कफिनो कैपिटल प्राइवेट लिमिटेड

प्राइवेसी पॉलिसी

विवरण (Detail)	मान (Value)
दस्तावेज़ संख्या (Doc. No.)	टीसीपीएल-आई एस एम एस-पी एल 25
जारी संख्या और तिथि (Issue No. & Date)	संस्करण 2.0 – 07-11-2025
सूचना का वर्गीकरण (Classification of Information)	आंतरिक और संरक्षित

टेबल ऑफ़ कंटेंट

1. मकसद
2. स्कोप
3. रोल और ज़िम्मेदारियां
4. एब्रीविएशन और डेफिनिशन
5. फॉर्म
6. पॉलिसी
7. हम जो जानकारी इकट्ठा करते हैं
8. सहमति और डेटा कलेक्शन फ्रेमवर्क
9. डिजिटल लेंडिंग गाइडलाइंस कंप्लायंस
10. हम आपकी पर्सनल जानकारी के साथ क्या करते हैं
11. डेटा शेयरिंग और थर्ड-पार्टी डिस्क्लोजर
12. क्रॉस-बॉर्डर डेटा ट्रांसफर कंप्लायंस
13. सेक्टर-स्पेसिफिक डेटा ट्रांसफर और लोकलाइज़ेशन रेगुलेशन
14. हम आपकी पर्सनल जानकारी कब तक रखेंगे?
15. इन्फॉर्मेशन सिक्योरिटी मेज़र
16. कुकीज़ का इस्तेमाल कैसे किया जाता है?
17. हमसे कैसे संपर्क करें?
18. कानूनी नोटिस
19. इस प्राइवेसी स्टेटमेंट में बदलाव
20. रेफरेंस डॉक्यूमेंट्स
21. एनफोर्समेंट

22. पॉलिसी डॉक्यूमेंट मैनेजमेंट

1. मकसद

इस पॉलिसी का मकसद पर्सनल जानकारी (जिसमें पर्सनली आइडेंटिफ़ाएबल जानकारी या PII शामिल है) और सेंसिटिव पर्सनल डेटा या जानकारी (SPDI) को सुरक्षित रखना है, इसके लिए पूरे ऑर्गनाइज़ेशन में सही कंट्रोल लगाए जाएंगे, समय-समय पर उनका रिव्यू किया जाएगा और ज़रूरत के हिसाब से उनमें सुधार किया जाएगा।

ऑर्गनाइज़ेशन यह पक्का करता है कि कस्टमर्स प्राइवेसी से जुड़ी ज़रूरी कानूनी ज़रूरतों और कॉन्ट्रैक्ट की ज़रूरतों का पालन करें, जिसमें शामिल हैं:

- भारतीय रिज़र्व बैंक (RBI) की जारी डिजिटल लेंडिंग गाइडलाइंस
- इन्फॉर्मेशन टेक्नोलॉजी (रीज़नेबल सिक्योरिटी प्रैक्टिस और प्रोसीजर और सेंसिटिव पर्सनल डेटा या जानकारी) रूल्स, 2011 ("SPDI रूल्स")
- डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 और उससे जुड़े रेगुलेशन
- डिजिटल लेंडिंग, आउटसोर्सिंग और डेटा स्टोरेज पर RBI की गाइडलाइंस
- क्रेडिट ब्यूरो रेगुलेशन और सेक्टोरल डेटा प्रोटेक्शन ज़रूरतें
- क्रॉस-बॉर्डर डेटा ट्रांसफर के बारे में सभी लागू लोकल, स्टेट और सेंट्रल गवर्नमेंट रेगुलेशन

2. स्कोप

- इस पॉलिसी के स्कोप में शामिल हैं:
- TCPL के सभी एम्प्लॉई और हमारे बिज़नेस एसोसिएट्स जिनके पास पर्सनल जानकारी और सेंसिटिव पर्सनल डेटा के कलेक्शन, इस्तेमाल, रिटेंशन, डिस्क्लोज़र और डिस्पोज़ल के लिए ज़िम्मेदारी है या है
- TCPL या उसके एफिलिएट्स द्वारा सीधे कस्टमर्स से TCPL के ऑनलाइन पोर्टल, इलेक्ट्रॉनिक कम्युनिकेशन या बिज़नेस के ज़रिए कलेक्ट की गई सभी पर्सनल जानकारी और सेंसिटिव पर्सनल डेटा या जानकारी प्रोसेस
- सभी क्रॉस-बॉर्डर डेटा फ़्लो और इंटरनेशनल डेटा ट्रांसफ़र
- डेटा प्रोसेसिंग में शामिल सभी थर्ड-पार्टी सर्विस प्रोवाइडर, वेंडर और आउटसोर्सिंग पार्टनर

3. भूमिकाएँ और ज़िम्मेदारियाँ

भूमिका (Role)	**जिम्मेदारी (Responsibility)**
मुख्य सूचना सुरक्षा अधिकारी (CISO)	सभी अनिवार्य दस्तावेज़ों और अनुपालन नीतियों को मंज़ूरी दें। डेटा संरक्षण और गोपनीयता अनुपालन की निगरानी। प्राधिकरण और नियामक निकायों के साथ अनुमोदन और संचार। सुनिश्चित करें कि सीमा-पार डेटा हस्तांतरण अनुपालन ढाँचा मौजूद है।

अनुपालन अधिकारी / कानूनी टीम	डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 की धारा 16 के तहत सूचनाओं के लिए नियामक निगरानी बनाए रखें। MeitY, RBI, और डेटा संरक्षण बोर्ड से अपडेट की निगरानी करें। सीमा-पार डेटा प्रवाह की सूची को बनाए रखें और अद्यतन करें। सभी नए सीमा-पार डेटा हस्तांतरणों और तृतीय-पक्ष सेवाओं की समीक्षा करें और उन्हें मंज़ूरी दें।
	क्षेत्र-विशिष्ट नियामक अनुपालन मूल्यांकनों का समन्वय करें।
आईटी/इंफ्रास्ट्रक्चर प्रमुख	डेटा सुरक्षा के लिए तकनीकी नियंत्रणों को लागू करें। विक्रेता संबंधों का प्रबंधन करें और डेटा स्थानीयकरण आवश्यकताओं को सुनिश्चित करें। अनुमोदित क्षेत्राधिकारों के भीतर वैकल्पिक डेटा भंडारण समाधानों को बनाए रखें। प्रतिबंधित देश की सूचनाओं पर तुरंत प्रतिक्रिया दें।
मानव संसाधन प्रमुख	इस नीति का दस्तावेज़ीकरण करें, संचार करें, और कार्यान्वयन और रखरखाव सुनिश्चित करें। सीमा-पार डेटा हस्तांतरण प्रतिबंधों पर कर्मचारियों को जागरूकता प्रशिक्षण प्रदान करें। सुनिश्चित करें कि सभी कर्मचारी डेटा हैंडलिंग आवश्यकताओं को समझते हैं।

