डिजिटल व्यक्तिगत डेटा सुरक्षा नीति

भारतीय बैंक की डिजिटल व्यक्तिगत डेटा सुरक्षा नीति ग्राहक की गोपनीयता के Sound सिद्धांतों की कल्पना करती है और डिजिटल व्यक्तिगत डेटा को इस प्रकार संसाधित करने का प्रावधान देती है जो व्यक्तियों के अपने व्यक्तिगत डेटा की रक्षा करने के अधिकार और कानूनी उद्देश्यों के लिए व्यक्तिगत डेटा को संसाधित करने की आवश्यकता दोनों को मान्यता देता है। इस नीति को प्राइवेसी पॉलिसी के रूप में भी संदर्भित किया जा सकता है। बैंक अपने ग्राहकों और अन्य हितधारकों के लिए उच्चतम स्तर की गोपनीयता की प्रतिज्ञा के लिए प्रतिबद्ध है।

ग्राहकों के लिए भारतीय बैंक की गोपनीयता प्रतिज्ञा:

जबकि जानकारी बैंक की उच्च सेवा और ग्राहक संतुष्टि प्रदान करने की क्षमता की आधारशिला है, बैंक की सबसे महत्वपूर्ण संपत्तियों में से एक ग्राहक का विश्वास है। ग्राहक की जानकारी को सुरक्षित रखना और इसे केवल उस तरीके और विशेष उद्देश्य के लिए उपयोग करना, जैसा कि ग्राहक बैंक से चाहेंगे, बैंक में हर किसी के लिए सर्वोच्च प्राथमिकता है। यह बैंक का अपने ग्राहकों और अन्य हितधारकों के प्रति वादा बन जाता है।

यह नीति बैंक द्वारा ग्राहक की व्यक्तिगत जानकारी और संवेदनशील व्यक्तिगत डेटा या जानकारी को कैसे एकत्रित, उपयोग, प्रसंस्करण, प्रकट, संग्रह, सुरक्षित और निपटाया जाता है, को नियंत्रित करती है। इस नीति में प्रस्तुत सामग्री सभी लागू कानूनों, संबंधित नियमों और आरबीआई दिशानिर्देशों का पालन करने के अधीन है। जब तक संदर्भ में अन्यथा आवश्यक न हो, इस नीति में किसी एक लिंग का उल्लेख दूसरे लिंग को भी शामिल करता है, एकवचन शब्द बहुवचन में शामिल होते हैं और प्राकृतिक व्यक्तियों का उल्लेख आर्टिफिशियल कानूनी व्यक्तियों को भी शामिल करता है और इसके विपरीत भी।

बैंक कौन सा डेटा एकत्र करता है?

