



भारत का राजपत्र The Gazette of India

असाधारण

EXTRAORDINARY

भाग III—खण्ड 4

PART III—Section 4

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं. 347]

नई दिल्ली, बुधवार, सितम्बर 14, 2016/भाद्र 23, 1938

No. 347]

NEW DELHI, WEDNESDAY, SEPTEMBER 14, 2016/BHADRA 23, 1938

भारतीय विशिष्ट पहचान प्राधिकरण

अधिसूचना

नई दिल्ली, 12 सितम्बर, 2016

भारतीय विशिष्ट पहचान प्राधिकरण (प्राधिकरण की बैठक में कार्य संचालन) विनियम, 2016

(2016 का सं. 1)

संख्या 13012/64/2016/विधि/यूआईडीएआई. (2016 का सं. 1).—आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 (2016 का 18वां) की धारा 19 की उप-धारा (1) के साथ पठित धारा 54 की उपधारा (2) की खंड (एच) के अंतर्गत प्राप्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा भारतीय विशिष्ट पहचान प्राधिकरण की बैठकों में कार्य संचालन को विनियमित करने के लिए निम्नलिखित विनियम बनाता है, नामतः :-

1. संक्षिप्त नाम और प्रारंभ :-

- (1) इन विनियमों को भारतीय विशिष्ट पहचान प्राधिकरण (प्राधिकरण की बैठकों में कार्य संचालन) विनियम, 2016 कहा जाएगा।
- (2) ये विनियम, इनके सरकारी राजपत्र में प्रकाशन की तिथि से प्रवृत्त 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 (2016 का 18वां) से है;
 - (ख) "प्राधिकरण" का अभिप्राय धारा 11 की उप-धारा (1) के तहत स्थापित भारतीय विशिष्ट पहचान प्राधिकरण से है;
 - (ग) "अध्यक्ष" में अधिनियम की धारा 12 के तहत नियुक्त प्राधिकरण के अध्यक्ष से है;
 - (घ) "सदस्य" में अधिनियम की धारा 12 के तहत नियुक्त प्राधिकरण के अध्यक्ष तथा सदस्य शामिल हैं;
 - (ङ) "मुख्य कार्यपालक अधिकारी" का अभिप्राय अधिनियम की धारा 18 की उप-धारा (1) के तहत नियुक्त मुख्य कार्यपालक अधिकारी से है, जो प्राधिकरण का सदस्य सचिव भी होगा;

(च) "बैठक" का अभिप्राय अधिनियम की धारा 19 की उपधारा (1) के तहत प्राधिकरण द्वारा आयोजित बैठक से है;

(छ) "अनुसूची" का अभिप्राय इन विनियमों की अनुलग्नक अनुसूची से है।

(2) यहां उपयोग किए गए शब्द या अभिव्यक्तियां, जिन्हें यहां परिभाषित नहीं किया गया है परन्तु अधिनियम में परिभाषित किया गया है, उनका वही अर्थ होगा, जो कि उन्हें अधिनियम में दिया गया है।

3. प्राधिकरण की बैठकें :-

(1) किसी एक वित्तीय वर्ष के दौरान, प्राधिकरण की कम से कम तीन बैठकें ऐसी तिथि तथा ऐसे स्थान पर आयोजित की जाएंगी जैसाकि अध्यक्ष आदेश दे तथा किसी भी स्थिति में दो बैठकों के बीच समय अंतराल पांच माह से अधिक नहीं होगा;

बशर्ते कि किसी वित्तीय वर्ष में प्राधिकरण की प्रथम बैठक उस वित्तीय वर्ष की प्रथम तिमाही में आयोजित की जाएगी।

(2) प्राधिकरण की प्रत्येक बैठक के नोटिस पर की जाने वाली बैठक का समय, तिथि तथा स्थान लिखकर मुख्य कार्यपालक अधिकारी द्वारा हस्ताक्षर किए जाएंगे।

(3) बैठक आयोजित किए जाने की तिथि से 15 दिवस पूर्व प्रत्येक सदस्य के पते पर डाक द्वारा अथवा ई-मेल अथवा कोरियर अथवा फ़ैक्स द्वारा जल्द से जल्द पहुंचाने के उद्देश्य से एक नोटिस भेजा जाए, जिसमें संक्षेप में बैठक की कार्यसूची, विचार किए जाने हेतु कार्य मदों का ब्यौरा दिया जाएगा।

(4) अति-आवश्यकता पड़ने पर अध्यक्ष पंद्रह दिनों से कम का नोटिस देकर किसी भी समय प्राधिकरण की बैठक बुला सकते हैं।

(5) प्राधिकरण की कोई बैठक लिखित में अध्यक्ष को संबोधित कर, अध्यक्ष को संबोधित कर, मुख्य कार्यपालक अधिकारी या कम से कम आधे सदस्यों के हस्ताक्षर द्वारा बुलाई जा सकेगी, जिसमें बुलाई जाने वाली बैठक का प्रयोजन तथा उसमें विचार किए जाने वाले कार्य का विवरण होगा।

(6) बैठक बुलाए जाने की मांग किए जाने पर, अध्यक्ष द्वारा निर्धारित किए गए समय पर बैठक बुलाई जा सकती है, जोकि इस प्रकार बैठक बुलाए जाने हेतु की गई मांग की प्राप्ति की तिथि से 15 दिन से ज्यादा नहीं होगी।

(7) यदि प्राधिकरण की किसी एक बैठक में कार्य की सभी मदों पर कार्रवाई नहीं की जा सके तो बैठक को समय-समय पर आस्थगित किया जा सकता है :

बशर्ते कि बैठक को आस्थगित किए जाने के बाद पुनः बुलाए जाने पर कार्यसूची में जिन मदों पर चर्चा पूर्ण नहीं की जा सकी, उन अपूर्ण मदों पर चर्चा की जाएगी तथा उस पर निर्णय लिया जाएगा।

4. प्राधिकरण की बैठकों की अध्यक्षता :-

(1) प्राधिकरण की बैठकों की अध्यक्षता प्राधिकरण का अध्यक्ष करेगा। उसकी अनुपस्थिति में प्राधिकरण की नियुक्ति की तिथि के अनुसार सदस्यगण और सदस्य सचिव में वरिष्ठतम, सदस्य द्वारा बैठकों की अध्यक्षता की जाएगी।

(2) बैठक का अध्यक्ष प्राधिकरण के किसी अधिकारी अथवा किसी अन्य व्यक्ति जोकि किसी बैठक में चर्चा किए जाने वाले मामले से पूर्णतः अवगत हो, को प्राधिकरण की किसी बैठक में भाग लेने के लिए बुला सकता है, जिससे सार्थक चर्चा की जा सके तथा ऐसे आमंत्रित बैठक की कार्यवाहियों में भाग ले सकते हैं परंतु उन्हें मतदान करने का कोई अधिकार नहीं होगा।

5. मुख्य कार्यपालक अधिकारी की सहभागिता :-

(1) मुख्य कार्यपालक अधिकारी प्राधिकरण के सदस्य-सचिव के रूप में प्राधिकरण की बैठक में भाग लेगा।

(2) मुख्य कार्यपालक अधिकारी, अध्यक्ष की अनुमति से प्राधिकरण की बैठकों से संबंधित अपने कर्तव्यों के निर्वहन हेतु किसी भी कर्मचारिवृंद की सहायता ले सकते हैं।

6. गणपूर्ति :-

(1) प्राधिकरण की किसी बैठक हेतु दो सदस्यों की गणपूर्ति होगी तथा प्राधिकरण की किसी बैठक में तब तक कोई कार्य नहीं किया जाएगा जब तक कि बैठक की समस्त अवधि के दौरान गणपूर्ति न हो।

(2) यदि प्राधिकरण की किसी बैठक में गणपूर्ति न हो तो, अध्यक्ष अथवा उसकी अनुपस्थिति में मुख्य कार्यपालक अधिकारी अथवा बैठक की अध्यक्षता करने वाला वरिष्ठतम सदस्य बैठक को ऐसी अन्य तिथि, समय तथा स्थान पर अधिकतम तीस दिनों के अंदर पुनः आयोजन करने के लिए स्थगित करेगा, जैसा कि उसके द्वारा विनिर्दिष्ट किया जाए :

बशर्ते कि इस प्रकार स्थगित की गई बैठक में यदि गणपूर्ति न हो तो, उप-विनियम (1) में अंतर्विष्ट किसी शर्त के रहते हुए उक्त स्थगित की गई बैठक में मौजूद सदस्यों की संख्या को ऐसी बैठक में चर्चा करने तथा केवल प्रारंभिक बैठक हेतु कार्यसूची में दिए कार्य की मदों के निपटान हेतु गणपूर्ति मानी जाएगी।

7. कार्यसूची :-

- (1) मुख्य कार्यपालक अधिकारी, प्राधिकरण की प्रत्येक बैठक के लिए कार्यसूची तैयार करने तथा उसे प्राधिकरण के सभी सदस्यों के बीच ऐसी प्रत्येक बैठक में कम से कम 7 दिनों की अवाधि पूर्व परिचालित करने के लिए उत्तरदायी होगा।
बशर्त कि मुख्य कार्यपालक अधिकारी, अध्यक्ष के परामर्श से बैठक की कार्यसूची तैयार करेगा :
बशर्त यह भी कि मुख्य कार्यपालक अधिकारी, अध्यक्ष के परामर्श से कार्यसूची को जारी करने के पश्चात् कार्यसूची में संशोधन कर सकता है अथवा उसमें नई मद को डाल सकता है अथवा पुरानी मद का लोप कर सकता है।
- (2) कार्यसूची में शामिल नहीं किये गए किसी कार्य को प्राधिकरण के अध्यक्ष अथवा बैठक की अध्यक्षता कर रहे अन्य सदस्य की अनुमति के बिना बैठक में नहीं उठाया जाएगा।
- (3) अध्यक्ष अथवा बैठक की अध्यक्षता कर रहे अन्य सदस्य की अनुमति से, बैठक के समापन पूर्व किसी भी समय कार्यसूची में तत्काल स्वरूप के प्रश्नों को शामिल किया जा सकता है अथवा कार्यसूची की किसी मद का लोप किया जा सकता है अथवा उसे बाद में आयोजित की जाने वाली आगामी बैठक में कार्रवाई करने के लिए ले जाया जा सकता है।

8. प्राधिकारी की बैठकों में निर्णय :-

- (1) यदि किसी सदस्य का बैठक में किए जाने वाले कार्य की किसी मद में कोई हित निहित हो तो वह ऐसी मद की कार्रवाई अथवा मतदान में भाग नहीं लेगा और ऐसे मामले में मद पर बैठक में भाग लेने वाले अन्य सदस्य के बहुमत से निर्णय लिया जाएगा।
- (2) अध्यक्ष अथवा बैठक की अध्यक्षता कर रहे अन्य सदस्य हमेशा प्रयास करेंगे कि वह किसी निर्णय अथवा सिफारिशों पर सदस्यों के बीच आपसी सहमति से निर्णय लें और यदि सहमति बनाने का प्रयास असफल रहे तो मतदान किया जाएगा। समान मतदान किए जाने की स्थिति में अध्यक्ष अथवा उसकी अनुपस्थिति में पीठासीन अधिकारी का मत निर्णायक होगा।
- (3) प्राधिकरण के सभी बैठकों में कार्यों की प्रत्येक मद पर हाथ उठाकर मतदान किया जाएगा।
- (4) प्राधिकरण के सभी निर्णयों पर प्राधिकरण के सदस्य-सचिव हस्ताक्षर करेंगे।
- (5) प्राधिकरण की प्रत्येक बैठक में लिए गए निर्णय को प्राधिकरण की वेबसाइट पर डाला जाएगा जब तक अध्यक्ष गोपनीयता सुनिश्चित करने के उद्देश्य से अन्यथा निर्णय न लें।

9. चर्चा का समापन :-

अध्यक्ष या बैठक की अध्यक्षता करने वाला सदस्य बैठक में विचार किए जाने वाले किसी कार्य की मद पर, जब उनके विचार से बैठक में चर्चा किए गए किसी कार्य पर सभी सदस्यों को अपने विचार व्यक्त करने का अवसर प्राप्त हो गया है, चर्चा के समापन के लिए प्रस्ताव रखेगा तथा इस संबंध में अध्यक्ष अथवा बैठक की अध्यक्षता कर रहे सदस्य का निर्णय अंतिम होगा।

10. प्राधिकरण की बैठकों के कार्यवृत्त-

- (1) मुख्य कार्यपालक अधिकारी, प्राधिकरण द्वारा आयोजित प्रत्येक बैठक का मसौदा कार्यवृत्त ऐसी बैठक समापन के दो सप्ताह के अंदर तैयार करवायेगा तथा इन्हें अध्यक्ष या बैठक की अध्यक्षता कर चुके सदस्य के अनुमोदनार्थ प्रस्तुत करेगा:
बशर्त कि किसी कारणवश यदि मुख्य कार्यपालक अधिकारी प्राधिकरण की बैठक में भाग न ले पाएं तो, अध्यक्ष इस अस्थायी प्रयोजन स्वरूप प्राधिकरण के किसी अन्य अधिकारी को बैठक में कार्यवृत्त तैयार करने के लिए निदेश दे सकता है।
- (2) प्राधिकरण की प्रत्येक बैठक के मसौदा कार्यवृत्त को अध्यक्ष या बैठक की अध्यक्षता कर रहे सदस्य द्वारा अनुमोदित किया जाएगा तथा इसे अगली बैठक में अंगीकार करने के लिए ऐसे अनुमोदन की तिथि से अधिकतम दो सप्ताह के अंदर प्रत्येक सदस्य को भेजा जाएगा।
बशर्त कि मसौदा कार्यवृत्त में किए गए ऐसे परिवर्तन, यदि कोई हों तो, पर अध्यक्ष का निर्णय अंतिम होगा।
- (3) प्राधिकरण की प्रत्येक बैठक के कार्यवृत्त में बैठक में हुई कार्रवाईयों का उचित तथा सटीक सारांश तथा सदस्यों के नाम अंतर्विष्ट होंगे, जिन्होंने चर्चा में भाग नहीं लिया अथवा बैठक में किसी कार्य की मद पर मतदान नहीं किया।
- (4) अध्यक्ष अथवा कोई अन्य सदस्य, जिसने बैठक की अध्यक्षता की, यदि उसके विचार से, कोई मामला कार्रवाईयों के लिए संगत अथवा विषयानुकूल नहीं है अथवा किसी व्यक्ति के संबंध में मानहानिकारक है तो वह किसी मामले को कार्यवृत्त में ऐसे शामिल किए जाने अथवा नहीं किए जाने के संबंध में निर्णय ले सकता है।
- (5) प्राधिकरण की प्रत्येक बैठक में, पिछली बैठक की अध्यक्षता करने वाले अध्यक्ष अथवा अन्य सदस्य द्वारा अनुमोदित पिछली बैठक के मसौदा कार्यवृत्त को संशोधनों और आशोधनों सहित अथवा उनके बिना, बैठक में पुष्टि तथा अंगीकार किए जाने के लिए रखा जाएगा और उस बैठक में पुष्टि किए जाने अथवा अंगीकार किए जाने पर, पिछली बैठक की कार्रवाईयों के अभिलेख की पुष्टि अथवा सटीकता के प्रमाण स्वरूप, बैठक की अध्यक्षता कर रहे अध्यक्ष अथवा अन्य सदस्य द्वारा हस्ताक्षर किये जाएंगे तथा उन्हें प्राधिकरण के अभिलेख के रूप में रखा जाएगा।

11. तत्काल कार्रवाई करने के लिए मुख्य कार्यपालक अधिकारी की शक्तियां :-

मुख्य कार्यपालक अधिकारी ऐसी कार्रवाई कर सकता है जो प्राधिकरण द्वारा तुरंत कार्रवाई किए जाने हेतु आपातकालीन स्थिति में की जानी अनिवार्य हों, जब प्राधिकरण की बैठक बुलाया जाना व्यावहारिक न हो और इस संबंध में कारणों को लिखित में दर्ज किया जाए :

बशर्ते कि ऐसी कार्रवाई अथवा निर्णय, जैसा भी मामला हो, के संबंध में सदस्यों को सात दिनों की अवधि के अंदर जानकारी दी जाएगी :

बशर्ते यह भी कि ऐसी किसी कार्रवाई की पुष्टि किए जाने हेतु इसे प्राधिकरण की अगली बैठक में रखा जाएगा।

12. परिचालन के माध्यम से निर्णय लिया जाना :-

(1) कार्य की कोई मद अथवा मुद्दा जिस पर प्राधिकरण द्वारा निर्णय लिया जाना हो, यदि उस संबंध में अध्यक्ष महोदय निदेश दें तो संकल्प के रूप में मामले को परिचालित कर सदस्यों को भेजा जा सकता है।

(2) किसी संकल्प को सदस्यों द्वारा पारित माना जाएगा, जब ऐसे मसौदे में परिचालित संकल्प तथा उसकी अनिवार्य सामग्री, यदि कोई हो तो, सहित सभी सदस्यों को उनके आधिकारिक ई-मेल पर भेजा गया हो तथा सदस्यों के बहुमत से अनुमोदित किया गया हो।

बशर्ते कि सभी सदस्यों के उत्तर, अधिकतम तीन दिनों की अवधि के अंदर प्राप्त किए जाएंगे।

(3) उप-विनियम(1) के तहत परिचालित कोई संकल्प जिसे मतदान करने हेतु अर्हक ऐसे सदस्यों द्वारा बहुमत से अनुमोदित किया गया हो, का ऐसा बाध्यकारी प्रभाव होगा जैसा कि बैठक में सदस्यों के बहुमत से इस पर निर्णय लिया गया हो।

(4) उप-विनियम(1) के तहत परिचालित मसौदा संकल्प पर किए गए मतदान तथा प्राप्त टिप्पणियों के आधार पर, अध्यक्ष—

(क) निर्णय को अंगीकार किया गया घोषित कर सकेगा;

(ख) निर्णय को अंगीकार नहीं किया गया घोषित कर सकेगा;

(ग) बराबर मत पड़ने पर प्राधिकरण की अगली बैठक में कार्रवाई करने के लिए मसौदा संकल्प को स्थगित कर सकेगा।

(5) परिचालन के माध्यम से पारित किसी संकल्प की पुष्टि करने के लिए प्राधिकरण की अगली बैठक के समक्ष रखा जाएगा।

13. कार्रवाइयों का अभिलेख :-

(1) मुख्य कार्यपालक अधिकारी, प्राधिकरण की बैठक में भाग लेगा तथा उसकी सभी कार्य की मदों पर की गई कार्रवाइयों के अभिलेखों का रख-रखाव करेगा।

(2) प्राधिकरण के प्रत्येक निर्णय तथा निदेश को लिखित में दर्ज किया जाएगा तथा अभिलेख के रूप में रखा जाएगा।

14. स्वायत्तता तथा गोपनीयता :-

(1) प्राधिकरण के सदस्य इसकी बैठकों में भागीदारी करने तथा उनमें शामिल होने के लिए प्रतिबद्ध होंगे।

(2) प्रत्येक सदस्य, प्राधिकरण की प्रत्येक बैठक में अनुसूची-I में निहित संबंधी विशिष्ट घोषणा प्रस्तुत करेंगे, जिसे कार्यसूची में किसी मद के संबंध में उनकी स्वायत्तता पर प्रतिकूल प्रभाव डालने वाला समझा जा सकता है।

(3) बैठक में भाग लेने वाला कोई सदस्य अथवा कोई भागीदार जो मानता हो कि उसके हित उसकी स्वायत्तता पर प्रतिकूल प्रभाव डाल सकते हैं, वह लिखित में अध्यक्ष को जानकारी देगा जो बैठकों अथवा प्राधिकरण के कार्य में उसकी भागीदारी के संबंध में निर्णय लेगा।

(4) प्राधिकरण के सदस्य तथा आमंत्रितगण अनुसूची-II में प्राधिकरण की बैठकों में किए गए कार्य की गोपनीयता को बरकरार रखने के लिए प्रारंभिक घोषणा पर हस्ताक्षर करेंगे।

15. सचिवालय :-

मुख्य कार्यपालक अधिकारी उपयुक्त प्रशासनिक सहायता सुनिश्चित करेंगे, जिससे प्राधिकरण को उसके कार्य करने में सक्षम बनाया जा सकेगा।

16. व्यय की प्रतिपूर्ति:-

प्राधिकरण की बैठक में विशेष आमंत्रितगण प्रत्येक बैठक में भाग लेने के लिए दो हजार रुपए के भुगतान तथा वास्तविक यात्रा तथा निर्वाह व्यय की प्रतिपूर्ति के लिए हकदार होंगे।

17. कठिनाई का निवारण :-

इन विनियमों के कार्यान्वयन अथवा तत्संबंधी निर्वचन के मामले में यदि कोई संदेह अथवा कठिनाई पैदा होती है तो इसे प्राधिकरण के समक्ष रखा जाएगा तथा इस पर प्राधिकरण का निर्णय अंतिम होगा।

अनुसूची-I

{विनियम 14(2) देखें}

हितों के संबंध में विशिष्ट घोषणा

नाम:.....

पेशा:.....

भारतीय विशिष्ट पहचान प्राधिकरण की बैठक

बैठक की तिथि	
स्थान	

क्र. संख्या	कार्यसूची की मदें	क्या सदस्य का कोई हितों का टकराव है (हां/नहीं) यदि हां, कृपया अध्यक्ष को निर्णय लेने हेतु सक्षम बनाने के लिए ब्यौरा दें

घोषणा: मैं घोषणा करता हूं कि उपर्युक्त उपलब्ध करायी गई जानकारी सत्य तथा पूर्ण है।

घोषणा.....दिन.....माह.....वर्ष में की गई

हस्ताक्षर.....

अनुसूची-II

{विनियम 14(4) देखें}

गोपनीयता के संबंध में घोषणा

नाम:.....

पद:

 भारतीय विशिष्ट पहचान प्राधिकरण का सदस्य अन्य विशेषज्ञ (बाह्य)

दिनांक:.....

मैं, एतद्वारा घोषणा करता हूं कि मैं गोपनीयता के संबंध में अपनी बाध्यता से अवगत हूं। मैं जानता हूं कि यदि भारतीय विशिष्ट पहचान प्राधिकरण में मेरे क्रियाकलापों के परिणामस्वरूप मुझे प्राप्त हुई कोई जानकारी, जो गोपनीय स्वरूप की हो, तो उसे उद्घटित नहीं करने के लिए बाध्य हूं और मैं, एतद्वारा वचन देता हूं कि मैं ऐसी गोपनीय जानकारी उद्घटित नहीं करूंगा। मैं, अन्य सदस्यों द्वारा बैठकों में चर्चा के दौरान अन्य सदस्यों द्वारा व्यक्त किए गए अथवा उनके द्वारा लिखित में रखे गए विचारों की गोपनीयता को बनाए रखूंगा।

घोषणा.....दिन.....माह.....वर्ष में की गई

हस्ताक्षर.....

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यपालक अधिकारी

[विज्ञापन-III/4/असा./238]

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

NOTIFICATION

New Delhi, the 12th September, 2016

UNIQUE IDENTIFICATION AUTHORITY OF INDIA (TRANSACTION OF BUSINESS AT MEETINGS OF THE AUTHORITY) REGULATIONS, 2016

(No. 1 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 1 of 2016).—In exercise of the powers conferred by clause (h) of sub-section (2) of section 54 read with sub-section (1) of section 19 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), the Unique Identification Authority of India hereby makes the following regulations regulating the transaction of business in the meetings of the Unique Identification Authority of India, namely:

1. Short Title and Commencement – (1) These Regulations may be called the Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulation, 2016.

(2) They 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 (18 of 2016);
- (b) “Authority” means the Unique Identification Authority of India established under sub-section (1) of Section 11 of the Act;
- (c) “Chairperson” means the Chairperson of the Authority appointed under Section 12 of the Act;
- (d) “Member” includes the Chairperson and Member of the Authority appointed under section 12;
- (e) “Chief Executive Officer” means the Chief Executive Officer, who shall be Member Secretary of the Authority, appointed under sub-section (1) of Section 18 of the Act;
- (f) “Meeting” means meeting convened by the Authority as per sub-section (1) of Section 19 of the Act;
- (g) “Schedule” means a Schedule appended to these regulations.

(2) Words and expressions used herein but not defined, and defined in the Act, shall have the same meanings assigned to them in the Act.

3. Meetings of the Authority– (1) There shall be no less than three meetings of the Authority in a financial year on such dates and at such places as the Chairperson may direct and the interval between any two meetings shall not in any case, be longer than five months:

Provided that the first meeting of the Authority in a financial year shall be held in the first quarter of that financial year.

(2) The notice of every meeting of the Authority shall be signed by the Chief Executive Officer intimating the time, date and place of the intended meeting.

(3) The notice shall be given to every member, at least 15 days before the date of the meeting by post to the address of every member or through e-mail or courier or Fax to facilitate speedy communication, stating therein the brief agenda of the meeting, setting out the items of business to be considered.

(4) The Chairperson, may, in case of urgency, at any time, call a meeting of the Authority at a lesser notice than fifteen days.

(5) A meeting of the Authority may be called on the requisition in writing, addressed to the Chairperson, and signed by the Chief Executive Office or signed by not less than half of the members, setting out therein the purpose of the meeting to be called and the business to be considered thereat.

(6) On receipt of the requisition of meeting, the Chairperson may direct to cause the meeting to be convened and held within such time as he may direct, but in any case not later than a period of 15 days from the date of receipt of such requisition.

(7) If all the items of business to be transacted at a meeting of the Authority cannot be completed in one sitting, the meeting may be adjourned from time to time:

Provided that at the meeting convened post adjournment only the unfinished items in the Agenda shall be discussed and decision taken thereon.

4. Chairperson of the meetings of the Authority – (1) The Chairperson shall preside over the meetings of the Authority. In his absence, the senior most among the Members and Member Secretary, in terms of date of appointment to the Authority, shall preside over the meetings of the Authority.

(2) The Chairperson of the meeting may also invite any officer of the Authority or any other person qualified in the matters to be discussed at any meeting to attend any meeting of the Authority, with a view to facilitate meaningful discussions and such invitee may participate in the proceedings of the meeting but shall have no right to vote.

5. Participation of the Chief Executive Officer – (1) The Chief Executive Officer shall participate in meeting of the Authority as Member Secretary of the Authority.

(2) The Chief Executive Officer may, with permission of Chairperson, take the assistance of any staff of the Authority for the purpose of discharging his duties relating to the meetings of the Authority.

6. Quorum. – (1) The quorum for any meeting of the Authority shall be two and no business shall be transacted at any meeting of the Authority unless the quorum is present throughout the meeting.

(2) If the quorum is not present at any meeting of the Authority, the Chairperson or in his absence, the Chief Executive Officer or the senior most Member presiding over the meeting, shall adjourn the meeting to such other date, time and place as may be specified by him not being later than thirty days:

Provided that if at such adjourned meeting quorum is not present, then, notwithstanding anything contained in sub-regulation (1), the Members present at the said adjourned meeting, shall constitute a quorum for such meeting to take up discussion and to dispose of only the items of business set out in the agenda for the initial meeting.

7. Agenda. – (1) The Chief Executive Officer shall be responsible for preparation of the agenda for each meeting of the Authority and circulation thereof to all the Members of the Authority at least a period of seven days before the date of each meeting:

Provided that the Chief Executive Officer shall prepare the agenda of meeting in consultation with the Chairperson:

Provided further that Chief Executive Officer may, in consultation with the Chairperson, amend or delete or add new item in the Agenda of business subsequent to its issue.

(2) Any business not included in the agenda shall not be transacted at a meeting of the Authority except with the permission of the Chairperson or other Member presiding over the meeting.

(3) With the permission of the Chairperson or other Member presiding over the meeting, urgent questions may be added to the Agenda at any time before the conclusion of the meeting, or any item on the Agenda may be deleted or carried over to a subsequent meeting.

8. Decision of meetings of the Authority– (1) If a Member has an interest in any item of business to be transacted at a meeting, he shall not participate or vote on such item and in such case, the decision on such item shall be taken by majority of the votes of other Members attending the meeting.

(2) The Chairperson or the other Member presiding over the meeting shall endeavour at all times to arrive at decisions or recommendations through a consensus among Members and voting shall be resorted to if attempts to arrive at a consensus fail. In the event of equality of votes, the Chairperson, or, in his absence, the presiding Member, shall have a casting vote.

- (3) Votes on every item of business to be transacted at a meeting of the Authority shall be taken by a show of hands.
- (4) All decisions of the Authority shall be signed by the Member-Secretary of the Authority.
- (5) Decisions taken at every meeting of the Authority shall be published on the website of Authority unless the Chairperson determines otherwise on grounds of ensuring confidentiality.

9. Closure of debates. – (1) The Chairperson or the Member presiding over the meeting may move for the closure of the debate or any item of business discussed at a meeting when he considers that all members have had the opportunity to express their views on any business discussed at the meeting and the decision of the Chairperson or the Member presiding shall be final.

10. Minutes of meeting of the Authority. – (1) The Chief Executive Officer shall cause the draft minutes of each meeting of the Authority to be prepared within a period of two weeks of conclusion of each meeting and submit the same to the Chairperson or other Member who presided over the meeting, for his approval:

Provided that if for any reasons the Chief Executive Officer is unable to attend any meeting of the Authority, the Chairperson may, for this temporary purpose direct any other officer of the Authority, to prepare minutes of the meeting.

(2) The draft minutes of each meeting of the Authority approved by the Chairperson or the other Member who presided over that meeting shall be forwarded to each member not later than a period of two weeks from such approval, for adoption at the next meeting:

Provided that the decision of the Chairperson on the changes, if any, to be made in the draft minutes, shall be final.

(3) The minutes of each meeting of the Authority shall contain a fair and correct summary of the proceedings thereat and the names of Members who did not participate in the discussion of, or vote on, any item of business transacted at the meeting.

(4) The Chairperson or other Member who presided over the meeting may decide the inclusion or non-inclusion of any matter in the minutes, if in his opinion, the same is not relevant or material to the proceedings or defamatory of any person.

(5) At every meeting of the Authority, the draft minutes of the previous meeting approved by the Chairperson or the other Member who presided over that previous meeting shall be placed before the meeting for confirmation and adoption, with or without amendments or modifications, and upon confirmation and adoption in that meeting, be signed by the Chairperson or other Member presiding over the meeting, as confirmation of correctness of the record of the proceedings of the previous meeting and be kept as a record of the Authority.

11. Power of the Chief Executive Officer to take urgent action. – The Chief Executive Officer may take such action as may be necessary in case of an emergency situation warranting immediate action by the Authority and when it is not feasible to call a meeting of the Authority, and for the reasons be recorded in writing:

Provided that any such action or decision, as the case may be, shall be communicated to all the Members within a period of seven days:

Provided further that any such action shall be placed in the next meeting of the Authority for its ratification.

12. Decision by circulation. – (1) Any item of business or issue which requires decision of the Authority, if the Chairperson so directs, may be referred to Members by circulation of the matter as a resolution.

(2) A resolution shall be deemed to have been passed by the Members when such a resolution circulated in the draft, together with necessary material, if any, to all the Members to their official email ids and the resolution is approved by the majority of the Members:

Provided that the replies of all Members shall be obtained within a period not more than three clear days.

(3) Any resolution circulated under sub-regulation (1) and approved by the majority of such of those Members entitled to vote thereon, shall have such effect and be binding as if such resolution were decided by the majority of the members at a meeting.

(4) Based upon the votes and comments received on the draft resolution circulated under sub-regulation (1), the Chairperson may-

- (a) declare the decision adopted; or
 (b) declare the decision not adopted; or
 (c) in case of neutrality of votes, postpone draft resolution for the next meeting of the Authority.

(5) Any resolution passed through circulation, shall be placed at the next meeting of the Authority for its ratification.

13. Record of Business. –(1) The Chief Executive Officer shall attend the meetings of the Authority, maintain the record of proceedings of all items of the business transacted there at.

(2) Every decision and direction of the Authority shall be recorded in writing and be kept as a record.

14. Independence and Confidentiality–(1) Members of the Authority shall make a commitment to attend and participate in its meetings.

(2) Every Member shall submit at each meeting of the Authority a Specific Declaration of Interest in Schedule I, which might be considered prejudicial to their independence in relation to any of the items on the agenda.

(3) Any Member or any other participant in a meeting, who believes that his interests may undermine his independence, shall inform the Chairperson in writing who thereon shall take a decision on his participation in the discussions at the meetings or the work of the Authority.

(4) Members of the Authority and invitees shall sign an initial Declaration at the first meeting of the Authority for maintaining the confidentiality of the business transacted at meetings of the Authority in Schedule II.

15. Secretariat. –Chief Executive Officer shall ensure appropriate administrative support to enable the Authority to carry out its work.

16. Reimbursement of expenses. – Special invitees to any meeting of the Authority shall be entitled to a payment of two thousand rupees for attending each meeting and the reimbursement of actual travel and subsistence expenses.

17. Removal of difficulty. – In the matter of implementation of these regulations or matters relating to interpretation thereof, if any doubt or difficulty arises, the same shall be placed before the Authority and the decision of the Authority thereon shall be final.

