the encrypted PID block is not stored, unless it is for buffered authentication where it may be held temporarily on the authentication device for a short period of time, and that the same is deleted after transmission;
- (d) identity information received during authentication is only used for the purpose specified to the Aadhaar number holder at the time of authentication, and shall not be disclosed further, except with the prior consent of the Aadhaar number holder to whom such information relates.
- (e) the identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected against access, use and disclosure not permitted under the Act and its regulations;
- (f) the private key used for digitally signing the authentication request and the license keys are kept secure and access controlled; and
- (g) all relevant laws and regulations in relation to data storage and data protection relating to the Aadhaar based identity information in their systems, that of their agents (if applicable) and with authentication devices, are complied with.

**18. Maintenance of logs by requesting entity.**—(1) A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely: -

- (a) specified parameters of authentication request submitted excluding Aadhaar number, Virtual ID, ANCS Token or UID token;
  - (b) specified parameters received as authentication response including full Aadhaar number or masked Aadhaar, as the case may be;
  - (c) the record of disclosure of purpose for which the authentication was performed, to the Aadhaar number holder or parent or guardian, in case of a child, at the time of authentication; and
  - (d) record of consent of the Aadhaar number holder, or parent or guardian, in case of a child, for authentication, but shall not, in any event, retain the PID information.
- (2) The logs of authentication transactions shall be maintained by the requesting entity for a period of 2 (two) years, during which period an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
- (3) Upon expiry of the period specified in sub-regulation (2), the logs shall be archived for a period of five years or the number of years as required by the laws or regulations governing

the entity, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained upon the order of a court not inferior to that of a Judge of a High Court or required to be retained for any pending disputes.

(4) The requesting entity shall not share the authentication logs with any person other than the concerned Aadhaar number holder upon his/her request or for grievance redressal and resolution of disputes or upon the order of a court not inferior to that of a Judge of a High Court. The authentication logs shall not be used for any purpose other than those stated in this sub-regulation.

(5) The requesting entity shall comply with all relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.

(6) The obligations relating to authentication logs as specified in these regulations shall continue to remain in force despite termination of appointment in accordance with these regulations.

**19. Roles, responsibilities and code of conduct of Authentication Service Agencies.**—An Authentication Service Agency shall have the following functions and obligations:-

- (a) provide secured connectivity to the CIDR to transmit authentication request from a requesting entity in the manner as may specified by the Authority for this purpose;
- (b) perform basic compliance and completeness checks on the authentication data packet before forwarding it to CIDR;
- (c) on receiving the response from CIDR, transmit the result of the transaction to the requesting entity that has placed the request;
- (d) only engage with the requesting entities approved by the Authority and keep the Authority informed of the list of requesting entities that it serves;
- (e) communicate to the Authority, all relevant information pertaining to any agreement that it may enter into with a requesting entity;
- (f) ensure that the persons employed by it for performing authentication and for maintaining necessary systems, infrastructure, processes, etc., possess requisite qualifications for undertaking such works;
- (g) ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis, and provide a certified audit report, to the Authority, confirming its compliance with the policies, processes, procedures, standards, or specifications, issued by the Authority in this regard, from time to time;
- (h) ensure that all infrastructure and operations including systems, processes, devices, software and biometric infrastructure, security, and other related aspects, are in compliance with the standards and specifications as may specified by the Authority for this purpose;

- (i) at all times, comply with directions, specifications, etc. issued by the Authority, in terms of network and other Information Technology infrastructure, processes, procedures, etc.
- (j) comply with all relevant laws and regulations relating, in particular, to data security and data management;
- (k) any value added service that an ASA provides to a requesting entity under a contract shall not form part of the Aadhaar authentication process;
- (l) shall be responsible to the Authority for all its authentication related operations, even in the event the ASA sub-contracts parts of its operations to other entities, the responsibility shall remain with the ASA;
- (m) in case of investigations relating to authentication related fraud or dispute, the ASA shall extend full cooperation to the Authority (or their agency) and/or any other authorized investigation agency, including providing access to its premises, records, systems, personnel, infrastructure, any other relevant resource or information and any other relevant aspect of its authentication operations;
- (n) may agree upon the authentication charges for providing services to a requesting entity, with such requesting entity, and the Authority shall have no say in this respect, for the time being; however, the Authority's right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;
- (o) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority.

**20. Maintenance of logs by Authentication Service Agencies.**—(1) An Authentication Service Agency shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:-

- (a) identity of the requesting entity;
- (b) parameters of authentication request submitted; and
- (c) parameters received as authentication response:

Provided that Aadhaar number, Virtual Id, UID Token, ANCS Token, PID information, device identity related data and e-KYC response data, where applicable shall not be retained.