1) बैंक अनुमति प्राप्त व्यक्तिगत, वित्तीय और विपणन डेटा एकत्र करता है ताकि उसे प्राप्त किया जा सके, रखा जा सके, संग्रहित किया जा सके, उपयोग किया जा सके, निपटाया जा सके, संभाला जा सके, स्थानांतरित किया जा सके और अन्यथा लागू कानूनों के अनुसार संसाधित किया जा सके।
    a. व्यक्तिगत डेटा: इसमें ग्राहक का नाम, पता, ईमेल पता, फोन/मोबाइल नंबर, केवाईसी/पहचान दस्तावेज़ (उदाहरण: आधार और पैन), बायोमेट्रिक डेटा, डिवाइस और स्थान डेटा आदि शामिल हैं।
    b. वित्तीय डेटा: इसमें ग्राहक के बैंक खाता विवरण, वित्तीय जानकारी, भुगतान क्रेडेंशियल, लेन-देन का डेटा, ऋण विवरण जैसे कि राशि और पुनर्भुगतान, क्रेडिट इतिहास और आय विवरण जैसी जानकारी शामिल है।
    c. विपणन डेटा: इसमें ग्राहक की ऐसी प्राथमिकताएँ शामिल हैं जो बैंक और उसके सेवा प्रदाताओं से विपणन संदेश प्राप्त करने या ग्राहक संचार प्राथमिकताओं से संबंधित हैं।
2) कोई भी व्यक्ति जो किसी विशेष उद्देश्य के लिए बैंक को उपर्युक्त जानकारी देता है, उसे माना जाएगा कि उसने उस उद्देश्य के लिए जानकारी का उपयोग, संरक्षण, संग्रह, संचालन, हस्तांतरण करने की सहमति दी है और इसे बेहतर ग्राहक अनुभव के लिए सेवाएँ प्रदान करने के लिए भी इस्तेमाल किया जा सकता है। किसी विशेष उत्पाद/सेवाओं के लिए ग्राहक द्वारा प्रदान की गई जानकारी का उपयोग बैंक द्वारा प्रदान किए जाने वाले अन्य उत्पादों/सेवाओं के लिए भी किया जा सकता है। ऐसे व्यक्ति को यह नोट करना चाहिए कि किसी भी चैनल के माध्यम से बैंक को प्रदान की गई उपरोक्त जानकारी/डेटा सही और सटीक है और वह सभी साझा की गई, प्रकट की गई, आदान-प्रदान की गई जानकारी/डेटा की सटीकता और पूर्णता सुनिश्चित करने का संकल्प करता है। व्यक्ति आगे यह भी संकल्प करता है कि बैंक को पहले से प्रदान की गई जानकारी/डेटा में किसी भी प्रकार के परिवर्तन की जानकारी अपडेट और सूचित करेगा।
3) ग्राहक व्यक्तिगत डेटा साझा न करने या सहमति वापस लेने का विकल्प चुन सकते हैं, लेकिन ऐसा करने से बैंक द्वारा प्रदान की जाने वाली सेवाओं में सीमाएं आ सकती हैं। हालांकि, ग्राहक किसी भी ऐसे

डेटा/सूचना को वापस नहीं ले पाएंगे, जो किसी भी वैधानिक/नियामक प्रावधान के तहत बैंक को अनिवार्य रूप से प्राप्त करनी होती हैं।

बैंक ग्राहक का डेटा कैसे एकत्र करता है?

4) बैंक ग्राहक जानकारी एकत्र करने के लिए विभिन्न तरीके और माध्यमों का उपयोग करता है ताकि सीधे मेल-मिलाप, ऑनलाइन एप्लिकेशन, सर्वेक्षण, बैंक के कॉल सेंटर के साथ टेलीफोन वार्तालाप और कानून और नियामक दिशानिर्देशों द्वारा अनुमति प्राप्त किसी भी अन्य संचार के माध्यम से सेवाएँ प्रदान की जा सकें।

डेटा एकत्र करने का उद्देश्य:

5) बैंक या इसके सेवा प्रदाता/ठेकेदार ग्राहक की व्यक्तिगत जानकारी को कंप्यूटर पर या अन्यथा, डिजिटल लेंडिंग या बैंक की वेबसाइट, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, कियोस्क्स, टैब बैंकिंग, शाखाओं और एसएमएस(यूएसएसडी) सेवाओं के माध्यम से अन्य गतिविधियों के संबंध में, ग्राहक को श्रेष्ठतम सेवाएँ/उत्पाद प्रदान करने के लिए ग्राहक डेटा का उपयोग व्यापार नियम इंजन निर्णय लेने, सांख्यिकीय विश्लेषण, क्रेडिट स्कोरिंग आदि के लिए कर सकते हैं।
6) बैंक ग्राहक की जानकारी के संग्रह और उपयोग को न्यूनतम आवश्यक स्तर तक सीमित करेगा, ग्राहकों को प्रभावी सेवा प्रदान करने के लिए, बैंक के व्यवसाय का प्रबंधन करने और ग्राहकों को बैंक के उत्पादों, सेवाओं और अन्य सुरक्षा उपायों के बारे में सलाह देने के लिए।
7) बैंक अपने उत्पादों और सेवाओं के संदर्भ में ग्राहक की व्यक्तिगत जानकारी का विश्लेषण करता है, जिसमें आवेदन, क्रेडिट निर्णय, उत्पादों या सेवाओं के लिए पात्रता निर्धारित करना शामिल है। इस प्रक्रिया में स्वचालित प्रोफाइलिंग और निर्णय लेने की प्रक्रिया शामिल हो सकती है, जिसका अर्थ है कि बैंक व्यक्तिगत डेटा को ऐसे सॉफ़्टवेयर का उपयोग करके संसाधित कर सकता है जो व्यक्तिगत पहलुओं का मूल्यांकन करने और जोखिम या परिणामों की भविष्यवाणी करने में सक्षम हो।

बैंक ग्राहक डेटा किसके साथ साझा करता है?