SCHEDULE-I

[See Regulation 14 (2)]

SPECIFIC DECLARATION OF INTERESTS

Name: _____

Profession: _____

Meeting of the Unique Identification Authority of India

Meeting dates	
Venue	

S.No.	Agenda Items	Whether the member has a conflict of interest. (YES/NO) If yes, please provide details to enable the chair to take a decision.

Declaration: I declare that the information provided above is true and complete.

Done at: _____ on this _____ day of _____.

Signature: _____

SCHEDULE-II
[See Regulation 14 (4)]
DECLARATION CONCERNING CONFIDENTIALITY

Name: _____

Position:

[] Member of the Unique Identification Authority of India

[] Other expert (external)

on _____

I hereby declare that I am aware of my obligation to respect confidentiality. I know that I am obliged not to divulge information acquired as a result of my activities in Unique Identification Authority of India, if the information is subject to a request for confidentiality and I hereby undertake not to divulge any such confidential information. I shall also respect the confidential nature of the opinions expressed by other Members or other experts during discussions in meetings or provided in written form.

Done at: _____ on this _____ day of _____.

Signature: _____

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ADVT.-III/4/Exty./238]

अधिसूचना

नई दिल्ली, 12 सितम्बर, 2016

आधार (नामांकन और अद्यतन) विनियम, 2016

(2016 का सं. 2)

सं. 13012/64/2016/विधि/यूआईडीएआई (2016 का सं. 2).— आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा 54 की उप-धारा (2) के उप-खंड (ए), (बी), (डी), (ई), (जे), (के), (एल), (एन), (आर), (एस) एवं (वी) तथा उप-धारा (1) के अंतर्गत प्राप्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा निम्नलिखित विनियम बनाता है, नामतः :-

अध्याय-I

प्रारंभिक

1. संक्षिप्त नाम और प्रारंभ :-

- (1) इन विनियमों को आधार (नामांकन और अद्यतन) विनियम, 2016 (2016 का सं. 2) कहा जाएगा।
- (2) ये विनियम इनके सरकारी राजपत्र में प्रकाशन की तिथि से प्रवृत्त 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;
 - (ख) **“आधार पत्र”** का अभिप्राय किसी निवासी को आधार नंबर संप्रेषित करने वाले दस्तावेज से है;
 - (ग) **“आधार नंबर धारक”** का अभिप्राय कोई व्यक्ति, जिसे अधिनियम के अंतर्गत आधार नंबर जारी किया गया है, से है;
 - (घ) **“अधिप्रमाणन”** का अभिप्राय, वह प्रक्रिया, जिसके द्वारा उसके आधार नंबर समेत किसी व्यक्ति की जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना उसके सत्यापन के लिए 'केन्द्रीय पहचान आंकड़े निक्षेपागार (सेंट्रल आइडेंटिटीज डाटा रिपोजिटरी) के पास जमा की जाती है और ऐसा निक्षेपागार उसकी शुद्धता अथवा कमी को उपलब्ध सूचनाओं के आधार पर सत्यापित करता है, से है;

- (च) "प्राधिकरण" का अभिप्राय अधिनियम की धारा 11 की उप-धारा (1) के तहत स्थापित भारतीय विशिष्ट पहचान प्राधिकरण से है;
- (छ) "केन्द्रीय पहचान आंकड़े निक्षेपागार" अथवा "सीआईडीआर" का अभिप्राय एक या एक से अधिक स्थानों पर केन्द्रीकृत डाटा बेस है, जिसमें आधार नंबर धारक को जारी आधार नंबर सहित ऐसे व्यक्तियों की जनसांख्यिकीय तथा बायोमैट्रिक सूचना तथा तत्संबंधी अन्य संबद्ध सूचना शामिल हैं, से है;
- (ज) "नामांकन एजेंसी" का अभिप्राय अधिनियम के अंतर्गत व्यक्तियों की जनसांख्यिकीय सूचना और बायोमैट्रिक सूचना एकत्रित करने के लिए प्राधिकरण अथवा किसी पंजीयक द्वारा नियुक्त एजेंसी से है;
- (झ) "नामांकन" का अभिप्राय इस अधिनियम के अंतर्गत विनियमों में विहित व्यक्तियों को अधिनियम के अंतर्गत आधार नंबर जारी करने के प्रयोजन से नामांकन एजेंसियों द्वारा उनसे जनसांख्यिकीय सूचना और बायोमैट्रिक सूचना एकत्र करने की प्रक्रिया से है;
- (ट) "नामांकन केंद्र" का अभिप्राय निवासियों के नामांकन और उनकी सूचना अद्यतित करने के लिए किसी नामांकन एजेंसी द्वारा बनाया गया स्थायी अथवा अस्थायी केंद्र से है;
- (ठ) "नामांकन आईडी" या "ईआईडी" का अभिप्राय नामांकन के समय निवासियों को आवंटित 28 अंकीय नामांकन पहचान नंबर से है;
- (ड) "परिवार का मुखिया" का अभिप्राय किसी निवासी के परिवार के किसी सदस्य से है जिसके संबंध में उस निवासी के साथ संबंध दर्शाने वाला कोई दस्तावेज दिया जा सकता है, और इसमें उस निवासी का पिता, माता अथवा पति या पत्नी शामिल हो सकता है;
- (ढ) "पहचान सूचना" में किसी व्यक्ति के संबंध में उसका आधार नंबर, जनसांख्यिकीय सूचना और बायोमैट्रिक सूचना शामिल हैं;
- (ण) "परिचयदाता" का अभिप्राय ऐसे निवासियों का परिचय देने के लिए, जिनके पास विहित संगत दस्तावेज नहीं हैं, पंजीयकों द्वारा अधिकृत व्यक्ति अभिप्रेत है;
- (त) "ऑपरेटर" से नामांकन केंद्रों पर नामांकन प्रक्रिया का संपादन करने के लिए नामांकन एजेंसियों द्वारा नियोजित प्रमाणित कार्मिक अभिप्रेत है;
- (थ) "पंजीयक" (रजिस्ट्रार) का अभिप्राय इस अधिनियम के तहत व्यक्तियों को नामांकित करने के प्रयोजनार्थ प्राधिकरण द्वारा प्राधिकृत या मान्यताप्राप्त किसी संस्था से है;
- (द) "विनियम" का अभिप्राय आधार (नामांकन और अद्यतन) विनियम, 2016 से है;
- (ध) "निवासी" का अभिप्राय ऐसा कोई व्यक्ति है, जिसने नामांकन आवेदन की तारीख से ठीक पहले के 12 महीनों में 182 दिन अथवा उससे अधिक की अवधि अथवा अवधियों में भारत में निवास किया हो;
- (न) "सेवा प्रदाता" का अभिप्राय नामांकन अथवा अद्यतन प्रक्रिया से जुड़े किसी कार्य का निर्वहन करने के कार्य में संलग्न सभी संस्थाएं शामिल हैं, से है;
- (प) "पर्यवेक्षक" का अभिप्राय नामांकन केंद्रों का संचालन और प्रबंध करने के लिए नामांकन एजेंसियों द्वारा नियोजित प्रमाणित कार्मिक से है;
- (फ) "सत्यापक" का अभिप्राय नामांकन केंद्रों पर दस्तावेजों के सत्यापन के लिए पंजीयकों द्वारा नियुक्त कार्मिक से है।
- (2) इन विनियमों के उपयोग के लिए सभी अन्य शब्द या अभिव्यक्ति, जिन्हें यहां परिभाषित नहीं किया गया है परन्तु अधिनियम अथवा उसके तहत बनाए गए नियमों तथा अन्य विनियमों में परिभाषित किया गया है, उनका क्रमशः वही अर्थ होगा, जो कि उन्हें अधिनियमों अथवा नियम अथवा अन्य विनियमों, जैसा भी मामला हो, में दिया गया है।

अध्याय-II

निवासी नामांकन प्रक्रिया

3. नामांकन के लिए अपेक्षित बायोमैट्रिक सूचना :-

- (1) नामांकन करवाने वाले सभी व्यक्तियों (पांच वर्ष से कम आयु वाले बच्चों के अलावा) से निम्नलिखित बायोमैट्रिक सूचना एकत्रित की जाएगी:
- चेहरे की आकृति,
 - सभी दस अंगुलियों की छाप, और
 - दोनों पुतलियों का स्कैन
- (2) बायोमैट्रिक सूचना एकत्र करने के मानक वे होंगे जो इस प्रयोजनार्थ प्राधिकरण द्वारा विहित किए जाएं।

4. नामांकन के लिए अपेक्षित जनसांख्यिकीय सूचना :-

- (1) नामांकन करवाने वाले सभी व्यक्तियों (पांच वर्ष से कम आयु वाले बच्चों के अलावा) से निम्नलिखित जनसांख्यिकीय सूचना एकत्रित की जाएगी:
 - (i) नाम
 - (ii) जन्म की तारीख
 - (iii) लिंग
 - (iv) आवासीय पता
- (2) नामांकन करवाने वाले व्यक्ति के विकल्प पर नामांकन के दौरान निम्नलिखित अतिरिक्त जनसांख्यिकीय सूचना भी एकत्र की जा सकती है:
 - (i) मोबाइल नंबर
 - (ii) ई-मेल पता
- (3) परिचयदाता-आधारित नामांकन की दशा में निम्नलिखित अतिरिक्त सूचनाएकत्र की जाएगी:
 - (i) परिचयदाता का नाम
 - (ii) परिचयदाता का आधार नंबर
- (4) परिवार के मुखिया पर आधारित सूचना की दशा में निम्नलिखित अतिरिक्त सूचना एकत्र की जाएगी:
 - (i) परिवार के मुखिया का नाम
 - (ii) संबंध
 - (iii) परिवार के मुखिया का आधार नंबर
 - (iv) परिवार के मुखिया की बायोमैट्रिक सूचना का एक प्रकार
- (5) उपर्युक्त जनसांख्यिकीय सूचना एकत्र करने के मानक वे होंगे, जो इस प्रयोजनार्थ प्राधिकरण द्वारा विहित किए जाएं।
- (6) जनसांख्यिकीय सूचना में निवासी की नस्ल, धर्म, जाति, जनजातीय नृजातीयता, भाषा, हकदारी का रिकॉर्ड, आय अथवा चिकित्सा इतिवृत्त शामिल नहीं होगा।

5. पांच वर्ष से कम आयु वाले बच्चों के नामांकन के लिए अपेक्षित सूचना :-

- (1) पांच वर्ष से कम आयु वाले बच्चों के लिए निम्नलिखित जनसांख्यिकीय और बायोमैट्रिक सूचना एकत्र की जाएगी:
 - (क) नाम
 - (ख) जन्म की तारीख
 - (ग) लिंग
 - (घ) माता या पिता में से किसी एक की नामांकन आईडी अथवा आधार नंबर, माता पिता दोनों के जीवित होने की दशा में अधिमानतः माता का अथवा अभिभावक का नामांकन आईडी अथवा आधार नंबर। ऐसे माता या पिता अथवा अभिभावक का आधार नंबर अथवा नामांकन आईडी आवश्यक है, और संबंध बताने के लिए एक फील्ड को रिकॉर्ड किया जाएगा।
 - (च) ऐसे बच्चे का पता जो कि सम्बद्ध माता पिता/अभिभावक के समान है।
 - (छ) बच्चे के चेहरे की आकृति ली जाएगी। नामांकन के दौरान माता पिता/अभिभावक में से किसी एक की बायोमैट्रिक सूचना ली जाएगी और इसको अधिप्रमाणित किया जाएगा।
- (2) सम्बद्ध माता पिता/अभिभावक और बच्चे के बीच संबंध स्थापित करने हेतु प्रमाण अनुसूची-II में सूचीबद्ध संबंध दर्शाने वाले दस्तावेज (पीओआर) का संग्रह नामांकन के समय किया जाएगा। संबंध दर्शाने वाले दस्तावेज के आधार पर केवल उन बच्चों का नामांकन किया जाएगा, जिनका नाम संबंध बताने वाले दस्तावेज (पीओआर), में दर्ज है।

6. बायोमैट्रिक अपवादों के साथ निवासियों का नामांकन-

- (1) जिन निवासियों के अंगुलियों के निशान चोट, विकृति, अंगुली/हाथ के कटे होने या किसी अन्य संबंधित कारण से लेना संभव न हो उनके केवल आंखों की पुतलियों के स्कैन लिए जाएंगे।

- (2) उन निवासियों के लिए प्राधिकरण नामांकन और अद्यतन सॉफ्टवेयर में अपवादों के लिए व्यवस्था करेगा जो इन विनियमों में अपेक्षित किसी बायोमैट्रिक सूचना को प्रदान नहीं कर सकते और इस प्रकार के नामांकन इस प्रयोजनार्थ प्राधिकरण द्वारा यथा विहित प्रक्रिया के अनुसार संपन्न किए जाएंगे।

7. पंजीयकों, नामांकन एजेंसियों आदि की नामांकन में भूमिका :-

- (1) प्राधिकरण द्वारा नियुक्त पंजीयक स्वयं अथवा उनके द्वारा अनुबंधित/नियुक्त किसी नामांकन एजेंसी के माध्यम से निवासियों का नामांकन कार्य करेंगे।
- (2) नामांकन एजेंसी निवासियों के नामांकन, उनकी सूचना का अद्यतन और त्रुटिशोधन करने के लिए नामांकन केंद्र स्थापित करेंगी। नामांकन केंद्र खोलना, प्रदान की जाने वाली सेवाएं और उनके संचालन के लिए अन्य दिशानिर्देश इस प्रयोजन के लिए प्राधिकरण द्वारा यथा विहित प्रक्रिया के अनुरूप होंगे।
- (3) नामांकन कार्य इस प्रयोजन के लिए बनाए गए स्थायी नामांकन केंद्रों और अस्थायी केंद्रों में किया जाएगा।
- (4) नामांकन केंद्रों में नामांकन कार्य ऑपरेटरों, सत्यापकों, पर्यवेक्षकों और अन्य अधिकृत कार्मिकों द्वारा संपन्न किया जाएगा।
- (5) पंजीयक विनियम 10 में विहित वैकल्पिक नामांकन तरीकों के माध्यम से ऐसे निवासियों का नामांकन करने के लिए युक्तियुक्त प्रयास करेगा, जिनके पास कोई संगत दस्तावेज नहीं है।

8. नामांकन में इस्तेमाल होने वाले उपकरण, सॉफ्टवेयर इत्यादि :-

- (1) पंजीयक और नामांकन एजेंसियां नामांकन के प्रयोजन से प्राधिकरण द्वारा दिए अथवा अधिकृत किए गए सॉफ्टवेयर का ही इस्तेमाल करेंगी।
- (2) मानक नामांकन/अद्यतन सॉफ्टवेयर में ऐसे सुरक्षा मानक होंगे, जो इस प्रयोजनार्थ प्राधिकरण द्वारा विहित किए जाएं।
- (3) नामांकन में इस्तेमाल होने वाले सभी उपकरण जैसे कम्प्यूटर, प्रिंटर, बायोमैट्रिक यंत्र और अन्य सहायक सामग्री इस प्रयोजनार्थ प्राधिकरण द्वारा विहित विनिर्देशन के अनुरूप होंगे।
- (4) नामांकन के लिए इस्तेमाल होने वाला बायोमैट्रिक यंत्र इस प्रयोजनार्थ प्राधिकरण द्वारा यथा विहित विनिर्देशन की अपेक्षाओं को पूर्ण करेगा और यथा विहित प्रक्रिया के अनुसार प्रमाणित किया जाएगा।

9. नामांकन के समय निवासियों को सूचना का प्रकटन :-

नामांकन एजेंसी नामांकन के समय नामांकन करवाने वाले व्यक्तियों को निम्नलिखित ब्योरे की सूचना देगी:

- (क) सूचना किस विधि से इस्तेमाल की जाएगी,
- (ख) उस प्राप्तिकर्ता का स्वरूप जिसके साथ अधिप्रमाणन के दौरान सूचना साझा की जाएगी, और
- (ग) सूचना की पहुंच के अधिकार का विद्यमान होना, ऐसी पहुंच के लिए अनुरोध करने की प्रक्रिया, जिसके समक्ष ऐसे अनुरोध किए जाएंगे उस व्यक्ति अथवा विभाग के प्रभारी का ब्योरा। निवासियों को उपर्युक्त ब्योरे की सूचना अनुसूची-I में दिए गए प्रपत्र में नामांकन फॉर्म के माध्यम से की जाएगी।

10. सूचना जमा करना और उसका सत्यापन- :-

- (1) नामांकन करवाने वाले निवासियों को नामांकन आवेदन पत्र के साथ पहचान काप्रमाण, पता और जन्म की तारीख के लिए संगत दस्तावेज किसी एक नामांकन केंद्र में जमा करने होंगे।
- (2) पहचान, पते और जन्म की तारीख के सत्यापन के लिए स्वीकार्य संगत दस्तोवजों की सांकेतिक सूची अनुसूची-II में दी गई है। प्राधिकरण स्वीकार्य संगत दस्तावेजों की इस सूची का विस्तार अथवा संशोधन समय-समय पर जारी परिपत्रों अथवा अधिसूचना के माध्यम से कर सकता है।
- (3) प्राधिकरण, भारत के महापंजीयक द्वारा निवासियों के नामांकन/अद्यतन की दशा में पते के प्रमाण और पहचान के प्रमाण संग्रह करने की अपेक्षा को समाप्त कर सकता है।
- (4) किसी निवासी के पास कोई संगत दस्तावेज न होने की दशा में नामांकन निम्नलिखित तरीकों से किया जा सकता है:
- (क) **परिचयदाता-आधारित नामांकन:** यदि कोई निवासी पहचान के प्रमाण अथवा पते के प्रमाण के लिए कोई दस्तावेज उपलब्ध करवाने में असमर्थ है तो उसका नामांकन पंजीयक अथवा प्राधिकरण के क्षेत्रीय केंद्रों में पूर्वनिर्धारित तरीके से पहचान किए गए और अधिसूचित परिचयदाता के माध्यम से किया जा सकता है। परिचयदाता के रूप में पंजीकृत व्यक्तियों में पंजीयकों के अपने कर्मचारी, स्थानीय निकायों के चुने हुए सदस्य, स्थानीय प्रशासनिक निकायों के सदस्य, डाकिया, प्रभावकारी व्यक्ति जैसे शिक्षक, स्वास्थ्य कामगार, डॉक्टर, आंगनवाड़ी/आशा कामगार, स्थानीय एनजीओ के प्रतिनिधि शामिल हो सकते हैं। ऐसे अनुमोदित परिचयदाता किसी निवासी का परिचय देंगे और ऐसे निवासी की सूचना

की सत्यता की जिम्मेदारी लेंगे। परिचयदाता को निवासी के नामांकन पत्र में भरी हुई सूचना का सत्यापन करना होगा, अपना नाम और आधार नंबर भरना होगा और अपने हस्ताक्षर एवं अंगूठे का निशान लगाना होगा।

(ख) **परिवार के मुखिया पर आधारित सूचना:** किसी निवासी के परिवार के मुखिया के पास संगत दस्तावेज होने और उन संगत दस्तावेजों के माध्यम से उसका नामांकन होने की दशा में उस निवासी का उन दस्तावेजों के आधार पर नामांकन किया जा सकता है बशर्ते (i) वह निवासी संबंध स्थापित करने का प्रमाण दे और (ii) संबंध दर्शाने वाले प्रमाण और संगत दस्तावेजों में वही पता होना चाहिए जो परिवार के सदस्य और परिवार के मुखिया का है।

(5) उपर्युक्त तीन तरीकों से नामांकन आंकड़ों का सत्यापन अनुसूची III में यथाविहित विधि के अनुसार होगा।

11. नामांकन केंद्रों में सूचना का एकत्रीकरण :-

- (1) नामांकन ऑपरेटर (i) निवासी द्वारा आवेदन पत्र में दी गई जनसांख्यिकीय सूचना, और (ii) प्राधिकरण द्वारा दिए अथवा अनुमोदित नामांकन सॉफ्टवेयर का इस्तेमाल करते हुए बायोमैट्रिक सूचना प्राप्त करेगा,
- (2) नामांकन ऑपरेटर अपेक्षित संगत दस्तावेजों की भौतिक प्रतियों को एकत्र करके उनको रिकॉर्ड में दाखिल करेगा, अथवा नामांकन केंद्र पर सुविधा उपलब्ध होने पर प्राधिकरण द्वारा यथा विहित प्रक्रिया के अनुसार उन भौतिक प्रतियों को इलेक्ट्रॉनिक रूप में तब्दील करेगा।
- (3) सूचना प्राप्त करने के बाद अपनी जानकारी की शुद्धता की जांच के लिए निवासी को एक अवसर प्रदान किया जाएगा।
- (4) नामांकन पूर्ण हो जाने पर नामांकन ऑपरेटर द्वारा हस्ताक्षरित नामांकन आईडी (ईआईडी) और अन्य नामांकन ब्योरे वाली पावती रसीद निवासी को दी जाएगी।
- (5) नामांकन (पांच वर्ष से कम के बच्चों के नामांकन और अपवाद वाली स्थितियों सहित) के दौरान अपनाई जाने वाली प्रक्रियाएं, मानक और दिशानिर्देश तथा नामांकन कार्य के लिए इस्तेमाल होने वाले फॉर्मेट, मसौदे, जांचसूची इस प्रयोजनार्थ प्राधिकरण द्वारा यथा विहित प्रक्रियाओं के अनुरूप होंगे।

12. सेवा के लिए आधार की अपेक्षा रखने वाली एजेंसियां :-

केंद्रीय अथवा राज्य सरकारी विभाग अथवा एजेंसी जो किसी व्यक्ति से अधिनियम की धारा-7 के परिणामस्वरूप किसी सब्सिडी, लाभ और सेवा प्राप्त करने के लिए अधिप्रमाणन करवाने अथवा आधार नंबर का प्रमाण प्रस्तुत करने की शर्त रखती है तो वह पंजीयकों के साथ समन्वय और सुविधाजनक स्थानों में नामांकन केंद्र बनाने अथवा स्वयं पंजीयक बनकर नामांकन सुविधा सहित उपयुक्त उपायों से अपने लाभार्थियों का नामांकन सुनिश्चित करेगी, जिनका नामांकन अभी होना है।

अध्याय-III

आधार नंबर तैयार कर निवासियों को इसे संप्रेषित करना

13. आधार नंबर तैयार करना :-

- (1) पंजीयक और नामांकन एजेंसियां प्राधिकरण द्वारा दिए गए सॉफ्टवेयर का इस्तेमाल करते हुए नामांकन पैकेट केंद्रीय पहचान आंकड़े निक्षेपागार पर अपलोड करेंगी।
- (2) प्राधिकरण पंजीयक द्वारा प्राप्त नामांकन आंकड़ों का प्रक्रमण करेगा और डीडुप्लीकेशन तथा प्राधिकरण द्वारा यथा विहित अन्य जांचों के बाद आधार नंबर तैयार करेगा।

14. नामांकन रद्द करना :-

- (1) निवासी द्वारा दो नामांकन करवाने, इसकी गुणवत्ता और किसी अन्य तकनीकी कारण से प्राधिकरण नामांकन को रद्द कर सकता है।
- (2) दोहरे नामांकन के कारण नामांकन रद्द होने की स्थिति में, निवासी को उस नामांकन के बारे में प्राधिकरण द्वारा यथा विहित विधि से सूचना दी जाएगी, जिसके लिए उसका आधार नंबर तैयार किया गया है।

15. आधार नंबर संप्रेषित करना :-

- (1) निवासी को आधार नंबर प्रत्यक्ष रूप में (पत्र अथवा कॉर्ड सहित) और/अथवा इलेक्ट्रॉनिक रूप में (प्राधिकरण की वेबसाइट के माध्यम से डाउनलोड के लिए उपलब्ध अथवा एसएमएस द्वारा) संसूचित किया जा सकता है।
- (2) प्रिंटिंग, प्रेषण और संप्रेषित से जुड़े अन्य कार्यों के लिए प्राधिकरण द्वारा लगाई गई सभी एजेंसियां लागू प्रक्रियाओं का अनुपालन करेंगी।

अध्याय-IV**निवासी की सूचना का अद्यतन****16. पहचान सूचना का अद्यतन करने के लिए अनुरोध :-**

आधार नंबर धारक, इस अध्याय में दी गई अद्यतन प्रक्रिया के अनुरूप अधिनियम की धारा-31 के अंतर्गत दिए गए मामलों में अपनी जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना में परिवर्तन करवा सकता है।

17. बच्चों के लिए अनिवार्य अद्यतन :-

प्राधिकरण की यह अपेक्षा है कि 5 वर्ष की आयु और 15 वर्ष की आयु पूर्ण हो जाने पर बच्चों की बायोमैट्रिक सूचना का प्राधिकरण द्वारा विहित प्रक्रिया के अनुरूप अद्यतन किया जाएगा।

18. अद्यतन के लिए इस्तेमाल होने वाले उपकरण, सॉफ्टवेयर, इत्यादि :-

- (1) अद्यतन प्रक्रिया में लगे हुए पंजीयक, नामांकन एजेंसियां अथवा अन्य सेवा प्रदाता अद्यतन प्रयोजन के लिए प्राधिकरण द्वारा उपलब्ध अथवा अनुमोदित सॉफ्टवेयर का ही इस्तेमाल करेंगे।
- (2) मानक अद्यतन सॉफ्टवेयर में ऐसे सुरक्षा मानक होंगे, जो इस प्रयोजनार्थ प्राधिकरण द्वारा तय किए जाएं।
- (3) अद्यतन के प्रयोजनों से इस्तेमाल होने वाले सभी उपकरण जैसे कम्प्यूटर, प्रिंटर, बायोमैट्रिक यंत्र और अन्य सहायक सामग्री समय-समय पर इस प्रयोजनार्थ प्राधिकरण द्वारा विहित विनिर्देशन के अनुरूप होंगी।

19. निवासियों की सूचना का अद्यतन का तरीका-

केंद्रीय पहचान आंकड़े निक्षेपागार में निवासियों की सूचना का अद्यतन करने की प्रक्रिया निम्नलिखित तरीकों से की जाएगी:

- (क) किसी भी नामांकन केंद्र पर ऑपरेटर और/अथवा पर्यवेक्षक की सहायता से निवासी का बायोमैट्रिक तरीके से अधिप्रमाणन किया जाएगा और अद्यतित की जाने वाले पहचान सूचना के साथ उसे अपना आधार नंबर उपलब्ध करवाना होगा।
- (ख) **ऑनलाइन मोड:** जनसांख्यिकीय सूचना का ऑनलाइन अद्यतन निर्धारित पोर्टल के माध्यम से आधार नंबर और पंजीकृत मोबाइल नंबर प्रस्तुत करने पर किया जा सकता है। प्रमाणीकरण का कार्य पंजीकृत मोबाइल नंबर पर भेजे गए वन टाइम पासवर्ड (ओटीपी) के माध्यम से संपन्न किया जाएगा।
- (ग) **पोस्टल मोड:** जनसांख्यिकीय सूचना के अद्यतन हेतु अनुरोध अनुसूची-IV में निर्धारित प्रपत्र में सत्यापन के लिए अपेक्षित संगत दस्तावेजों के साथ डाक के माध्यम से भेजा जा सकता है।

अद्यतन की स्थिति की जांच करने के लिए निवासी को एक अद्यतन आईडी दी जाएगी और संशोधित आधार पत्र इस प्रयोजनार्थ प्राधिकरण द्वारा विहित की गई प्रक्रिया के अनुरूप प्रत्यक्ष अथवा इलेक्ट्रॉनिक रूप में निवासी को उपलब्ध करवाया जाएगा। अद्यतन करने की प्रक्रिया, पालन किए जाने वाले मानक और दिशानिर्देश तथा अद्यतन कार्य के लिए इस्तेमाल होने वाले फॉर्मेट, मसौदे, जांचसूची इस प्रयोजनार्थ प्राधिकरण द्वारा यथा विहित विधि के अनुरूप होंगे।

20. सुविधा शुल्क :-

प्राधिकरण पंजीयकों को निवासियों से सुविधा शुल्क वसूलने के लिए अधिकृत कर सकता है। यह राशि जनसांख्यिकीय सूचना और बायोमैट्रिक सूचना के अद्यतन के लिए प्राधिकरण द्वारा विहित राशि से अधिक नहीं होगी।

अध्याय-V**पंजीयकों, नामांकन एजेंसियों और अन्य प्रदाताओं की नियुक्ति****21. पंजीयकों की नियुक्ति:-**

- (1) पूरे देश में निवासियों का नामांकन और अद्यतन करने के लिए प्राधिकरण द्वारा पंजीयकों की नियुक्ति समझौता ज्ञापनों अथवा करारों के माध्यम से की जाएगी और इनमें वे संस्थाएं भी शामिल हो सकती हैं, जो अपने कार्यक्रमों के कार्यान्वयन के सामान्य क्रम में निवासियों से परस्पर संवाद करती हैं। पंजीयकों के रूप में नियुक्त होने वाली संस्थाएं हैं राज्य/संघ राज्य सरकार, केंद्रीय मंत्रालय और उनके अधीन विभाग/एजेंसियां, केंद्र/राज्य सरकार की सार्वजनिक क्षेत्र की कंपनियां, सार्वजनिक क्षेत्र के बैंक और नेशनल सिक्योरिटी डिपॉजिटरी लिमिटेड, यूटीआई इन्फ्रास्ट्रक्चर टेक्नोलॉजी एंड सर्विसेस लिमिटेड जैसी विनियमित संस्थाएं, सीएससी ई-गवर्नंस सर्विसेस इंडिया लिमिटेड सहित केंद्र अथवा राज्य सरकार द्वारा बनाए गए स्पेशल परपज व्हीकल। नियुक्ति होने पर प्रत्येक पंजीयक को एक पंजीयक कोड दिया जाएगा।
- (2) पंजीयक क्षेत्र स्तरीय कार्यान्वयन, मॉनीटरिंग और लेखापरीक्षा के लिए उत्तरदायी होगा।
- (3) पंजीयक अपने द्वारा उपयोग में लाए जा रहे अथवा अपनी ओर से किसी अन्य व्यक्ति द्वारा उपयोग में लाए जाने वाले परिसर में प्राधिकरण को युक्तियुक्त पहुंच की अनुमति प्रदान करेगा और पंजीयक अथवा उसकी ओर से किसी अन्य व्यक्ति के कब्जे में रखी

हुई किसी पुस्तक, रिकॉर्ड, दस्तावेज और कम्प्यूटर डाटा की जांच के लिए युक्तियुक्त सुविधा भी देगा और वे दस्तावेज अथवा अन्य सामग्री भी प्रदान करेगा, जो प्राधिकरण की राय में लेखापरीक्षा के प्रयोजन से संगत हैं।

- (4) पंजीयक नामांकन के दौरान संग्रह की गई सूचना का इस्तेमाल केंद्रीय पहचान आंकड़े निक्षेपागार में अपलोड करने के सिवाए किसी अन्य प्रयोजन से नहीं करेगा।
- (5) पंजीयक अपनी वेबसाइट पर संपर्क व्यक्ति के संपर्क ब्योरे और निवासियों के लिए उपलब्ध सेवाओं सहित नामांकन और अद्यतन सेवाओं के बारे में पर्याप्त और उपयुक्त सूचना का प्रदर्शन करेगा।
- (6) पंजीयक यह सुनिश्चित करेगा कि उनके द्वारा नामांकन और अद्यतन कार्यों के लिए नियोजित अथवा नियुक्त एजेंसी और/अथवा व्यक्ति सक्षम और उपयुक्त हैं और इस प्रकार नियोजित अथवा नियुक्त क्षमता में संगत व्यावसायिक प्रशिक्षण अथवा अनुभव रखते हुए अन्यथा अर्हता प्राप्त हैं।
- (7) पंजीयक नामांकन एजेंसियों के नामांकन कार्यों को तीसरे पक्ष को संविदा के द्वारा देने की अनुमति नहीं देगा। पंजीयक क्षेत्र स्तर पर कार्मिकों को तीसरे पक्षकार से काम करवाने की अनुमति दे सकता है परंतु नामांकन एजेंसी उन संस्थाओं का ब्योरा उपलब्ध करवाएगी जिनसे इस प्रकार के कार्मिक लिए जाएंगे।
- (8) पंजीयक इन विनियमों की अनुसूची-V में विहित आचार संहिता का हर हालत में पालन करेगा।
- (9) पंजीयक प्राधिकरण द्वारा विहित किए गए विवरणों सहित समय समय पर जारी प्रक्रियाओं, नीतियों और दिशानिर्देशों, जांचसूचियों, फॉर्मों और मसौदों का पालन करेगा और नामांकन एजेंसियों द्वारा ऐसी प्रक्रियाओं इत्यादि का अनुपालन भी सुनिश्चित करेगा।