4. शॉर्ट फ़ॉर्म और डेफ़िनिशन

4.1 शॉर्ट फ़ॉर्म

संक्षिप्त रूप (Abbreviation)	**विस्तार (Expansion)**
टीसी पीएल	टेकफिनो कैपिटल प्राइवेट लिमिटेड
डीपीडीपी एक्ट	डेटा संरक्षण अधिनियम, 2023
एसपी डीआई रूल्स	सूचना प्रौद्योगिकी (उचित सुरक्षा पद्धतियाँ और प्रक्रियाएँ तथा संवेदनशील व्यक्तिगत डेटा या सूचना) नियम, 2011
आरबीआई	भारतीय रिजर्व बैंक
मे आईटी वाई	इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय
डीएलजी	डिजिटल ऋण दिशानिर्देश (RBI)
पीआईआई	व्यक्तिगत रूप से पहचान योग्य जानकारी
एसपी डीआई	संवेदनशील व्यक्तिगत डेटा या सूचना
एमएलआई	सदस्य ऋण देने वाली संस्था
सीआईएसओ	मुख्य सूचना सुरक्षा अधिकारी
सास	सेवा के रूप में सॉफ्टवेयर

4.2 परिभाषाएँ

शर्तें (Terms)	परिभाषाएँ (Definitions)
व्यक्तिगत जानकारी	कोई भी जानकारी जो किसी प्राकृतिक व्यक्ति से सीधे या अप्रत्यक्ष रूप से, TCPL के पास उपलब्ध या उपलब्ध होने की संभावना वाली अन्य जानकारी के संयोजन में संबंधित है, ऐसे व्यक्ति की पहचान करने में सक्षम है। इसमें नाम, ईमेल, संपर्क विवरण, पता, पदनाम, क्रेडिट जानकारी, और कोई अन्य पहचान योग्य डेटा शामिल है।
संवेदनशील व्यक्तिगत डेटा या जानकारी (SPDI)	एसपी डीआई नियम, 2011 के नियम 3 के तहत परिभाषित, इसमें शामिल हैं: पासवर्ड; वित्तीय जानकारी जैसे बैंक खाता, क्रेडिट कार्ड, डेबिट कार्ड विवरण; शारीरिक, शारीरिक और मानसिक स्वास्थ्य की स्थिति; यौन रुझान; मेडिकल रिकॉर्ड और इतिहास; बायोमेट्रिक जानकारी; आनुवंशिक जानकारी; ट्रेडिंग और वित्तीय इतिहास; आगे साझा न किए जाने के स्पष्ट उद्देश्य से प्रदान की गई कोई भी जानकारी।
सहमति	डेटा विषय द्वारा उनकी व्यक्तिगत जानकारी या एसपी डीआई के संग्रह, प्रसंस्करण, उपयोग और प्रकटीकरण के लिए स्वैच्छिक, सूचित और स्पष्ट समझौता। सहमति स्पष्ट, पूर्व और दस्तावेजी ऑडिट ट्रेल के साथ क्लिक-रैप तंत्र के माध्यम से प्राप्त की जानी चाहिए।
क्लिक-रैप तंत्र	एक इलेक्ट्रॉनिक सहमति पद्धति जहां डेटा एकत्र या संसाधित होने से पहले नियमों की समझ और स्वीकृति की पुष्टि करने के लिए उपयोगकर्ता को सक्रिय रूप से "मैं सहमत हूँ," "स्वीकार करें," या इसी तरह की कार्रवाई पर क्लिक करना होगा। इलेक्ट्रॉनिक ऑडिट ट्रेल बनाने के लिए सिस्टम को टाइमस्टैम्प, उपयोगकर्ता कार्रवाई और आईपी पता रिकॉर्ड करना होगा।
सीमा-पार डेटा स्थानांतरण	क्लाउड स्टोरेज, सास प्लेटफॉर्म, आउटसोर्सिंग साझेदारी, अंतर्राष्ट्रीय कार्यालयों, या किसी अन्य माध्यम से भारत से भारत के बाहर किसी भी देश में व्यक्तिगत जानकारी या एसपी डीआई का संचलन।
प्रतिबंधित देश	कोई भी देश या क्षेत्राधिकार जिसे डीपीडीपी अधिनियम, 2023 की धारा 16 के तहत व्यक्तिगत डेटा स्थानांतरण के लिए निषिद्ध के रूप में भारत की केंद्र सरकार द्वारा अधिसूचित किया गया है।
डेटा स्थानीयकरण	लागू कानूनों या विनियमों द्वारा अनिवार्य रूप से, किसी विशिष्ट भौगोलिक क्षेत्राधिकार, आमतौर पर भारत के भीतर व्यक्तिगत जानकारी या एसपी डीआई को बनाए रखने की आवश्यकता या अभ्यास।

5. फ़ॉर्म

डॉक्यूमेंट का नाम

फ़ॉर्म नंबर

6. पॉलिसी

TCPL अपने कस्टमर्स की प्राइवेसी, कॉन्फिडेंशियलिटी और ऑर्गनाइज़ेशन के पास मौजूद उनकी पर्सनल जानकारी की सिक्योरिटी से जुड़ी उम्मीदों को समझता है।

TCPL, मेंबर लेंडिंग इंस्टीट्यूशन्स (MLIs) के साथ काम कर रहा है, जो बैंकिंग और फाइनेंशियल सर्विस इंडस्ट्री में हैं और अलग-अलग क्रेडिट गारंटी स्कीम के तहत TCPL के साथ रजिस्टर्ड हैं। बॉरोअर्स की पर्सनल जानकारी को सुरक्षित रखना, इकट्ठा की गई जानकारी का इस्तेमाल सिर्फ़ सही बिज़नेस और डेटा वैलिडेशन के मकसद से करना, और जानकारी के किसी भी गलत इस्तेमाल को रोकना TCPL की सबसे बड़ी प्राथमिकता है।

TCPL ने एक पूरी प्राइवेसी पॉलिसी अपनाई है जिसका मकसद बॉरोअर्स और दूसरे डेटा सब्जेक्ट्स की पर्सनल जानकारी को सुरक्षित रखना है, जिन्हें मेंबर लेंडिंग इंस्टीट्यूशन्स (MLIs) और दूसरे बिज़नेस पार्टनर्स ने सौंपा और बताया है।

प्राइवेसी पॉलिसी यह तय करती है कि ऑर्गनाइज़ेशन कैसे:

- पर्सनल जानकारी और सेंसिटिव पर्सनल डेटा इकट्ठा करता है
- ऐसी जानकारी का इस्तेमाल करता है, बताता है, स्टोर करता है और सुरक्षित रखता है
- DPDP एक्ट के सेक्शन 16 और RBI गाइडलाइंस के हिसाब से क्रॉस-बॉर्डर ट्रांसफर मैनेज करता है
- रखरखाव पीरियड के आखिर में पर्सनल जानकारी को डिस्पोज़ करता है
- डिजिटल लेंडिंग गाइडलाइंस, खासकर पैराग्राफ 10 और 12 का पालन पक्का करता है

TCPL ये करने के लिए कमिटेड है:

- सभी डेटा इकट्ठा करने और प्रोसेसिंग के लिए क्लिक-रैप मैकेनिज्म के ज़रिए साफ़, पहले से मंज़ूरी लेना
- सभी डेटा हैंडलिंग एक्टिविटीज़ में ट्रांसपेरेंसी बनाए रखना
- डेटा सब्जेक्ट्स के अपने डेटा को एक्सेस करने, ठीक करने, डिलीट करने और पोर्ट करने के अधिकारों का सम्मान करना
- ISO 27001:2022 के हिसाब से मज़बूत सिक्योरिटी कंट्रोल लागू करना
- सभी सेक्टर-स्पेसिफिक रेगुलेशन का पालन करना, खासकर डिजिटल लेंडिंग और डेटा लोकलाइज़ेशन पर RBI गाइडलाइंस का
- क्रॉस-बॉर्डर डेटा ट्रांसफर प्रैक्टिस का रेगुलर ऑडिट और अपडेट करना

7. हम जो जानकारी इकट्ठा करते हैं

हम डिजिटल लेंडिंग गाइडलाइंस और SPDI नियमों का सख्ती से पालन करते हुए, सिर्फ़ सही बिज़नेस के मकसद के लिए ज़रूरी जानकारी इकट्ठा करते हैं।

7.1 पर्सनल जानकारी

आपको ये पर्सनल जानकारी देनी पड़ सकती है:

- पूरा नाम
- ईमेल ID और कॉन्टैक्ट डिटेल्स (फ़ोन, मोबाइल)
- रहने का पता और बातचीत का पता
- डेज़िग्नेशन और नौकरी की जानकारी
- क्रेडिट जानकारी और फ़ाइनेंशियल हिस्ट्री
- उधार लेने वाले की पहचान की जानकारी
- यूनिक आइडेंटिफ़िकेशन नंबर (जैसा लागू हो)

7.2 सेंसिटिव पर्सनल डेटा या जानकारी (SPDI)

जब लागू हो और साफ़ सहमति से, हम ये इकट्ठा कर सकते हैं:

- फ़ाइनेंशियल जानकारी (बैंक अकाउंट डिटेल्स, क्रेडिट कार्ड, डेबिट कार्ड नंबर)
- मेडिकल रिकॉर्ड और हेल्थ से जुड़ी जानकारी
- बायोमेट्रिक जानकारी (फ़िंगरप्रिंट, आइरिस स्कैन, लागू नियमों के अनुसार)
- फ़िज़िकल, फ़िज़ियोलॉजिकल और मेंटल हेल्थ स्टेटस
- जेनेटिक जानकारी
- ट्रेडिंग हिस्ट्री और फ़ाइनेंशियल परफ़ॉर्मेंस डेटा
- पासवर्ड और सिक्योरिटी क्रेडेंशियल

7.3 इकट्ठा करने के तरीके

हम पर्सनल जानकारी इकट्ठा कर सकते हैं:

- जब आप साइन अप करते हैं तो सीधे आपसे, रजिस्टर करें, सर्विस का अनुरोध करें, या अपनी मर्ज़ी से जानकारी दें
- अपने एम्प्लॉयर या मेंबर लेंडिंग इंस्टीट्यूशन (MLI) के ज़रिए
- सार्वजनिक रूप से उपलब्ध डेटाबेस से (जहां कानून द्वारा अनुमति हो)
- थर्ड-पार्टी पार्टनर से जिनके साथ आपने जानकारी शेयर करने की अनुमति दी है
- हमारे डिजिटल प्लेटफ़ॉर्म पर एनालिटिकल टूल और कुकीज़ के ज़रिए

8. सहमति और डेटा कलेक्शन फ्रेमवर्क

8.1 साफ़ सहमति की ज़रूरत

TCPL किसी भी पर्सनल जानकारी या SPDI को इकट्ठा करने, प्रोसेस करने या शेयर करने से पहले सभी डेटा सब्जेक्ट से साफ़, पहले से लिखी हुई सहमति लेगा। सहमति इस तरह होगी:

- अपनी मर्ज़ी से: ज़बरदस्ती या दबाव में नहीं ली गई
- जानकारी दी गई: डेटा सब्जेक्ट को डेटा कलेक्शन का मकसद, दायरा और असर समझना चाहिए
- खास: कलेक्शन और प्रोसेसिंग के हर मकसद के लिए साफ़ तौर पर बताया गया हो
- साफ़: साफ़ तौर पर पॉज़िटिव एक्शन के ज़रिए बताया गया

8.2 क्लिक-रैप सहमति का तरीका (रूल 5(1) - SPDI रूल्स, 2011)

पर्सनल जानकारी और SPDI कलेक्शन के लिए सभी सहमति, SPDI रूल्स, 2011 के रूल 5(1) के हिसाब से इलेक्ट्रॉनिक क्लिक-रैप तरीके से ली जाएगी। इस तरीके में ये चीज़ें शामिल होंगी:

ज़रूरी चीज़ें:

1. साफ़ और साफ़ दिखने वाला नोटिस: कोई भी डेटा कलेक्शन से पहले, एक खास नोटिस में ये दिखाना होगा: डेटा कलेक्शन का मकसद; इकट्ठा किया जा रहा डेटा का टाइप; डेटा का इस्तेमाल और शेयर करना; डेटा रखने का समय; डेटा सब्जेक्ट के अधिकार।

2. एक्टिव ऑप्ट-इन: डेटा सब्जेक्ट को सहमति दिखाने के लिए एक्टिव रूप से "मैं सहमत हूँ," "स्वीकार करो," "कन्फर्म करो," या इसी तरह के बटन पर क्लिक करना होगा। पहले से चेक किए गए बॉक्स की इजाज़त नहीं है।

3. ऑडिट ट्रेल: सिस्टम को अपने आप रिकॉर्ड करना और बनाए रखना होगा: सहमति का टाइमस्टैम्प; डेटा सब्जेक्ट का IP एड्रेस; सहमति देने वाले पक्ष का यूनिक आइडेंटिफायर या ईमेल; सहमति की शर्तों का स्वीकृत वर्शन; सहमति का तरीका (क्लिक-रैप); सहमति में कोई भी बदलाव।

4. एक्सेसिबिलिटी: सहमति फ़ॉर्म इस तरह होने चाहिए: आसान, समझने लायक भाषा में; कई भाषाओं में उपलब्ध (अंग्रेजी, हिंदी और स्थानीय भाषाएँ जहाँ लागू हो); विकलांग लोगों के लिए एक्सेसिबल; आसानी से प्रिंट और डाउनलोड किया जा सके।

5. अलग-अलग सहमति: अलग-अलग मकसद के लिए अलग-अलग सहमति फ़ॉर्म होंगे: आम पर्सनल जानकारी इकट्ठा करने के लिए सहमति; SPDI इकट्ठा करने के लिए अलग सहमति; तीसरे पक्ष के साथ डेटा शेयर करने के लिए अलग सहमति; क्रॉस-बॉर्डर डेटा ट्रांसफ़र के लिए अलग सहमति; मार्केटिंग या एनालिटिक्स के मकसद के लिए अलग सहमति।

6. रद्द करना: डेटा सब्जेक्ट को admin@techfino.in पर रिक्वेस्ट सबमिट करके किसी भी समय सहमति वापस लेने में सक्षम होना चाहिए। TCPL सहमति वापस लेने के 5 बिज़नेस दिनों के अंदर प्रोसेसिंग बंद कर देगा।