(2) Authentication logs shall be maintained by the ASA for a period of 2 (two) years, during which period the Authority and/or the requesting entity may require access to such records for grievance redressal, dispute redressal and audit in accordance with the procedure specified in these regulations. The authentication logs shall not be used for any purpose other than stated in this sub-regulation.

(3) Upon expiry of the period specified in sub-regulation (2), the authentication logs shall be archived for a period of five years, and upon expiry of the said period of five years or the number of years as required by the laws or regulations governing the entity whichever is later, the authentication logs shall be deleted except those logs required to be retained by a

court not inferior to that of a Judge of a High Court or which are required to be retained for any pending disputes.

(4) The ASA shall comply with all applicable laws in respect of storage and maintenance of these logs, including the Information Technology Act, 2000.

(5) The obligations relating to authentication logs as specified in this regulation shall continue to remain in force despite termination of appointment in accordance with these regulations.

**20A. Optional Maintenance of Logs by Offline Verification Seeking Entity.**— (1) An Offline Verification Seeking Entity may maintain logs of the verification transactions processed by it, if deemed necessary by the OVSE and with consent of the resident, containing any of the following transaction details, namely:-

- (a) the offline Aadhaar data document shared by the resident in a suitably secure manner ;
- (b) any other data shared by the resident during the course of verification including mobile number, email id, photo etc;
- (c) local verification transaction logs between OVSE and the resident;
- (d) details of the notification related to the Offline Verification sent to the Aadhaar number holder. but shall not, in any event, store the Aadhaar number or Virtual ID of the Aadhaar number holder.

(2) The OVSE shall not share the logs with any person other than the concerned Aadhaar number holder or for grievance redressal and resolution of disputes in accordance with the provisions of the Act. The verification logs shall not be used for any purposes other than those stated in this sub-regulation.

**21. Audit of requesting entities, Authentication Service Agencies and Offline Verification Seeking Entities.**—(1) The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including their Sub-AUAs and Sub-KUAs, Authentication Service Agencies and Offline Verification Seeking Entities, either by itself or through audit agencies appointed by it, to ensure that such entities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued by the Authority.

(2) The Authority may conduct audits of the operations and systems of the entities referred to in sub-regulation (1), either by itself or through an auditor appointed by the Authority. The frequency, time and manner of such audits shall be as may be notified by the Authority from time to time.

(3) An entity subject to audit shall provide full co-operation to the Authority or any agency approved and/or appointed by the Authority in the audit process, and provide to the Authority or any agency approved and/or appointed by the Authority, complete access to its procedures, records and information pertaining to services availed from the Authority. The cost of audits shall be borne by the concerned entity.

(4) On identification of any deficiency by the Authority, the Authority may require the concerned entity to furnish necessary clarifications and/or information as to its activities and may also require such entity either to rectify the deficiencies or take action as specified in these regulations.

(5) Notwithstanding anything contained in clause (4), and without prejudice to any action which may be taken under the Act, the Authority may initiate action under Regulation 25(1A) on identification of any deficiency pursuant to the audit conducted.

**22. Data Security.**—(1) Requesting entities and Authentication Service Agencies/OVSEs shall have their servers used for Aadhaar authentication request formation and routing to CIDR/Offline Verification respectively, to be located within data centres or cloud storage centres located in India.

(1A) Authentication requests shall not be accepted from entities located outside the territorial borders of India. For allowing authentication requests from outside India, the requesting entity shall take specific permission from the Authority.

(2) Authentication Service Agency shall establish dual redundant, secured leased lines or MPLS connectivity with the data centres of the Authority, in accordance with the procedure and security processes as may be specified by the Authority for this purpose.

(3) Requesting entities shall use appropriate license keys to access the authentication facility provided by the Authority only through an ASA over secure network, as may be specified by the Authority for this purpose.

(4) Requesting Entities, Authentication Service Agencies and Offline Verification Seeking Entities shall adhere to all regulations, information security policies, processes, standards, specifications and guidelines issued by the Authority from time to time.

**23. Surrender of the access to authentication facility by requesting entity or Authentication Service Agency.**— (1) A Requesting Entity or ASA, appointed under these regulations, desirous of surrendering the access to the authentication facility granted by Authority, may make a request for such surrender to the Authority.

(2) While disposing such surrender request under these regulations, the Authority may require the requesting entity or ASA to satisfy the Authority about any matter necessary for smooth discontinuance or termination of services, including -

- (a) the arrangements made by the requesting entity for maintenance and preservation of authentication logs and other documents in accordance with these regulations and procedures as may be specified by the Authority for this purpose;
- (b) the arrangements made by the requesting entity for making authentication record available to the respective Aadhaar number holder on such request;
- (c) records of redressal of grievances, if any;
- (d) settlement of accounts with the Authority, if any;

- (e) in case of surrender by ASAs, the ASA, prior to the surrender of its access, shall ensure that its associated requesting entities are given adequate time to migrate to other ASAs in operation.