22. इन विनियमों के प्रारंभ से पहले लगाए गए पंजीयक :-

- (1) इन विनियमों के प्रारंभ से पहले लगाए गए पंजीयकों को इस अधिनियम के अंतर्गत प्राधिकरण द्वारा नियुक्त समझा जाएगा: परंतु योजना आयोग, भारत सरकार के अधिसूचना संख्या ए-43011/02/2009-प्रशासन-1, दिनांक 28 जनवरी, 2009 के द्वारा स्थापित भारतीय विशिष्ट पहचान प्राधिकरण अथवा प्राधिकरण के किसी अधिकारी द्वारा उनके साथ किए गए करार उस सीमा तक प्रभावी रहेंगे, जो इस अधिनियम के उपबंधों, प्राधिकरण द्वारा जारी इन विनियमों और अन्य विनियमों, नीतियों, प्रक्रियाओं, प्रक्रमणों, मानकों और विनिर्देशनों से असंगत न हों।
- (2) इन विनियमों के प्रारंभ से पूर्व लगे हुए किसी पंजीयक के इस अधिनियम के अंतर्गत पंजीयक न रहने की इच्छा जाहिर करने की दशा में वह पंजीयक इस प्रयोजन के लिए प्राधिकरण द्वारा विनिर्दिष्ट प्रारूप में प्राधिकरण को आवेदन कर सकता है और वह पंजीयक के पद से हट जाएगा और उसके पास नामांकन करने अथवा नामांकन के लिए नामांकन एजेंसियों को लगाने की शक्ति नहीं रह जाएगी।

23. नामांकन एजेंसियों का पैनल बनाया जाना :-

- (1) प्राधिकरण मुक्त पैनल अनुरोध प्रक्रिया के माध्यम से नामांकन एजेंसियों का पैनल बनाएगा और पैनल बनाने की पात्रता, निबंधन एवं शर्तें प्राधिकरण द्वारा समय-समय पर अधिसूचित की जाएंगी।
- (2) इच्छुक एजेंसियां पैनल अनुरोध की पात्रता और अन्य तकनीकी और वित्तीय मापदंड पूरा करने पर पैनल में शामिल होने के लिए आवेदन कर सकती हैं।
- (3) प्राधिकरण एजेंसियों के आवेदन पत्रों का मूल्यांकन करेगा और पैनल अनुरोध की अपेक्षाओं को पूर्ण करने के पश्चात पात्र एजेंसी को नामांकन एजेंसियों के रूप में पैनल में शामिल कर सकता है।
- (4) प्राधिकरण नामांकन एजेंसी कोड प्रदान करेगा, जिसका इस्तेमाल करते हुए पंजीयक किसी पैनल में शामिल नामांकन एजेंसी को केंद्रीय पहचान आंकड़ा भंडार में ऑनबोर्ड कर सकता है।
- (5) प्राधिकरण पंजीयकों को जांच और करार की उपयुक्त प्रक्रिया का पालन करते हुए ऐसी एजेंसियों को नामांकन एजेंसियों के रूप में लगाने के लिए अनुमति प्रदान कर सकता है जैसा प्राधिकरण द्वारा विहित किया जाए।
- (6) नामांकन एजेंसी क्षेत्र स्तरीय कार्यान्वयन और लेखापरीक्षा के लिए उत्तरदायी होगी। नामांकन एजेंसी द्वारा स्वयं इस्तेमाल किए जाने वाले अथवा अपनी ओर से किसी अन्य व्यक्ति द्वारा इस्तेमाल में लाए जाने वाले परिसर में प्राधिकरण को युक्तियुक्त पहुंच की अनुमति प्रदान की जाएगी और नामांकन एजेंसी अथवा उसकी ओर से किसी अन्य व्यक्ति के कब्जे में रखी हुई किसी पुस्तक, रिकॉर्ड, दस्तावेज और कम्प्यूटर डाटा की जांच के लिए युक्तियुक्त सुविधा भी दी जाएगी और वे दस्तावेज अथवा अन्य सामग्री भी प्रदान करेगा जो प्राधिकरण की राय में लेखापरीक्षा के प्रयोजन से संगत है।
- (7) नामांकन एजेंसी नामांकन के दौरान संग्रह की गई सूचना का इस्तेमाल केंद्रीय पहचान आंकड़े निक्षेपागार में अपलोड करने के सिवाए किसी अन्य प्रयोजन से नहीं करेगा।
- (8) नामांकन एजेंसी यह सुनिश्चित करेगा कि उनके द्वारा नामांकन और अद्यतन कार्यों के लिए नियोजित अथवा नियुक्त एजेंसी और/अथवा व्यक्ति सक्षम और उपयुक्त हैं और इस प्रकार नियोजित अथवा नियुक्त क्षमता में संगत व्यावसायिक प्रशिक्षण अथवा अनुभव रखते हुए अन्यथा अर्हता प्राप्त हैं।
- (9) नामांकन एजेंसी इन विनियमों की अनुसूची-V में विहित आचार संहिता का हर समय पालन करेगा।

- (10) नामांकन एजेंसी प्राधिकरण द्वारा विहित किए गए विवरणों सहित समय-समय पर जारी प्रक्रियाओं, नीतियों और दिशानिर्देशों, जांचसूचियों, फॉर्मों और मसौदों का पालन करेगा।
- (11) इस अधिनियम के अंतर्गत प्राधिकरण की स्थापना से पूर्व प्राधिकरण द्वारा पैनल में शामिल की गई नामांकन एजेंसियों को इस अधिनियम के अंतर्गत प्राधिकरण द्वारा पैनल में शामिल समझा जाएगा।

24. अन्य सेवा प्रदाता :-

- (1) निवासी नामांकन प्रक्रिया अथवा सूचना का अद्यतन से संबंधित किसी कार्य को करने के लिए प्राधिकरण द्वारा समय-समय पर अन्य सेवा प्रदाताओं को लगाया जा सकता है।
- (2) ऐसे सभी सेवा प्रदाता प्राधिकरण द्वारा विहित किए गए विवरणों सहित समय-समय पर जारी आदेशों, प्रक्रियाओं, नीतियों और दिशानिर्देशों, जांचसूचियों, फॉर्मों और मसौदों का और इन विनियमों की अनुसूची-V में दी गई यथा लागू आचार संहिता का पालन करेगा।

25. नामांकन के लिए नियुक्त स्टाफ का परीक्षण और प्रमाणन:-

- (1) प्रत्येक नामांकन एजेंसी यह सुनिश्चित करेगी कि उसके द्वारा नियोजित अथवा लगाए गए ऑपरेटर, पर्यवेक्षक, और अन्य नामांकन स्टाफ प्राधिकरण द्वारा विहित प्रमाणन प्रक्रिया के माध्यम से नामांकन कार्य करने के लिए विधिवत् प्रमाणित हैं।
- (2) प्राधिकरण इस प्रयोजनार्थ परीक्षण और प्रमाणन एजेंसियों को नियत कर सकता है।
- (3) प्राधिकरण ऐसे कार्मिकों को नामांकन की किसी प्रक्रिया में लगाए जाने के लिए उनकी नियुक्ति की प्रक्रिया, ऐसे कार्मिकों की विस्तृत भूमिका और उत्तरदायित्व हेतु न्यूनतम अर्हता तय कर सकता है।

26. पंजीयकों, नामांकन एजेंसियों और अन्य सेवा प्रदाताओं का उत्तरदायित्व और चूक की स्थिति में कार्रवाई:-

- (1) पंजीयक, नामांकन एजेंसियां और अन्य सेवा प्रदाता तथा पर्यवेक्षक, ऑपरेटर अथवा उनके द्वारा नियोजित कोई अन्य व्यक्ति अथवा एजेंसी प्राधिकरण द्वारा समय-समय पर जारी समस्त विनियमों, प्रक्रमणों, मानकों, दिशानिर्देशों और आदेशों और अनुसूची-V में दी गई आचार संहिता का अनुपालन करेंगे।
- (2) प्राधिकरण पंजीयकों, नामांकन एजेंसियों और ऑपरेटरों, पर्यवेक्षकों तथा नामांकन में लगे हुए अन्य कार्मिकों की निगरानी करेगा।
- (3) इस अधिनियम के अंतर्गत की जा सकने वाली किसी कार्रवाई पर प्रतिकूल प्रभाव डाले बिना, किसी सेवा प्रदाता अथवा किसी अन्य व्यक्ति द्वारा किसी विनियम, प्रक्रमण, मानक, दिशानिर्देश अथवा आदेश का उल्लंघन होने पर ऐसे सेवा प्रदाता अथवा संबंधित व्यक्तियों की गतिविधियों का तत्काल निलंबन होगा और प्राधिकरण द्वारा उपयुक्त जांच करने के बाद इस अधिनियम अथवा इन विनियमों के परिणामस्वरूप उन्हें जारी किए गए प्रमाणपत्रों, संहिताओं और अनुमतियों का रद्दीकरण हो जाएगा।

अध्याय-VI

आधार नंबर और पहचान सूचना में चूक अथवा उसका निष्क्रियण

27. ऐसे मामले जिनमें आधार नंबर का लोप होगा :-

- (1) किसी आधार नंबर धारक का आधार नंबर निम्नलिखित परिस्थितियों में रद्द किया जाएगा:
- (क) यदि यह स्थापित हो जाए कि एक व्यक्ति को एक से अधिक आधार नंबर जारी कर दिए गए हैं, तब पहले नामांकन से जारी किया गया आधार नंबर बना रहेगा और बाद के सभी आधार नंबरों को रद्द कर दिया जाएगा।
- (ख) जहां आधार नंबर विहित दिशानिर्देशों का उल्लंघन करते हुए बनाया गया है-
- (i) फोटो पर फोटो वाले मामले जहां मुख्य बायोमैट्रिक सूचना उपलब्ध नहीं होती: जहां किसी नामांकन केंद्र पर नामांकन के लिए नया फोटोग्राफ खींचने के स्थान पर पहले से खिंचा हुआ फोटो इस्तेमाल किया गया है, और जहां नामांकन के दौरान मुख्य बायोमैट्रिक सूचना प्राप्त नहीं की गई है वहां निवासी का आधार नंबर रद्द कर दिया जाएगा।
- (ii) असत्य बायोमैट्रिक अपवाद वाले मामले: जहां बायोमैट्रिक अपवाद वाले मामले के रूप में नामांकन गलती से कर दिया गया है वहां आधार नंबर को रद्द कर दिया जाएगा।
- (iii) जहां बायोमैट्रिक सूचना देने से बचने के लिए किसी वयस्क का नामांकन पांच साल से छोटे बच्चे के रूप में कर दिया गया है वहां आधार नंबर रद्द कर दिया जाएगा।
- (iv) कोई अन्य ऐसा मामला जहां प्राधिकरण को नामांकन कपटपूर्ण प्रतीत होने से रद्दीकरण करना उचित जान पड़ता है।
- (2) रद्दीकरण हो जाने पर प्राधिकरण द्वारा आधार नंबर धारक को दी गई सभी सेवाएं स्थायी रूप से बंद कर दी जाएंगी।

28. ऐसे मामले जहां आधार नंबर को निष्क्रिय किया जाएगा:—

- (1) किसी आधार नंबर धारक का आधार नंबर निम्नलिखित परिस्थितियों में निष्क्रिय कर दिया जाएगा:
 - (क) फोटो पर फोटो और मुख्य बायोमैट्रिक सूचना उपलब्ध होना: जहां किसी नामांकन केंद्र पर नामांकन के लिए नया फोटोग्राफ खींचने के स्थान पर पहले से खिंचा हुआ फोटो इस्तेमाल किया गया है, और जहां निवासी की मुख्य बायोमैट्रिक सूचना प्राप्त कर ली गई है वहां आधार नंबर को निष्क्रिय कर दिया जाएगा, और निवासी को अपना फोटोग्राफ अद्यतित करने के लिए कहा जाएगा। उसके फोटोग्राफ का सफलतापूर्ण अद्यतन होने पर आधार नंबर पुनः सक्रिय किया जा सकता है।
 - (ख) असत्य आंशिक बायोमैट्रिक अपवाद के मामले: जहां बायोमैट्रिक सूचना के कुछ घटकों को निवासी द्वारा प्रदान किए जाने की स्थिति में होने के बावजूद भी नहीं लिया गया है वहां आधार नंबर निष्क्रिय किया जाएगा।
 - (ग) जहां बाद के चरण में यह पाया जाता है कि नामांकन कार्य संगत दस्तावेजों के बिना किया गया है तो वहां आधार नंबर, आधार नंबर धारक द्वारा वैध संगत दस्तावेजों के प्रस्तुतीकरण तक निष्क्रिय कर दिया जाएगा।
 - (घ) जहां ली गई सूचना की घटिया डाटा के रूप में पहचान कर ली गई है और इसका अद्यतन जरूरी है (जैसे मिश्रित/असंगत बायोमैट्रिक सूचना, निवासी की जनसांख्यिकीय सूचना में अनुचित/पूरक शब्द और अभद्र भाषा होना, उर्फ लगाकर एक ही नाम के कई नाम होना) वहां आधार नंबर, आधार नंबर धारक द्वारा अद्यतित किए जाने तक निष्क्रिय रहेगा।
 - (च) जहां कोई बालक 5 अथवा 15 वर्ष की आयु पूर्ण करने पर उसके दो वर्ष के भीतर भी अपनी बायोमैट्रिक सूचना का अद्यतन नहीं कर पाता वहां उसके आधार नंबर को निष्क्रिय कर दिया जाएगा। जहां ऐसा अद्यतन कार्य आधार नंबर के निष्क्रिय किए जाने के एक वर्ष के अंदर नहीं किया जाता, वहां आधार नंबर का लोप कर दिया जाएगा।
 - (छ) ऐसा कोई अन्य मामला जहां निष्क्रियण प्राधिकरण द्वारा आवश्यक समझा जाए।
- (2) निष्क्रियकरण हो जाने पर प्राधिकरण द्वारा आधार नंबर धारक को दी जाने वाली सेवाएँ अस्थायी रूप से तब तक बंद कर दी जाएगी, जब तक आधार नंबर धारक वैसी सूचनाओं, जिसके कारण उसका आधार नंबर प्राधिकरण द्वारा निष्क्रिय कर दिया गया हो, को अद्यतित या शुद्ध कर लेता है।

29. लोप अथवा निष्क्रियण वाले मामलों की जांच:—

- (1) लोप अथवा विनिष्क्रियण की अपेक्षा रखने वाले रिपोर्ट अथवा पहचाने गए मामले की फील्ड स्तर पर जांच की जा सकती है जिसमें उस व्यक्ति की सुनवाई शामिल है, जिसके आधार नंबर का लोप या उसका निष्क्रियण किया जाना है।
- (2) प्राधिकरण द्वारा इस प्रयोजनार्थ नामित किसी एजेंसी द्वारा यथा विहित प्रक्रियाओं के अनुसार उसकी जांच कर रिपोर्ट प्राधिकरण को भेजी जाएगी।
- (3) प्राधिकरण रिपोर्ट की प्राप्ति होने पर आवश्यक कार्रवाई प्रारंभ कर सकता है और प्राधिकरण के पास आधार नंबर का लोप अथवा निष्क्रियण करने का निर्णय लेने का अधिकार होगा।

30. आधार नंबर धारक को संसूचना:—

- (1) आधार नंबर धारक को एसएमएस, पंजीकृत ई-मेल आईडी, टेलीकॉलिंग, पत्र अथवा प्राधिकरण द्वारा उचित समझ गए किसी माध्यम से उसके आधार नंबर के लोप अथवा निष्क्रियण होने के कारण सहित सूचना दी जाएगी।
- (2) ऐसे लोप अथवा निष्क्रियण के संबंध में किसी आधार नंबर धारक की शिकायत का निवारण प्राधिकरण द्वारा स्थापित शिकायत निवारण तंत्र के द्वारा किया जाएगा।

31. सुधारात्मक कार्रवाई :-

- (1) कई आधार नंबर हो जाने से भिन्न कारणों से आधार नंबर का लोप होने की स्थिति में निवासी को पुनः नामांकन करना होगा।
- (2) निष्क्रियण होने की स्थिति में निवासी को प्राधिकरण द्वारा यथा निर्धारित दिशानिर्देशों अथवा नीतियों के अनुरूप अपनी पहचान सूचना को अंशतः अथवा पूर्णतः अद्यतित करना होगा।

अध्याय—VII**शिकायत निवारण तंत्र****32. शिकायत निवारण के लिए संपर्क केंद्र स्थापित करना :-**

- (1) प्राधिकरण एक संपर्क केंद्र स्थापित करेगा जो निवासियों के प्रश्नों और शिकायतों के निवारण के लिए केंद्रीय बिंदु के रूप में काम करेगा। निवासी इस केंद्र पर प्रयोजनार्थ प्राधिकरण द्वारा यथा विहित विधि के अनुसार टॉल-फ्री नंबर और अथवा ई-मेल के माध्यम से संपर्क कर सकता है।

- (2) संपर्क केंद्र:
- (क) प्रश्नों अथवा शिकायतों को दर्ज करने और मामले के समापन तक उसकी निगरानी करने के लिए निवासी को विशिष्ट रेफरेंस नंबर देने की व्यवस्था की जाएगी,
- (ख) यथा संभव क्षेत्रीय भाषा में सहायता प्रदान की जाएगी,
- (ग) निवासियों से उनकी पहचान सूचना के संबंध में प्राप्त किसी सूचना की सुरक्षा सुनिश्चित करेगा,
- (घ) प्राधिकरण द्वारा इस प्रयोजनार्थ विहित प्रक्रियाओं और प्रक्रमणों का अनुपालन करेगा।
- (3) निवासी प्राधिकरण के क्षेत्रीय कार्यालयों में जाकर अथवा प्राधिकरण द्वारा यथा विहित विधि के अनुसार किसी अन्य अधिकारी अथवा चैनल को अपनी शिकायत दर्ज कर सकते हैं।

अध्याय-VIII

विविध

33. व्यावृत्ति :-

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 ऐसे प्राधिकरण के किसी अधिकारी द्वारा अथवा अधिनियम के तहत प्राधिकरण की स्थापना पूर्व जारी सभी कार्यपद्धति, आदेश, प्रक्रियाएं, मानक तथा नीतियां अथवा हस्ताक्षर किए सभी समझौता ज्ञापन, करार अथवा सविदाएं उस सीमा तक लागू रहेंगी, जबतक कि वे अधिनियम के उपबंधों तथा तत्संबंध तैयार किए गए अधिनियम अथवा विनियम के तहत असंगत सिद्ध न हो जाएं।

34. नीतियां, प्रक्रियां दस्तावेज आदि जारी करने संबंधी शक्तियां :-

प्राधिकरण इन विनियमों के अनुरूप संगत नीतियां, आदेश, प्रक्रियाएं, मानक, विनिर्देशन तथा अन्य दस्तावेज जारी कर सकता है, जिन्हें इन विनियमों के तहत विनिर्दिष्ट किया जाना अपेक्षित है अथवा जिनके लिए इन विनियमों को प्रभावी बनाने हेतु उपबंध किया जाना अनिवार्य है।

35. 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 परिपत्र के रूप में स्पष्टीकरण तथा दिशानिर्देश जारी कर सकता है।

अनुसूची-I

नामांकन फॉर्म का फॉर्मेट

(इन विनियमों का विनियम 9 देखें)

आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा 3 के अंतर्गत

आधार नामांकन/त्रुटिशोधन फॉर्म

आधार नामांकन निशुल्क और स्वैच्छिक है। नामांकन के 96 घंटों के अंदर त्रुटिशोधन भी निशुल्क है। फॉर्म और आधार नामांकन के लिए कोई शुल्क नहीं है। त्रुटिशोधन की स्थिति में अपनी नामांकन आईडी, नाम और वे ही भाग बताएं जिसमें त्रुटिशोधन किया जाना है।

त्रुटिशोधन करने की दशा में यहां अपना नामांकन आईडी दें:

कृपया फॉर्म भरते समय पिछले पृष्ठ पर दिए गए अनुदेशों का पालन करें। केवल बड़े अक्षरों का इस्तेमाल करें।

1	नामांकन पूर्व आईडी:	2	एनपीआर रसीद/टिन नंबर
3	पूरा नाम:		
4	लिंग: पुरुष () महिला () ट्रांसजेंडर ()	5	आयु: वर्ष अथवा जन्म की तारीख: घोषित सत्यापित
6	पता: संरक्षक () पुत्री () पुत्र () पत्नी () पति () मकान नंबर/बिल्डिंग/अपार्टमेंट पहचान का निशान गांव/कस्बा/शहर जिला ई-मेल		गली/रोड/लेन क्षेत्र/स्थान/सेक्टर डाकघर उप-जिला राज्य मोबाइल नंबर पिनकोड
7	ब्योरा: पिता () माता () अभिभावक () पति () पत्नी () का पांच वर्ष से कम के बच्चों के लिए पिता/माता/अभिभावक का ब्योरा अनिवार्य है। वयस्कों के लिए यह सूचना वैकल्पिक है।		
	नाम		

	नामांकन आईडी/आधार नंबर:	
	सत्यापन का प्रकार: दस्तावेज आधारित () परिचयदाता आधारित () परिवार के मुखिया आधारित () उपर्युक्त में से किसी एक का चुनाव करें। परिचयदाता अथवा परिवार के मुखिया के विकल्प का तभी चुनाव करें यदि आपके पास कोई पहचान और/अथवा पते का प्रमाण/दस्तावेज न हो। दस्तावेज आधारित सत्यापन के मामले में परिचयदाता और परिवार के मुखिया का ब्योरा देना आवश्यक नहीं है।	
8	दस्तावेज आधारित (प्रस्तुत किए गए दस्तावेज का नाम लिखें। वैध दस्तावेजों की सूची के लिए इस फार्म का पिछला भाग देखें) क. पहचान का प्रमाण ख. पते का प्रमाण ग. जन्म की तारीख घ. संबंध का प्रमाण (सत्यापित जन्म की तारीख के मामलों में अनिवार्य)	
9	परिचयदाता आधारित-परिचयदाता का आधार नंबर	परिवार के मुखिया आधारित पिता () माता () अभिभावक () पति () पत्नी () का ब्योरा परिवार के मुखिया की नामांकन आईडी/आधार नंबर
	मैं एतद्वाराकी पहचान और पते को सत्य, सही और यथातथ्य होने की पुष्टि करता हूँ। परिचयदाता/परिवार के मुखिया का नाम: परिचयदाता/परिवार के मुखिया के हस्ताक्षर	

आधार (वित्तीय और अन्य सब्सिडियों, लाभों और अन्य सेवाओं की लक्षित संप्रेषित) अधिनियम, 2016 की धारा 3(2) के अंतर्गत प्रकटन

मैं एतद्वारा पुष्टि करता हूँ कि मैंने पिछले 12 माह में कम से कम 182 दिन भारत में निवास किया है और भारतीय विशिष्ट पहचान प्राधिकरण को मेरे द्वारा बायोमैट्रिक सहित दी गई सूचना और यहां दी गई सूचना मेरी अपनी और सत्य, सही और यथातथ्य है। मुझे यह ज्ञान है कि बायोमैट्रिक सहित मेरी सूचना आधार तैयार करने और प्रमाणन के लिए इस्तेमाल होगी। मुख्य बायोमैट्रिक के सिवाए मेरी सूचना किसी एजेंसी को मेरी अनुमति लेकर प्रमाणन के दौरान उस एजेंसी को दी जा सकती है। मुख्य बायोमैट्रिक के सिवाए मुझे अपनी पहचान की सूचना तक पहुंचने का अधिकार भारतीय विशिष्ट पहचान प्राधिकरण द्वारा बनाई गई प्रक्रिया का पालन करके प्राप्त होगा।

सत्यापक की मुहर और हस्ताक्षर:

आवेदक के हस्ताक्षर/अंगूठे का निशान

(मुहर उपलब्ध न होने की स्थिति में सत्यापक अपना नाम लिखें)

केवल नामांकन एजेंसी द्वारा भरा जाए:

नामांकन की तारीख और समय:

नामांकन फॉर्म भरने के लिए अनुदेश

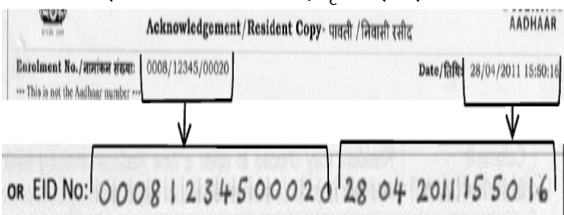
फील्ड 2 एनपीआर नंबर	निवासी अपनी राष्ट्रीय जनसंख्या रजिस्टर सर्वेक्षण स्लिप साथ लाएं और कॉलम को भरें
फील्ड 3 नाम	बिना संबोधन के अपना पूरा नाम लिखें। कृपया अपनी पहचान का मूल प्रमाण साथ लाएं (कृपया नीचे दी गई सूची-क देखें)। पहचान के प्रमाण में और निवासी के नाम में भिन्नता उस सीमा तक अनुमत है जहां तक स्पेलिंग की यह भिन्नता नगण्य है और पहचान के प्रमाण में नाम परिवर्तन नहीं करती हो। उदाहरणार्थ के लिए यदि पहचान का प्रमाण निवासी का नाम "Preeti" पढ़ता है तो निवासी के चाहने पर नाम "Priti" रिकॉर्ड किया जा सकता है।
फील्ड 5 जन्म की तारीख/आयु	जन्म की तारीख दिन/माह/वर्ष के फॉर्मेट में भरें। यदि सही जन्म की तारीख नहीं पता तो उपलब्ध स्थान में वर्ष लिखा जा सकता है। उपलब्ध होने पर कृपया जन्म की तारीख का मूल प्रमाण साथ लाएं (कृपया नीचे दी गई सूची घ देखें)। वैध जन्म की तारीख का दस्तावेज न होने की स्थिति में घोषित चैकबॉक्स चुना जाए। सत्यापित चैकबॉक्स वहां चुना जाता है निवासी ने जन्म की तारीख के प्रमाण के तौर पर दस्तावेज जमा किया हो
फील्ड 6 पता	पूरा पता लिखें। कृपया पते के प्रमाण का मूल दस्तावेज साथ लाएं (कृपया नीचे दी गई सूची ख देखें)। यह ध्यान रहे कि आधार पत्र केवल दिए गए पते पर ही संप्रेषित किया जाएगा। • माता या पिता/अभिभावक/पति या पत्नी का नाम शामिल करने के लिए उपयुक्त बॉक्स को चुनें और व्यक्ति का नाम उसमें लिखें। • पते को पूरा करने के लिए नगण्य त्रुटिशोधन/परिवर्धन मान्य होगा पर इससे पते के प्रमाण/दस्तावेज में दिए गए मूल पते में परिवर्तन न हो।
फील्ड 7 संबंध	• पांच वर्ष से कम आयु के बच्चों के लिए पिता/माता/अभिभावक का ब्योरा उसके आधार अथवा नामांकन आईडी नंबर देना आवश्यक है। • यदि निवासी के पास पहचान का प्रमाण नहीं है और वह नामांकन के लिए परिवार के मुखिया की पहचान का इस्तेमाल कर रहा है तो परिवार के मुखिया के आधार नंबर अथवा नामांकन आईडी सहित ब्योरा देना आवश्यक है। कृपया नामांकन आईडी भरने के लिए नीचे दिए गए दृष्टांत को देखें। कृपया संबंध दर्शाने वाला मूल प्रमाण/दस्तावेज लाएं (कृपया नीचे दी गई सूची ग देखें) • अन्य मामलों में निवासी को संबंध दर्शाने वाले ब्योरे भरना वैकल्पिक है।

फील्ड 8 दस्तावेज	पहचान के प्रमाण और पते का प्रमाण वाले दस्तावेजों का नाम लिखें। जन्म की तारीख का प्रमाण उपलब्ध होने की दशा में जन्म की तारीख के दस्तावेज का नाम लिखें। यदि निवासी के पास पहचान का प्रमाण नहीं है और वह परिवार के मुखिया आधारित नामांकन का इस्तेमाल करता है तो संबंध दर्शाने वाले दस्तावेज का नाम लिखें। वैध दस्तावेजों की सूची के लिए नीचे दिए गए दस्तावेजों की सूची देखें।
फील्ड 9 परिचयदाता/परिवार का मुखिया	जिस निवासी के पास पहचान का प्रमाण और पते का प्रमाण नहीं है वो किसी परिचयदाता/परिवार के मुखिया के माध्यम से अपना नामांकन करवा सकता है। अधिक जानकारी के लिए कृपया नजदीकी नामांकन केंद्र अथवा अपने पंजीयक से संपर्क करें।

सूची क. पहचान का प्रमाण/दस्तावेज**सूची ख. पते का प्रमाण/दस्तावेज**

1. पासपोर्ट	1. पासपोर्ट	19. पेंशनर कार्ड
2. पैन कार्ड	2. बैंक विवरणी/पासबुक	20. स्वतंत्रता सेनानी कार्ड
3. राशन/पीडीएस फोटो कार्ड	3. डाकघर खाता विवरणी/पासबुक	21. किसान पासबुक
4. वोटर आईडी	4. राशन कार्ड	22. सीजीएचएस/ईसीएचएस कार्ड
5. ड्राइविंग लाइसेंस	5. वोटर आईडी	23. सांसद अथवा विधायक अथवा राजपत्रित अधिकारी द्वारा जारी पते का प्रमाणपत्र जिस पर फोटो लगी हो
6. सरकारी फोटो आईडी कार्ड/पीएसयू द्वारा जारी सेवा संबंधी फोटो आईडी कार्ड	6. ड्राइविंग लाइसेंस	24. ग्रामीण क्षेत्रों के मामलों में ग्राम पंचायत प्रमुख अथवा उसके समकक्ष प्राधिकारी द्वारा जारी पते का प्रमाणपत्र
7. मनरेगा जॉब कार्ड	7. सरकारी फोटो आईडी कार्ड/पीएसयू द्वारा जारी सेवा संबंधी फोटो आईडी कार्ड	25. आयकर निर्धारण आदेश
8. मान्यता प्राप्त शैक्षिक संस्थान द्वारा जारी फोटो आईडी	8. बिजली का बिल तीन माह से अधिक पुराना न हो	26. वाहन पंजीकरण प्रमाणपत्र
9. हथियार का लाइसेंस	9. पानी का बिल तीन माह से अधिक पुराना न हो	27. पंजीकृत विक्रय/पट्टा/भाडा करार
10. फोटो बैंक एटीएम कार्ड	10. टेलीफोन लैंडलाइन बिल तीन माह से अधिक पुराना न हो	28. डाक विभाग द्वारा जारी पता कार्ड जिसमें फोटो लगा हो
11. फोटो क्रेडिट कार्ड	11. संपत्ति कर रसीद तीन माह से अधिक पुरानी न हो	29. राज्य सरकार द्वारा जारी जाति अथवा मूल निवास प्रमाणपत्र जिसपर फोटो लगा हो
12. पेंशनर फोटो कार्ड	12. क्रेडिट कार्ड विवरणी तीन माह से अधिक पुरानी न हो	30. संबंधित राज्य/संघ राज्य क्षेत्र सरकारों/प्रशासनों द्वारा जारी अपंगता आईडी कार्ड/दिव्यांग चिकित्सा प्रमाणपत्र
13. स्वतंत्रता सेनानी फोटो कार्ड	13. बीमा पॉलिसी	31. गैस कनेक्शन का बिल जो तीन माह से अधिक पुराना न हो
14. किसान फोटो पासबुक	14. बैंक द्वारा लेटरहेड पर हस्ताक्षर हों जिस पर फोटो लगा हो	32. पति/पत्नी का पासपोर्ट
15. सीजीएचएस/ईसीएचएस फोटो कार्ड	15. पंजीकृत कंपनी द्वारा लेटरहेड पर हस्ताक्षर हों जिस पर फोटो लगा हो	33. नाबालिग होने की दशा में माता पिता का पासपोर्ट
16. डाक विभाग द्वारा जारी पता कार्ड जिसमें नाम और फोटो लगा हो	16. मान्यता प्राप्त शैक्षिक संस्थान लेटरहेड पर हस्ताक्षर हों जिस पर फोटो लगा हो	
17. राजपत्रित अधिकारी अथवा तहसीलदार द्वारा अपने लेटरहेड पर जारी पहचान प्रमाणपत्र जिसमें फोटो लगा हो	17. मनरेगा जॉब कार्ड	
18. संबंधित राज्य/संघ राज्य क्षेत्र सरकारों/प्रशासनों द्वारा जारी अपंगता आईडी कार्ड/दिव्यांग चिकित्सा प्रमाणपत्र	18. हथियार का लाइसेंस	

सूची ग. संबंध दर्शाने वाला प्रमाण/दस्तावेज**सूची घ. जन्म की तारीख का प्रमाण/दस्तावेज**