8) ग्राहक का डेटा केवल उस ग्राहक की सहमति से ही एकत्र किया जाएगा और उपयोग किया जाएगा। ग्राहक के पास सहमति वापस लेने का विकल्प होगा। हालांकि, इससे बैंक द्वारा प्रदान की जाने वाली सेवाओं में कुछ सीमाएँ आ सकती हैं। हालांकि, ग्राहक किसी ऐसी सहमति को वापस नहीं ले पाएंगे जो किसी भी वैधानिक/नियामक प्रावधान के तहत बैंक द्वारा अनिवार्य रूप से प्राप्त की जानी हो।
9) बैंक ग्राहक की जानकारी किसी बाहरी संगठन को तभी प्रकट करेगा जब बैंक ने पहले ग्राहक को खुलासों या अनुबंधों में सूचित किया हो और ग्राहक द्वारा अधिकृत किया गया हो या कानून और वैधानिक/नियामक अधिकारियों द्वारा आवश्यकता अनुसार।
10) जब भी बैंक सहायक सेवाएँ प्रदान करने के लिए अन्य संस्थाओं को काम पर रखता है, तो बैंक उनसे अपने गोपनीयता नीति मानकों का पालन करने की अपेक्षा करेगा। .
11) क्रेडिट रिपोर्टिंग, बकाया राशि वसूली, जोखिम प्रबंधन, पहचान सत्यापन, या अपराधों की रोकथाम, पता लगाने, जांच करने सहित साइबर घटनाओं की जांच, अभियोजन और दंड, या जब किसी कानूनी दायित्व के पालन के लिए प्रकटीकरण आवश्यक हो, के उद्देश्य से, बैंक ग्राहक जानकारी को सरकारी एजेंसियों, वैधानिक एजेंसियों के साथ साझा कर सकता है जैसा कि कानून के तहत अनिवार्य हो।

ग्राहक डेटा का संरक्षण:

12) बैंक ग्राहक से एकत्रित व्यक्तिगत डेटा को हमारे सिस्टम या थर्ड पार्टी के पास उतनी ही अवधि तक रखता है, जितनी उस उद्देश्य के लिए आवश्यक है जिसके लिए इसे प्राप्त किया गया है, या यहाँ तक कि लेन-देन या खाते आधारित संबंध की समाप्ति के बाद भी:

a. किसी भी कानूनी और नियामक दायित्वों के पालन के लिए जिनके अधीन हम हैं, या
b. कानूनी दावों की स्थापना, अभ्यास या रक्षा के लिए। . तृतीय-पक्ष लिंक:

13) बैंक की वेबसाइट, मोबाइल बैंकिंग एप्लिकेशन और इंटरनेट बैंकिंग प्लेटफ़ॉर्म में ग्राहक लेन-देन और ऋण कारोबार को सुविधाजनक बनाने के लिए बाहरी सरकारी और निजी संस्थाओं के लिंक हो सकते हैं। जबकि ऐसे लिंक ग्राहक की सुविधा के लिए और नियामक दिशानिर्देशों के अनुसार प्रदान किए जाते हैं, ग्राहक को यह जानना चाहिए कि इन लिंक को एक्सेस करना उनके अपने जोखिम पर है क्योंकि इन वेबसाइटों की अपनी गोपनीयता नीतियाँ हो सकती हैं और हम किसी भी ऐसे लिंक के लिए कोई जिम्मेदारी या उत्तरदायित्व स्वीकार नहीं करते हैं। बैंक जुड़ी वेबसाइटों की जानकारी प्रबंधन प्रथाओं के संबंध में कोई आश्वासन नहीं दे सकता। इसके अलावा, बैंक किसी भी ऐसे व्यक्तिगत डेटा उल्लंघन के लिए जिम्मेदार नहीं है जो ग्राहक की जानकारी जैसे लॉगिन आईडी, पासवर्ड, OTP आदि किसी अन्य व्यक्ति के साथ साझा करने, किसी अन्य दुर्भावनापूर्ण/धोखाधड़ीपूर्ण वेबसाइट/एप्लिकेशन पर देने या किसी अन्य कारण से हुए हों।