**24. Agencies appointed before commencement of these regulations.**—(1) Any Authentication User Agency (AUA) or e-KYC User Agency (KUA), appointed prior to the commencement of these regulations shall be deemed to be a requesting entity, and any Authentication Service Agency (ASA) or e-KYC Service Agency (KSA) shall be deemed to be an Authentication Service Agency, under these regulations, and all the agreements entered into between such agencies and the Unique Identification Authority of India, established vide notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or any officer of such authority shall continue to be in force to the extent not inconsistent with the provisions of the Act, these regulations, and other regulations, policies, processes, procedures, standards and specifications issued by the Authority.

(2) Notwithstanding anything contained in sub-regulation (1), any deemed requesting entity or Authentication Service Agency referred to in sub-regulation (1) shall be required to comply with the provisions of the Act, these regulations, other regulations framed by the Authority, and the policies, processes, procedures, standards and specifications issued by the Authority.

(3) In the event any such agency referred to in sub-regulation(1) seeks to discontinue using the authentication facility as specified in these regulations, it may immediately make an application for termination of its credentials and stop its functions forthwith:

Provided that in such cases, no compensation shall be payable to the agency or to the Authority upon such termination.

(4) On discontinuance under sub-regulation (3), the concerned entity shall be required to comply with the closure requirements listed in regulation 23(2).

**25. Liability and action in case of default.**—(1) Where any requesting entity or an ASA appointed under the Act,

- (a) fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time;
- (b) is in breach of its obligations under the Act and these regulations;
- (c) uses the Aadhaar authentication facilities for any purpose other than those specified in the application for appointment as requesting entity or ASA,
- (d) fails to furnish any information required by the Authority for the purpose of these regulations; or
- (e) fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority, the Authority may, without prejudice to any other action which may be taken under the Act, take such steps to impose disincentives on the requesting entity or an ASA for contravention of the provisions of the Act, rules and regulations

thereunder, including suspension of activities of such entity or agency, or other steps as may be more specifically provided for in the agreement entered into by such entities with the Authority:

Provided that the entity or agency shall be given the opportunity of being heard before the termination of appointment and discontinuance of its operations relating to Aadhaar authentication.

(1A). Where any Offline Verification seeking entity,

- (a) fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time; is in breach of its obligations under the Act and these regulations;
- (b) uses the Aadhaar Offline Verification facilities for purposes other than those specified;
- (c) fails to furnish any information required by the Authority for the purpose of these regulations; or
- (d) fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority, the Authority may, without prejudice to any other action which may be taken under the Act, including such criminal action as it may deem fit, take such steps to impose disincentives on the Offline Verification seeking entity for contravention of the provisions of the Act, rules and regulations thereunder.

Provided that the entity or agency shall be given the opportunity of being heard before any action is taken.

(2) Any such action referred to in sub-regulation (1) may also be taken against any entity or Sub-AUA or sub- KUA.

(3) Upon termination of appointment by the Authority, the requesting entity or the ASA shall, forthwith, cease to use the Aadhaar name and logo for any purposes, and in any form, whatsoever, and may be required to satisfy the Authority of necessary aspects of closure, including those enumerated in regulation 23(2).

#### ***CHAPTER IV***

#### **AUTHENTICATION TRANSACTION DATA AND AUTHENTICATION RECORDS**

**26. Storage and Maintenance of Authentication Transaction Data.**—(1) The Authority shall store and maintain authentication transaction data, which shall contain the following information: -

- (a) authentication request data received including PID block;
- (b) authentication response data sent
- (c) any authentication server side configurations as necessary

Provided that the Authority shall not, in any case, store the purpose of authentication or any meta data (other than process meta data) about any transaction.

**27. Duration of storage.**—(1) Authentication transaction data shall be retained by the Authority for a period of 6 months. The Authority may prescribe procedure to archive and perform analysis, for research purposes, from aggregated and anonymised authentication transaction data in the form of circulars.

(2) Upon expiry of the period of six months specified in sub-regulation (1), the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by the order of a court not inferior to that of a Judge of a High Court or in connection with any pending dispute.

**28. Access by Aadhaar number holder.**—(1) An Aadhaar number holder shall have the right to access his authentication records subject to conditions laid down and payment of such fees as prescribed by the Authority by making requests to the Authority within the period of retention of such records before they are archived.