1. पीडीएस कार्ड	1. जन्म प्रमाणपत्र
2. मनरेगा जॉब कार्ड	2. एसएसएलसी पुस्तक/प्रमाणपत्र
3. सीजीएचएस/राज्य सरकार/ईसीएचएस/ईएसआईसी चिकित्सा कार्ड	3. पासपोर्ट
4. पेंशन कार्ड	4. ग्रुप ए के राजपत्रित अधिकारी द्वारा लेटरहेड पर जारी जन्म की तारीख का प्रमाणपत्र
5. सेना कैप्टन कार्ड	नामांकन आईडी संख्या भरने के लिए दृष्टांत आईडी संख्या
6. पासपोर्ट	
7. जन्म पंजीयक, नगर निगम अथवा अन्य अधिसूचित स्थानीय निकायों जैसे तालुक, तहसील आदि द्वारा जारी जन्म प्रमाणपत्र	
8. केंद्रीय/राज्य सरकार द्वारा जारी कोई परिवार हकदारी दस्तावेज	
9. सरकार द्वारा जारी विवाह प्रमाणपत्र	

– जहां मूल दस्तावेज उपलब्ध न हों, पब्लिक नोटरी/राजपत्रित अधिकारी द्वारा प्रमाणित प्रतियां स्वीकार्य होंगी।

अनुसूची-II

सत्यापन के लिए स्वीकार्य संगत दस्तावेजों की सूची

[इन विनियमों के विनियम 10(3) को देखें]

सूची क. पहचान का प्रमाण/दस्तावेज

- 1 पासपोर्ट
- 2 पैन कार्ड
- 3 राशन/पीडीएस फोटो कार्ड
- 4 वोटर आईडी
- 5 ड्राइविंग लाइसेंस
- 6 सरकारी फोटो आईडी कार्ड/पीएसयू द्वारा जारी सेवा संबंधी फोटो आईडी कार्ड
- 7 मनरेगा जॉब कार्ड
- 8 मान्यता प्राप्त शैक्षिक संस्थान द्वारा जारी फोटो आईडी
- 9 हथियार का लाइसेंस
- 10 फोटो बैंक एटीएम कार्ड
- 11 फोटो क्रेडिट कार्ड
- 12 पेंशनर फोटो कार्ड
- 13 स्वतंत्रता सेनानी फोटो कार्ड
- 14 किसान फोटो पासबुक
- 15 सीजीएचएस/ईसीएचएस फोटो कार्ड
- 16 डाक विभाग द्वारा जारी पता कार्ड जिसमें नाम और फोटो लगा हो
- 17 राजपत्रित अधिकारी अथवा तहसीलदार द्वारा अपने लेटरहेड पर जारी पहचान प्रमाणपत्र जिसमें फोटो लगा हो
- 18 संबंधित राज्य/संघ राज्य क्षेत्र सरकारों/प्रशासनों द्वारा जारी अपंगता आईडी कार्ड/दिव्यांग चिकित्सा प्रमाणपत्र

सूची ख. पते का प्रमाण/दस्तावेज

- 1 पासपोर्ट
- 2 बैंक विवरणी/पासबुक
- 3 डाकघर खाता विवरणी/पासबुक
- 4 राशन कार्ड
- 5 वोटर आईडी
- 6 ड्राइविंग लाइसेंस
- 7 सरकारी फोटो आईडी कार्ड/पीएसयू द्वारा जारी सेवा संबंधी फोटो आईडी कार्ड
- 8 बिजली का बिल तीन माह से अधिक पुराना न हो
- 9 पानी का बिल तीन माह से अधिक पुराना न हो
- 10 टेलीफोन लैंडलाइन बिल तीन माह से अधिक पुराना न हो
- 11 संपत्ति कर रसीद तीन माह से अधिक पुरानी न हो
- 12 क्रेडिट कार्ड विवरणी तीन माह से अधिक पुरानी न हो
- 13 बीमा पॉलिसी
- 14 बैंक द्वारा लेटरहेड पर हस्ताक्षर हों जिस पर फोटो लगा हो

- 15 पंजीकृत कंपनी द्वारा लेटरहेड पर हस्ताक्षर हों जिस पर फोटो लगा हो
- 16 मान्यता प्राप्त शैक्षिक संस्थान लेटरहेड पर हस्ताक्षर हों जिस पर फोटो लगा हो
- 17 मनरेगा जॉब कार्ड
- 18 हथियार का लाइसेंस
- 19 पेंशनर कार्ड
- 20 स्वतंत्रता सेनानी कार्ड
- 21 किसान पासबुक
- 22 सीजीएचएस/ईसीएचएस कार्ड
- 23 सांसद अथवा विधायक अथवा राजपत्रित अधिकारी द्वारा जारी पते का प्रमाणपत्र जिस पर फोटो लगी हो
- 24 ग्रामीण क्षेत्रों के मामलों में ग्राम पंचायत प्रमुख अथवा उसके समकक्ष प्राधिकारी द्वारा जारी पते का प्रमाणपत्र
- 25 आयकर निर्धारण आदेश
- 26 वाहन पंजीकरण प्रमाणपत्र
- 27 पंजीकृत विक्रय/पट्टा/भाडा करार
- 28 डाक विभाग द्वारा जारी पता कार्ड जिसमें फोटो लगा हो
- 29 राज्य सरकार द्वारा जारी जाति अथवा मूल निवास प्रमाणपत्र जिसपर फोटो लगा हो
- 30 संबंधित राज्य/संघ राज्य क्षेत्र सरकारों/प्रशासनों द्वारा जारी अपंगता आईडी कार्ड/दिव्यांग चिकित्सा प्रमाणपत्र
- 31 गैस कनेक्शन का बिल जो तीन माह से अधिक पुरान न हो
- 32 पति/पत्नी का पासपोर्ट
- 33 नाबालिग होने की दशा में माता पिता का पासपोर्ट

सूची ग. संबंध दर्शाने वाला प्रमाण/दस्तावेज

- 1 पीडीएस कार्ड
- 2 मनरेगा जॉब कार्ड
- 3 सीजीएचएस/राज्य सरकार/ईसीएचएस/ईएसआईसी चिकित्सा कार्ड
- 4 पेंशन कार्ड
- 5 सेना कैप्टीन कार्ड
- 6 पासपोर्ट
- 7 जन्म पंजीयक, नगर निगम अथवा अन्य अधिसूचित स्थानीय निकायों जैसे तालुक, तहसील आदि द्वारा जारी जन्म प्रमाणपत्र
- 8 केंद्रीय/राज्य सरकार द्वारा जारी कोई परिवार हकदारी दस्तावेज
10. सरकार द्वारा जारी विवाह प्रमाणपत्र

सूची घ. जन्म की तारीख संबंधी दस्तावेज

- 1 जन्म प्रमाणपत्र
- 2 एसएसएलसी पुस्तक/प्रमाणपत्र
- 3 पासपोर्ट
- 4 ग्रुप ए के राजपत्रित अधिकारी द्वारा लेटरहेड पर जारी जन्म की तारीख का प्रमाणपत्र

अनुसूची-III

नामांकन सूचना का सत्यापन

[इन विनियमों के विनियम 10(6) को देखें]

सूचना	फील्ड	अपेक्षित सत्यापन?	सत्यापन प्रक्रिया
वैयक्तिक ब्योरा	नाम	हां	—पहचान वाले दस्तावेज में से कोई एक। —जिसके पास कोई दस्तावेज नहीं है उनके लिए परिचयदाता/परिवार के मुखिया।
	जन्म की तारीख	—	यह दर्शाने के लिए पताका लगाया गया है कि जन्म की तारीख सत्यापित, घोषित, अथवा लगभग अनुमानित है।
	लिंग	नहीं	—
पते का ब्योरा	आवासीय पता (आधार पत्र और अन्य संसूचनाओं की संप्रेषित के लिए)	हां	—पता दर्शाने वाले दस्तावेज में से कोई एक —जिसके पास कोई दस्तावेज नहीं हैं उनके लिए परिचयदाता/परिवार के मुखिया
माता पिता/ अभिभावक ब्योरा	पिता/माता/अभिभावक/ पति/पत्नी का नाम	सशर्त	—वयस्क होने की स्थिति में पिता/पति/अभिभावक का सत्यापन आवश्यक नहीं है। —प्रमाणन के प्रयोजन से पांच वर्ष से कम के बच्चों के पिता/माता/अभिभावक का नाम, आधार नंबर और बायोमैट्रिक (कोई एक तरीका) सूचना ली जाएगी। —वयस्कों के लिए पिता/पति/अभिभावक अथवा माता/पत्नी/अभिभावक संबंधी सूचना वैकल्पिक होगी।
	पिता/माता/अभिभावक/ पति/पत्नी की नामांकन आईडी/आधार नंबर		
परिचयदाता/ परिवार के मुखिया का ब्योरा	परिचयदाता/परिवार के मुखिया का नाम परिचयदाता/परिवार के मुखिया की विशिष्ट आईडी	हां	—फॉर्म में परिचयदाता/परिवार के मुखिया का नाम, विशिष्ट आईडी —परिचयदाता/परिवार के मुखिया के बायोमैट्रिक अधिप्रमाणन (केवल एक विधि) से लिए जाएं।
संप्रक्र का ब्योरा	मोबाइल नंबर	नहीं	—
	ईमेल का पता	नहीं	—

अनुसूची-IV

अद्यतन फॉर्म का फॉर्मेट

(इन विनियमों का विनियम 19 देखें)

आधार (वित्तीय और अन्य सहायिकियों, लाभों और अन्य सेवाओं की लक्षित संप्रेषित) अधिनियम, 2016 (आधार अधिनियम) की धारा 3 के अंतर्गत

आधार नामांकन/त्रुटिशोधन फॉर्म

यह फार्म अद्यतन/त्रुटिशोधन अनुरोधों के लिए इस्तेमाल किया जाता है और डाक द्वारा भेजा जाए। केवल बड़े अक्षरों का इस्तेमाल करें। अद्यतन/त्रुटिशोधन के लिए फील्ड पर ध्यान दिए बिना पूरा फॉर्म भरें। किसी भी फील्ड में अद्यतन/त्रुटिशोधन के लिए मोबाइल नंबर देना आवश्यक है।

अद्यतन/त्रुटिशोधन की फील्ड: चुनें नाम लिंग जन्म की तारीख पता मोबाइल ईमेल आईडी			
आधार नंबर (कृपया यहां आधार नंबर के सही 12 अंक लिखें)			
फील्ड	इस कॉलम में अंग्रेजी के बड़े अक्षरों में ब्योरा भरें	इस कॉलम में स्थानीय भाषा में ब्योरा भरें (आपके आधार पत्र में दी गई स्थानीय भाषा का ही इस्तेमाल करें)	
निवासी का नाम			
लिंग	चुनें	पुरुष महिला ट्रांसजेंडर	
जन्म की तारीख			
पते का ब्योरा:	चुनें	संरक्षक पुत्री पुत्र पत्नी पति	
अभिभावक/माता पिता/पति या पत्नी का नाम			
मकान/बिल्डिंग/अपार्टमेंट			
गली/रोड/लेन			
पहचान चिह्न			
क्षेत्र/स्थान/सेक्टर			
गांव/कस्बा/शहर			

जिला		
डाकघर		
राज्य		
पिनकोड		
मोबाइल नंबर (अनिवार्य)		ई-मेल (स्वैच्छिक)
दस्तावेज का ब्योरा (संलग्न दस्तावेज का नाम लिखें। वैध दस्तावेजों के लिए अनुलग्नक 1 देखें)		
क. पहचान का प्रमाण (नाम में त्रुटिशोधन के लिए)	ख. पहचान का प्रमाण (नाम में परिवर्तन के लिए)	
जन्म की तारीख	पते का प्रमाण	

आधार (वित्तीय और अन्य सब्सिडियों, लाभों और अन्य सेवाओं की लक्षित संप्रेषित) अधिनियम, 2016 की धारा 3(2) के अंतर्गत प्रकटन

मैं एतद्वारा पुष्टि करता हूँ कि मैंने पिछले 12 माह में कम से कम 182 दिन भारत में निवास किया है और भारतीय विशिष्ट पहचान प्राधिकरण को मेरे द्वारा बायोमैट्रिक सहित दी गई सूचना और यहां दी गई सूचना मेरी अपनी है और सत्य, सही और यथातथ्य है। मुझे यह ज्ञान है कि बायोमैट्रिक सहित मेरी सूचना आधार तैयार करने और प्रमाणन के लिए इस्तेमाल होगी। मुख्य बायोमैट्रिक के सिवाए मेरी सूचना किसी एजेंसी को मेरी अनुमति लेकर प्रमाणन के दौरान उस एजेंसी को दी जा सकती है। मुख्य बायोमैट्रिक के सिवाए मुझे अपनी पहचान की सूचना तक पहुंचने का अधिकार भारतीय विशिष्ट पहचान प्राधिकरण द्वारा बनाई गई प्रक्रिया का पालन करके होगा।

अद्यतन अनुरोध डाक से भेजने के लिए पता

आवेदक के हस्ताक्षर/अंगूठे का निशान

भारतीय विशिष्ट पहचान प्राधिकरण पोस्ट बॉक्स नंबर 10, छिंदवाड़ा, मध्यप्रदेश-480001, भारत	भारतीय विशिष्ट पहचान प्राधिकरण पोस्ट बॉक्स नंबर 99, बंजारा हिल्स हैदराबाद-500034, भारत
--	--

अनुसूची-V

सेवा प्रदाताओं के लिए आचार संहिता

1. सेवा प्रदाता निवासी के हितों की संरक्षा के लिए सर्वोत्तम प्रयास करेगा।
2. सेवा प्रदाता निवासियों के आधार नामांकन और अद्यतन कार्यों में उच्च स्तरीय नैतिकता, सत्यनिष्ठा, गरिमा और शुद्धता बनाए रखेगा।
3. सेवा प्रदाता अपने दायित्वों का तत्परता, नैतिकता और पेशेवर ढंग से निर्वहन करेगा।
4. सेवा प्रदाता हर समय पूरी सतर्कता बरतेगा, पूर्णतः ध्यान रखेगा और स्वतंत्र पेशेवर निर्णय के साथ काम करेगा।
5. सेवा प्रदाता उन स्थिति के सिवाए, जहां सूचना का प्रकटन इस अधिनियम अथवा तत्समय प्रवृत्त किसी अन्य विधि के अनुपालन हेतु अपेक्षित है निवासियों के बारे में उसके संज्ञान में आई किसी गोपनीय सूचना का मौखिक अथवा लिखित रूप में प्रत्यक्षतः अथवा अप्रत्यक्षतः खुलासा नहीं करेगा।
6. सेवा प्रदाता किसी अनुचित व्यवहार में लिप्त नहीं होगा।
7. सेवा प्रदाता यह सुनिश्चित करेगा कि निवासियों की शिकायतों का निवारण समय पर और उपयुक्त विधि से हो।
8. सेवा प्रदाता दुर्ब्यपदेशन को दूर करने के लिए युक्तियुक्त प्रयास करेगा और यह सुनिश्चित करेगा कि निवासियों को दी गई सूचना भ्रामक न हो।
9. सेवा प्रदाता इस अधिनियम के उपबंधों, सरकार और प्राधिकरण द्वारा समय समय पर जारी यथा लागू नियमों, विनियमों का पालन करेगा।
10. सेवा प्रदाता प्राधिकरण को दिए गए किसी दस्तावेज, रिपोर्ट, पेपर, अथवा सूचना में कोई असत्य कथन नहीं करेगा अथवा किसी सारभूत तथ्य को नहीं छिपाएगा।
11. सेवा प्रदाता यह सुनिश्चित करेगा कि उसके द्वारा किसी प्राधिकरण अथवा किसी अन्य विनियामक निकाय की किसी विधि, नियम, विनियम और दिशानिर्देश के सारभूत उल्लंघन अथवा अनुपालन न होने के लिए उसके विरुद्ध शुरु की गई किसी कार्रवाई, विधिक कार्यवाही, इत्यादि के बारे में प्राधिकरण को तुरंत सूचित किया जाए।
12. सेवा प्रदाता उसकी नामांकन और अद्यतन सेवाओं के संचालन में उसकी एजेंसियों और कर्मचारियों के कृत्यों और लोपों के लिए उत्तरदायी होगा।
13. सेवा प्रदाता के पास निवासियों को ऋजु, तत्पर और सक्षम सेवाएं प्रदान करने के लिए पर्याप्त रूप से प्रशिक्षित स्टाफ होना चाहिए।
14. सेवा प्रदाता आंतरिक ऑपरेशनों के विनियमन के लिए आंतरिक आचार संहिता विकसित करेगा और अपनी एजेंसियों, कर्मचारियों और अधिकारियों द्वारा उनके दायित्वों के निर्वहन के लिए उपयुक्त आचरण के मानक तय करेगा। उपर्युक्त संहिता में पेशेवर उत्कृष्टता और आदर्श बनाए रखना, सत्यनिष्ठा, गोपनीयता, वस्तुनिष्ठता और हितों के टकरावों को दूर करने जैसे घटक शामिल हो सकते हैं।
15. सेवा प्रदाता नामांकन और आंकड़ा अद्यतन में यथातथ्यता सुनिश्चित करने के लिए अपने क्रियाकलापों में निर्माता-जांचकर्ता संकल्पना का अनुपालन करेगा।
16. सेवा प्रदाता नामांकन और अद्यतन प्रक्रिया में किसी छल्युक्त, कपटपूर्ण व्यवहार में लिप्त नहीं होगा।
17. सेवा प्रदाता प्राधिकरण द्वारा इस प्रयोजनार्थ यथा विहित नीतियों और प्रक्रमणों के अनुसार निवासियों से इकट्ठा किए गए समस्त आंकड़ों (जनसांख्यिकीय/बायोमैट्रिक) की सुरक्षा और संरक्षा सुनिश्चित करेगा।

18. सेवा प्रदाता यथा लागू नामांकन एजेंसियों, ऑपरेटरों, पर्यवेक्षकों इत्यादि के निलंबन/प्रविरत करने/पैनल से हटाने के संबंध में प्राधिकरण के निर्णय को लागू करेगा।
19. सेवा प्रदाता प्राधिकरण द्वारा विहित डाटा फील्ड, डाटा सत्यापन और बायोमैट्रिक फील्डों के लिए तय किए गए मानकों का पालन करेगा।
20. सेवा प्रदाता जरूरत पड़ने पर केवल उन यंत्रों और आईटी प्रणालियों का इस्तेमाल करेगा जिसके विनिर्देशन प्राधिकरण द्वारा अनुमोदित हों।
21. सेवा प्रदाता रिकॉर्ड के रखरखाव और अनुरक्षण के लिए प्राधिकरण द्वारा विहित किए गए नियमों का पालन करेगा।
22. सेवा प्रदाता इकट्ठा किए गए डाटा के पारेषण के लिए प्राधिकरण द्वारा विहित प्रक्रम और प्रणालियों का पालन करेगा।
23. सेवा प्रदाता प्राधिकरण द्वारा यथा विहित गोपनीयता, निजता और सुरक्षा के नियमों का पालन करेगा।
24. सेवा प्रदाता आधार परियोजना के संदेशों, अर्तवस्तु और अभिप्रायों के प्रसार और संसूचन के लिए प्राधिकरण द्वारा यथा विहित नियमों का पालन करेगा। आधार लोगो और ब्रांड नाम प्राधिकरण की संपत्ति है इसलिए प्राधिकरण अपने लोगो, ब्रांड नाम, ब्रांड आकृति और अन्य संसूचन और जागरुकता सामग्रियों के इस्तेमाल की विधि और सीमा तय करेगा।
25. सेवा प्रदाता आधार प्रक्रमणों के कार्यान्वयन के लिए प्राधिकरण द्वारा विहित नियमों, प्रक्रमणों और मानकों का पालन करेगा।
26. सेवा प्रदाता नामांकन की आवधिक रिपोर्ट प्राधिकरण द्वारा यथा विहित प्रारूप और विधि में प्राधिकरण को भेजेगा।
27. सेवा प्रदाता समय समय पर प्राधिकरण द्वारा किए गए अनुरोधों के माध्यम से आधार प्रक्रमणों से संबंधित सूचना प्राधिकरण को प्रदान करेगा।

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यपालक अधिकारी
[विज्ञापन-III/4/असा./238]

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (ENROLMENT AND UPDATE) REGULATIONS, 2016

(No. 2 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 2 of 2016).—In exercise of the powers conferred by sub-section (1), and sub-clauses (a), (b), (d), (e), (j), (k), (l), (n), (r), (s), and (v) of sub-section (2), of Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, 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 (Enrolment and Update) Regulations, 2016 (1 of 2016).
- (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 to therwise requires,-
 - (a) “Act” means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
 - (b) “Aadhaar Letter” means a document for conveying the Aadhaar number to a resident;
 - (c) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;
 - (d) “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;
 - (e) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;
 - (f) “Central Identities Data Repository” or “CIDR” means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

- (g) “enrolling agency” means an agency appointed by the Authority or a Registrar, as the case may be, for collecting demographic and biometric information of individuals under the Act;
- (h) “enrolment” means the process, as specified in these regulations, to collect demographic and biometric information from individuals by the enrolling agencies for the purpose of issuing Aadhaar numbers to such individuals under the Act;
- (i) “enrolment centre” means a permanent or temporary centre set up by an enrolling agency for carrying out enrolment of residents and updating their information;
- (j) “Enrolment ID” or “EID” means a 28 digit Enrolment Identification Number allocated to residents at the time of enrolment.
- (k) “Head of Family” means any member of a family of a resident in respect of whom a document evidencing proof of relationship with the resident can be furnished, and could include father, mother or spouse of the resident;
- (l) “identity information” in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information;
- (m) “introducer” means persons authorised by Registrars to introduce residents who do not possess any of the prescribed supporting documents;
- (n) “operator” means the certified personnel employed by enrolling agencies to execute the process of enrolment at the enrolment centers;
- (o) “Registrar” means any entity authorised or recognised by the Authority for the purpose of enrolling individuals under this Act;
- (p) “regulations” means the Aadhaar (Enrolment and Update) Regulations, 2016;
- (q) “resident” means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment;
- (r) “service provider” includes all entities engaged for discharging any function related to the enrolment or update process;
- (s) “supervisor” means the certified personnel employed by enrolling agencies to operate and manage the enrolment centres;
- (t) “verifier” means the personnel appointed by Registrars for verification of documents at enrolment centres;
- (2) all other words and expressions used in these regulations but not defined, and defined in the Act and the rules and other regulations made there under, shall have the meanings respectively assigned to them in the Act or the rules or other regulations, as the case may be.

CHAPTER II

RESIDENT ENROLMENT PROCESS

3. Biometric information required for enrolment. —

- (1) The following biometric information shall be collected from all individuals undergoing enrolment (other than children below five years of age):
- (i) Facial image;
 - (ii) All ten fingerprints; and
 - (iii) Scans of both irises.
- (2) The standards for collecting the biometric information shall be as specified by the Authority for this purpose.

4. Demographic information required for enrolment. —

- (1) The following demographic information shall be collected from all individuals undergoing enrolment (other than children below five years of age):
- (i) Name

- (ii) Date of Birth
 - (iii) Gender
 - (iv) Residential Address
- (2) The following demographic information may also additionally be collected during enrolment, at the option of the individual undergoing enrolment:
- (i) Mobile number
 - (ii) Email address
- (3) In case of Introducer-based enrolment, the following additional information shall be collected:
- (i) Introducer name
 - (ii) Introducer's Aadhaar number
- (4) In case of Head of Family based enrolment, the following additional information shall be collected:
- (i) Name of Head of Family
 - (ii) Relationship
 - (iii) Head of Family's Aadhaar number
 - (iv) One modality of biometric information of the Head of Family
- (5) The standards of the above demographic information shall be as may be specified by the Authority for this purpose.
- (6) The demographic information shall not include race, religion, caste, tribe, ethnicity, language, record of entitlement, income or medical history of the resident.

5. Information required for enrolment of children below five years of age. —

- (1) For children below the five years of age, the following demographic and biometric information shall be collected:
- (a) Name
 - (b) Date of Birth
 - (c) Gender
 - (d) Enrolment ID or Aadhaar number of any one parent, preferably that of the mother in the event both parents are alive, or guardian. The Aadhaar number or EID of such parent or guardian is mandatory, and a field for relationship will also be recorded.
 - (e) The address of such child which is the same as that of the linked parent / guardian.
 - (f) Facial image of the child shall be captured. The biometric information of any one parent / guardian shall be captured or authenticated during the enrolment.
- (2) The Proof of Relationship (PoR) document as listed in schedule II for establishing the relationship between the linked parent/guardian and the child shall be collected at the time of enrolment. Only those children can be enrolled based on the relationship document (PoR), whose names are recorded in the relationship document.

6. Enrolment of residents with biometric exceptions. —

- (1) For residents who are unable to provide fingerprints, owing to reasons such as injury, deformities, amputation of the fingers/ hands or any other relevant reason, only Iris scans of such residents will be collected.
- (2) For residents who are unable to provide any biometric information contemplated by these regulations, the Authority shall provide for handling of such exceptions in the enrolment and update software, and such enrolment shall be carried out as per the procedure as may be specified by the Authority for this purpose.

7. Role of Registrars, enrolling agencies, etc. in enrolment. —

- (1) The Registrars appointed by the Authority shall carry out the enrolment of residents by themselves or through enrolling agencies contracted/appointed by them.

- (2) The enrolling agencies shall set up enrolment centres for enrolment of residents as well as for correction or update of residents' information. The opening of enrolment centres, the services offered and other guidelines for their operations shall be in accordance with the procedure as may be specified by the Authority for this purpose.
- (3) Enrolment shall be carried out at permanent enrolment centres and through temporary centres set up for this purpose.
- (4) Enrolment shall be carried out by the operators, verifiers, supervisors and other authorized personnel at the enrolment centres.
- (5) Registrars shall make reasonable efforts to enrol residents who do not possess any of the prescribed supporting documents, through alternate modes of enrolment specified in Regulation 10.

8. Equipment, software, etc. used in enrolment. —

- (1) The Registrars and enrolling agencies shall use only the software provided or authorised by the Authority for enrolment purposes.
- (2) The standard enrolment/update software shall have the security features as may be specified by the Authority for this purpose.
- (3) All equipment used in enrolment, such as computers, printers, biometric devices and other accessories shall be as per the specifications issued by the Authority for this purpose.
- (4) The biometric devices used for enrolment shall meet the specifications, and shall be certified as per the procedure, as may be specified by the Authority for this purpose.

9. Disclosure of information to residents at the time of enrolment. —

At the time of enrolment, the enrolling agency shall inform the individual undergoing enrolment of the following details: (a) the manner in which the information shall be used;

(b) the nature of recipients with whom the information is intended to be shared during authentication; and

(c) the existence of a right to access information, the procedure for making requests for such access, and details of the person or department in-charge to whom such requests can be made. The above details shall be communicated to residents through the enrolment form, in a format provided in Schedule I .

10. Submission and verification of information. —

- (1) Residents seeking enrolment shall be required to submit an application for enrolment along with copies of supporting documents for proof of identity, address and date of birth, at an enrolment centre.
- (2) An indicative list of supporting documents accepted for verification of identity, address and date of birth is prescribed in Schedule II. The Authority may expand or modify the list of acceptable supporting documents through circulars or notifications from time to time.
- (3) The Authority may dispense with requirement of collecting proof of address and proof of identity of the residents in case of enrolment/update by Registrar General of India.
- (4) In the event a resident does not possess any of the required supporting documents, enrolment may be carried out through the following modes:
 - (a) **Introducer-based enrolment:** If a resident is unable to provide documentary proof of identity or proof of address, he can be enrolled through a pre-designated introducer identified and notified by the Registrar or the regional offices of the Authority. Persons registered with the Authority as introducers could include the Registrars' own employees, elected local body members, members of local administrative bodies, postman, influencers such as teachers, health workers, doctors, aanganwadis / asha workers, representative of local NGOs. Such approved introducers shall introduce a resident and vouch for the validity of resident's information. An introducer shall verify the information filled, fill up his name and Aadhaar number, and affix his signature or thumb impression on the resident's enrolment form.
 - (b) **Head of Family (HoF) based enrolment:** In the event the head of family of a resident possesses the required supporting documents and has been enrolled through such supporting documents, the resident may be enrolled through such documents provided that (i) the resident can furnish proof of relationship, and (ii) the proof of relationship and the supporting documents record the same address for the family member and the head of family.
- (5) The verification of the enrolment data in the above three methods shall be as provided in Schedule III.

11. Collection of information at enrolment centres. —

- (1) The enrolment operator shall capture (i) the demographic information as submitted by the resident in the application form; and (ii) the biometric information using the enrolment software provided or approved by the Authority.
- (2) The enrolment operator shall collect and record the physical copies of the requisite supporting documents, or, if facility exists at the enrolment centre, convert the physical copies into electronic format, as per the process as may be specified by the Authority.
- (3) After capturing the information, a resident shall be given the opportunity of verifying his information for accuracy.
- (4) On completion of enrolment, an acknowledgement slip containing the EID and other enrolment details signed by the enrolment operator shall be provided to the resident.
- (5) The procedures, standards and guidelines to be followed during enrolment (including for enrolment of children below five years of age and for exception handling) and formats, templates, checklists to be used for carrying out enrolment shall be as per procedures as may be specified by the Authority for this purpose.

12. Agencies requiring Aadhaar as condition for receipt of service, etc. —

Any Central or State department or agency which requires an individual to undergo authentication or furnish proof of possession of Aadhaar number as a condition for receipt of any subsidy, benefit or service pursuant to Section 7 of the Act, shall ensure enrolment of its beneficiaries who are yet to be enrolled, through appropriate measures, including co-ordination with Registrars and setting up enrolment centres at convenient locations or providing enrolment facilities by becoming a Registrar itself.

CHAPTER II**GENERATION OF AADHAAR NUMBERS AND DELIVERY TO RESIDENTS****13. Generation of Aadhaar numbers. —**

- (1) The registrars and enrolling agencies shall upload the enrolment packet to the CIDR using the software provided by the Authority.
- (2) The Authority shall process the enrolment data received from the Registrar and after deduplication and other checks as specified by the Authority, generate the Aadhaar number.

14. Rejection of enrolment. —

- (1) The Authority may reject an enrolment due to there being duplicate enrolments by the resident, quality or any other technical reason.
- (2) In case of rejection due to duplicate enrolment, resident may be informed about the enrolment against which his Aadhaar number has been generated in the manner as may be specified by the Authority.

15. Delivery of Aadhaar number. —

- (1) The Aadhaar number may be communicated to residents in physical form (including letters or cards) and/ or electronic form (available for download through the Authority's website or through SMS).
- (2) All agencies engaged by the Authority for printing, dispatch, and other functions related to delivery shall comply with the applicable processes.

CHAPTER IV**UPDATE OF RESIDENT INFORMATION****16. Request for update of identity information. —**

An Aadhaar number holder may seek alteration of his demographic information or biometric information in cases specified under Section 31 of the Act in accordance with update procedure specified in this Chapter.

17. Mandatory update for children. —

The Authority shall require the biometric information of children to be updated upon attaining five years of age and fifteen years of age in accordance with the procedure specified by the Authority.

18. Equipment, software, etc. used for update. —

- (1) The Registrars, enrolling agencies or other service providers involved in the update process shall use only the software provided or approved by the Authority for updating purposes.

- (2) The standard update software shall have the security features as laid down by the Authority for this purpose.
- (3) All equipment used for updating purposes, such as computers, printers, biometric devices and other accessories shall be as per specifications laid down by the Authority from time to time.

19. Mode of updating residents' information. —

The process of updating residents' information in the CIDR may be carried out through the following modes:—

- (a) At any enrolment centre with the assistance of the operator and/ or supervisor. The resident will be biometrically authenticated and shall be required to provide his Aadhaar number along with the identity information sought to be updated.
- (b) Online mode: Demographic information may be updated online through designated portals upon submission of Aadhaar number and the registered mobile number. Authentication will be carried out through a One-Time Password (OTP) sent to the registered mobile number.
- (c) Postal mode: An update request for demographic information may also be sent in the format specified in Schedule IV through post along with the requisite supporting documents for verification.

The resident shall be assigned an update ID for tracking the status update, and the revised Aadhaar letter may be made available to the resident in physical or electronic form in accordance with the procedure as may be specified by the Authority for this purpose. The procedures for update, standards and guidelines to be followed along with the formats, templates, checklist to be used for carrying the update shall be as may be specified by the Authority for this purpose.

20. Convenience fee. —

The Authority may authorise Registrars to charge convenience fee from the residents, not exceeding an amount specified by the Authority, for update of demographic information and biometric information.