8.3 थर्ड-पार्टी शेयरिंग के लिए सहमति

किसी थर्ड पार्टी के साथ पर्सनल जानकारी या SPDI शेयर करने से पहले, TCPL को ये करना होगा:

- डेटा सब्जेक्ट से खास लिखित सहमति लेनी होगी
- थर्ड पार्टी या थर्ड पार्टी की कैटेगरी की पहचान बतानी होगी
- शेयर करने का मकसद बताना होगा
- यह बताना होगा कि कौन सा डेटा शेयर किया जाएगा

- डेटा सब्जेक्ट को TCPL सर्विस इस्तेमाल करने की उनकी क्षमता पर असर डाले बिना शेयर करने से मना करने की इजाज़त देनी होगी

9. डिजिटल लेंडिंग गाइडलाइंस का पालन

TCPL इन तरीकों से RBI की डिजिटल लेंडिंग गाइडलाइंस का पालन पक्का करता है:

डेटा कलेक्शन स्टैंडर्ड:

- पर्सनल और फाइनेंशियल जानकारी का कलेक्शन पूरी तरह से ज़रूरत के हिसाब से होता है
- डेटा कलेक्शन सिर्फ़ क्रेडिट असेसमेंट, लोन शुरू करने और रेगुलेटरी कम्प्लायंस के लिए ज़रूरी जानकारी तक ही सीमित है
- कोई भी बहुत ज़्यादा या गैर-ज़रूरी डेटा इकट्ठा नहीं किया जाता है
- डेटा सब्जेक्ट को हर डेटा एलिमेंट के बिज़नेस मकसद के बारे में साफ़ तौर पर बताया जाता है

मकसद की लिमिट:

- पर्सनल जानकारी का इस्तेमाल सिर्फ़ उसी मकसद के लिए किया जाता है जिसके लिए इसे इकट्ठा किया गया था
- ओरिजिनल मकसद से अलग किसी भी इस्तेमाल के लिए नई, साफ़ सहमति की ज़रूरत होती है
- TCPL अलग से सहमति लिए बिना डेटा का दोबारा इस्तेमाल दूसरे मकसदों के लिए नहीं करेगा
- एनालिटिक्स, मार्केटिंग या दूसरे मकसदों के लिए डेटा के सभी इस्तेमाल के लिए साफ़ सहमति की ज़रूरत होती है

थर्ड-पार्टी शेयरिंग कंट्रोल:

- डेटा सब्जेक्ट की साफ़, पहले से सहमति के बिना पर्सनल जानकारी थर्ड पार्टी के साथ शेयर नहीं की जाती है
- ऐसे मामलों में जहाँ शेयरिंग कानूनी तौर पर ज़रूरी है (RBI, क्रेडिट ब्यूरो रेगुलेशन, कानूनी ज़रूरतों के हिसाब से), TCPL डेटा सब्जेक्ट को ऐसी ज़रूरी शेयरिंग के बारे में बताएगा
- क्रेडिट ब्यूरो शेयरिंग सिर्फ़ क्रेडिट रिपोर्टिंग के मकसद के लिए ज़रूरी जानकारी तक ही सीमित है
- कोई डेटा नहीं प्रमोशनल, मार्केटिंग, या गैर-ज़रूरी थर्ड-पार्टी मकसद के लिए डेटा सब्जेक्ट की साफ़ सहमति के बिना शेयर किया जाता है

बॉरोअर एम्पावरमेंट:

- TCPL बॉरोअर्स को इस बारे में साफ़ जानकारी देता है कि उनके डेटा का एक्सेस किसके पास है
- बॉरोअर्स उन सभी थर्ड पार्टी को जानने का रिक्वेस्ट कर सकते हैं जिनके साथ उनका डेटा शेयर किया जाता है
- बॉरोअर्स डेटा शेयरिंग पर रोक लगा सकते हैं (जहां कानूनी तौर पर इजाज़त हो)
- बॉरोअर्स अपने अकाउंट से जुड़े सभी डेटा एक्सेस और शेयरिंग इवेंट्स का ऑडिट लॉग देख सकते हैं

- बॉरोअर्स रिक्वेस्ट करने पर, कानूनी रिटेंशन ज़रूरतों के तहत, TCPL सिस्टम से डेटा मिटाने और हटाने का काम शुरू कर सकते हैं

डेटा प्रैक्टिस में ट्रांसपेरेंसी:

- यह प्राइवेसी पॉलिसी सभी डेटा हैंडलिंग प्रैक्टिस को साफ़ तौर पर बताती है
- डेटा सब्जेक्ट्स को यह साफ़ तौर पर बताया जाता है कि उनके डेटा का इस्तेमाल, शेयर, स्टोर और प्रोटेक्ट कैसे किया जाएगा
- TCPL एक डेटा रजिस्टर रखता है जिसमें सभी डेटा कलेक्शन, प्रोसेसिंग और शेयरिंग एक्टिविटीज़ का डॉक्यूमेंटेशन होता है
- रेगुलेटरी अथॉरिटीज़ के लिए रिक्वेस्ट करने पर रेगुलर ट्रांसपेरेंसी रिपोर्ट तैयार की जाती हैं

अका उंटेबिलिटी मैकेनिज्म:

- एक डेडिकेटेड कम्प्लायंस टीम सभी डेटा हैंडलिंग एक्टिविटीज़ की देखरेख करती है
- इस पॉलिसी और लागू कानूनों का पालन पक्का करने के लिए रेगुलर इंटरनल ऑडिट किए जाते हैं

  सभी डेटा एक्सेस, प्रोसेसिंग और शेयरिंग के लिए एक ऑडिट ट्रेल बनाए रखा जाता है।
- सीनियर मैनेजमेंट हर तीन महीने में डेटा हैंडलिंग प्रैक्टिस का रिव्यू करता है।
- नॉन-कम्प्लायंस की जानकारी तुरंत CISO और कम्प्लायंस ऑफिसर को दी जाती है।

शिकायत का समाधान:

- डेटा सब्जेक्ट admin@techfino.in पर प्राइवेसी शिकायतें सबमिट कर सकते हैं।
- शिकायतों को 5 बिज़नेस दिनों के अंदर स्वीकार किया जाता है।
- TCPL 30 दिनों के अंदर शिकायतों को हल करने का वादा करता है।
- अगर डेटा सब्जेक्ट TCPL के जवाब से संतुष्ट नहीं हैं, तो वे RBI या संबंधित अधिकारियों से संपर्क कर सकते हैं।

10. हम आपकी पर्सनल जानकारी का क्या करते हैं?