(2) The Authority may provide mechanisms such as online portal or mobile application or designated contact centers for Aadhaar number holders to obtain their digitally signed authentication records within the period of retention of such records before they are archived as specified in these regulations.

(3) The Authority may provide digitally signed e-KYC data to the Aadhaar number holder through biometric or OTP authentication, subject to payment of such fees and processes as specified by the Authority,

(4) The authentication records and e-KYC data shall not be shared with any person or entity:

(a) other than with the Aadhaar number holder to whom the records or e-KYC data relate in accordance with the verification procedure specified. Aadhaar number holder may share their digitally signed authentication records and e-KYC data with other entities which shall not further share with any other agencies without obtaining consent of the Aadhaar holder every time before such sharing.

(b) Except in accordance with the provisions of the Act.

## **CHAPTER V**

### **MISCELLANEOUS**

**29. Repeal and savings.**—(1) All procedures, orders, processes, standards, specifications and policies issued and MOUs, agreements or contracts entered by the Unique Identity Authority of India, established vide notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or any officer of such authority, prior to the establishment of the Authority under the Act shall continue to be in force to the extent that they are not inconsistent with the provisions of the Act and regulations framed thereunder.

(2) Notwithstanding the repeal of the Aadhaar (Authentication) Regulations, 2016, anything done or any action taken under the said Regulations shall be deemed to have been done or taken under the corresponding provisions of these Regulations.

**30. Power to issue clarifications, guidelines and removal of difficulties.**—In order to remove any difficulties or clarify any matter pertaining to application or interpretation of these regulations, the Authority may issue clarifications and guidelines in the form of circulars.

**31. Power to issue policies, process documents, etc.**—The Authority may issue policies, orders, processes, standards, specifications and other documents not inconsistent with these regulations, which are required to be specified under these regulations or for which provision is necessary for the purpose of giving effect to these regulations.

<sup>9</sup>**[32. Doing of act or thing related to delegated power or function.**—(1) Any act or thing that is to be or may be done by the Authority under these regulations may also be done by any Member or officer of the Authority or any other person to whom the Authority has delegated the related power or function by general or special order in writing, under section 51 of the Act.

(2) The Authority may determine whether or not an act or thing done by a Member, officer or other person under sub-regulation (1) is related to a power or function delegated as referred to in the said sub-regulation.]

<sup>10</sup>[\*\*\*]

<sup>11</sup>[<sup>10</sup>[*SCHEDULE A*

## **ELIGIBILITY CRITERIA OF AUTHENTICATION SERVICE AGENCIES**

[See regulation 12(2A)]

1. Entities seeking appointment as ASA are categorised as follows:

<b>S. No.</b>	<b>Organisation category</b>
<b>Category 1</b>	A Ministry or Department of the Central Government ora State Government, or an undertaking owned or controlled by the Central Government or a State Government
<b>Category 2</b>	An authority constituted under any Central or State Act
<b>Category 3</b>	Any other entity of national importance in the opinion of the Authority
<b>Category 4</b>	A company registered in India under the Companies Act, 2013 (18 of 2013)
<b>Category 5</b>	An AUA or a KUA

<sup>9</sup>Inserted *vide* notification No. HQ-13073/1/2020-AUTH.II (E), dated 29.9.2023 (w.e.f. 3.10.2023).

<sup>10</sup>“Schedule A” omitted *vide* notification No. HQ-13011/240/2021-AUTH-II (No. 01 of 2023) dated 24.2.2023 (w.e.f. 27.2.2023) and“Schedule B” was substituted by “Schedule A” *vide* the said notification No. HQ-13011/240/2021-AUTH-II (No. 01 of 2023) dated 24.2.2023(w.e.f. 27.2.2023).

<sup>11</sup>“Schedule A” substituted *vide* notification No. HQ-13073/1/2020-AUTH.II (E), dated 29.9.2023 (w.e.f. 3.10.2023).

2. The technical and financial criteria for entities for appointment as ASA are as under:

Category	Financial requirement	Technical requirement
<b>Category 1, 2 and 3</b>	—	—
<b>Category 4</b>	Annual turnover of at least ₹100 crores as per the audited financial statements for last three financial years	<p>A Telecom Service Provider {Unified Licensee having Access Services authorisation or Unified Access Services Licensee, granted licence under section 4 of the Indian Telegraph Act, 1885 (13 of 1885)},having a minimum of 100 Multiprotocol Label Switching (MPLS) Points of Presence (PoP) in India</p> <p style="text-align: center;">OR</p> <p>A Network Service Provider or System Integrator having pan-India network connectivity for data transmission,having at least 100 MPLS PoPs in India</p>
<b>Category 5</b>	—	An AUA or KUA that meetssuch authentication transaction criteria as the Authority may determine from time to time.].