CHAPTER V

APPOINTMENT OF REGISTRARS, ENROLLING AGENCIES AND OTHER SERVICE PROVIDERS

21. Appointment of Registrars. —

- (1) Registrars shall be appointed by the Authority, through MOUs or agreements, for enrolment and update of residents across the country, and could include entities which interact with residents in the usual course of implementation of their programmes. The eligible entities for appointment as registrars are State/ UT Governments, Central ministries and departments / agencies under them, Public Sector companies of Central / State Governments, Public Sector banks and regulated entities including National Securities Depository Limited, UTI Infrastructure Technology and Services Ltd, Special Purpose Vehicles (SPV) created by Central or State Government including CSC e-Governance services India Ltd. Upon appointment, a Registrar code shall be assigned to each Registrar.
- (2) Registrars shall be responsible for field level execution, monitoring and audit.
- (3) Registrars shall allow the Authority reasonable access to the premises occupied by it or by any other person on its behalf and also extend reasonable facility for examining any books, records, documents and computer data in the possession of the Registrar or any other person on their behalf and also provide copies of the document or other materials which, in the opinion of the Authority are relevant for the purpose of audit.
- (4) Registrars shall not use the information collected during enrolment for any purpose other than uploading information to the CIDR.
- (5) Registrars shall display on their websites adequate and appropriate information about enrolment and update services, including contact details of persons and services available to residents.
- (6) Registrars shall ensure that any agency and/ or person employed or appointed by them to conduct the enrolment and update operations is fit and proper and otherwise qualified to act, in the capacity so employed or appointed including having relevant professional training or experience.
- (7) Registrars shall not permit sub-contracting of enrolment functions by enrolling agencies to third parties. Registrars may permit field level manpower to be hired through third parties provided the enrolling agencies furnishes details of the entities from which such manpower is sought to be hired.
- (8) Registrars shall at all times abide by the Code of Conduct as specified in Schedule V of these regulations.
- (9) Registrars shall adhere to the processes, policies and guidelines, checklists, forms and templates issued by the

Authority from time to time and shall also ensure compliance by the enrolling agencies of such procedures, etc.

22. Registrars engaged before commencement of these regulations. —

- (1) The Registrars engaged prior to commencement of these regulations shall be deemed to be appointed as Registrars by the Authority under the Act:

Provided that the agreements entered into with them by 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) In the event any Registrar engaged prior to commencement of these regulations wishes to cease being a Registrar under the Act, it may apply to the Authority in a form as may be specified by the Authority for this purpose, and shall cease to be a Registrar and to have the power to conduct enrolment or engage enrolling agencies for enrolment.

23. Empanelment of Enrolling Agencies. —

- (1) The Authority shall empanel the enrolling agencies through an open Request for Empanelment (RFE) process and the eligibility, terms and conditions of the empanelment shall be notified by the Authority from time to time.
- (2) The interested agencies may apply for empanelment by fulfilling the eligibility and other technical and financial criteria of the RFE.
- (3) The Authority shall evaluate the applications of agencies and empanel the eligible agencies as enrolling agencies after completing the requirements of the RFE.
- (4) The Authority shall provide an Enrolling Agency Code using which the Registrar can onboard an empaneled enrolling agency to the CIDR.
- (5) The Authority may also permit Registrars to engage other agencies as enrolling agencies after following a suitable process for screening and engaging such agencies, as may be specified by the Authority for this purpose.
- (6) The enrolling agency shall be responsible for field level execution and audit. The enrolling agency shall allow the Authority reasonable access to the premises occupied by it or by any other person on its behalf and also extend reasonable facility for examining any books, records, documents and computer data in the possession of enrolling agency or any other person on their behalf and also provide copies of the document or other materials which, in the opinion of the Authority are relevant for the purpose of audit.
- (7) The enrolling agencies shall not use the information collected during enrolment for any purpose other than uploading information to the CIDR.
- (8) Enrolling agencies shall ensure that any agency and/ or person employed or appointed by them to conduct the enrolment and update operations is fit and proper and otherwise qualified to act, in the capacity so employed or appointed including having relevant professional training or experience.
- (9) The enrolling agencies shall at all times abide by the Code of Conduct for service providers as specified in Schedule V of these regulations.
- (10) The enrolling agencies shall adhere to the various process, policies and guidelines, checklists, forms and templates issued by the Authority from time to time.
- (11) The enrolling agencies empaneled by the Authority prior to establishment of the Authority under the Act shall be deemed to have been empaneled as enrolling agencies by the Authority under the Act.

24. Other service providers. —

- (1) Other service providers may be appointed or engaged by the Authority from time to time for discharging any function related to the resident enrolment process or updating of information.
- (2) All such service providers shall adhere to the regulations, processes, standards, guidelines, and orders issued by the Authority from time to time, and the code of conduct provided in Schedule V of these regulations, as applicable.

25. Testing and certification of staff appointed for enrolment. —

- (1) An enrolling agency shall ensure that the operators, supervisors, and other enrolment staff employed or engaged by it are duly certified for carrying out enrolment through a certification process as may be specified by the Authority.
- (2) The Authority may designate testing and certification agencies for this purpose.

- (3) The Authority may specify the minimum qualifications required for being engaged for any of the roles in the enrolment process, the process of their appointment, and the detailed roles and responsibilities of such personnel.

26. Liability of Registrars, enrolling agencies and other service providers and action in case of default. —

- (1) The Registrars, enrolling agencies, and other service providers, and the supervisors, operators or any other persons or agencies employed by them shall adhere to all regulations, processes, standards, guidelines, and orders issued by the Authority from time to time, and the code of conduct provided in Schedule V.
- (2) The Authority shall monitor the enrolment activities of the Registrars, enrolling agencies and the operators, supervisors and other personnel associated with enrolment.
- (3) Without prejudice to action that may be taken under the Act, violation of any regulation, process, standard, guideline or order by any service provider or other person may result in immediate suspension of the activities of such service providers or the concerned persons, and after holding due inquiry as deemed fit by the Authority, cancellation of their credentials, codes and permissions issued to them pursuant to the Act or these regulations.

CHAPTER VI

OMISSION OR DEACTIVATION OF AADHAAR NUMBER AND IDENTITY INFORMATION

27. Cases requiring omission of Aadhaar Number. —

- (1) The Aadhaar number of an Aadhaar number holder shall be cancelled in the following circumstances:—
- (a) If it is established that more than one Aadhaar numbers have been issued to the same person, then the Aadhaar number assigned from the earlier enrolment shall be retained, and all subsequent Aadhaar numbers shall be cancelled .
- (b) Where the Aadhaar number has been generated in violation of the prescribed guidelines:—
- (i) “Photo on Photo” case where core biometric information is not available: Where an existing photograph is used for enrolment instead of capturing a new photograph at the enrolment centre, and where core biometric information has not been captured during enrolment, the resident’s Aadhaar number shall be cancelled
- (ii) “False Biometric Exception” cases: Where the enrolment has been wrongly carried out as a ‘biometric exception’ case, the Aadhaar number shall be cancelled.
- (iii) Where an adult has been enrolled as a child below five years of age to avoid capturing of biometric information, Aadhaar number shall be cancelled.
- (iv) Any other case requiring cancellation owing to the enrolment appearing fraudulent to the Authority
- (2) Upon cancellation, services that are provided by the Authority to the Aadhaar number holder shall be disabled permanently.

28. Cases requiring deactivation of Aadhaar Number. —

- (1) The Aadhaar number of an Aadhaar number holder shall be deactivated in the following circumstances:
- (a) “Photo on Photo” and core biometric information is available: Where an existing photograph is used instead of capturing a fresh photograph at the enrolment centre, and where core biometric information of the resident has been captured, the Aadhaar number shall be de-activated, and the resident asked to update his photograph. Upon successful update of his photograph, the Aadhaar number may be re-activated.
- (b) “False Partial Biometric Exception” cases: Where certain attributes constituting biometric information have not been captured despite the resident being in a position to provide them, the Aadhaar number shall be de-activated.
- (c) Where it is found at a later stage that enrolment has been carried out without valid supporting documents, the Aadhaar number shall be deactivated till it is updated by the Aadhaar number holder after furnishing valid supporting documents.
- (d) Where the information captured has been flagged as having bad data and requiring update (such as mixed/anomalous biometrics information, abusive/expletive words and unparliamentary language in resident demographics, multiple names in single name using ‘urf’ or ‘Alias’), the Aadhaar number shall be deactivated till it is updated by Aadhaar holder.
- (e) Where a child having attained the age of five or fifteen years of age fails to update his biometric information within two years of attaining such age, his Aadhaar number shall be deactivated. In cases where such update has not been carried out at the expiry of one year after deactivation, the Aadhaar number shall be omitted.

(f) Any other case requiring deactivation as deemed appropriate by the Authority.

- (2) Upon deactivation, services that are provided by the Authority to the Aadhaar number holder shall be discontinued temporarily till such time the Aadhaar number holder updates or rectifies the information, owing to which his Aadhaar number has been deactivated by the Authority.

29. Inquiry into cases requiring omission or deactivation. —

- (1) Any case reported or identified as a possible case requiring omission or deactivation may require field inquiry which may include hearing the persons whose Aadhaar number is sought to be omitted or deactivated.
- (2) An agency nominated by the Authority shall examine/inquire and submit a report to the Authority as per the procedures as may be specified by the Authority for this purpose.
- (3) The Authority may initiate necessary action upon receiving the report and the decision to omit or deactivate an Aadhaar number shall lie with the Authority.

30. Communication to the Aadhaar number holder. —

- (1) An Aadhaar number holder shall be informed of the omission or deactivation of their Aadhaar number along with reasons through SMS, registered e-mail ID, tele-calling, letter or through such means as deemed fit by the Authority.
- (2) Any complaint of an Aadhaar number holder in respect of such omission or deactivation may be addressed through the grievance redressal mechanism set up by the Authority.

31. Rectification action. —

- (1) In case of omission of Aadhaar number for reasons other than multiple Aadhaar numbers having been issued, residents shall be required to re-enrol.
- (2) In case of deactivation, a resident shall be required to update his identity information partly or fully as required, as per the guidelines or policies as may be specified by the Authority.

CHAPTER VII

GRIEVANCE REDRESSAL MECHANISM

32. Setting up of a contact centre for grievance redressal. —

- (1) The Authority shall set up a contact centre to act as a central point of contact for resolution of queries and grievances of residents, accessible to residents through toll free number(s) and/ or e-mail, as may be specified by the Authority for this purpose.
- (2) The contact centre shall:
- a. Provide a mechanism to log queries or grievances and provide residents with a unique reference number for further tracking till closure of the matter;
 - b. Provide regional language support to the extent possible;
 - c. Ensure safety of any information received from residents in relation to their identity information;
 - d. Comply with the procedures and processes as may be specified by the Authority for this purpose.
- (3) Residents may also raise grievances by visiting the regional offices of the Authority or through any other officers or channels as may be specified by the Authority.

CHAPTER VIII

MISCELLANEOUS

33. Savings. —

All procedures, orders, processes, standards, specifications and policies issued and MOUs, agreements or contracts entered by 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, 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.

34. 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.

35. 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.

Instructions to follow while filling up the enrolment form

Field 2 NPR NUMBER	Resident may bring his/her National Population Register Survey slip (if available) and fill up the column.
Field 3 NAME	Write full name without salutations/titles. Please bring the original* Proof of Identity (POI) document. (See list A below). Variation in Resident's Name in contrast to PoI is permissible as long as the change is minor spelling only, without altering the Name in PoI document. For Example: If Resident's PoI reads "Preeti", then "Priti" can be recorded if Resident wants so.
Field 5 DOB / AGE	Fill in Date of Birth in DDMYYYY format. If exact Date of Birth is not known, approximate age in Years may be filled in the space provided. Please bring the original Proof of Date of Birth (DoB), if available. (See list D below). Declared checkbox may be selected if Resident does not have a valid proof of Date of Birth document. Verified checkbox is selected where Resident has provided documents as proof of Date of birth.
Field 6 ADDRESS	Write complete address. Please bring the original Proof of Address (POA) document. (See list B below). Please note that the Aadhaar letter will be delivered at the given address only. <ul style="list-style-type: none"> To include Parent / Guardian / Spouse name as part of the address, select the appropriate box and enter the name of the person. Minor Corrections / Enhancements are permissible to make the address complete without altering the base address as mentioned in the POA document.
Field 7 RELATIONSHIP	<ul style="list-style-type: none"> In case of children below 5 years, it is mandatory to provide father/mother/guardian details with their Aadhaar or EID number. If the resident is not holding a Proof of Identity & using the Head of the Family identity for enrolment, it is mandatory to provide Head of the family's details with his/her Aadhaar or EID number. Please refer illustration below for filling EID. Please bring the original Proof of Relationship (POR) document. (See list C below). For other cases, it is optional for the resident to fill up the relationship details.
Field 8 DOCUMENTS	Write the name of Documents for PoI and PoA. In case proof of Date of Birth is available, then write the name of Date of Birth document. If the resident is not holding a Proof of Identity & using the Head of Family based enrolment, then write the name of Proof of Relationship document. For Valid list of documents, please refer list of Documents below.
Field 9 INTRODUCER/HoF	Resident who does not have POI and POA may get enrolled through an Introducer/ Head of Family. PI contact nearest enrolment centre or your Registrar, for further details.

List A. POI documents

- Passport
- PAN Card
- Ration/ PDS Photo Card
- Voter ID
- Driving License
- Government Photo ID Cards/ service photo identity card issued by PSU
- NREGS Job Card
- Photo ID issued by Recognized Educational Institution
- Arms License
- Photo Bank ATM Card
- Photo Credit Card
- Pensioner Photo Card
- Freedom Fighter Photo Card
- Kissan Photo Passbook
- CGHS / ECHS Photo Card
- Address Card having Name and Photo issued by Department of Posts
- Certificate of Identity having photo issued by Gazetted Officer or Tehsildar on letterhead
- Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations

List B. POA documents

- Passport
- Bank Statement/ Passbook
- Post Office Account Statement/Passbook
- Ration Card
- Voter ID
- Driving License
- Government Photo ID cards/ service photo identity card issued by PSU
- Electricity Bill (not older than 3 months)
- Water bill (not older than 3 months)
- Telephone Landline Bill (not older than 3 months)
- Property Tax Receipt (not older than 3 months)
- Credit Card Statement (not older than 3 months)
- Insurance Policy
- Signed Letter having Photo from Bank on letterhead
- Signed Letter having Photo issued by registered Company on letterhead
- Signed Letter having Photo issued by Recognized Educational Institution on letterhead
- NREGS Job Card
- Arms License
- Pensioner Card
- Freedom Fighter Card

- Kissan Passbook
- CGHS / ECHS Card
- Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead
- Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
- Income Tax Assessment Order
- Vehicle Registration Certificate
- Registered Sale / Lease / Rent Agreement
- Address Card having Photo issued by Department of Posts
- Caste and Domicile Certificate having Photo issued by State Govt.
- Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
- Gas Connection Bill (not older than 3 months)
- Passport of Spouse
- Passport of Parents(in case of Minor)

List C. POR documents

- PDS Card
- MNREGA Job Card
- CGHS/State Government/ECHS/ESIC Medical card
- Pension Card
- Army Canteen Card
- Passport
- Birth Certificate issued by Registrar of Birth, Municipal Corporation and other notified local government bodies like Taluk, Tehsil etc.
- Any other Central/State government issued family entitlement document
- Marriage Certificate Issued by the Government.

List D. DOB documents

- Birth Certificate
- SSLC Book/Certificate
- Passport
- Certificate of Date of Birth issued by Group A Gazetted Officer on Letterhead

Illustration for filling up EID No.

Acknowledgement/Resident Copy - पावती / निवासी स्वीद		AADHAAR
Enrolment No./आधारक संख्या: 0008/12345/00020	Date/दिनांक: 28/04/2011 15:50:16	
OR EID No: 0008123450002028042011155016		

*In instances where original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted.

SCHEDULE II

**List of acceptable supporting documents for verification
(See Regulation 10(2) of these Regulations)**

List A. POI (Proof of Identity) documents

- Passport
- PAN Card
- Ration/ PDS Photo Card
- Voter ID
- Driving License
- Government Photo ID Cards/ service photo identity card issued by PSU
- NREGS Job Card
- Photo ID issued by Recognized Educational Institution
- Arms License

10. Photo Bank ATM Card
11. Photo Credit Card
12. Pensioner Photo Card
13. Freedom Fighter Photo Card
14. Kissan Photo Passbook
15. CGHS / ECHS Photo Card
16. Address Card having Name and Photo issued by Department of Posts
17. Certificate of Identify having photo issued by Gazetted Officer or Tehsildar on letterhead
18. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations

List B. POA (Proof of Address) documents

1. Passport
2. Bank Statement/ Passbook
3. Post Office Account Statement/Passbook
4. Ration Card
5. Voter ID
6. Driving License
7. Government Photo ID cards/ service photo identity card issued by PSU
8. Electricity Bill (not older than 3 months)
9. Water bill (not older than 3 months)
10. Telephone Landline Bill (not older than 3 months)
11. Property Tax Receipt (not older than 3 months)
12. Credit Card Statement (not older than 3 months)
13. Insurance Policy
14. Signed Letter having Photo from Bank on letterhead
15. Signed Letter having Photo issued by registered Company on letterhead
16. Signed Letter having Photo issued by Recognized Educational Institution on letterhead
17. NREGS Job Card
18. Arms License
19. Pensioner Card
20. Freedom Fighter Card
21. Kissan Passbook
22. CGHS / ECHS Card
23. Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead
24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
25. Income Tax Assessment Order
26. Vehicle Registration Certificate
27. Registered Sale / Lease / Rent Agreement
28. Address Card having Photo issued by Department of Posts
29. Caste and Domicile Certificate having Photo issued by State Govt.
30. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
31. Gas Connection Bill (not older than 3 months)
32. Passport of Spouse
33. Passport of Parents(in case of Minor)

List C. POR (Proof of Relationship) documents

1. PDS Card
2. MNREGA Job Card
3. CGHS/State Government/ECHS/ESIC Medical card
4. Pension Card
5. Army Canteen Card
6. Passport

7. Birth Certificate issued by Registrar of Birth, Municipal Corporation and other notified local government bodies like Taluk, Tehsil etc.
8. Any other Central/State government issued family entitlement document.
9. Marriage Certificate issued by the Government

List D. DOB (Date of Birth) documents

1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on Letterhead

SCHEDULE III
Verification of enrolment information
(See Regulation 10(5) of these Regulations)

Information	Fields	Verification Required?	Verification Procedure
Personal Details	Name	Yes	<ul style="list-style-type: none"> ○ Any of the Proof of Identity documents. ○ Introducer/Head of Family for people who have no documents.
	Date of Birth	<ul style="list-style-type: none"> ○ A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.
	Gender	No	---
Address Details	Residential Address (for Aadhaar letter delivery and other communications)	Yes	<ul style="list-style-type: none"> ○ Any of the Proof of Address documents. ○ Introducer / Head of Family for people who have no documents.
Parent / Guardian Details	Father's/Mother's/ Guardian's/Husband's / Wife's Name	Conditional	<ul style="list-style-type: none"> ○ No verification of Father/Husband/Guardian in the case of adults. ○ For children below five years of age, Father /Mother / Guardian's name, Aadhaar number and biometric information (any one modality) shall be captured for authentication. ○ For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is optional.
	Father's/Mother's/ Guardian's/Husband's/ Wife's Enrolment ID / Aadhaar number		
Introducer / HoF Details	Introducer / HoF Name	Yes	<ul style="list-style-type: none"> ○ Introducer's / HoF's Name, UID on the form. ○ Introducer / HoF biometrics (any one modality) captured for authentication.
	Introducer's / HoF's UID		
Contact Details	Mobile Number	No	---
	Email Address	No	---

SCHEDULE IV
Format for Update Form
(See Regulation 19 of these Regulations)



Under Section 3 of THE AADHAAR (TARGETTED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES,
BENEFITS AND SERVICES) ACT, 2016 (Aadhaar Act)



AADHAAR DATA UPDATE/CORRECTION FORM

This form is used for sending Update/Correction Requests through Post. Use capital letters only. Fill the complete form irrespective of the field/s for update/correction. Providing mobile number is mandatory for Update/Change in any of the fields.

Field for Update/Correction: Select <input checked="" type="checkbox"/> Name <input type="checkbox"/> Gender <input type="checkbox"/> Date of Birth <input type="checkbox"/> Address <input type="checkbox"/> Mobile <input type="checkbox"/> Email ID		
Aadhaar No. (Please provide accurate 12-digit Aadhaar number here):		
Field	Fill Details in English in this column (Use Capital Letters)	Fill Details in Local Language in this column (Use same local language as in your Aadhaar letter)
Resident's Name		
Gender	Select <input checked="" type="checkbox"/> Male () Female () Transgender ()	
Date of Birth	DD MM YYYY	
Address C/O Details	Select <input checked="" type="checkbox"/> C/o () D/o () S/o () W/o () H/o ()	
Guardian/ Parent/Spouse Name	NAME	NAME
House / Bldg./Apt.		
Street/Road/Lane		
Landmark		
Area/locality/sector		
Village/Town /City		
District		
Post Office		
State		
PIN CODE		
Mobile No (mandatory)		E Mail (optional)
Document Details (Write Names of the documents attached. Refer Annexure I for Valid documents)		
a. POI (for Name Correction)	b. POI (for Name Change)	
c. DOB	d. POA	

Disclosure under section 3(2) of THE AADHAAR (TARGETTED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

I confirm that I have been residing in India for at least 182 days in the preceding 12 months & information (including biometrics) provided by me to the UIDAI is my own and is true, correct and accurate. I am aware that my information including biometrics will be used for generation of Aadhaar and authentication. I understand that my identity information (except core biometric) may be provided to an agency only with my consent during authentication or as per the provisions of the Aadhaar Act. I have a right to access my identity information (except core biometrics) following the procedure laid down by UIDAI.

Applicant's signature/Thumbprint

Addresses For sending Update Request By Post:

UIDAI, Post Box No. 10, Chhindwara, Madhya Pradesh - 480001, India	UIDAI, Post Box No. 99, Banjara Hills, Hyderabad - 500034, India
--	--

SCHEDULE V
Code of Conduct for Service Providers

1. Service Providers shall make best efforts to protect the interests of residents.
2. Service Providers shall maintain high standards of ethics, integrity, dignity and fairness in the conduct of Aadhaar enrolment and update of residents.

3. Service Providers shall fulfil their obligations in a prompt, ethical and professional manner.
4. Service Providers shall at all times exercise due diligence, ensure proper care and exercise independent professional judgment.
5. Service Providers shall not divulge to anybody either orally or in writing, directly or indirectly, any confidential information about the residents which has come to their knowledge, except where such disclosures are required to be made in compliance with the Act or any other law for the time being in force.
6. Service Providers shall not indulge in any unfair practice.
7. Service Providers shall ensure that grievances of residents are redressed in a timely and appropriate manner.
8. Service Providers shall make reasonable efforts to avoid misrepresentation and ensure that the information provided to the residents is not misleading.
9. Service Providers shall abide by the provisions of the Act and the rules, regulations issued by the Government and the Authority, from time to time, as may be applicable.
10. Service Providers shall not make untrue statements or suppress any material fact in any documents, reports, papers or information furnished to the Authority.
11. Service Providers shall ensure that the Authority is promptly informed about any action, legal proceeding, etc., initiated against it in respect of any material breach or non-compliance by it, of any law, rules, regulations and directions of the Authority or of any other regulatory body.
12. Service Providers shall be responsible for the acts or omissions of their agencies and employees in respect of the conduct of their enrolment and update services.
13. Service Providers should have adequately trained staff and arrangements to render fair, prompt and competence services to residents.
14. Service Providers shall develop their own internal code of conduct for governing internal operations and laying down standards of appropriate conduct for their agencies, employees and officers in the carrying out of their duties. Such a code may extend to the maintenance of professional excellence and standards, integrity, confidentiality, objectivity, and avoidance of conflict of interests.
15. Service Providers shall follow maker-checker concept in their activities to ensure accuracy of enrolment and update data.
16. Service Providers shall not indulge in manipulative, fraudulent practices in the process of enrolment and updation.
17. Service Providers shall ensure security and protection of all data (demographic/biometric) collected from residents in accordance with policies and processes as may be specified by the Authority for this purpose.
18. Service Providers shall enforce the decision of Authority regarding suspension/debarment/dis-empowerment of enrolling agencies, operators, supervisors etc, as applicable.
19. Service Providers shall follow the standards for data fields, data verification and biometric fields specified by the Authority.
20. Where required, Service Providers shall use only those devices and IT systems whose specifications have been approved by the Authority.
21. Service Providers shall follow the protocols prescribed by the Authority for record keeping and maintenance.
22. Service Providers shall follow the process and systems specified by the Authority for transmission of the data collected.
23. Service Providers shall follow the confidentiality, privacy and security protocols as may be specified by the Authority.
24. Service Providers shall follow protocols as may be specified by the Authority for spreading and communicating the message, content and intent of the Aadhaar project. Since the Aadhaar logo and brand name are properties of the Authority, the Authority will specify the manner and limits of the use of the Authority logo, brand name, brand design and other communication and awareness materials.

25. Service Providers shall follow protocols, processes and standards specified by the Authority for the implementation of the Aadhaar processes.
26. Service Providers shall submit periodic reports of enrolment to the Authority in the form and manner as may be specified by the Authority.
27. Service Providers shall provide information related to the Aadhaar processes from time to time as requested by the Authority.

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ADVT.-III/4/Exty./238]

अधिसूचना

नई दिल्ली, 12 सितम्बर, 2016

आधार (अधिप्रमाणन) विनियम, 2016

(2016 का सं. 3)

सं. 13012/64/2016/विधि/यूआईडीएआई (2016 का सं.3).—आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा 54 की उप-धारा (2) के उप-खंड (एफ) एवं (डब्ल्यू) तथा उप-धारा (1) के अंतर्गत प्राप्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा निम्नलिखित विनियम बनाता है, नामतः—

अध्याय - 1

प्रारंभिक

1. **संक्षिप्त नाम और प्रारंभ :-**
 - (1) इन विनियमों को आधार (अधिप्रमाणन) विनियम, 2016 कहा जाएगा।
 - (2) ये प्राधिकरण द्वारा सरकारी राजपत्र में जारी की गई अधिसूचना में नियुक्त तिथि को 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;
 - (ख) **“आधार नंबर धारक”** का अभिप्राय कोई व्यक्ति, जिसे अधिनियम के अंतर्गत आधार नंबर जारी किया गया है, से है;
 - (ग) **“अधिप्रमाणन”** का अभिप्राय, वह प्रक्रिया, जिसके द्वारा किसी व्यक्ति की जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना सहित आधार संख्या उसके सत्यापन के लिए ‘केन्द्रीय पहचान आंकड़े निक्षेपागार (सेंट्रल आइडेंटिटीज डाटा रिपोजिटरी)’ के पास जमा की जाती है और ऐसा निक्षेपागार उसकी शुद्धता अथवा कमी को उपलब्ध सूचनाओं के आधार पर सत्यापित करता है, से है;
 - (घ) **“अधिप्रमाणन सुविधा”** का अभिप्राय, वह सुविधा है, जो हां/ना प्रत्युत्तर अथवा ई-केवाईसी डाटा, जो भी प्रयोज्य हो, को उपलब्ध कराते हुए अधिप्रमाणन प्रक्रिया द्वारा आधार नंबर धारक की पहचान सूचना के सत्यापन के लिए उपलब्ध कराई जाती है;
 - (च) **“अधिप्रमाणन अभिलेख”** का अभिप्राय अधिप्रमाणन के समय तथा अनुरोधकर्ता संस्था की पहचान एवं उससे अनुलग्न प्राधिकरण द्वारा उपलब्ध कराये गए प्रत्युत्तर के अभिलेख से है;
 - (छ) **“अधिप्रमाणन सेवा एजेसी”** अथवा **“एएसए”** का अभिप्राय, वह संस्था होगी, जो प्राधिकरण द्वारा उपलब्ध कराई गयी अधिप्रमाणन सुविधा का उपयोग करते हुए अधिप्रमाणन के निष्पादन के लिए अनुरोधकर्ता संस्था को सक्षम बनाने के लिए सुरक्षित नेटवर्क संयोजन एवं सम्बद्ध सेवाएं सुनिश्चित करने के लिए आवश्यक अवसंरचना उपलब्ध करा रही है;
 - (ज) **“अधिप्रमाणन उपयोक्ता एजेसी”** अथवा **“एयूए”** का अभिप्राय वह 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 आंकड़े निक्षेपागार”** अथवा **“सीआईडीआर”** का अभिप्राय एक या एक से अधिक स्थानों पर केन्द्रीकृत डाटा बेस है, जिसमें आधार नंबर धारक को जारी आधार नंबर सहित ऐसे व्यक्तियों की जनसांख्यिकीय तथा बायोमैट्रिक सूचना तथा तत्संबंधी अन्य संबद्ध सूचना शामिल हैं, से है;

- (ठ) "ई-केवाईसी अधिप्रमाणन सुविधा" का अभिप्राय उस अधिप्रमाणन सुविधा से है, जिसमें अनुरोधकर्ता संस्था के माध्यम से आधार नंबर धारक की सहमति द्वारा बायोमैट्रिक सूचना तथा/अथवा ओटीपी एवं आधार नंबर सुरक्षित रूप से जमा की जाती है, जिसका मिलान सीआईडीआर में उपलब्ध डाटा से किया जाता है जिस पर प्राधिकरण अधिप्रमाणन लेन-देन से सम्बद्ध अन्य तकनीकी विवरणों सहित ई-केवाईसी डाटा वाला एक डिजिटल रूप से हस्ताक्षरित प्रत्युत्तर प्रदान करता है;
- (ड) "ई-केवाईसी डाटा" का अभिप्राय किसी आधार नंबर धारक की जनसांख्यिकीय सूचना एवं फोटोग्राफ से है;
- (ढ) "ई-केवाईसी उपयोक्ता एजेंसी" अथवा "केयूए" का अभिप्राय उस अनुरोधकर्ता संस्था से है, जो एयूए होने के अतिरिक्त प्राधिकरण द्वारा प्रावधानित ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग करती है;
- (ण) "लाइसेंस कुंजी" से अभिप्राय, प्राधिकरण द्वारा निर्धारित प्रक्रिया के अनुसार अनुरोधकर्ता संस्था द्वारा जनित कुंजी से है;
- (त) "पीआईडी ब्लॉक" का अभिप्राय है, व्यक्तिगत पहचान डाटा (पर्सनल आईडेंटिटी डाटा) घटक, जिसके अन्तर्गत अधिप्रमाणन के दौरान आधार नंबर धारक से संग्रहीत आवश्यक जनसांख्यिकीय तथा/अथवा बायोमैट्रिक तथा/अथवा ओटीपी सम्मिलित हैं;
- (थ) "अनुरोध करने वाली संस्था" से अभिप्राय किसी एजेंसी या व्यक्ति से जो कि अधिप्रमाणन के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार को किसी व्यक्ति विशेष के आधार नंबर तथा जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना प्रस्तुत करता है, से है;
- (द) "हां/ना अधिप्रमाणन सुविधा" का अभिप्राय एक प्रकार की अधिप्रमाणन सुविधा से है, जिसमें किसी अनुरोधकर्ता संस्था के माध्यम से आधार नंबर धारक की सहमति द्वारा पहचान संबंधी सूचना एवं आधार नंबर को सुरक्षित रूप से जमा किया जाता है और तत्पश्चात सीआईडीआर में उपलब्ध डाटा से उसका मिलान किया जाता है, तथा प्राधिकरण अधिप्रमाणन संव्यवहार से सम्बद्ध अन्य तकनीकी विवरण सहित "हां" या "ना" वाले प्रत्युत्तर पहचान संबंधी सूचना के बिना डिजिटल रूप से हस्ताक्षरित करके देता 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 तथा अन्य विनियमों अथवा सूचना प्रौद्योगिकी अधिनियम, 2000 में परिभाषित किया गया है।

अध्याय - 2

आधार अधिप्रमाणन तंत्र

3. अधिप्रमाणन के प्रकार : -

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

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

4. अधिप्रमाणन के माध्यम :-

- (1) प्राधिकरण के इन विनियमों के अनुसार तथा निर्दिष्टियों के अनुरूप इलेक्ट्रॉनिक रूप में किसी निवेदक संस्था द्वारा प्रेषित किसी अनुरोध को ही अधिप्रमाणन अनुरोध, के रूप में प्राधिकरण द्वारा स्वीकार किया जाएगा।
- (2) अधिप्रमाणन को निम्नलिखित माध्यमों द्वारा सम्पन्न किया जा सकता है :
- (क) **जनसांख्यिकीय अधिप्रमाणन** : आधार नंबर धारक द्वारा प्राप्त आधार नंबर धारक के आधार नंबर एवं जनसांख्यिकीय सूचना का मिलान, सीआईडीआर में आधार नंबर धारक की जनसांख्यिकीय सूचना के साथ किया जाता है।
- (ख) **वन-टाइम पिन आधारित अधिप्रमाणन** : सीमित समय की वैधता वाला एक वन टाइम पिन (ओटीपी) प्राधिकरण में पंजीकृत आधार नंबर धारक के मोबाइल नंबर तथा/अथवा ई-मेल पते पर भेजा जाता है, अथवा अन्य उचित साधनों द्वारा सृजित किया जाता है। आधार नंबर धारक अधिप्रमाणन के दौरान अपने आधार नंबर सहित इस ओटीपी को उपलब्ध करायेगा और इसका मिलान प्राधिकरण द्वारा सृजित ओटीपी से किया जाएगा।
- (ग) **बायोमैट्रिक आधारित अधिप्रमाणन** : आधार नंबर धारक द्वारा जमा किया गया आधार नंबर तथा बायोमैट्रिक सूचना का मिलान, सीआईडीआर में भंडारित कथित आधार नंबर की बायोमैट्रिक सूचना से किया जाता है। यह या तो फिंगरप्रिंट आधारित अथवा पुतली आधारित अधिप्रमाणन अथवा सीआईडीआर में भंडारित बायोमैट्रिक सूचना पर आधारित अन्य बायोमैट्रिक रूपात्मकता हो सकती है।
- (घ) **बहुकारकीय अधिप्रमाणन** : उपर्युक्त दो अथवा दो से अधिक माध्यमों के संयोजन का उपयोग अधिप्रमाणन के लिए किया जा सकता है।
- (3) कोई अनुरोधकर्ता संस्था अपनी वांछनीयताओं के अनुसार किसी विशेष सेवा कार्य व्यापार के लिए उप-विनियम (2) में निर्दिष्ट माध्यमों से वृहत्तर सुरक्षा के लिए बहुकारकीय अधिप्रमाणन सहित अधिप्रमाणन का उपयुक्त माध्यम चुन सकती है। किसी सन्देह के निराकरण के लिए यह स्पष्ट किया जाता है कि ई-केवाईसी अधिप्रमाणन केवल ओटीपी तथा/अथवा बायोमैट्रिक अधिप्रमाणन के उपयोग द्वारा ही सम्पन्न किया जाएगा।