सुरक्षा:

14) बैंक सुरक्षित और गोपनीय तरीके से किसी भी जानकारी की सुरक्षा करेगा जो ग्राहक बैंक के साथ साझा करते हैं। बैंक अपने इस परंपरा को जारी रखेगा कि वह ग्राहकों के खाते की लेनदेन जानकारी किसी के साथ साझा नहीं करेगा, सिवाय इसके कि कानून या वैधानिक/नियामक एजेंसियों द्वारा आवश्यक होने पर।
15) बैंक केवल उन्हीं कर्मचारियों को ग्राहक जानकारी तक पहुँच देगा जिन्हें ग्राहक जानकारी को संभालने का अधिकार प्राप्त है। ऐसे कर्मचारी जो बैंक की गोपनीयता वाचा का उल्लंघन करेंगे, उन्हें बैंक की सामान्य अनुशासनात्मक प्रक्रिया का पालन करना होगा।
16) बैंक और बैंक द्वारा नियुक्त LSPs (लेंडिंग सर्विस प्रोवाइडर) विभिन्न तकनीकी मानकों, साइबर सुरक्षा संबंधी आवश्यकताओं, RBI और अन्य एजेंसियों द्वारा आईटी सेवाओं के आउटसोर्सिंग पर दिशानिर्देशों का पालन करते हैं, या समय-समय पर निर्दिष्ट किये गए दिशा-निर्देशों का पालन करते हैं, ताकि डिजिटल लेंडिंग की प्रक्रिया को अंजाम दिया जा सके।

सोशल मीडिया:

17) बैंक विभिन्न सुविधाएँ प्रदान करता है जैसे कि बैंक की वेबसाइट, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, टैब बैंकिंग/फीट-ऑन-स्ट्रीट के माध्यम से असिस्टेड डिजिटल बैंकिंग, डिजिटल बैंकिंग यूनिट्स (DBUs), सेल्फ-सर्विस कियोस्क या किसी अन्य आगामी डिजिटल चैनल्स के माध्यम से ग्राहकों का डिजिटल ऑन-बोर्डिंग। इस प्रकार प्रदान किए गए उत्पाद / सेवाएं बैंक की लागू नीतियों / दिशानिर्देशों के अनुसार संचालित होंगी।
    a. डिजिटल बैंकिंग उत्पाद और सेवाओं पर नीति,
    b. जमा नीति,
    c. ग्राहक को जानें (KYC) / मनी लॉन्ड्रिंग विरोधी (AML) / आतंकवाद वित्त पोषण विरोध (CFT) नीति,
    d. डिजिटल भुगतान सुरक्षा नीति, डिजिटल भुगतान सुरक्षा नियंत्रणों पर SOP और डिजिटल लेंडिंग नीति - RBI

ड्यू डिलिजेंस:

18) बैंक द्वारा एकत्र की गई जानकारी की सटीकता सुनिश्चित करने के लिए उचित परिश्रम अपनाया जाएगा।
19) बैंक स्वत: एंटी-मनी लॉन्ड्रिंग और प्रतिबंध जांच भी कर सकता है। इसका मतलब है कि यदि प्रक्रियाओं से पता चलता है कि ग्राहक का व्यवहार मनी लॉन्ड्रिंग या ज्ञात धोखाधड़ी प्रवृत्ति के अनुरूप है, पिछली प्रस्तुतियों के साथ असंगत है, या उन्होंने अपनी सच्ची पहचान जानबूझकर छुपाई है, तो बैंक स्वचालित रूप से यह तय कर सकता है कि ग्राहक धोखाधड़ी या मनी लॉन्ड्रिंग का जोखिम रखते हैं। बैंक इस तरह