5. आधार नंबर धारक के लिए सूचना :-

- (1) अधिप्रमाणन के समय अनुरोधकर्ता संस्था आधार नंबर धारक को निम्नलिखित विवरणों की सूचना देगी :
- (क) सूचना की प्रकृति, जिसे अधिप्रमाणन पर प्राधिकरण द्वारा सहभाजित किया जाएगा;

- (ख) उपयोग, जिसके लिए अधिप्रमाणन के दौरान प्राप्त सूचना रखी जा सकती है; और;
 (ग) पहचानसंबंधी जानकारी प्रस्तुत करने के विकल्प।

(2) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि ऊपर उप-विनियम (1) में संदर्भित सूचना स्थानीय भाषा में भी आधार नंबर धारक को उपलब्ध करायी जायेगी।

6. आधार नंबर धारक की सहमति:-

- (1) विनियम 5 के अनुरूप सूचना के संचारण के पश्चात अनुरोधकर्ता संस्था अधिप्रमाणन हेतु आधार नंबर धारक की सहमति प्राप्त करेगी।
 (2) अनुरोधकर्ता संस्था ऊपर उप-विनियम (1) में सन्दर्भित सहमति भौतिक रूप में अथवा विषेशतः इलेक्ट्रॉनिक प्रारूप में प्राप्त करेगी और इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट तरीके अथवा प्रारूप में प्राप्त सहमति के लॉग अथवा अभिलेख रखेगी।

7. अनुरोधकर्ता संस्था द्वारा बायोमैट्रिक सूचना ग्रहण करना :-

- (1) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा निर्धारित प्रक्रियाओं तथा विशिष्टियों के अनुसार प्रमाणित बायोमैट्रिक उपकरणों के प्रयोग द्वारा आधार नंबर धारक की बायोमैट्रिक सूचना को ग्रहण करेगी।
 (2) अनुरोधकर्ता संस्था, आवश्यक रूप से प्राधिकरण द्वारा निर्धारित विशिष्टियों के अनुरूप ग्रहण करते समय बायोमैट्रिक डाटा कूटबद्ध एवं सुरक्षित करेगी।
 (3) बायोमैट्रिक सूचना ग्रहण करने में अनुकूलतम परिणाम हेतु अनुरोधकर्ता संस्था इस उद्देश्य के लिए प्राधिकरण द्वारा समय-समय पर निर्दिष्ट प्रक्रियाओं को स्वीकार करेगी।

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

- (1) अधिप्रमाणन के लिए प्रयुक्त समस्त यन्त्र एवं उपकरण इस उद्देश्य हेतु प्राधिकरण द्वारा समय-समय पर वांछनीयता एवं निर्गत विशिष्टियों के अनुसार प्रमाणित किये जाएंगे।
 (2) अधिप्रमाणन के उद्देश्य हेतु अनुरोधकर्ता संस्था द्वारा प्रयोग में लाये जाने वाले क्लाइंट एप्लीकेशन्स अर्थात् सॉफ्टवेयर इस उद्देश्य हेतु समय-समय पर प्राधिकरण द्वारा निर्दिष्ट मानक एपीआई तथा विशिष्टियों के अनुरूप होंगे।

9. अधिप्रमाणन अनुरोध भेजने की प्रक्रिया :-

- (1) अनुरोधकर्ता संस्था द्वारा प्रावधानित आधार नम्बर अथवा कोई अन्य अभिज्ञापक (आइडेंटिफायर) जो आधार नंबर के साथ संयोजित की गयी है तथा आधार नंबर धारक से आवश्यक जनसांख्यिकीय तथा/अथवा बायोमैट्रिक सूचना तथा/अथवा ओटीपी संग्रहीत करने के पश्चात प्राधिकरण द्वारा निर्दिष्ट विशिष्टियों के अनुसार क्लाइंट एप्लीकेशन तुरन्त किसी पारेषण से पूर्व इन इनपुट पैरामीटरों को पीआईडी ब्लॉक में पैकेज और कूटबद्ध करेगा, और सुरक्षित प्रोटोकॉल, जो इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट किया गया है, के प्रयोग द्वारा अनुरोधकर्ता संस्था के सर्वर के पास भेज देगा।
 (2) विधिमान्यकरण के उपरान्त अनुरोधकर्ता संस्था का सर्वर प्राधिकरण द्वारा निर्दिष्ट विशिष्टियों के अनुसार अधिप्रमाणन सेवा एजेंसी के सर्वर के माध्यम से अधिप्रमाणन अनुरोध को सीआईडीआर के पास भेज देगा। अधिप्रमाणन अनुरोधकर्ता संस्था तथा/अथवा अधिप्रमाणन सेवा एजेंसी द्वारा उनके पारस्परिक समझौते के अनुसार डिजिटल रूप से हस्ताक्षरित करेगा।
 (3) अधिप्रमाणन अनुरोध के माध्यम के आधार पर सीआईडीआर स्वयं भंडारित डाटा के विरुद्ध इनपुट पैरामीटरों का विधिमान्यकरण करेगा और डिजिटल रूप से हस्ताक्षरित 'हां' या 'ना' अधिप्रमाणन प्रत्युत्तर, अथवा कूटबद्ध ई-केवाईसी डाटा सहित डिजिटल रूप से हस्ताक्षरित ई-केवाईसी, जैसी स्थिति हो, को अधिप्रमाणन संव्यवहार से सम्बद्ध अन्य तकनीकी विवरणों के साथ वापस करेगा।
 (4) अधिप्रमाणन के सभी माध्यमों में, आधार नंबर अनिवार्य है और इसे उपर्युक्त उप-विनियम (1) में निर्दिष्ट इनपुट पैरामीटरों के साथ इस प्रकार जमा किया जाता है कि अधिप्रमाणन सदैव 1 : 1 के मिलान के साथ शेष रहे।
 (5) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि प्राधिकरण द्वारा निर्दिष्ट विशिष्टियों एवं प्रक्रियाओं के अनुसार अधिप्रमाणन उपकरण द्वारा ग्रहण (कैचर) करते समय पीआईडी ब्लॉक का एन्क्रिप्शन होता रहे।

10. आधार नंबर धारक को अधिप्रमाणन की अधिसूचना :-

आधार नंबर धारक को किसी बायोमैट्रिक तथा/अथवा ओटीपी आधारित अधिप्रमाणन से अधिप्रमाणन के समय, प्राधिकरण द्वारा निर्धारित पंजीकृत ई-मेल तथा/अथवा आधार नंबर धारक के मोबाइल नंबर के माध्यम से अधिसूचित किया जा सकता है।

11. बायोमैट्रिक लॉकिंग:-

- (1) प्राधिकरण बायोमैट्रिक अधिप्रमाणन हेतु आवश्यकतानुसार आधार नंबर धारक को उसके बायोमैट्रिकस को स्थायी तौर पर लॉक करने तथा अस्थायी तौर पर अनलॉक करने की स्वतन्त्रता देगा।

- (2) ऐसे लॉक किए गए किसी बायोमैट्रिक अभिलेख के विरुद्ध समस्त बायोमैट्रिक अधिप्रमाणन एक उचित प्रत्युत्तर कोड सहित "नहीं" विकल्प के साथ असफल होंगे।
- (3) आधार नंबर धारक को अधिप्रमाणन हेतु अपने बायोमैट्रिकस को अस्थायी तौर पर अनलॉक करने की अनुमति दी जाएगी और ऐसा अस्थायी अनलॉकिंग प्राधिकरण द्वारा निर्दिष्ट समयावधि के पश्चात अथवा अधिप्रमाणन संव्यवहार की पूर्णता तक, जो भी पहले हो, जारी नहीं रहेगा।
- (4) प्राधिकरण आधार नंबर धारक के लिए सुरक्षित तरीके से किसी भी समय ऐसे स्थायी लॉकिंग को समाप्त करने का प्रावधान करेगा।

अध्याय - 3

अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की नियुक्ति

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

- (1) प्राधिकरण द्वारा प्रावधानित अधिप्रमाणन सुविधा के उपयोग के लिए अनुरोधकर्ता संस्था बनने वाली एजेंसियां इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट विधानों के अनुसार अनुरोधकर्ता संस्था के रूप में नियुक्ति के लिए आवेदन करेंगी। केवल अनुसूची 'क' के मानदंडों को पूरा करने वाली अनुरोधकर्ता संस्थाएं ही आवेदन करने की पात्र होंगी। प्राधिकरण आदेश द्वारा समय-समय पर अनुसूची 'क' में संशोधन कर कर सकता है ताकि पात्रता मानदंड को संशोधित किया जा सके।
- (2) अधिप्रमाणन सेवा एजेंसियों के रूप में नियुक्ति चाहने वाली संस्थाएं इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट विधानों के अनुरूप नियुक्ति के लिए आवेदन करेंगी। केवल अनुसूची 'ख' के मानदंडों को पूरा करने वाली संस्थाएं ही आवेदन करने की पात्र होंगी। प्राधिकरण आदेश द्वारा समय-समय पर अनुसूची 'ख' में संशोधन कर सकता है ताकि पात्रता मानदंड को संशोधित किया जा सके।
- (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 निर्धारित समय के अन्दर निर्दिष्ट प्राधिकरण की सन्तुष्टि के अनुरूप ऐसी सूचना तथा स्पष्टीकरण का उल्लेख करेगा।
- (5) आवेदन पर विचार करते समय, आवेदक द्वारा प्रस्तुत की गयी सूचना और उसकी पात्रता को प्राधिकरण दस्तावेजों के प्रत्यक्ष सत्यापन, अवसंरचना एवं तकनीकी संबलका सत्यापन कर सकता है, जिन्हें आवेदक के पास होना आवश्यक 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 अनुमोदित कर सकता है; तथा
 - (ख) संस्था अथवा एजेंसी के साथ प्राधिकरण की अधिप्रमाणन सुविधा के अनुरोधकर्ता संस्था द्वारा उपयोग के लिए नियमों एवं शर्तों अथवा एएसए द्वारा सेवाओं के प्रावधान में दायित्वों के गैर-निष्पादन की स्थिति में क्षतियों तथा हतोत्साहन के शर्तोंसमेत करते हुए उचित करार कर सकती है।
- (7) प्राधिकरण, समय-समय पर आवेदन शुल्क, वार्षिक सदस्यता शुल्क तथा वैयक्तिक अधिप्रमाणन संव्यवहार के लिए शुल्क सहित संस्थाओं द्वारा उनकी नियुक्ति के दौरान उनके द्वारा देय शुल्क एवं प्रभार निर्धारित कर सकती है।

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

- (1) यदि, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी, जैसी स्थिति हो, की नियुक्ति के लिए आवेदन प्राधिकरण द्वारा निर्दिष्ट वांछनीयताओं को सन्तुष्ट नहीं करती है तो प्राधिकरण आवेदन निरस्त कर सकता है।
- (2) आवेदन निरस्त 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, तो वह इस निर्णय पर पुनर्विचार करने के लिए इस सूचना की प्राप्ति की तिथि के तीस दिनों के अंदर 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 संस्था की भूमिका तथा उत्तरदायित्व :-

- (1) अनुरोधकर्ता संस्था को निम्नलिखित कार्य एवं उत्तरदायित्वों का निर्वहन करना होगा :
 - (क) स्वयं के तंत्र, प्रक्रियाओं, अवसंरचना, तकनीक, सुरक्षा आदि सहित अधिप्रमाणन से संबंधित 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) 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;

- (घ) केवल उन्हीं यन्त्रों, उपकरण, अथवा सॉफ्टवेयर का उपयोग करना जो आवश्यक रूप से प्राधिकरण द्वारा पंजीकृत अथवा अनुमोदित अथवा प्रमाणित या प्राधिकरण द्वारा निर्दिष्ट हैं और इस उद्देश्य हेतु प्राधिकरण द्वारा निर्धारित मानकों और विशिष्टियों के अनुरूप हैं;
- (च) इस संबंध में प्राधिकरण द्वारा समय-समय पर निर्गत एवं सूचित नियमों एवं शर्तों, मानकों, निर्देशों तथा विशिष्टियों के लिए अपने यंत्रों तथा उपकरणों के प्रचालन की आवर्ती आधार पर निगरानी करना;
- (छ) 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 के विषय में प्राधिकरण को निरन्तर सूचित करना, जिसके साथ उसका समझौता हुआ है;
- (झ) सुनिश्चित करना कि उसके प्रचालन तथा तंत्र प्राधिकरण के मानकों तथा विशिष्टियों 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 लेखापरीक्षा रिपोर्ट अनुरोध किए जाने पर प्राधिकरण के साथ सहभाजित करनी होगी;
- (ट) आधार नंबर धारकों को अधिप्रमाणन सेवाओं के सुचारु प्रावधान सुनिश्चित करने हेतु अपवाद संचलन क्रियाविधि तथा बैंक-अप पहचान अधिप्रमाणन क्रियाविधि क्रियान्वित 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;
- (ड) अनुरोधकर्ता संस्था द्वारा अपने आधार अधिप्रमाणन तंत्र को अपने स्थानीय अधिप्रमाणन तंत्र से समेकन की इच्छा करने की स्थिति में, ऐसे समेकन समय-समय पर प्राधिकरण द्वारा निर्गत मानकों तथा विशिष्टियों के अनुरूप सम्पादित करने होंगे;
- (ढ) वह 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 धोखाधड़ी संस्था धोखाधड़ी की शिकार है अथवा उसे आधार प्रमाणीकरण से संबंधित धोखाधड़ी जांच प्रणाली के माध्यम से किसी धोखाधड़ी की जानकारी प्राप्त होती है, वह उस धोखाधड़ी से संबंधित समस्त समस्त जानकारी प्राधिकरण को सहभाजित करेगी।
- (ण) वह अधिप्रमाणन प्रचालनों तथा परिणामों के लिए उत्तरदायी होगी, भले ही उसने 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 विशिष्टियों के अनुरूप हैं और उनकी अनुमोदित स्वतन्त्र लेखापरीक्षा एजेंसियोंद्वारा नियमित लेखापरीक्षा करवाई गयी है;
- ऐसे ग्राहकों के साथ, अपने ग्राहकों को अधिप्रमाणन सेवाएं उपलब्ध कराने के लिए अधिप्रमाणन प्रभारों हेतु सहमत हो सकती है और प्राधिकरण कुछ समय के लिए इस संबंध में कुछ नहीं कहेगा; किन्तु भविष्य में इस संबंध में एक भिन्न क्रियाविधि निर्धारित करने का प्राधिकरण का अधिकार सुरक्षित माना जायेगा;
- (त) वह प्रत्येक समय प्राधिकरण द्वारा प्रावधानित अधिप्रमाणन सुविधाओं के उपयोग के उद्देश्यों के लिए प्राधिकरण द्वारा निर्गत किसी अनुबन्धित शर्तों एवं समस्त नियमों, विनियमों, नीतियों, नियमावलियों, प्रक्रियाओं, विशिष्टियों, मानकों तथा निर्देशों के अनुरूप होगी।

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 द्वारा प्रावधानित हां/ना अधिप्रमाणन सुविधा का उपयोग कर सकती है।
- (2) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा प्रावधानित पोर्टल के माध्यम से किसी अन्य एजेंसी अथवा संस्था को प्रत्येक ऐसी संस्था के लिए एक अलग से लाइसेंस कुंजी के सृजन तथा सहभाजिता द्वारा कथित संस्था को हां/ना अधिप्रमाणन निष्पादन के लिए अनुज्ञा दे सकती है। सन्देह के निराकरण के लिए यह स्पष्ट किया जाता है कि लाइसेंस कुंजी की ऐसी सहभाजिता केवल हां/ना अधिप्रमाणन के निष्पादन हेतु ही अनुज्ञेय 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 सहभाजित नहीं करेगी; तथा
- (ख) आधार नंबर धारक की व्यक्तिगत सूचना, डाटा सुरक्षा एवं अनुरोधकर्ता संस्था के लिए प्रयोज्य अन्य प्रासंगिक उत्तरदायित्वों से सम्बद्ध समस्त दायित्वों का अनुपालन करेगी।

- (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, दिशा-निर्देशों, विशिष्टियों तथा प्रोटोकॉल के अनुरूप हैं।
- (5) अनुरोधकर्ता संस्था, लाइसेंस कुंजी सहभाजित की गयी संस्था अथवा एजेंसी सहित प्राधिकरण के विनियमों, प्रक्रियाओं, मानकों, दिशा-निर्देशों तथा प्रोटोकॉल की गैर-अनुरूपता के लिए संयुक्त रूप से तथा पृथक-पृथक उत्तरदायी होगी।

16. ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग :-

- (1) केयूए अपने स्वयं के उद्देश्यों के लिए आधार नंबर धारक का ई-केवाईसी डाटा प्राप्त करने के लिए प्राधिकरण द्वारा प्रावधानित ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग कर सकता है।
- (2) केयूए अन्य एजेंसियों के माध्यम से ई-केवाईसी अधिप्रमाणन निष्पादित कर सकता है, और निर्दिष्ट उद्देश्य के लिए आधार नंबर धारक की सहमति प्राप्त करने के उपरांत इस उद्देश्य के लिए उस एजेंसी के साथ ई-केवाईसी डाटा सहभाजित कर सकता है।
- (3) केयूए आधार नंबर धारक की सहमति से कूटबद्ध प्रारूप में ई-केवाईसी अधिप्रमाणन से प्राप्त किसी आधार नंबर धारक का ई-केवाईसी डाटा भंडारित कर सकता है और तत्पश्चात किसी निर्दिष्ट उद्देश्य के लिए इस ई-केवाईसी डाटा को कथित उद्देश्य के लिए प्रत्येक बार सहभाजित की अलग से सहमति प्राप्त करने के उपरान्त किसी अन्य एजेंसी के साथ सहभाजित कर सकता है।
- (4) वह एजेंसी जिसके साथ केयूए ने आधार नंबर धारक का ई-केवाईसी डाटा सहभाजित किया है, वह एजेंसी केवल आधार नंबर धारक द्वारा कथित उद्देश्य की पूर्ति के लिए सहभाजिता के लिए दी गयी विशेष सहमति के समापन के पश्चात, किसी अन्य एजेंसी से ई-केवाईसी डाटा सहभाजित नहीं करेगी।
- (5) आधार नंबर धारक किसी भी समय अपना ई-केवाईसी डाटा भंडारण करने अथवा इसे किसी तीसरे पक्ष के साथ सहभाजित करने के लिए दी गयी सहमति को वापस ले सकता है, और प्रतिसंहरण की इस स्थिति में केयूए ई-केवाईसी डाटा को डिलीट (समाप्त) करेगा और भावी सहभाजिता अवरुद्ध कर देगा।
- (6) उप-विनियम (4) में उल्लिखित भावी सहभाजिता की निषिद्धि के अतिरिक्त, आधार नंबर धारक की व्यक्तिगत सूचना से सम्बन्धित अन्य समस्त दायित्व, अनुरोधकर्ता संस्थाओं के लिए प्रयोज्य डाटा सुरक्षा एवं अन्य प्रासंगिक उत्तरदायित्व भी उस एजेंसी अथवा संस्था के लिए भी प्रयोज्य होंगे, जिनके साथ विनियम 16 के अनुरूप ई-केवाईसी डाटा सहभाजित किया जा चुका है।
- (7) अनुरोध करने पर केयूए आधार नंबर धारक को ई-केवाईसी डाटा की डिजिटल रूप से हस्ताक्षरित इलेक्ट्रॉनिक प्रति उपलब्ध करायेगा, और आधार नंबर धारक कथित प्रति को किसी भी एजेंसी के साथ सहभाजित कर सकता है।
- बशर्ते कि वह एजेंसी जो आधार नंबर धारक से ई-केवाईसी डाटा के लिए अनुरोध कर रही है, वह ऐसा करने के उद्देश्य के विषय में सूचित करेगी और आधार नंबर धारक की सहमति लेगी।
- बशर्ते कि वह एजेंसी, जिसके साथ आधार नंबर धारक ने ई-केवाईसी डाटा सहभाजित किया है, आधार नंबर धारक द्वारा कथित उद्देश्य की पूर्ति के लिए सहभाजिता के लिए दी गयी विशेष सहमति के समापन के पश्चात किसी अन्य एजेंसी से ई-केवाईसी डाटा सहभाजित नहीं करेगी।
- (8) केयूए ऐसे सभी संव्यवहारों का प्राधिकरण द्वारा निर्दिष्ट समयावधि के लिए एक लेखापरीक्षणिय संलेख अनुरक्षित करेगा, जहां डाटा अन्य एजेंसियों के साथ सहभाजित किया गया है।

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

- (1) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि :
- (क) आधार नंबर धारक से संग्रहीत मुख्य बायोमैट्रिक सूचना को किसी भी उद्देश्य के लिए भंडारित, सहभाजित अथवा प्रकाशित नहीं किया गया है, और उसके पास मुख्य बायोमैट्रिक सूचना की कोई प्रति शेष नहीं है;
- (ख) संग्रहीत मुख्य बायोमैट्रिक 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 भंडारित 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 निर्दिष्ट उद्देश्य के लिए प्रयुक्त की गयी है, और जिस कार्ड नंबर धारक से यह सूचना सम्बद्ध है, उसकी पूर्व सहमति लिए बिना पुनः प्रकट नहीं की जाएगी;
- (च) अधिप्रमाणन के दौरान, आधार नंबर धारक की पहचान सूचना तथा अधिप्रमाणन प्रक्रिया के दौरान सृजित कोई अन्य सूचना जैसे अभिगम, उपयोग एवं प्रकटन के विरुद्ध संरक्षित रखी गयी है जिसकी अनुमति अधिनियम तथा इसके विनियम के अधीन नहीं है।

- (छ) अधिप्रमाणन अनुरोध के डिजिटल रूप में हस्ताक्षर के लिए प्रयुक्त प्राइवेट (निजी) कुंजी तथा लाइसेंस कुंजी सुरक्षित रखे गये हैं और अभिगम नियन्त्रित हैं; तथा
- (ज) अपने तंत्र में आधार-आधारित पहचान सूचना से सम्बद्ध डाटा भंडारण तथा डाटा संरक्षण से सम्बन्धित समस्त प्रासंगिक कानून एवं विनियम, जो उनके एजेंट (यदि लागू हो) के तथा अधिप्रमाणन उपकरण के विषय में हैं, अनुपालित हैं।

18. अनुरोधकर्ता संस्था द्वारा लॉग का रख-रखाव :-

- (1) अनुरोधकर्ता संस्था को अपने द्वारा अधिप्रमाणित किए गए कार्य के संबंध में नीचे सूचीबद्ध विवरण सहित कार्य लॉग का रख-रखाव करना होगा :-
- (क) आधार नंबर , जिसके अंतर्गत अधिप्रमाणन अपेक्षित है;
- (ख) प्रस्तुत अधिप्रमाणन अनुरोध के लिए विशिष्ट मापदंड;
- (ग) प्राप्त अधिप्रमाणन प्रतिक्रिया के लिए विशिष्ट मापदंड;
- (घ) अधिप्रमाणन के समय आधार नंबर धारक को किया गया सूचना प्रकटीकरण अभिलेख; तथा
- (च) अधिप्रमाणन के लिए आधार नंबर धारक की सहमति का अभिलेख
- परन्तु, किसी भी स्थिति में पीआईडी सूचना का रख-रखाव नहीं किया जाएगा।
- (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 तथा उक्त अवधि की समाप्ति के पश्चात किसी न्यायालय अथवा किसी बकाया विवाद के लिए अपेक्षित अभिलेख के अलावा अन्य अभिलेख हटाया जा सकेगा।
- (4) अनुरोधकर्ता संस्था द्वारा संबंधित आधार नंबर धारक से प्राप्त अनुरोध अथवा शिकायत सुनवाई तथा विवादों के समाधान अथवा लेखापरीक्षा उद्देश्यों से प्राधिकरण के अलावा किसी भी अन्य व्यक्ति के साथ अधिप्रमाणन लॉग का सहभाजन नहीं किया जाएगा। इस उप विनियम में उल्लिखित उद्देश्य के अलावा किसी अन्य उद्देश्य से अधिप्रमाणन लॉग का प्रयोग नहीं किया जाना है।
- (5) अनुरोधकर्ता संस्था द्वारा लॉग के भंडारण के संबंध में सूचना प्रौद्योगिकी अधिनियम, 2000 तथा साक्ष्य अधिनियम, 1872 सहित, परन्तु 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 ट्रांसमिट करने के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार (सीआईडीआर) के साथ प्राधिकरण द्वारा इस उद्देश्य हेतु विनिर्दिष्ट विधि के अनुसार सुरक्षित क्वेक्टिविटी उपलब्ध करवाना;
- (ख) सीआईडीआर को प्रेषित करने से पूर्व अधिप्रमाणन डाटा पैकेट से संबंधित बुनियादी अनुपालन एवं पूर्णतः जांच से संबंधित अनुपालन करना;
- (ग) सीआईडीआर से प्रतिक्रिया प्राप्त होने पर अनुरोधकर्ता संस्था को अनुरोध पर किए गए कार्य के परिणाम संप्रेषित करना;
- (घ) केवल प्राधिकरण द्वारा अनुमोदित अनुरोधकर्ता संस्थाओं के साथ कार्य करना तथा स्वयं द्वारा सेवित 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 स्वयं द्वारा नियुक्त व्यक्ति अधिप्रमाणन कार्य तथा आवश्यक सिस्टम, अवसंरचना, प्रक्रियाओं इत्यादि के रख-रखाव के कार्यों के लिए अपेक्षित योग्यता प्राप्त हैं;
- (ज) प्रचालनों की लेखापरीक्षा किसी मान्यता प्राप्त निकाय द्वारा प्रमाणित सूचना प्रणाली लेखापरीक्षकों द्वारा वार्षिक आधार पर किया जाए तथा इस संबंध में समय-समय पर प्राधिकरण द्वारा जारी नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों, अथवा विशिष्टताओं के अनुपालन की पुष्टि की प्रमाणित लेखापरीक्षा रिपोर्ट प्राधिकरण को उपलब्ध करवाना सुनिश्चित करना;
- (झ) इस उद्देश्य से सिस्टम, प्रक्रियाएं, उपकरण, सॉफ्टवेयर एवं बायोमैट्रिक अवसंरचना, सुरक्षा तथा अन्य संबंधित घटकों सहित सभी अवसंरचनाएं एवं प्रचालन प्राधिकरण द्वारा विनिर्दिष्ट मानकों एवं विशिष्टताओं के अनुरूप होना सुनिश्चित करना;
- (ट) नेटवर्क तथा अन्य सूचना प्रौद्योगिकी अवसंरचना, प्रक्रियाओं, कार्यविधियों इत्यादि के संबंध में प्राधिकरण द्वारा जारी निदेशों, विशिष्टताओं इत्यादि का पूर्णतः अनुसरण करना;
- (ठ) सभी संबंधित विधानों तथा विनियमों, विशेष रूप से डाटा सुरक्षा तथा डाटा प्रबंधन, का अनुपालन;
- (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) प्राधिकरण के प्रति अधिप्रमाणन से संबंधित सभी प्रचालनों, अधिप्रमाणन सेवा एजेंसी के उप-अनुबंध के अंतर्गत अपने प्रचालन अन्य संस्थाओं को दिए जाने के मामले में भी, के लिए 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 जांच एजेंसी को अपने परिसर, अभिलेख, सिस्टम, कर्मियों, अवसंरचना, अन्य किसी संबंधित संसाधन अथवा सूचना तथा अन्य अधिप्रमाणन प्रचालनों से संबंधित अन्य घटक तक पहुँच 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 से, प्राधिकरण का इस मामले में सामयिक तौर पर कोई हस्तक्षेप नहीं होगा, तथापि, ऐसे मामले में प्राधिकरण के पास भविष्य में किसी भिन्न तंत्र व्यवस्था के निर्धारण करने का अधिकार सुरक्षित होगा;
- (थ) प्राधिकरण द्वारा किसी भी समय पर जारी प्रत्येक संविदागत शर्तों तथा सभी नियमों, विनियमों, नीतियों, मैनुअलों, प्रक्रियाओं, विशिष्टताओं, मानकों तथा निदेशों का पूर्णतः पालन किया जाएगा।

20. अधिप्रमाणन सेवा एजेंसियों द्वारा लॉग का रखरखाव :-

- (1) अधिप्रमाणन सेवा एजेंसी द्वारा स्वयं निष्पादित अधिप्रमाणन कार्यों के लॉग का रख-रखाव किया जाएगा, जिसके कार्य में नीचे उल्लिखित विवरण होगा नामतः-
- (क) अनुरोधकर्ता संस्था की पहचान;
- (ख) प्रस्तुत अधिप्रमाणन अनुरोध के मापदंड; तथा
- (ग) प्राप्त अधिप्रमाणन प्रक्रिया के मापदंड:
- बशर्ते यह कि जहां लागू होगा, वहां आधार नंबर, पीआईडी सूचना, उपकरण पहचान से संबंधित डाटा तथा ई-केवाईसी प्रतिक्रिया डाटा, का प्रतिधारण नहीं किया जाएगा।
- (2) अधिप्रमाणन सेवा एजेंसी द्वारा अधिप्रमाणन कार्य के लॉग का रख-रखाव 2 (2) वर्ष की अवधि के लिए किया जाएगा तथा इस दौरान प्राधिकरण तथा/अथवा अनुरोधकर्ता संस्था द्वारा शिकायत निवारण, विवाद निपटान तथा लेखापरीक्षा कार्यों से इन विनियमों में विनिर्दिष्ट प्रक्रिया के अनुसार ऐसे अभिलेख के प्रयोग की मांग की जा सकेगी। इस उप विनियम में उल्लिखित उद्देश्य के अलावा किसी अन्य उद्देश्य से 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 संचालन करने वाले विनियमों के अनुसार अपेक्षित वर्षों की नंबर के लिए, इनमें से जो भी बाद में हो, पुरालेख के तौर पर रखा जाएगा तथा उक्त अवधि की समाप्ति के पश्चात किसी न्यायालय अथवा किसी बकाया विवाद के लिए अपेक्षित लॉग के अलावा अन्य अभिलेख हटाया जा सकेगा।
- (4) अधिप्रमाणन सेवा एजेंसी द्वारा लॉग के भंडारण 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।

21. अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की लेखापरीक्षा :-

- (1) प्राधिकरण स्वयं अथवा उसके द्वारा नियुक्त अपनी लेखापरीक्षा एजेंसियों के माध्यम से अधिनियम, नियमावली, विनियमों, नीतियों, प्रक्रियाओं, प्राधिकरण द्वारा जारी दिशानिर्देशों के अनुपालन को सुनिश्चित करने के लिए अनुरोधकर्ता संस्थाओं, ऐसी एजेंसियों अथवा संस्थाओं सहित, जिनके साथ उन्होंने लाइसेंस कुंजी का सहभाजन किया है अथवा ऐसी संस्थाओं, जिनकी ओर से वे अधिप्रमाणन कार्य का निष्पादन कर रहे हैं तथा अधिप्रमाणन सेवा एजेंसियों का उनके प्रचालनों, अवसंरचना, सिस्टम एवं प्रक्रियाओं के संबंध में लेखापरीक्षा करसकता है।
- (2) प्राधिकरण स्वयं अथवा प्राधिकरण द्वारा नियुक्त लेखापरीक्षा के माध्यम से उप-विनियम (1) में संदर्भित संस्थाओं के प्रचालनों तथा सिस्टम का लेखापरीक्षा कर सकती है। ऐसे 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/अथवा नियुक्त एजेंसी को अपनी प्रक्रिया, अभिलेखों तथा प्राधिकरण से प्राप्त सेवाओं से संबंधित सूचना के लिए पूर्ण पहुंच 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।

22. डाटा सुरक्षा :-

- (1) अनुरोधकर्ता संस्था तथा अधिप्रमाणन सेवा एजेंसी द्वारा आधार अधिप्रमाणन अनुरोध कार्यों एवं केन्द्रीय पहचान आंकड़े निक्षेपागार (सीआईडीआर) को सम्प्रेषण के लिए भारत में स्थित डाटा केन्द्रों से अपने सर्वरों का उपयोग करना होगा।
- (2) अधिप्रमाणन सेवा एजेंसी प्राधिकरण के डाटा केन्द्र 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 संस्थाओं अधिप्रमाणन सेवा पहुंच के माध्यम से केवल प्राधिकरण से उपलब्ध करवाई गई अधिप्रमाणन सुविधा पर पहुंच के लिए उचित लाइसेंस कुंजी का प्रयोग, केवल प्राधिकरण द्वारा इस उद्देश्य से निर्दिष्ट सुरक्षित नेटवर्क से करेगी।
- (4) अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियाँ प्राधिकरण द्वारा समय-समय पर जारी सभी विनियमों, सूचना सुरक्षा नीतियों, प्रक्रियाओं, मानकों, विनिर्देशों तथा दिशा-निर्देशों का अनुपालन करेगी।

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 छोड़नेकी इच्छुक, इन विनियमों के अंतर्गत नियुक्त की गई, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी ऐसे सरेंडर 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 की सेवाओं को समाप्त करने के लिए निम्नलिखित सहित किसी भी आवश्यक मामले के प्रति प्राधिकरण को संतुष्ट करने की अपेक्षा की जा सकती है :-
 - (क) अधिप्रमाणन अभिलेख के रख-रखाव 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 रख-रखाव 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 करने 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 नंबर 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 प्रावधानों, इनके विनियमों तथा अन्य विनियमों, नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों तथा विशिष्टताओं 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 विशिष्टताओं का अनुपालन 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(2) 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, विशिष्टताओं 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 निर्दिष्ट के अलावा किन्हीं अन्य उद्देश्यों से 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 पृष्ठताछ 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 प्रावधानों, 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 सुनवाई का अवसर प्रदान किया जाएगा ।

- (2) उप-विनियम (1) में संदर्भित ऐसी कार्रवाई किसी संस्था अथवा एजेंसी, जिसके साथ किसी अधिप्रमाणन सेवा एजेंसी द्वारा हॉ/नहीं अधिप्रमाणन की लाइसेंस कुंजी का सहभाजन किया गया हो तथा किसी ऐसी संस्था जिसके साथ ई-केवाईसी प्रयोक्ता एजेंसी द्वारा ई-केवाईसी डाटा का सहभाजन किया गया हो, के विरुद्ध भी की जा सकेगी ।
- (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 सूचीबद्ध घटकों सहित समापन के आवश्यक घटकों के प्रति प्राधिकरण को संतुष्ट करना होगा ।

अध्याय-4

अधिप्रमाणन कार्य क्रिया डाटा तथा अधिप्रमाणन अभिलेख

26. अधिप्रमाणन कार्यक्रियाडाटा का भंडारण एवं रख-रखाव :-

- (1) प्राधिकरण द्वारा निम्नलिखित सूचना से युक्त अधिप्रमाणन कार्य क्रिया डाटा का भंडारण एवं रख-रखाव किया जा सकेगा :-
 - (क) पीआईडी ब्लॉक सहित प्राप्त अधिप्रमाणन अनुरोध डाटा
 - (ख) प्रेषित अधिप्रमाणन प्रतिक्रिया डाटा
 - (ग) कार्य संचलन से सम्बद्ध मेटा डाटा
 - (घ) आवश्यकतानुसार अधिप्रमाणन सर्वर साईड विन्यास
 बशर्ते कि प्राधिकरण द्वारा किसी भी मामले में अधिप्रमाणन के उद्देश्य का भंडारण नहीं किया जाएगा ।

27. भंडारण की अवधि :-

- (1) प्राधिकरण द्वारा अधिप्रमाणन कार्य डाटा का भंडारण 6 माह की अवधि के लिए किया जाएगा तथा इसे 5 वर्ष की अवधि के लिए पुरालेख के तौर पर रखा जाएगा ।
- (2) उप - विनियम (1) में उल्लिखित 5 वर्ष की निर्दिष्ट अवधि की समाप्ति के पश्चात किसी न्यायालय अथवा किसी बकाया विवाद के लिए अपेक्षित अभिलेख के लिए रख-रखाव के अलावा अन्य अभिलेख हटाया जा सकेगा ।

28. आधार नंबर धारक द्वारा एक्सेस :-

(1)	विहित शर्तों तथा प्राधिकरण द्वारा निर्धारित शुल्क का भुगतान करने पर आधार नंबर धारक को अभिलेखों का पुरालेख किए जाने से पूर्व अनुरक्षण किए जाने की अवधि के दौरान, 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, आधार नंबर धारकों को अपने डिजिटली हस्ताक्षरित सत्यापित अभिलेख की प्राप्ति के लिए प्राधिकरण द्वारा ऑनलाईन पोर्टल अथवा मोबाइल एप्लीकेशन अथवा निर्दिष्ट संपर्क केन्द्र की सुविधा उपलब्ध करवाई जा सकती है ।
(3)	प्राधिकरण द्वारा बायोमैट्रिक अथवा ओटीपी के माध्यम से निर्धारित शुल्क के भुगतान तथा प्रक्रियाओं के अनुसार आधार नंबर धारकों को डिजिटली हस्ताक्षरित ई-केवाईसी डाटा उपलब्ध करवाया जा सकता है ।
(4)	सत्यापित अभिलेख तथा ई-केवाईसी डाटा का सहभाजन किसी व्यक्ति अथवा संस्था के साथ नहीं किया जा सकेगा :-
	(क) आधार नंबर धारक जिनसे अभिलेख या ई-केवाईसी डाटा विनिर्दिष्ट अधिप्रमाणन प्रक्रिया के अनुसार संबंधित है, के अलावा किसी अन्य के साथ । आधार नंबर धारक द्वारा अपने डिजिटली हस्ताक्षरित सत्यापित अभिलेख तथा ई-केवाईसी डाटा का सहभाजन अन्य संस्थाओं के साथ किया जा सकेगा, जो ऐसे सहभाजन आधार नंबर धारक से प्रत्येक बार अनुमति प्राप्त किए बिना नहीं करेंगे ।
	(ख) अधिनियम में किए गए उल्लेख के अलावा ।

अध्याय - 5

विविध

29. व्यावृत्ति :-

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 ऐसे प्राधिकरण के किसी अधिकारी अथवा अधिनियम के तहत प्राधिकरण की स्थापना पूर्व द्वारा जारी सभी कार्यपद्धति, आदेश, प्रक्रियाएं, मानक तथा नीतियां अथवा हस्ताक्षर किए सभी समझौता ज्ञापन, करार अथवा सविदाएं उस सीमा तक लागू रहेंगी, जबतक कि वे अधिनियम के उपबंधों तथा इनके तहत तैयार किए गए अधिनियम अथवा विनियम के तहत असंगत सिद्ध न हो जाएं।

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 दिशानिर्देश जारी करने की शक्ति होगी, जिनका प्रभाव विनियम के समान होगा।

अनुसूची- क

अनुरोधकर्ता संस्थाओं की नियुक्ति के लिए पात्रता मापदंड

विनियम 10(1)देखें

1. अनुरोधकर्ता संस्था के रूप में प्राधिकरण द्वारा उपलब्ध करवाई जाने वाली अधिप्रमाणन सुविधा के प्रयोग की अपेक्षा रखने वाली संस्थाओं के लिए अधिप्रमाणन उपयोक्ता एजेंसी (एयूए) तथा/अथवा ई-केवाईसी उपयोक्ता एजेंसी (केयूए), जैसा भी मामला हो, की नियुक्ति के लिए निम्नलिखित श्रेणियां वर्गीकृत की गई हैं :-

क्रम संख्या	संस्था श्रेणी
श्रेणी - 1	सरकारी संस्थाएं
1.1	केन्द्र/राज्य सरकार के मंत्रालय/विभाग तथा उनके सम्बद्ध अथवा अधीनस्थ कार्यालय
1.2	केन्द्र/राज्य सरकार के स्वामित्व तथा अधीन उपक्रम (सरकारी क्षेत्र के उपक्रम)
1.3	केन्द्रीय/राज्य अधिनियम के अंतर्गत स्थापित प्राधिकरण/केन्द्र/राज्य सरकार द्वारा संस्थापित विशेष उद्देश्य संस्थान
श्रेणी - 2	विनियमित सेवा प्रदाता
2.1	भारतीय रिजर्व बैंक द्वारा विनियमित/लाइसेंस प्राप्त-बैंक तथा भुगतान एवं निपटान प्रणाली
2.1.1	सरकारी क्षेत्र के बैंक
2.1.2	निजी बैंक, भारत में प्रचालन के लिए भारतीय रिजर्व बैंक से लाइसेंस प्राप्त विदेशी बैंक, भुगतान बैंक, लघु वित्त बैंक
2.1.3	क्षेत्रीय ग्रामीण बैंक
2.1.4	सहकारी बैंक राज्य सहकारी बैंक जिला सहकारी बैंक अनुसूचित शहरी सहकारी बैंक गैर अनुसूचित शहरी सहकारी बैंक
2.1.5	भुगतान एवं निपटान प्रणाली नेटवर्क वित्तीय बाजार अवसंरचना 2 खुदरा भुगतान संस्था 3 कार्ड भुगतान नेटवर्क 4 एटीएम नेटवर्क 5 पूर्व-भुगतान प्रपत्र 6 व्हाईट लेबल एटीएम ऑपरेटर 7 इन्स्टैंट मनी ट्रांसफर
2.1.6	गैर बैंकिंग वित्त कम्पनियां
2.2	आईआरडीए/पीएफआरडीए द्वारा विनियमित-वित्तीय संस्थान
2.3	भारतीय दूरसंचार विनियामक प्राधिकरण द्वारा विनियमित - दूरसंचार
2.4	सीसीए द्वारा विनियमित - प्रमाणन प्राधिकरण, डिजीटल लॉकर प्रदाता, ई-हस्ताक्षर प्रदाता
2.5	सेबी द्वारा विनियमित - केवाईसी पंजीकरण एजेंसी (केआरए), डिपोजिटरी पार्टिसिपेंट (डीपी), एस्सेट मैनेजमेंट कम्पनी

क्रम संख्या	संस्था श्रेणी
	(एएमसी), ट्रेडिंग एक्सचेंज , रजिस्ट्रार एंड ट्रांसफर एजेंट
2.6	राष्ट्रीय आवास बैंक द्वारा संचालित
श्रेणी - 3	अन्य संस्थाएं
3.1	3.1.1 कंपनी अधिनियम, 1956 / कंपनी अधिनियम, 2013 के अंतर्गत भारत में पंजीकृत कम्पनी (समूह कम्पनियों के अंतर्गत किसी कम्पनी को अलग से आवेदन करना होगा)
	3.1.2 भारतीय साझेदारी अधिनियम, 1932 अथवा सीमित दायित्व साझेदारी अधिनियम, 2008 के अंतर्गत भारत में पंजीकृत साझेदारी
	3.1.3 स्वामित्व वाली फर्म
	3.1.4 गैर लाभकारी संगठन (कंपनी अधिनियम 1956 के खंड 25 के अधीन)
	3.1.5 अकादमिक संस्थान / अनुसंधान एवं विकास संगठन
	3.1.6 इंडियन सोसायटिज रजिस्ट्रेशन अधिनियम, 1860 अथवा भारतीय न्यास अधिनियम, 1882 अथवा कंपनी अधिनियम, 2013 (खंड 8) / सहकारी समिति अधिनियम, 1912 के अंतर्गत पंजीकृत सोसायटियां
	3.1.7 उपर्युक्त श्रेणियों के अलावा अन्य संस्थान

2. अनुरोधकर्ता संस्था के तौर पर संस्थाओं की नियुक्ति के लिए तकनीकी एवं वित्तीय मापदंड निम्नानुसार हैं:-

श्रेणी	अधिप्रमाणन उपयोक्ता एजेंसी (एयूए)		ई-केवाईसी उपयोक्ता एजेंसी के लिए अतिरिक्त अपेक्षाएं (केयूए)
	तकनीकी अपेक्षाएं	वित्तीय अपेक्षाएं	
श्रेणी - 1	1. आधार अधिप्रमाणन के उद्देश्य से संस्था के पास सर्वर, डाटाबेस इत्यादि जैसी विशेषतः अपेक्षित बैकएंड अवसंरचना भारतीय क्षेत्र में स्थापित होनी चाहिए ।	कोई वित्तीय अपेक्षाएं नहीं	केयूए के लिए कोई अतिरिक्त अपेक्षाएं नहीं
श्रेणी - 2	2. संस्था के पास अपने स्वामित्व अथवा बाह्य स्रोतों से प्राप्त प्रतिमाह 1 लाख अधिप्रमाणन कार्यों के लिए सक्षम आईटी अवसंरचना होनी चाहिए । 3. लाभग्राही की गोपनीयता के संरक्षण के लिए संस्था के पास निर्धारित डाटा गोपनीयता नीति होनी चाहिए । 4. संस्था के पास आईटी अधिनियम, 2000 के अनुसार अंगीकृत डाटा सुरक्षा अपेक्षाएं होनी चाहिए ।	कोई वित्तीय अपेक्षाएं नहीं	केयूए के लिए कोई अतिरिक्त अपेक्षाएं नहीं
श्रेणी - 3	1. आधार अधिप्रमाणन के उद्देश्य से संस्था के पास सर्वर, डाटाबेस इत्यादि जैसी विशेषतः अपेक्षित बैकएंड अवसंरचना भारतीय क्षेत्र में स्थापित होनी चाहिए । 2. संस्था के पास अपने स्वामित्व अथवा बाह्य स्रोतों से प्राप्त प्रतिमाह 1 लाख अधिप्रमाणन कार्यों के लिए सक्षम आईटी अवसंरचना होनी चाहिए । 3. लाभग्राही की गोपनीयता के संरक्षण के लिए संस्था के पास निर्धारित डाटा गोपनीयता नीति होनी चाहिए । 4. संस्था के पास आईटी अधिनियम, 2000 के अनुसार अंगीकृत डाटा सुरक्षा अपेक्षाएं होनी चाहिए । 5. संस्था इस व्यवसाय को प्रारम्भ करने की तिथि से कम से कम 1 वर्ष से इस व्यवसाय में होनी चाहिए ।	न्यूनतम 1 (एक) करोड़ की चुकता पूंजी अथवा पिछले वित्तीय वर्ष के दौरान न्यूनतम 5 (पांच) करोड़ रुपए की वार्षिक टर्नओवर	संस्था प्राधिकरण द्वारा समय-समय पर निर्धारित अधिप्रमाणन कार्य मापदंडों के अनुरूप होनी चाहिए ।

अनुसूची- ख

अधिप्रमाणन सेवा एजेंसियों के लिए पात्रता मापदंड

विनियम 10(2) देखें

1. अधिप्रमाणन सेवाओं के लिए अनुरोधकर्ता संस्थाओं के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार (सीआईडीआर) एक्सेस की अपेक्षा रखने वाली संस्थाओं को अभिप्रमाणन सेवा एजेंसी के तौर पर नियुक्ति के लिए निम्नलिखित श्रेणियों में वर्गीकृत किया गया है :-

क्र. संख्या	संस्था श्रेणी
श्रेणी - 1	केन्द्र/राज्य सरकार के मंत्रालय/विभाग तथा केन्द्र/राज्य सरकार के सम्बद्ध अथवा अधीनस्थ कार्यालय
श्रेणी - 2	केन्द्र/राज्य अधिनियम के अध्याधीन स्थापित प्राधिकरण
श्रेणी - 3	प्राधिकरण द्वारा निश्चित राष्ट्रीय महत्व की कोई संस्था
श्रेणी - 4	कंपनी अधिनियम, 1956 के अधीन भारत में पंजीकृत कोई कंपनी
श्रेणी - 5	अधिप्रमाणन उपयोक्ता एजेंसी (एयूए)/ई-केवाईसी उपयोक्ता एजेंसी(केयूए)

2. अधिप्रमाणन सेवा एजेंसी के तौर पर संस्थाओं की नियुक्ति के लिए तकनीकी एवं वित्तीय मापदंड निम्नानुसार हैं :-

श्रेणी	वित्तीय अपेक्षाएं	तकनीकी अपेक्षाएं
श्रेणी 1, 2 तथा 3	कोई वित्तीय अपेक्षाएं नहीं	कोई तकनीकी अपेक्षाएं नहीं
श्रेणी - 4	पिछले तीन वित्तीय वर्षों में वार्षिक टर्नओवर कम से कम 100 करोड़ रूपए	दूरसंचार सेवा प्रदाता (टीएसपी) सहित सभी संघटित लाइसेंसी (एक्सेस सेवा प्राधिकार से युक्त)/संघटित लाइसेंसी (एएस)/संघटित एक्सेस सेवा लाइसेंसी/ सेल्युलर मोबाइल टेलीफोन सेवा लाइसेंस धारक, जो पैन-इंडिया फाइबर ऑप्टिक नेटवर्क का प्रचालन कर रहे हैं तथा जिनके पास सभी राज्यों के लिए न्यूनतम 100 एमपीएलएस प्वाइंट(पीओएस) उपलब्ध है। अथवा नेटवर्क सेवा प्रदाता (एनएसपी) अथवा डाटा ट्रांसमिशन के लिए पैन-इंडिया नेटवर्क कनेक्टिविटी के लिए सिस्टम इन्टीग्रेटर होना चाहिए तथा भारत में 100 एमपीएलएस पीओपी (पीओपी) होनी चाहिए।
श्रेणी - 5	कोई वित्तीय अपेक्षाएं नहीं	प्राधिकरण द्वारा समय-समय पर निर्धारित अधिप्रमाणन कार्य मापदंडों को पूरा करने वाली अधिप्रमाणन उपयोक्ता एजेंसी(एयूए) अथवा ई-केवाईसी उपयोक्ता एजेंसी।

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यपालक अधिकारी

[विज्ञापन-III/4/असा./238]

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (AUTHENTICATION) REGULATIONS, 2016

(No. 3 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 3 of 2016).—In exercise of the powers conferred by sub-section (1), and sub-clauses (f) and (w) of sub-section (2) of Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, 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) Regulations, 2016.
- (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;

- (b) **“Aadhaar number holder”** means an individual who has been issued an Aadhaar number under the Act;
- (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 verifying the identity 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 an 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 all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;
- (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 demographic information and photograph of an Aadhaar number holder;
- (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;
- (m) **“License Key”** is the key generated by a requesting entity as per the process laid down by the Authority
- (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.
- (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; 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.—**

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).**

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 sub-regulation (2) for a particular service or business function as per its requirement, including multiple factor authentication for enhancing security. For the avoidance of doubt, it is clarified that e-KYC authentication shall only be carried out using OTP and/ or biometric authentication.

5. Information to the Aadhaar number holder.—

- (1) **At the time of authentication,** a requesting entity shall inform the Aadhaar number holder of the following details:—
 - (a) the nature of information that will be shared by the Authority upon authentication;
 - (b) the uses to which the information received during authentication may be put; and
 - (c) alternatives to submission of identity information.
- (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.

6. Consent of the Aadhaar number holder.—

- (1) After communicating the information in accordance with regulation 5, a requesting entity shall obtain the consent of the Aadhaar number holder for the authentication.
- (2) A requesting entity 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.
- (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 of authentication to Aadhaar number holder.—

The Aadhaar number holder may be notified of any biometric and/or OTP based authentication, through the registered email and/or mobile number of the Aadhaar number holder as determined by the Authority, at the time of authentication.

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.

CHAPTER III**APPOINTMENT OF REQUESTING ENTITIES AND AUTHENTICATION SERVICE AGENCIES****12. Appointment of Requesting Entities and Authentication Service Agencies.—**

- (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. 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.
- (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 B are eligible to apply. The Authority may by order, amend Schedule B 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.

13. Procedure where application for appointment is not approved. —

- (1) In the event an application for appointment of requesting entity or 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;
- (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;
- (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 services to Aadhaar number holders;
- (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;
- (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;
- (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;

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;
- (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.

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 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.
- (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 may perform e-KYC authentication on behalf of other agencies, and share the e-KYC data with such agency for a specified purpose, upon obtaining consent from the Aadhaar number holder for such purpose.
- (3) A KUA may store, with consent of the Aadhaar number holder, e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, in encrypted form and subsequently share the e-KYC data with any other agency, for a specified purpose, upon obtaining separate consent for every such sharing from the Aadhaar number holder for that purpose.
- (4) The agency 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 except for completing the transaction for which the Aadhaar number holder has specifically consented to such sharing.
- (5) The Aadhaar number holder may, at any time, revoke consent given to a KUA for storing his e-KYC data or for sharing it with third parties, and upon such revocation, the KUA shall delete the e-KYC data and cease any further sharing.
- (6) In addition to the restriction on further sharing contained in sub-regulation (4), 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 agency or entity with whom e-KYC data has been shared in accordance with this regulation 16.
- (7) Upon request, a KUA shall provide a digitally signed electronic copy of the e-KYC data to the Aadhaar number holder, and the Aadhaar number holder may subsequently share the said copy with any agency:

Provided that the agency that is requesting e-KYC data from the Aadhaar number holder shall inform the purpose of doing so and take the consent of the Aadhaar number;

Provided further that the agency with whom the Aadhaar number holder has shared the e-KYC data shall not share it further with any other entity/agency except for completing the transaction for which the Aadhaar number holder specifically consented to such sharing.

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

17. Obligations relating to use of identity information by requesting entity.—

- (1) A requesting entity shall ensure that:
 - (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) the Aadhaar number against which authentication is sought;
 - (b) specified parameters of authentication request submitted;
 - (c) specified parameters received as authentication response;
 - (d) the record of disclosure of information to the Aadhaar number holder at the time of authentication; and
 - (e) record of consent of the Aadhaar number holder 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 by a 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 request or for grievance redressal and resolution of disputes or with the Authority for audit purposes. The authentication logs shall not be used for any purpose other than 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 this regulation 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 co-operation 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 no Aadhaar number, PID information, device identity related data and e-KYC response data, where applicable shall 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 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.

21. Audit of requesting entities and Authentication Service Agencies.—

- (1) The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they have performed authentication, and Authentication Service Agencies, 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.

22. Data Security. —

- (1) Requesting entities and Authentication Service Agencies shall have their servers used for Aadhaar authentication request formation and routing to CIDR to be located within data centres located in India.
- (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 and Authentication Service Agencies 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 there under, 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.

- (2) Any such action referred to in sub-regulation (1) may also be taken against any entity or agency with which an AUA has shared its license key for Yes/ No authentication and any entity with which a KUA has shared e-KYC data.
- (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) meta data related to the transaction.
 - (d) any authentication server side configurations as necessary

Provided that the Authority shall not, in any case, store the purpose of authentication.

27. Duration of storage. —

- (1) Authentication transaction data shall be retained by the Authority for a period of 6 months, and thereafter archived for a period of five years.
- (2) Upon expiry of the period of five years specified in sub-regulation (1), the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by a 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 Act.

CHAPTER V**MISCELLANEOUS****29. Savings.—**

All procedures, orders, processes, standards, specifications and policies issued and MOUs, agreements or contracts entered by 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, 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.

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.

Schedule A**Eligibility criteria for appointment as requesting entities
See Regulation 10 (1)**

1. Entities seeking to use authentication facility provided by the Authority as requesting entities are classified under following categories for appointment as Authentication User Agency (AUA) and/or e-KYC User Agency (KUA), as the case may be:

S.No.	Organisation Category
Category 1	Government Organisation
1.1	A Central/ State Government Ministry/Department and their attached or sub-ordinate offices.
1.2	An undertaking owned and managed by Central / State Government (PSU)
1.3	An Authority constituted under the Central / State Act/Special Purpose Organisation constituted by Central/State govt.
Category 2	Regulated Service Providers
2.1	Regulated / Licensed by RBI – Banks and Payment & Settlement System
2.1.1	Public Sector Banks (PSB)
2.1.2	Private Banks, Foreign Banks Licensed by RBI to operate in India, Payment Banks, Small Finance Banks
2.1.3	Regional Rural Banks
2.1.4	Co-operative Banks 5. State Co-operative Banks 6. District Co-operative Banks 7. Scheduled Urban Cop-operatives Banks 8. Non Scheduled Urban Co-operative Banks
	2.1.5 Payment & Settlement System Network 1. Financial market infrastructure 2. Retails payments Organisation 3. Cards payment network 4. ATM networks 5. Pre-paid payment instruments 6. White label ATM operators 7. Instant Money Transfer
	2.1.6 Non-Banking Financial Company
2.2	Regulated by IRDA/PFRDA - Financial Institutions
2.3	Regulated by TRAI – Telecom
2.4	Regulated by CCA – Certifying Authority, Digital Locker providers, e-Sign providers
2.5	Regulated by SEBI – KYC Registration Agency (KRA), Depository Participant (DP), Asset Management Company (AMC), Trading Exchanges, Registrar and Transfer Agents
2.6	Regulated by National Housing Bank
Category 3	Other Entities
3.1	3.1.1 Company registered in India under the Companies Act 1956 / The companies Act 2013 (Company under group of companies has to apply individually)
	3.1.2 Partnership registered under the India Partnership Act 1932 or under the Limited Liability Partnership Act, 2008
	3.1.3 Proprietorship firm
	3.1.4 Not-for-profit Organisations (under section 25 under The Companies Act 1956)
	3.1.5 Academic Institutions / Research and Development Organisations

S.No.	Organisation Category
	3.1.6 Societies registered under Indian Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The Companies Act, 2013 (Sec 8) / The Co-operative Societies Act 1912
	3.1.7 Any entity other than above mentioned categories

2. Technical and Financial criteria for entities for appointment as requesting entity are as under:-

Category	Authentication User Agency (AUA)		Additional requirements for eKYC User Agency (KUA)
	Technical Requirements	Financial Requirements	
Category 1	1. Backend infrastructure, such as servers, databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located within the territory of India.	No financial requirement	No additional requirement for KUA
Category 2	<p>2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transactions per month.</p> <p>3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy.</p> <p>4. Organisation should have adopted data security requirements as per the IT Act 2000.</p>	No financial requirement	No additional requirement for KUA
Category 3	<p>1. Backend infrastructure, such as servers, databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located within the territory of India.</p> <p>2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transaction per month.</p> <p>3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy.</p> <p>4. Organisation should have adopted Data security requirements as per the IT Act 2000.</p> <p>5. Entity should be in business for minimum of 1 year from date of commencement of Business.</p>	<p>1. Paid up capital of minimum • 1 (one) Crore.</p> <p style="text-align: center;">OR</p> <p>Annual turnover of minimum • 5 (Five) Crore during the last Financial year.</p>	Entity should meet Authentication Transaction Criteria as laid down by the Authority from time to time.

Schedule B

Eligibility criteria of Authentication Service Agencies

See Regulation 10(2)

1. Entities seeking to provide secure access to CIDR to requesting entities for enabling authentication services are classified under following categories for appointment as Authentication Service Agency:

S. No	Organisation Category
Category 1	A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government
Category 2	An Authority constituted under the Central / State Act
Category 3	Any other entity of national importance as determined by the Authority
Category 4	A company registered in India under the Indian Companies Act 1956
Category 5	AUA / KUA

2. Technical and Financial criteria for entities for appointment as Authentication Service Agency are as under:-

Category	Financial Requirement	Technical Requirement
Category 1, 2 and 3	No financial requirements	No technical requirements
Category 4	An annual turnover of at least • 100 crores in last three financial years	A Telecom Service Provider (TSP) including All Unified Licensees (having Access Service Authorization) / Unified Licensees (AS) / Unified Access Services Licensees / Cellular Mobile Telephone Service Licensees operating pan-India fiber optics network and should have a minimum of 100 MPLS Points of Presence (PoP) across all states OR Should be a Network Service Provider (NSP) or System Integrator having pan-India network connectivity for data transmission and should have 100 MPLS PoPs in India,
Category 5	No Financial requirements	Any AUA or KUA meeting authentication transaction criteria as laid down by the Authority from time to time

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ADVT.-III/4/Exty./238]

अधिसूचना

नई दिल्ली, 12 सितम्बर, 2016

आधार (डाटा सुरक्षा) विनियम, 2016

(2016 का 4)

सं. 13012/64/2016/विधि/यूआईडीएआई (2016 का 4).—आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा 54 की उप-धारा(2) के उप-खंड (पी) के अंतर्गत प्राप्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा निम्नलिखित विनियम बनाता है, नामतः—

1. संक्षिप्त नाम और प्रारंभ :-

- (1) इन विनियमों को आधार (डाटा सुरक्षा) विनियम, 2016 कहा जाएगा।
- (2) ये विनियम, इनके सरकारी राजपत्र में प्रकाशन की तिथि से प्रवृत्त 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 (2016 का 18वां) से है;
- (ख) "प्राधिकरण" का अभिप्राय धारा 11 की उप-धारा (1) के तहत स्थापित भारतीय विशिष्ट पहचान प्राधिकरण से है;
- (ग) "केन्द्रीय पहचान आंकड़े निक्षेपागार" अथवा "सीआईडीआर" का अभिप्राय एक या एक से अधिक स्थानों पर केन्द्रीकृत डाटा बेस है, जिसमें आधार नंबर धारक को जारी आधार नंबर सहित ऐसे व्यक्तियों की जनसांख्यिकीय तथा बायोमैट्रिक सूचना तथा तत्संबंधी अन्य संबद्ध सूचना शामिल हैं, से है;

- (घ) "नामांकन एजेंसी" का अभिप्राय इस अधिनियम के तहत व्यक्तियों की जनांकिकीय तथा बायोमैट्रिक सूचना का संग्रहण करने हेतु प्राधिकरण या किसी रजिस्ट्रार द्वारा नियुक्त एजेंसी, जैसा भी मामला हो, से है;
- (ङ) "सूचना सुरक्षा संबंधी नीति" का अभिप्राय इन विनियमों के विनियम 3 के तहत प्राधिकरण द्वारा विनिर्दिष्ट नीति से है;
- (च) "कार्मिक" का अभिप्राय प्राधिकरण द्वारा इस अधिनियम के तहत किन्ही कृत्यों के निर्वहन के लिए प्राधिकरण अथवा सेवा प्रदाताओं द्वारा कार्यरत अथवा संलग्न किए गए सभी अधिकारियों, कर्मचारियों, स्टाफ व अन्य व्यक्तियों से है;
- (छ) "रजिस्ट्रार" का अभिप्राय इस अधिनियम के तहत व्यक्तियों को नामांकित करने के प्रयोजनार्थ प्राधिकरण द्वारा प्राधिकृत या मान्यताप्राप्त किसी संस्था से है;
- (ज) "विनियम" का अभिप्राय इस अधिनियम के तहत प्राधिकरण द्वारा बनाए गए विनियम से है;
- (झ) "अनुरोध करने वाली संस्था" का अभिप्राय किसी एजेंसी या व्यक्ति से है, जो कि अधिप्रमाणन के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार को किसी व्यक्ति विशेष के आधार नंबर तथा जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना प्रस्तुत करता है;
- (ट) "सेवा प्रदाता" में प्राधिकरण द्वारा इसकी प्रक्रियाओं के संबंध में किन्ही कृत्यों से निर्वहन हेतु प्राधिकरण द्वारा अनुबंधित संस्थाएं शामिल हैं।
- (2) इन विनियमों के उपयोग के लिए अन्य शब्द या वाक्य, जिन्हें यहां परिभाषित नहीं किया गया है परन्तु अधिनियम अथवा सूचना प्रौद्योगिकी अधिनियम, 2000 और/अथवा उसके तहत बनाए गए नियमों तथा अन्य विनियमों में परिभाषित किया गया है, उनका क्रमशः वही अर्थ होगा, जो कि उन्हें अधिनियमों अथवा नियम अथवा अन्य विनियमों अथवा किन्ही सांविधिक आशोधनों अथवा तत्संबंधी पुर्न-अधिनियम, जैसा भी मामला हो, में दिया गया है।