के सभी डेटा/सूचना उल्लंघनों की रिपोर्ट कानून के तहत निर्धारित कानूनी/नियामक प्राधिकरण को करेगा।

20) बैंक सुरक्षा उद्देश्यों के लिए ग्राहक के साथ संचार को रिकॉर्ड और मॉनिटर कर सकता है।

डेटा नष्ट करना:

21) संग्रहित डेटा की समय वैधता को ध्यान में रखते हुए, डेटा नष्ट करने की प्रक्रिया लागू की जाएगी। डेटा की महत्वता और प्रासंगिकता के अनुसार, संग्रहित डेटा और मीडिया को समय-समय पर नष्ट किया जाएगा ताकि गलत इस्तेमाल से बचा जा सके और निर्धारित संग्रह अवधि के बाद प्रणाली में पुराने डेटा के गलती से लोड होने की संभावना को रोका जा सके। जब जानकारी अन्य रूपों में उपलब्ध हो या अन्य साधनों से निकाली जा सके, तो ऐसे पुराने और गैर-महत्वपूर्ण डेटा जो बैकअप टेप्स में उपलब्ध हैं, वह अप्रचलित हो जाते हैं। एक वर्ष की अवधि के बाद ऐसे डेटा बैकअप को नष्ट किया जा सकता है जब यह सुनिश्चित किया जाए कि अन्य रूपों में पर्याप्त बैकअप उपलब्ध हैं और बाहरी मीडिया / स्टोरेज को उचित फॉर्मेटिंग प्रक्रियाओं के साथ पुन: उपयोग किया जा सकता है।

22) ऐसे अप्रचलित और गैर-आवश्यक डेटा और मीडिया को नष्ट करते समय, मीडिया और डेटा और नष्ट करने के तरीके के बारे में उचित रिकॉर्ड रखा जाएगा। यह सुनिश्चित करने के लिए उचित प्रक्रियाएं स्थापित की जाएंगी कि डेटा और मीडिया पूरी तरह से नष्ट हो जाएं और पुनर्प्राप्ति की कोई संभावना न रहे। डेटा को डिगॉसिंग करने और थर्मल या रासायनिक माध्यम से मीडिया को नष्ट करने जैसे तरीकों का उपयोग किया जाना चाहिए।

23) गतिविधि के विवरण के साथ डेटा नाश लॉग रखा जाएगा। यदि यह गतिविधि किसी तीसरे पक्ष को आउटसोर्स की जाती है, तो बैंक विक्रेता से एक डेटा नाश प्रमाण पत्र प्राप्त करेगा कि डेटा सफलतापूर्वक मिटा दिया गया और इसे पुनर्प्राप्त नहीं किया जा सकता।

शिकायत निवारण तंत्र

24) बैंक ने डिजिटल व्यक्तिगत डेटा सुरक्षा से संबंधित ग्राहकों की सभी शिकायतों के निवारण के लिए एक नोडल शिकायत निवारण अधिकारी नियुक्त किया है। विवरण इस प्रकार हैं: नाम-

श्री अमित चौधरी
पद: महाप्रबंधक [KYC/AML]
पता: इंडियन बैंक,मुख्यालय,

संख्या 66, राजाजी सलाई,

चेन्नई – 600001
ईमेल: nodalofficer[at]indianbank[dot]co[dot]in

https://apps.indianbank.bank.in/cgrc/frm_cgrs_cust_welcome_new_UA1.aspx

बैंक लगातार यह सुनिश्चित करेगा कि ग्राहक की गोपनीयता का सम्मान किया जाए और बैंक का व्यवसाय उस तरीके से संचालित किया जाए जो बैंक के वादे को पूरा करता हो। इंडियन बैंक द्वारा प्रकाशित सभी सामग्री सुरक्षित हैं और उनका स्वामित्व या नियंत्रण इंडियन बैंक या उस पार्टी के पास है जिसे सामग्री के प्रदाता के रूप में मान्यता दी गई है।