3. सूचना की सुरक्षा सुनिश्चित करने के लिए उपाय :-

- (1) प्राधिकरण, सूचना सुरक्षा संबंधी नीति के साथ ही साथ प्राधिकरण तथा इसके कर्मियों द्वारा अंगीकार की जाने वाली तकनीकी तथा संगठनात्मक उपयोग के साथ ही प्राधिकरण, रजिस्ट्रार, नामांकन एजेंसी, अनुरोध करने वाली संस्था तथा अधिप्रमाणन एजेंसियों द्वारा अनुबंधित एजेंसियों, परामर्शदाताओं, सलाहकार तथा अन्य सेवा प्रदाताओं द्वारा अपनाए जाने वाले सुरक्षा उपायोग को विनिर्दिष्ट कर सकता है।
- (2) ऐसी सुरक्षा संबंधी नीति में निम्नलिखित के लिए उपबंध होगा :-
- (क) सूचना और सूचना को संसाधित करने वाली सुविधाओं से संबद्ध परिसम्पत्तियों की वस्तु-सूची की पहचान तथा उनका रख-रखाव;
- (ख) परिसम्पत्तियों की कोई हानि, क्षति, चोरी अथवा उन्हें जोखिम में डालने से बचने के लिए नियंत्रण प्रक्रियाओं को लागू करना;
- (ग) गोपनीय सूचना तक केवल नियंत्रित पहुंच प्रदान करना;
- (घ) वॉयरस/मैलवेयरों का पता लगाने या उनके विरुद्ध सुरक्षा के लिए नियंत्रण करना;
- (च) परिवर्तन किए जाने के दौरान, सूचना की सुरक्षा सुनिश्चित करने के लिए परिवर्तन प्रबंधन प्रक्रिया;
- (छ) भेद्यता तथा सुरक्षा जोखिमों से सूचना प्रणालियों को सुरक्षित बनाने के लिए एक 'पैच मैनेजमेंट सिस्टम';
- (ज) असामान्य घटनाओं तथा पैटर्नों की पहचान करने के लिए एक सुदृढ निगरानी प्रक्रिया स्थापित करना, जो सूचना प्रणालियों की सुरक्षा तथा कार्यनिष्पादन को प्रभावित कर सकता है तथा उपर्युक्त सूचना प्रदान करने तथा तत्संबंधी न्यूनीकरण प्रक्रिया;
- (झ) बायोमैट्रिक सूचना वाले डाटा पेकेटों को कूटबद्ध करना तथा केवल सुरक्षित अवस्थितियों में उसकी अकूटबद्धता सुनिश्चित करना;
- (ट) जोखिम तथा विश्वास आधार पर सीआईडीआर नेटवर्क का पार्टिशन करना;
- (ठ) सीआईडीआर नेटवर्क को सुरक्षित बनाने के लिए अनिवार्य तकनीकी नियंत्रण लगाना;
- (ड) आपदा की स्थिति में सेवा को जारी रखना;
- (ढ) उपकरण, प्रणालियों तथा नेटवर्कों की निगरानी;
- (ण) धोखाधड़ी से बचने तथा धोखाधड़ी होने पर प्रभावी उपचार के लिए उपाय करना;
- (त) कर्मियों के साथ गैर-प्रकटन करार करने संबंधी आवश्यकता;
- (थ) आंतरिक प्रणालियां तथा नेटवर्कों की लेखापरीक्षा करने के लिए उपबंध;
- (द) प्रक्रियाओं, प्रणालियों तथा नेटवर्कों से संबंधित कमियों पर निगरानी रखना;
- (ध) प्राधिकरण द्वारा अनुबंधित एजेंसियों, परामर्शदाताओं, सलाहकारों अथवा अन्य व्यक्तियों के साथ किए गए करार तथा व्यवस्थाओं में सुरक्षा तथा गोपनीयता दायित्वों को शामिल करना।
- (3) प्राधिकरण, सूचना की सुरक्षा संबंधी नीति तथा अन्य सुरक्षा संबंधी अपेक्षाओं की आंतरिक लेखापरीक्षाओं अथवा स्वतंत्र एजेंसियों के माध्यम से अनुपालन किए जाने की निगरानी करेगा।
- (4) प्राधिकरण, सूचना सुरक्षा संबंधी नीति तथा प्राधिकरण के अन्य सुरक्षा संबंधी कार्यक्रम तथा पहल की निगरानी करने तथा उसका प्रसार करने के लिए एक अधिकारी को मुख्य सूचना सुरक्षा अधिकारी के रूप में पदनामित करेगा।

4. कर्मियों का सुरक्षा संबंधी दायित्व :-

- (1) कर्मी, प्राधिकरण द्वारा समय-समय पर जारी सूचना सुरक्षा नीति तथा अन्य नीतियों, दिशानिर्देशों, प्रक्रियाओं आदि का अनुपालन करेंगे।
- (2) अधिनियम के तहत की जाने वाली कार्रवाई पर प्रतिकूल प्रभाव डाले बिना, कर्मचारियों पर प्राधिकरण द्वारा इस प्रयोजनार्थ विनिर्दिष्ट प्रक्रियाओं के अनुरूप कार्रवाई की जा सकती है:
बशर्ते कि संबंधित कर्मी के विरुद्ध सुने जाने हेतु एक उपर्युक्त अवसर दिए बिना कोई कार्रवाई नहीं की जाएगी।

5. सेवा प्रदाताओं आदि का सुरक्षा संबंधी दायित्व :-

प्राधिकरण द्वारा प्रक्रियाओं से संबंधित किन्ही कृत्यों के निर्वहन हेतु अनुबंधित एजेंसियां, परामर्शदाता, सलाहकार तथा अन्य सेवा प्रदाता निम्नलिखित सुनिश्चित करेंगे :-

- (क) प्राधिकरण द्वारा विनिर्दिष्ट सूचना सुरक्षा संबंधी नीति का अनुपालन सुनिश्चित करेंगे;
- (ख) सुरक्षा संबंधी नीति तथा संविदागत आवश्यकताओं, जैसाकि प्राधिकरण द्वारा अपेक्षित हो, की अनुपालना के संबंध में आवधिक रिपोर्ट प्रस्तुत करेंगे;
- (ग) प्राधिकरण के कार्यकरण से संबंधित सूचना की गोपनीयता, पूर्णता तथा उपलब्धता को प्रभावित करने वाले किन्ही सुरक्षा संबंधी घटनाओं के बारे में त्वरित रूप से प्राधिकरण को जानकारी देना;
- (घ) प्राधिकरण से संबंधित अभिलेखों को हानि होने, नाश होने, फर्जीवाड़े, अप्राधिकृत पहुंच तथा अप्राधिकृत रूप से जारी किए जाने से रक्षा किया जाना सुनिश्चित करेंगे;
- (च) करार की अवधि के दौरान तथा उसके समाप्त होने पर गोपनीयता संबंधी दायित्वों का अनुपालन सुनिश्चित किया जाएगा;
- (छ) यह सुनिश्चित किया जाए कि कर्मचारियों तथा स्टॉफ के सदस्यों के साथ करार में उपर्युक्त सुरक्षा तथा गोपनीय संबंधी दायित्वों का उपबंध किया जाए;
- (ज) यह सुनिश्चित किया जाए कि सीआईडीआर डाटा केन्द्रों तथा वास्तविक तथा लॉजिकल पहुंच प्राप्त कर्मचारियों की पृष्ठभूमि की जांच आवश्यक रूप से की जाए;
- (झ) संवेदनशील सूचना रखने वाली सुरक्षा परिधि को परिभाषित करें तथा यह सुनिश्चित करें कि ऐसे क्षेत्र तक केवल प्राधिकृत व्यक्ति को ही पहुंच प्रदान की जाए, जिससे डाटा के चोरी होने तथा उसके दुरुपयोग से रोका जा सके;
- (ट) जहां कर्मचारी, बायोमेट्रिक डाटा का संचालन करें, वहां यह सुनिश्चित किया जाए कि वे केवल ऐसे बायोमेट्रिक उपकरणों का ही उपयोग करें, जोकि प्राधिकरण द्वारा किसी अधिप्रमाणन निकाय द्वारा प्रमाणित हो तथा यह सुनिश्चित करें कि बायोमेट्रिक डाटा की सुरक्षा सुनिश्चित करने के लिए उपयुक्त प्रणालियां स्थापित की गई हैं।

6. सेवा प्रदाताओं की लेखापरीक्षा तथा निरीक्षण आदि :-

- (1) प्राधिकरण द्वारा अनुबंधित सभी एजेंसियां, परामर्शदाता, सलाहकार तथा अन्य सेवा प्रदाता तथा अन्य भागीदारों जैसे रजिस्ट्रार, अनुरोध करने वाली संस्थाएं, अधिप्रमाणन उपयोगकर्ता एजेंसियां तथा अधिप्रमाणन सेवा एजेंसियां अपने प्रचालनों की लेखापरीक्षा, सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत किसी मान्यता प्राप्त निकाय से अनुप्रमाणित करवाएंगे तथा प्राधिकरण द्वारा मांगे जाने पर अथवा प्राधिकरण द्वारा प्राधिकरण को लेखापरीक्षा रिपोर्ट उपलब्ध कराएंगे।
- (2) उप-विनियम (1) में संदर्भित लेखापरीक्षा के अतिरिक्त, प्राधिकरण स्वयं अथवा प्राधिकरण द्वारा नियुक्त किसी लेखापरीक्षक के माध्यम से ऐसी संस्थाओं तथा व्यक्तियों के प्रचालन तथा प्रणालियों की लेखापरीक्षा कर सकता है।

7. गोपनीयता :-

प्राधिकरण द्वारा गोपनीय माने जाने वाली सुरक्षा संबंधी सभी कार्यपद्धतियों, आदेश, प्रक्रियाएं, मानक तथा नयाचार को इसके सभी कर्मियों द्वारा गोपनीय माना जाएगा तथा सभी पक्षों द्वारा केवल उस सीमा तक उद्घटन किया जाएगा, जहां तक वे सुरक्षा उपायों को मूर्तरूप देने के लिए अनिवार्य हों। जब तक कि अधिनियम के तहत अधिदेशित न किया गया हो, सूचना जिन्हें प्राधिकरण से सांझा नहीं किया जा सकता है, उसमें असीमित रूप से सीआईडीआर में सूचना, प्रौद्योगिकी संबंधी ब्यौरा, नेटवर्क संरचना, सूचना की सुरक्षा संबंधी नीति तथा प्रक्रियाएं, सॉफ्टवेयर कोड, आंतरिक रिपोर्ट, लेखापरीक्षा तथा मूल्यांकन रिपोर्ट, अनुप्रयोग के संबंध में ब्यौरे, परिसम्पत्ति ब्यौरा, संविदागत करार, विद्यमान तथा भावी आयोजना संबंधी अवसरचरणात्मक ब्यौरा, सुरक्षा संबंधी सेवा तथा प्रणाली की सक्षमता शामिल हैं।

8. व्यावृत्ति :-

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 ऐसे प्राधिकरण के किसी अधिकारी, अधिनियम के तहत प्राधिकरण की स्थापना पूर्व, द्वारा जारी सभी कार्यपद्धति, आदेश, प्रक्रियाएं, मानक तथा नीतियां अथवा हस्ताक्षर किए सभी समझौता ज्ञापन, करार अथवा संविदाएं उस सीमा तक लागू रहेंगी, जबतक कि वे अधिनियम के उपबंधों तथा तत्संबंध के तहत तैयार किए गए अधिनियम अथवा विनियम के तहत असंगत सिद्ध न हो जाएं।

9. नीतियां, प्रक्रियाएं दस्तावेज आदि जारी करने संबंधी शक्तियां :-

प्राधिकरण ऐसी नीतियां, प्रक्रियाएं, मानक तथा अन्य दस्तावेज जारी कर सकता है, जो इन विनियमों के विरुद्ध नहीं हैं तथा जिन्हें इन विनियमों के तहत विनिर्दिष्ट किया जाना अपेक्षित है अथवा जिनके लिए इन विनियमों को प्रभावी बनाने हेतु उपबंध किया जाना अनिवार्य है।

10. 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 दिशानिर्देश जारी करने की शक्ति होगी, जिनका प्रभाव विनियम के समान होगा।

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यपालक अधिकारी

[विज्ञापन—III/4/असा./238]

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (DATA SECURITY) REGULATIONS, 2016

(No. 4 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 4 of 2016).—In exercise of the powers conferred by clause (p) of sub-section (2) of section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the Unique Identification Authority of India makes the following Regulations, namely: -

1. Short title and commencement. —

- (1) These regulations may be called the Aadhaar (Data Security) Regulations, 2016
- (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 (18 of 2016);
- (b) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;
- (c) “Central Identities Data Repository” or “CIDR” means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;
- (d) “enrolling agency” means an agency appointed by the Authority or a Registrar, as the case may be, for collecting demographic and biometric information of individuals under this Act;
- (e) “information security policy” means the policy specified by the Authority under regulation 3 of these regulations;
- (f) “personnel” means all officers, employees, staff and other individuals employed or engaged by the Authority or by the service providers for discharging any functions under the Act;
- (g) “registrar” means any entity authorised or recognised by the Authority for the purpose of enrolling individuals under this Act;
- (h) “regulations” means the regulations made by the Authority under this Act;
- (i) “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;
- (j) “service provider” includes all entities engaged by the Authority for discharging any function related to its processes.

(2) All other words and expressions used but not defined in these regulations, but defined in the Act or the Information Technology Act, 2000 and/or the rules and regulations made thereunder shall have the same meaning as respectively assigned to them in such Acts or rules or regulations or any statutory modification or re-enactment thereto, as the case may be.

3. Measures for ensuring information security. —

(1) The Authority may specify an information security policy setting out *inter alia* the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and Authentication Service Agencies.

- (2) Such information security policy may provide for:—
- (a) identifying and maintaining an inventory of assets associated with the information and information processing facilities;
 - (b) implementing controls to prevent and detect any loss, damage, theft or compromise of the assets;
 - (c) allowing only controlled access to confidential information;
 - (d) implementing controls to detect and protect against virus/malwares;
 - (e) a change management process to ensure information security is maintained during changes;
 - (f) a patch management process to protect information systems from vulnerabilities and security risks;
 - (g) a robust monitoring process to identify unusual events and patterns that could impact security and performance of information systems and a proper reporting and mitigation process;
 - (h) encryption of data packets containing biometrics, and enabling decryption only in secured locations;
 - (i) partitioning of CIDR network into zones based on risk and trust;
 - (j) deploying necessary technical controls for protecting CIDR network;
 - (k) service continuity in case of a disaster;
 - (l) monitoring of equipment, systems and networks;
 - (m) measures for fraud prevention and effective remedies in case of fraud;
 - (n) requirement of entering into non-disclosure agreements with the personnel;
 - (o) provisions for audit of internal systems and networks;
 - (p) restrictions on personnel relating to processes, systems and networks.
 - (q) inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the Authority.
- (3) The Authority shall monitor compliance with the information security policy and other security requirements through internal audits or through independent agencies.
- (4) The Authority shall designate an officer as Chief Information Security Officer for disseminating and monitoring the information security policy and other security-related programmes and initiatives of the Authority.

4. Security obligations of the personnel —

- (1) The personnel shall comply with the information security policy, and other policies, guidelines, procedures, etc. issued by the Authority from time to time.
- (2) Without prejudice to any action that may be taken under the Act, personnel may be liable to action in accordance with procedures specified by the Authority for this purpose:

Provided that no such action shall be taken without giving the concerned personnel a reasonable opportunity of being heard.

5. Security obligations of service providers, etc. —

The agencies, consultants, advisors and other service providers engaged by the Authority for discharging any function relating to its processes shall:

- (a) ensure compliance with the information security policy specified by the Authority;
- (b) periodically report compliance with the information security policy and contractual requirements, as required by the Authority;
- (c) report promptly to the Authority any security incidents affecting the confidentiality, integrity and availability of information related to the Authority's functions;
- (d) ensure that records related to the Authority shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release;
- (e) ensure confidentiality obligations are maintained during the term and on termination of the agreement;
- (f) ensure that appropriate security and confidentiality obligations are provided for in their agreements with their employees and staff members;
- (g) ensure that the employees having physical access to CIDR data centers and logical access to CIDR data centers undergo necessary background checks;
- (h) define the security perimeters holding sensitive information, and ensure only authorised individuals are allowed access to such areas to prevent any data leakage or misuse; and

- (i) where they are involved in the handling of the biometric data, ensure that they use only those biometric devices which are certified by a certification body as identified by the Authority and ensure that appropriate systems are built to ensure security of the biometric data.

6. Audits and inspection of service providers, etc. —

- (1) All agencies, consultants, advisors and other service providers engaged by the Authority, and ecosystem partners such as registrars, requesting entities, Authentication User Agencies and Authentication Service Agencies shall get their operations audited by an information systems auditor certified by a recognised body under the Information Technology Act, 2000 and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority.
- (2) In addition to the audits referred to in sub-regulation (1), the Authority may conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

7. Confidentiality. —

All procedures, orders, processes, standards and protocols related to security, which are designated as confidential by the Authority, shall be treated as confidential by all its personnel and shall be disclosed to the concerned parties only to the extent required for giving effect to the security measures. The nature of information that cannot be shared outside the Authority unless mandated under the Act includes, but not limited to, Information in CIDR, Technology details, Network Architecture, Information security policy and processes, software codes, internal reports, audit and assessment reports, applications details, asset details, contractual agreements, present and future planned infrastructure details, protection services, and capabilities of the system.

8. Savings. —

All procedures, orders, processes, standards and policies issued and MOUs, agreements or contracts entered by 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, 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.

9. Power to issue policies, process documents, etc. —

The Authority may issue policies, processes, standards 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.

10. Power to issue clarifications, guidelines and removal of difficulties. —

In order to clarify any matter pertaining to application or interpretation of these regulations, or to remove any difficulties in implementation of these regulations, the Authority shall have the power to issue clarifications and guidelines in the form of circulars which shall have effect of these regulations.

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ADVT.-III/4/Exty./238]

अधिसूचना

नई दिल्ली, 12 सितम्बर, 2016

आधार (सूचना की सहभाजिता) विनियम, 2016

(2016 का 5)

सं. :-13012/64/2016/विधि/यूआईडीएआई (2016 का 5).—आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा 23 की उप-धारा (2) के उप-खंड (के) तथा धारा 29 की उप-धारा (2) तथा (4) के साथ पठित धारा 54 की उप-धारा (2) के उप-खंड (ओ) तथा उप-धारा (1) के अंतर्गत प्राप्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा निम्नलिखित विनियम बनाता है, नामतः :-

अध्याय- 1

प्रारंभिक

1. संक्षिप्त नाम और प्रारंभ :-

- (1) इन विनियमों को आधार (सूचना की सहभाजिता) विनियम, 2016 कहा जाएगा।
- (2) ये विनियम, इनके सरकारी राजपत्र में प्रकाशन की तिथि से प्रवृत्त 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;
 - (ख) "आधार पत्र" का अभिप्राय किसी निवासी को आधार नंबर के संप्रेषित करने वाले दस्तावेज से है;
 - (ग) "आधार नंबर धारक" का अभिप्राय कोई व्यक्ति, जिसे अधिनियम के अंतर्गत आधार नंबर जारी किया गया है, से है;
 - (घ) "प्राधिकरण" का अभिप्राय धारा 11 की उप-धारा (1) के तहत स्थापित भारतीय विशिष्ट पहचान प्राधिकरण से है;
 - (च) "अनुरोध करने वाली संस्था" का अभिप्राय किसी एजेंसी या व्यक्ति से है, जो कि अधिप्रमाणन के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार को किसी व्यक्ति विशेष का आधार नंबर तथा जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना प्रस्तुत करता है;
- (2) इन विनियमों के उपयोग के लिए अन्य सभी शब्द या अभिव्यक्तियां, जिन्हें इन विनियमों में परिभाषित नहीं किया गया है परन्तु अधिनियम तथा उसके तहत बनाए गए नियमों तथा अन्य विनियमों में परिभाषित किया गया है, उनका क्रमशः वही अर्थ होगा, जो कि उन्हें अधिनियम अथवा नियम अथवा अन्य विनियमों, जैसा भी मामला हो, में दिया गया है।

अध्याय-2

पहचान संबंधी सूचना की सहभाजिता पर प्रतिबंध

3. प्राधिकरण द्वारा पहचान संबंधी सूचना का सहभाजन :-

- (1) अधिनियम के तहत प्राधिकरण द्वारा संग्रहित मुख्य बायोमैट्रिक सूचना को किसी भी कारण से किसी भी व्यक्ति के साथ सहभाजित नहीं किया जाएगा।
- (2) आधार (अधिप्रमाणन) विनियम, 2016 तथा अधिनियम के उपबंधों के अनुरूप अधिप्रमाणन प्रक्रिया के लिए आधार नंबर धारक से सहमति प्राप्त करने के उपरांत इनके संबंध में अनुरोध करने वाली संस्था के अनुरोध पर अधिनियम के तहत प्राधिकरण द्वारा संग्रहित व्यक्ति विशेष सूचना की जनसांख्यिकीय सूचना तथा फोटोग्राफ को किसी अनुरोध करने वाली संस्था द्वारा ऐसे व्यक्ति विशेष के संबंध में ई-केवाईसी संबंधी डाटा के अधिप्रमाणन संबंधी अनुरोध किए जाने पर प्राधिकरण द्वारा सहभाजित किया जा सकता है।
- (3) प्राधिकरण, आधार (अधिप्रमाणन) विनियम, 2016 के विनियम 28 के अनुरूप आधार नंबर धारक के अधिप्रमाणन अभिलेखों को सहभाजित करेगा।
- (4) प्राधिकरण अधिनियम की धारा 33 के अनुरूप, जब ऐसा करने की आवश्यकता हो, आधार नंबर धारक की जनसांख्यिकीय सूचना तथा फोटोग्राफ तथा अधिप्रमाणन अभिलेखों को सहभाजित करेगा।

4. अनुरोध करने वाली संस्था के साथ सूचना का सहभाजन :-

- (1) अनुरोध करने वाली संस्था द्वारा आधार नंबर धारक के संबंध में अधिप्रमाणन के समय संग्रहित अथवा प्राप्त की गई मुख्य बायोमैट्रिक सूचना को आधार (अधिप्रमाणन) विनियम, 2016 में यथा-विनिर्दिष्ट बफर अधिप्रमाणन के अलावा संचयित नहीं किया जाएगा और किसी भी कारण से से किसी व्यक्ति के साथ सांझा नहीं किया जाएगा।
- (2) अनुरोध करने वाली संस्था के पास उपलब्ध पहचान संबंधी सूचना को :-
 - (क) अनुरोध करने वाली संस्था द्वारा अधिप्रमाणन हेतु पहचान संबंधी सूचना को प्रस्तुत करने के समय, आधार नंबर धारक के विनिर्दिष्ट प्रयोजन के अलावा किसी अन्य प्रयोजन के लिए उपयोग नहीं किया जाएगा; और
 - (ख) आधार नंबर धारक की पूर्व सहमति के बिना आगे उद्घाटित/प्रकट नहीं किया जाएगा।
- (3) अनुरोध करने वाली संस्था, आधार नंबर धारक के अधिप्रमाणन संबंधी लॉग की संबंधित सूचना को आधार (अधिप्रमाणन) विनियम, 2016 के विनियम 18 में यथाविनिर्दिष्ट आधार नंबर धारक के साथ उसके अनुरोध किए जाने या शिकायत निवारण हेतु एवं विवादों के समाधान हेतु एवं प्राधिकरण के साथ लेखापरीक्षा प्रयोजनार्थ सहभाजित कर सकता है।

5. आधार नंबर के संबंध में अनुरोध करने वाली संस्था के अलावा अन्य एजेंसी या संस्था का उत्तरदायित्व :-

- (1) कोई भी व्यक्ति विशेष, एजेंसी या संस्था, जो आधार नंबर या आधार नंबर अंतर्विष्ट किसी दस्तावेज का संग्रहण करती है, वह:-

- (क) केवल विधि-सम्मत प्रयोजनों के लिए आधार नंबर का संग्रहण, भंडारण तथा उपयोग करेगी;
- (ख) निम्नलिखित ब्यौरे के संबंध में आधार नंबर धारक को सूचित करेगी:-
- (i) प्रयोजन, जिसके लिए सूचना का संग्रहण किया गया है;
- (ii) क्या ऐसे प्रयोजनार्थ आधार नंबर या आधार का साक्ष्य दिया जाना अनिवार्य है या ऐच्छिक है और यदि अनिवार्य है तो इसे अधिदेशित करने वाला विधिक उपबंध क्या है;
- (iii) आधार नंबर अथवा आधार नंबर अंतर्विष्ट दस्तावेज को जमा करने का विकल्प, यदि कोई हो तो;
- (ग) विनिर्दिष्ट प्रयोजनार्थ आधार नंबर के संग्रहण, भंडारण उपयोग हेतु आधार नंबर धारक की सहमति प्राप्त करना;
- (2) ऐसा व्यक्ति विशेष, एजेंसी या संस्था आधार नंबर धारक से सहमति प्राप्त करने के समय विनिर्दिष्ट शर्तों के अलावा किसी अन्य प्रयोजनार्थ आधार नंबर का उपयोग नहीं करेगा।
- (3) ऐसा व्यक्ति विशेष, एजेंसी या संस्था आधार नंबर को आधार नंबर धारक की सहमति के बिना किसी व्यक्ति के साथ सहभाजित नहीं करेगा।

6. **आधार नंबर को सहभाजित करने, परिचालित करने या प्रकाशित करने पर प्रतिबंध :-**

- (1) किसी व्यक्ति विशेष के आधार नंबर को किसी व्यक्ति या संस्था या एजेंसी द्वारा प्रकाशित, प्रदर्शित अथवा सार्वजनिक रूप से पोस्ट नहीं किया जाएगा।
- (2) ऐसा कोई व्यक्ति विशेष संस्था या एजेंसी, जिसके पास आधार नंबर धारकों के आधार नंबर हैं, वह आधार नंबर वाले किसी अभिलेख या डाटा बेस की सुरक्षा एवं गोपनीयता सुनिश्चित करेगी।
- (3) उप-विनियम (1) और (2) पर बिना प्रतिकूल प्रभाव डाले, अनुरोध करने वाली संस्था सहित कोई भी संस्था, जिसके पास किसी आधार नंबर धारक का आधार नंबर है, वह व्यक्ति विशेष के आधार नंबर वाले किसी भी डाटा बेस या अभिलेख को सार्वजनिक नहीं करेगा, जबतक कि प्रिंट या इलेक्ट्रॉनिक, दोनों रूपों में उपयुक्त तरीके से आधार नंबर को हटा या मिटा न दिया गया हो।
- (4) अनुरोध करने वाली संस्था सहित कोई भी संस्था अपने किसी भी व्यक्ति को अपने आधार नंबर को इंटरनेट के माध्यम से भेजने को तभी कहेगी जबकि वैसा भेजा जाना सुरक्षित हो तथा आधार नंबर को कूटबद्ध रूप से भेजा जाए, केवल उस स्थिति को छोड़कर, जहां इस प्रकार से आधार नंबर भेजा जाना, त्रुटि सुधार किए जाने या शिकायत का निपटान किए जाने के लिए अपेक्षित हो।
- (5) अनुरोध करने वाली संस्था सहित कोई भी संस्था आधार नंबर या किसी दस्तावेज या डाटा बेस, जिसमें आधार नंबर हो, को आधार नंबर धारक की सहमति लेने के समय विनिर्दिष्ट प्रयोजन के लिए आवश्यक समय से अधिक समय तक अपने पास नहीं रखेगी।

7. **विनियमों का उल्लंघन किए जाने पर दायित्व निर्धारण :-**

अधिनियम के तहत की जाने वाली किसी कार्रवाई पर बिना प्रतिकूल प्रभाव डाले, इन विनियमों के विनियम 3, 4, 5 और 6 का कोई भी उल्लंघन अधिनियम की धारा 29 की उप-धारा (2) का उल्लंघन माना जाएगा।

8. **आधार नंबर धारक की शिकायतों का निवारण :-**

आधार नंबर धारक की पहचान संबंधी सूचना को अधिनियम या विनियमों के उपबंधों के प्रतिकूल किसी पद्धति से सहभाजित किए जाने या प्रकाशित किए जाने पर आधार नंबर धारक, आधार (नामांकन तथा अद्यतन) विनियम, 2016 के विनियम 32 के अनुरूप प्रश्न पूछ सकता है तथा शिकायत कर सकता है।

अध्याय-3

विविध

9. **आधार नंबर को सहभाजित किए जाने के बारे में सूचना का प्रसार :-**

प्राधिकरण, आधार नंबर के उपयोग तथा इसको सहभाजित किए जाने के दुष्परिणामों के बारे में आधार नंबर धारक को शिक्षित करने के लिए अनिवार्य उपाय कर सकता है।

10. **व्यावृत्ति :-**

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 ऐसे प्राधिकरण के किसी अधिकारी अथवा अधिनियम के तहत प्राधिकरण की स्थापना पूर्व जारी सभी कार्य-पद्धति, आदेश, प्रक्रियाएं, मानक तथा नीतियां अथवा हस्ताक्षर किए गए सभी समझौता ज्ञापन, करार अथवा सविदाएं उस

सीमा तक लागू रहेंगी, जबतक कि वे अधिनियम के उपबंधों तथा तत्संबंध के तहत तैयार किए गए अधिनियम अथवा विनियम के तहत असंगत सिद्ध न हो जाएं।

11. **स्पष्टीकरण तथा दिशानिर्देशों को जारी करने की शक्ति—**

इन विनियमों के अनुप्रयोग तथा निर्वचन के संबंध में किसी समस्या का निराकरण करने अथवा किसी मामले में स्पष्टीकरण करने के लिए प्राधिकरण परिपत्र के रूप में स्पष्टीकरण अथवा दिशानिर्देश जारी कर सकता है।

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यपालक अधिकारी

[विज्ञापन—III/4/असा./238]

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (SHARING OF INFORMATION) REGULATIONS, 2016

(No. 5 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 5 of 2016).—In exercise of the powers conferred by sub-section (1), and sub-clause (o) of sub-section (2), of Section 54 read with sub-clause (k) of sub-section (2) of Section 23, and sub-sections (2) and (4) of Section 29, of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, 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 (Sharing of Information) Regulations, 2016.
- (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;
 - (b) “Aadhaar Letter” means a document for conveying the Aadhaar number to a resident;
 - (c) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;
 - (d) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11;
 - (e) “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.

(2) All other words and expressions used in these regulations but not defined, and defined in the Act and the rules and other regulations made there under, shall have the meanings respectively assigned to them in the Act or the rules or other regulations, as the case may be.

CHAPTER II

RESTRICTIONS ON SHARING OF IDENTITY INFORMATION

3. Sharing of information by the Authority. —

- (1) Core biometric information collected by the Authority under the Act shall not be shared with anyone for any reason whatsoever.
- (2) The demographic information and photograph of an individual collected by the Authority under the Act may be shared by the Authority with a requesting entity in response to an authentication request for e-KYC data pertaining to such individual, upon the requesting entity obtaining consent from the Aadhaar number holder for the authentication process, in accordance with the provisions of the Act and the Aadhaar (Authentication) Regulations, 2016.
- (3) The Authority shall share authentication records of the Aadhaar number holder with him in accordance with regulation 28 of the Aadhaar (Authentication) Regulations, 2016.

(4) The Authority may share demographic information and photograph, and the authentication records of an Aadhaar number holder when required to do so in accordance with Section 33 of the Act.

4. Sharing of information by a requesting entity. —

(1) Core biometric information collected or captured by a requesting entity from the Aadhaar number holder at the time of authentication shall not be stored except for buffered authentication as specified in the Aadhaar (Authentication) Regulations, 2016, and shall not be shared with anyone for any reason whatsoever.

(2) The identity information available with a requesting entity:

(a) shall not be used by the requesting entity for any purpose other than that specified to the Aadhaar number holder at the time of submitting identity information for authentication; and

(b) shall not be disclosed further without the prior consent of the Aadhaar number holder.

(3) A requesting entity may share the authentication logs of an Aadhaar number holder with the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes, as specified in regulation 18 of the Aadhaar (Authentication) Regulations, 2016.

5. Responsibility of any agency or entity other than requesting entity with respect to Aadhaar number. —

(1) Any individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number, shall:

(a) collect, store and use the Aadhaar number for a lawful purpose;

(b) inform the Aadhaar number holder the following details:—

i. the purpose for which the information is collected;

ii. whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it;

iii. alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any;

(c) obtain consent of the Aadhaar number holder to the collection, storage and use of his Aadhaar number for the specified purposes.

(2) Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent.

(3) Such individual, agency or entity shall not share the Aadhaar number with any person without the consent of the Aadhaar number holder.

6. Restrictions on sharing, circulating or publishing of Aadhaar number. —

(1) The Aadhaar number of an individual shall not be published, displayed or posted publicly by any person or entity or agency.

(2) Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers.

(3) Without prejudice to sub-regulations (1) and (2), no entity, including a requesting entity, which is in possession of the Aadhaar number of an Aadhaar number holder, shall make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form.

(4) No entity, including a requesting entity, shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances.

(5) No entity, including a requesting entity, shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent.

7. Liability for contravention of the regulations. —

Without prejudice to any action that may be taken under the Act, any contravention of regulations 3, 4, 5 and 6 of these regulations shall constitute a violation of sub-section (2) of Section 29 of the Act.

8. Redressal of grievances of Aadhaar number holders. —

In the event the identity information of an Aadhaar number holder has been shared or published in a manner contrary to the provisions of the Act or regulations, the Aadhaar number holder may raise queries and grievances in accordance with the regulation 32 of the Aadhaar (Enrolment and Update) Regulations, 2016.

CHAPTER III**MISCELLANEOUS****9. Information dissemination about sharing of Aadhaar numbers. —**

The Authority may take necessary measures to educate Aadhaar number holders about the uses of Aadhaar numbers and implications associated with its sharing.

10. Savings. —

All procedures, orders, processes, standards and policies issued and MOUs, agreements or contracts entered by 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, 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.

11. Power to issue clarifications and guidelines. —

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.

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ADVT.-III/4/Exty./238]