10.1 इस्तेमाल का मकसद

हम पर्सनल जानकारी और SPDI का इस्तेमाल सिर्फ़ उन्हीं खास मकसदों के लिए करते हैं जिनके लिए यह दी गई है और उन कम्पैटिबल मकसदों के लिए जिनकी डेटा सब्जेक्ट उम्मीद कर सकते हैं। इन मकसदों में शामिल हैं:

लेजिटिमेट बिज़नेस मकसद:

- क्रेडिट असेसमेंट और लोन अंडरराइटिंग
- लोन डिस्बर्समेंट और रीपेमेंट मैनेजमेंट

- RBI और क्रेडिट ब्यूरो को रेगुलेटरी कम्प्लायंस और रिपोर्टिंग
- आइडेंटिटी वेरिफिकेशन और KYC (नो योर कस्टमर) की ज़रूरतें
- फ्रॉड की रोकथाम और पता लगाना
- कस्टमर सर्विस और सपोर्ट
- रिकॉर्ड अपडेट करना और कस्टमर की सही जानकारी बनाए रखना

ज़रूरी ऑपरेशनल मकसद:

- बॉरोअर्स और मेंबर लेंडिंग इंस्टीट्यूशन्स (MLIs) के साथ कॉन्ट्रैक्ट के तहत जिम्मेदारियों को मैनेज, एडमिनिस्टर और पूरा करना
- सरकार, RBI, कोर्ट या दूसरी अथॉरिटीज़ की कानूनी और रेगुलेटरी ज़रूरतों का पालन करना
- ऑडिट और कम्प्लायंस के मकसदों के लिए रिकॉर्ड बनाए रखना
- अनऑथराइज़्ड एक्सेस या फ्रॉड को रोकना या पता लगाना

एनालिटिकल और इम्प्रूवमेंट (सिर्फ़ साफ़ सहमति से):

- बिज़नेस इंटेलिजेंस के लिए बॉरोअर डेटा में ट्रेंड्स का एनालिसिस करना (सिर्फ़ अलग सहमति से)
- हमारी सर्विसेज़ और यूज़र एक्सपीरियंस को बेहतर बनाना (सिर्फ़ अलग सहमति से)
- उधार देने के तरीकों और मार्केट ट्रेंड्स पर रिसर्च करना (सिर्फ़ एनॉनिमाइज़्ड/स्यूडोनिमाइज़्ड डेटा के साथ)

11. डेटा शेयरिंग और थर्ड-पार्टी डिस्क्लोजर

11.1 नॉन-शेयरिंग कमिटमेंट

TCPL डेटा शेयरिंग के बारे में इन सिद्धांतों को मानता है:

- हम इस पॉलिसी में साफ़ तौर पर इजाज़त दिए जाने के अलावा किसी भी थर्ड पार्टी के साथ पर्सनल डेटा शेयर या बेचते नहीं हैं
- हम मार्केटिंग, एडवरटाइजिंग या ब्रोकर अरेंजमेंट के ज़रिए पर्सनल डेटा से कमाई नहीं करते हैं
- हम कमर्शियल फायदे के लिए डेटा ब्रोकर या कमर्शियल एंटिटी को पर्सनल डेटा ट्रांसफर नहीं करते हैं

11.2 इजाज़त वाली डेटा शेयरिंग

पर्सनल जानकारी या SPDI सिर्फ़ इन हालात में थर्ड पार्टी के साथ शेयर की जा सकती है:

1. डेटा सब्जेक्ट की साफ़ सहमति से

TCPL डेटा सब्जेक्ट को इन चीज़ों का साफ़ डिस्क्लोजर देता है: थर्ड पार्टी की पहचान या कैटेगरी; शेयर करने का मकसद; कौन सा खास डेटा शेयर किया जाएगा; थर्ड पार्टी कितने समय तक एक्सेस कर पाएंगे। डेटा सब्जेक्ट TCPL सर्विस तक अपने एक्सेस पर पेनल्टी लगाए बिना शेयर करने से मना कर सकते हैं।

2. कानूनी तौर पर ज़रूरी जानकारी के साथ

- भारतीय रिज़र्व बैंक (RBI): डिजिटल लेंडिंग गाइडलाइंस के हिसाब से लोन डेटा, बॉरोअर की जानकारी और कम्प्लायंस रिपोर्ट
- क्रेडिट ब्यूरो: क्रेडिट हिस्ट्री और रीपेमेंट की जानकारी (क्रेडिट ब्यूरो रेगुलेशन में बताए गए मकसद तक ही सीमित)
- सरकारी एजेंसियां: टैक्स अथॉरिटी, लॉ एनफोर्समेंट, या कानूनी अथॉरिटी के तहत काम करने वाली दूसरी सरकारी संस्थाएं
- कोर्ट और ज्यूडिशियल ऑर्डर: कोर्ट के ऑर्डर, कानूनी समन, या ज्यूडिशियल निर्देशों का जवाब
- रेगुलेटरी अथॉरिटी: डेटा प्रोटेक्शन बोर्ड, मिनिस्ट्री ऑफ़ इलेक्ट्रॉनिक्स एंड इन्फॉर्मेशन टेक्नोलॉजी (MeitY), या दूसरी रेगुलेटरी संस्थाएं
- फाइनेंशियल इंटेलिजेंस यूनिट (FIU): संदिग्ध ट्रांज़ैक्शन रिपोर्ट और एंटी-मनी लॉन्ड्रिंग (AML) कम्प्लायंस

12. क्रॉस-बॉर्डर डेटा ट्रांसफर कम्प्लायंस

TCPL, DPDP एक्ट, 2023 के तहत केंद्र सरकार द्वारा ज़रूरी क्रॉस-बॉर्डर डेटा ट्रांसफर पर सभी पाबंदियों का पालन करेगा। विदेशी अधिकार क्षेत्रों में सभी पर्सनल डेटा ट्रांसफर सरकारी नोटिफिकेशन और मंज़ूरी के अधीन हैं।

12.2 रेगुलेटरी वॉच - जिन देशों पर रोक लगी है उनकी मॉनिटरिंग

तय ज़िम्मेदारी:

कम्प्लायंस ऑफिसर या लीगल टीम को क्रॉस-बॉर्डर डेटा ट्रांसफर पाबंदियों से जुड़े सभी नोटिफ़िकेशन और अपडेट की मॉनिटरिंग की ज़िम्मेदारी दी गई है। इस काम को एक ज़रूरी कम्प्लायंस एक्टिविटी माना जाएगा।

मॉनिटरिंग के तरीके:

- प्राइमरी सोर्स: MeitY, डेटा प्रोटेक्शन बोर्ड, RBI, और डिपार्टमेंट ऑफ़ टेलीकम्युनिकेशन्स से सरकारी नोटिफ़िकेशन की रेगुलर चेकिंग
- सेकेंडरी सोर्स: इंडस्ट्री एसोसिएशन (ASSOCHAM, FICCI, CII, NASSCOM, फ़िनटेक कंसोर्टियम), लीगल और कम्प्लायंस फ़ोरम, रेगुलेटरी न्यूज़लेटर
- फ़्रीक्वेंसी: रेगुलेटरी अपडेट का मंथली रिव्यू; अगर कोई नई रोक अनाउंस होती है तो तुरंत कार्रवाई
- डॉक्यूमेंटेशन: सभी पाबंद देशों और नोटिफ़िकेशन की तारीख का एक रजिस्टर मेंटेन करें

12.3 क्रॉस-बॉर्डर डेटा फ़्लो की इन्वेंटरी

TCPL सभी क्रॉस-बॉर्डर डेटा फ़्लो की एक पूरी इन्वेंटरी बनाए रखेगा और मेंटेन करेगा। इस इन्वेंट्री में ये बातें डॉक्यूमेंट होंगी:

- ट्रांसफर किए जा रहे पर्सनल डेटा का टाइप (कस्टमर डेटा, फाइनेंशियल डेटा, ऑपरेशनल डेटा)

- वॉल्यूम (रिकॉर्ड्स की संख्या, GB में साइज़) और ट्रांसफर की फ्रीक्वेंसी
- क्लाउड सर्विस प्रोवाइडर का नाम और सर्वर लोकेशन वाला देश
- SaaS एप्लिकेशन और उनके डेटा स्टोरेज वाले देश
- TCPL डेटा एक्सेस करने वाले इंटरनेशनल ऑफिस या सब्सिडियरी
- इंटरनेशनल मौजूदगी वाले आउटसोर्सिंग वेंडर और शामिल देश

12.4 रिस्ट्रिक्टेड देशों के लिए कंटिंजेंसी प्लान

TCPL इन्वेंट्री में पहचानी गई हर क्रॉस-बॉर्डर डेटा डिपेंडेंसी के लिए कंटिंजेंसी प्लान बनाएगा और बनाए रखेगा। अगर किसी देश को रिस्ट्रिक्टेड घोषित किया जाता है, तो ये प्लान तेज़ी से रिस्पॉन्स पक्का करते हैं।

कंटिंजेंसी प्लान के हिस्से:

- रिस्क असेसमेंट: अगर उस देश में डेटा ट्रांसफर ब्लॉक हो जाता है, तो ऑपरेशनल, बिज़नेस और रेगुलेटरी असर की पहचान करें
- दूसरे समाधान: भारत में मौजूद सर्विस प्रोवाइडर, मंज़ूर देश के विकल्प, या हाइब्रिड तरीकों की पहचान करें
- वेंडर कॉन्ट्रैक्ट क्लॉज़: सभी वेंडर एग्रीमेंट में डेटा रिलोकेशन क्लॉज़, एग्जिट क्लॉज़, कम्प्लायंस क्लॉज़ और टर्मिनेशन क्लॉज़ शामिल होने चाहिए
- ट्रांज़िशन टाइमलाइन: दिन 0-2: तुरंत एस्केलेशन; दिन 2-5: असर का असेसमेंट; दिन 5-15: डेटा माइग्रेशन पूरा करें; दिन 15-30: ट्रांज़िशन पूरा करें
- कम्युनिकेशन प्लान: इंटरनल स्टेकहोल्डर्स, MLIs, कस्टमर्स और रेगुलेटरी अथॉरिटीज़ को बताएं

12.5 प्रोक्योरमेंट और प्रोजेक्ट्स में डेटा फ्लो गवर्नेंस

सभी प्रोक्योरमेंट एक्टिविटीज़ और नए प्रोजेक्ट शुरू करने में वेंडर चुनने या टूल डिप्लॉयमेंट से पहले डेटा फ्लो असेसमेंट शामिल होना चाहिए।

प्रोक्योरमेंट चेकलिस्ट - क्रॉस-बॉर्डर डेटा ट्रांसफर सवाल:

1. क्या इस वेंडर/टूल/सर्विस में भारत के बाहर कोई डेटा ट्रांसफर शामिल है?

2. डेटा प्रोसेसिंग या स्टोरेज में कौन से देश शामिल हैं?

3. क्या सभी पहचाने गए देश अभी DPDP एक्ट के सेक्शन 16 के तहत डेटा ट्रांसफर के लिए अप्रूव्ड हैं?

4. किस तरह का डेटा ट्रांसफर किया जाता है?

5. क्या इस क्रॉस-बॉर्डर ट्रांसफर के लिए डेटा सब्जेक्ट की साफ़ सहमति है?

6. क्या वेंडर के साथ डेटा प्रोसेसिंग एग्रीमेंट (DPA) किया गया है?

7. क्या यह एक रेगुलेटरी कम्प्लायंस ज़रूरत (RBI, क्रेडिट ब्यूरो, वगैरह) है?

अप्रूवल अथॉरिटी: प्रोक्योरमेंट को फ़ाइनल करने से पहले कम्प्लायंस ऑफिसर को डेटा फ्लो पर साइन करना होगा। क्रॉस-बॉर्डर डेटा से जुड़े किसी भी वेंडर/टूल/सर्विस को कम्प्लायंस अप्रूवल के बिना डिप्लॉय नहीं किया जा सकता है।

12.6 क्रॉस-बॉर्डर ट्रांसफर पर इंटरनल पॉलिसी स्टेटमेंट

TCPL क्रॉस-बॉर्डर डेटा ट्रांसफर पॉलिसी:

TCPL अपने कस्टमर्स, बॉरोअर्स, या डेटा सब्जेक्ट्स का पर्सनल डेटा, सेंसिटिव पर्सनल डेटा या जानकारी, या कोई दूसरा रेगुलेटेड डेटा किसी ऐसे देश में ट्रांसफर नहीं करेगा, जिसे डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 के सेक्शन 16 के तहत भारत की सेंट्रल गवर्नमेंट ने ऐसे ट्रांसफर के लिए मना किया है।

TCPL सेंट्रल गवर्नमेंट द्वारा तय की गई सभी शर्तों का सख्ती से पालन करेगा, अगर कुछ खास ज्यूरिस्डिक्शन में ट्रांसफर के लिए कोई शर्तें बताई गई हैं।

सभी क्रॉस-बॉर्डर डेटा ट्रांसफर कम्प्लायंस ऑफिसर द्वारा पहले से अप्रूव किए जाते हैं और लगातार मॉनिटर किए जाते हैं। अगर किसी देश को रिस्ट्रिक्टेड घोषित किया जाता है, तो TCPL तुरंत डेटा ट्रांसफर को सस्पेंड कर देगा और 30 दिनों के अंदर डेटा को अप्रूव्ड ज्यूरिस्डिक्शन में माइग्रेट कर देगा।

एम्प्लॉइज, कॉन्ट्रैक्टर्स, और वेंडर्स को बिना साफ कम्प्लायंस अप्रूवल के किसी भी विदेशी ज्यूरिस्डिक्शन में पर्सनल डेटा ट्रांसफर करने से मना किया गया है। इस पॉलिसी का उल्लंघन करने पर डिसिप्लिनरी एक्शन लिया जाएगा, जिसमें नौकरी या कॉन्ट्रैक्ट खत्म करना भी शामिल है।

स्टाफ़ अवेयरनेस:

सभी कर्मचारियों, कॉन्ट्रैक्टर और संबंधित थर्ड पार्टी को क्रॉस-बॉर्डर डेटा ट्रांसफर पर रोक, मना किए गए कामों के साफ़ उदाहरण, एस्केलेशन प्रोसेस और नियम न मानने के नतीजों पर सालाना ट्रेनिंग दी जाएगी।

12.7 जिन देशों में डेटा ट्रांसफ़र पर रोक है, उनके लिए तुरंत जवाब देने का तरीका

सरकार से यह नोटिफ़िकेशन मिलने पर कि किसी देश में डेटा ट्रांसफ़र पर रोक है:

- तुरंत कार्रवाई (2 घंटे के अंदर): कंप्लायंस ऑफ़िसर नोटिफ़िकेशन को वेरिफ़ाई करता है; CISO को बताया जाता है; इमरजेंसी मीटिंग बुलाई जाती है
- पहचान का फ़ेज़ (पहले दिन के आखिर तक): डेटा फ़्लो इन्वेंटरी के साथ उस देश का क्रॉस-रेफ़रेंस लें जिस पर असर पड़ा है; सभी वेंडर और सर्विस की पहचान करें
- एस्केलेशन (दूसरे दिन तक): सभी स्टेकहोल्डर को बताएं; वेंडर को ट्रांसफ़र रोकने का निर्देश दें; दूसरे उपाय शुरू करें
- कम करने का तरीका (2-30 दिन): इमरजेंसी प्लान लागू करें; सारा डेटा मंज़ूर किए गए अधिकार क्षेत्र में माइग्रेट करें; जो एग्रीमेंट कंप्लायंस नहीं करते, उन्हें खत्म करें
- कम्युनिकेशन और कंप्लायंस (30वें दिन से आगे): पूरा रिलोकेशन वेरिफ़ाई करें; RBI के पास कंप्लायंस सर्टिफ़िकेशन फ़ाइल करें; प्राइवेसी पॉलिसी और इन्वेंटरी अपडेट करें

13. सेक्टर-स्पेसिफिक डेटा ट्रांसफर और लोकलाइज़ेशन रेगुलेशन

13.1 लागू सेक्टर-स्पेसिफिक रेगुलेशन की पहचान

आम DPDP एक्ट, 2023 के अलावा, TCPL सेक्टर-स्पेसिफिक डेटा प्रोटेक्शन और लोकलाइज़ेशन रेगुलेशन के अधीन है। इनमें शामिल हैं:

डिजिटल लेंडिंग और फिनटेक के लिए RBI रेगुलेशन:

- डिजिटल लेंडिंग गाइडलाइन्स (2022, अपडेटेड 2025): डेटा कलेक्शन स्टैंडर्ड, बॉरोअर की सहमति की ज़रूरतें और आउटसोर्सिंग नॉर्म्स बताएं
- RBI आउटसोर्सिंग गाइडलाइन्स: डेटा को सिर्फ़ मंज़ूर जगहों पर ही आउटसोर्स करने की ज़रूरत है, जहाँ खास सिक्योरिटी और कॉन्फिडेंशियलिटी की ज़रूरतें हों
- क्रेडिट इन्फॉर्मेशन पॉलिसी: बताएं कि क्रेडिट डेटा कैसे कलेक्ट, स्टोर, शेयर और इस्तेमाल किया जा सकता है
- पेमेंट सिस्टम रेगुलेशन: पेमेंट से जुड़ा डेटा भारत में ही स्टोर और प्रोसेस किया जाना ज़रूरी है

क्रेडिट ब्यूरो रेगुलेशन:

क्रेडिट ब्यूरो द्वारा कलेक्ट की गई क्रेडिट इन्फॉर्मेशन का इस्तेमाल सिर्फ़ क्रेडिट रिपोर्टिंग और स्कोरिंग के मकसद से किया जाना चाहिए; क्रेडिट ब्यूरो लाइसेंस की ज़रूरतों के हिसाब से स्टोर और प्रोसेस किया जाता है; बिना साफ़ मंज़ूरी के थर्ड पार्टी के साथ शेयर नहीं किया जाता; आम तौर पर भारत में या मंज़ूर जगहों पर स्टोर किया जाता है।

दूसरे लागू नियम:

- आधार एक्ट, 2016: आधार डेटा को भारत के बाहर ट्रांसफर नहीं किया जा सकता या बिना इजाज़त के इस्तेमाल नहीं किया जा सकता
- टेलीकॉम नियम: अगर TCPL टेलीकॉम डेटा हैंडल करता है, तो उसे डेटा लोकलाइज़ेशन पर TRAI के नियमों का पालन करना होगा

  पेमेंट कार्ड इंडस्ट्री डेटा सिक्योरिटी स्टैंडर्ड (PCI-DSS): अगर कार्ड डेटा हैंडल कर रहे हैं, तो इंटरनेशनल स्टैंडर्ड्स का पालन करना होगा (सेंसिटिव डेटा को लोकलाइज़ करते समय)
- एम्प्लॉयमेंट डेटा: एम्प्लॉई डेटा को एम्प्लॉयमेंट कोड्स के तहत प्रोटेक्ट किया जाना चाहिए और इसे मनमाने ढंग से ट्रांसफर नहीं किया जा सकता

13.2 गैप एनालिसिस - मौजूदा प्रैक्टिस बनाम रेगुलेटरी ज़रूरतें

TCPL सभी लागू सेक्टरल रेगुलेशंस के साथ मौजूदा डेटा हैंडलिंग प्रैक्टिस की तुलना करके एक गैप एनालिसिस करेगा।

गैप एनालिसिस प्रोसेस:

- सभी सिस्टम और प्रोसेस की लिस्ट बनाएं: डेटा हैंडल करने वाले सभी सिस्टम और उनकी लोकेशन (इंडिया/फॉरेन) को डॉक्यूमेंट करें
- क्रॉस-रेफरेंस रेगुलेटरी ज़रूरतें: हर सिस्टम के लिए, लागू रेगुलेशन की पहचान करें
- गैप की पहचान करें: असल बनाम ज़रूरी प्रैक्टिस की तुलना करें
- रिमेडिएशन प्लान: हर गैप के लिए, तुरंत एक्शन, टाइमलाइन, ज़िम्मेदार पार्टी और रिसोर्स डॉक्यूमेंट करें

- डॉक्यूमेंटेशन: एक गैप एनालिसिस रजिस्टर बनाए रखें जिसमें हर पहचाने गए गैप, रेगुलेटरी बेसिस, गंभीरता, टाइमलाइन और स्टेटस को डॉक्यूमेंट किया गया हो

13.3 साफ़ कंप्लायंस स्टेटमेंट

सेक्टरल कंप्लायंस पर TCPL की इंटरनल पॉलिसी:

TCPL यह मानता है कि DPDP एक्ट, 2023 जैसे आम डेटा प्रोटेक्शन कानूनों के अलावा, कंपनी रिज़र्व बैंक ऑफ़ इंडिया, क्रेडिट ब्यूरो रेगुलेटर और दूसरी अथॉरिटी द्वारा जारी किए गए सेक्टर-स्पेसिफिक रेगुलेशन के तहत आती है

कंपनी ये करने के लिए कमिटेड है:

1. डेटा कलेक्शन, बॉरोअर की सहमति, डेटा स्टोरेज और थर्ड-पार्टी शेयरिंग पर RBI की डिजिटल लेंडिंग गाइडलाइंस का पालन करना
2. अप्रूव्ड ज्यूरिस्डिक्शन और वेंडर कॉन्फिडेंशियलिटी पर RBI की आउटसोर्सिंग गाइडलाइंस का पालन करना
3. सिर्फ इंडिया में स्टोरेज और क्रेडिट डेटा के लिमिटेड इस्तेमाल पर क्रेडिट ब्यूरो रेगुलेशंस का पालन करना
4. आधार एक्ट, टेलीकॉम रेगुलेशंस, एम्प्लॉयमेंट लॉज़ और इनकम टैक्स लॉज़ सहित दूसरे लागू कानूनों का पालन करना
5. कम्प्लायंस का हायरार्की: अलग-अलग ज़रूरतों के मामले में, TCPL सबसे सख्त ज़रूरत का पालन करेगा
6. रेगुलर रिव्यू और अपडेट: TCPL इन पॉलिसीज़ का हर साल या नई रेगुलेटरी गाइडेंस मिलने पर रिव्यू करेगा
7. एनफोर्समेंट: वायलेशन करने पर एम्प्लॉइज के खिलाफ डिसिप्लिनरी एक्शन लिया जाएगा और वेंडर्स के कॉन्ट्रैक्ट खत्म कर दिए जाएंगे

13.4 लीगल और कंप्लायंस टीमों के साथ कोऑर्डिनेशन

जब भी TCPL किसी नई सर्विस, वेंडर, टूल या प्रोसेस पर विचार करता है जिसमें क्रॉस-बॉर्डर डेटा हैंडलिंग शामिल है, तो नीचे दिया गया अप्रूवल प्रोसेस ज़रूरी है:

- स्टेप 1 - बिज़नेस रिक्वेस्ट (दिन 0): डिपार्टमेंट कंप्लायंस ऑफिसर को क्रॉस-बॉर्डर डेटा रिक्वेस्ट फ़ॉर्म जमा करता है
- स्टेप 2 - कंप्लायंस रिव्यू (दिन 1-3): कंप्लायंस ऑफिसर देश की अप्रूवल, डेटा टाइप, सेक्टर-स्पेसिफिक पाबंदियों और सहमति की ज़रूरतों का असेसमेंट करता है
- स्टेप 3 - लीगल ड्यू डिलिजेंस (दिन 3-7): लीगल टीम वेंडर की शर्तों, इंडियन लॉ कंप्लायंस और सिक्योरिटी एडिक्वेसी का असेसमेंट करती है
- स्टेप 4 - अप्रूवल या रिजेक्शन (दिन 7): अगर कंप्लायंट है, तो अप्रूव; अगर नियमों का पालन नहीं किया, तो दूसरे ऑप्शन सुझाकर रिजेक्ट कर दिया जाएगा
- स्टेप 5 - कॉन्ट्रैक्ट और DPA (दिन 7-14): वेंडर कॉन्ट्रैक्ट में डेटा लोकलाइज़ेशन क्लॉज़ और डेटा प्रोसेसिंग एग्रीमेंट शामिल होना चाहिए
- स्टेप 6 - इम्प्लीमेंटेशन (दिन 14+): टूल/वेंडर को कॉन्ट्रैक्ट पूरा होने, DPA साइन करने, इन्वेंट्री अपडेट और ट्रेनिंग के बाद ही लगाया जाएगा

13.5 उदाहरण और स्टाफ़ की जानकारी

TCPL सेक्टर-स्पेसिफिक डेटा प्रोटेक्शन ट्रेनिंग - खास बातें। सभी स्टाफ़ को नीचे दिए गए उदाहरणों के बारे में पता होना चाहिए:

- **उदाहरण 1 - पेमेंट डेटा:** RBI के नियमों के कारण पेमेंट से जुड़ा डेटा भारत में ही रहना चाहिए। अगर आपका डिपार्टमेंट इंटरनेशनल पेमेंट प्रोसेसर इस्तेमाल करता है, तो पक्का करें कि वे डेटा को सिर्फ़ भारतीय डेटा सेंटर में ही प्रोसेस और स्टोर करें। नियम तोड़ने पर RBI पेनल्टी लग सकती है।

- **उदाहरण 2 - आधार जानकारी**: आधार जानकारी किसी भी विदेशी सिस्टम को न भेजें। आधार एक्ट के तहत आधार डेटा भारत से बाहर नहीं जा सकता। आधार को विदेश में ट्रांसफर करना एक क्रिमिनल ऑफ़ेंस है।

- **उदाहरण 3 - क्रेडिट जानकारी:** बॉरोअर्स का क्रेडिट डेटा भारत के बाहर शेयर या स्टोर नहीं किया जा सकता। अगर TCPL क्रेडिट ब्यूरो सर्विस का इस्तेमाल करता है, तो पक्का करें कि क्रेडिट डेटा भारत में ही रहे।

- **उदाहरण 4 - विदेशी वेंडर और आउटसोर्सिंग:** अगर आपका डिपार्टमेंट कस्टमर डेटा को संभालने के लिए किसी विदेशी कॉल सेंटर, BPO, या सर्विस प्रोवाइडर को हायर करता है, तो हमें RBI आउटसोर्सिंग गाइडलाइंस का पालन करना होगा। वेंडर को RBI से पहले से अप्रूव्ड होना चाहिए या किसी अप्रूव्ड ज्यूरिस्डिक्शन में होना चाहिए।

- **उदाहरण 5 - नए SaaS टूल्स:** कोई नया क्लाउड-बेस्ड टूल (CRM, एनालिटिक्स, HR सिस्टम) अपनाने से पहले, कंप्लायंस ऑफिसर से चेक करें कि टूल किसी अप्रूव्ड देश में डेटा स्टोर करता है या नहीं। पक्का करें कि देश सेक्शन 16 के तहत अप्रूव्ड है, कोई भी सेक्टर-स्पेसिफिक रेगुलेशन स्टोरेज पर रोक नहीं लगाता है, एक डेटा प्रोसेसिंग एग्रीमेंट है, और डेटा सब्जेक्ट की सहमति ली गई है। कंप्लायंस साइन-ऑफ के बिना डिप्लॉय न करें।

- **उदाहरण 6 - पर्सनल डेटा बनाम SPDI:** अलग-अलग डेटा के लिए अलग-अलग प्रोटेक्शन की ज़रूरत होती है। फाइनेंशियल डेटा भारत में ही रहना चाहिए (RBI नियमों के अनुसार)। आधार डेटा विदेश नहीं जा सकता (आधार एक्ट के अनुसार)। हेल्थ डेटा के लिए साफ़ सहमति की ज़रूरत होती है (SPDI नियमों के अनुसार)। हमेशा पूछें: क्या यह SPDI है? अगर हाँ, तो ज़्यादा सख़्त प्रोटेक्शन अप्लाई करें।

ट्रेनिंग डॉक्यूमेंटेशन:

- सेक्टर-स्पेसिफिक डेटा रेगुलेशन पर सालाना ज़रूरी ट्रेनिंग
- ऑडिट के मकसद से ट्रेनिंग रिकॉर्ड मेंटेन किए जाते हैं
- केस स्टडी और असल दुनिया के उदाहरणों पर चर्चा
- समझ को वेरिफ़ाई करने के लिए क्विज़ या असेसमेंट
- नए रेगुलेशन जारी होने पर रिफ्रेशर ट्रेनिंग

14. हम आपकी पर्सनल जानकारी कब तक रखेंगे?

हम आपका पर्सनल डेटा सिर्फ़ उतने समय तक रखेंगे, जितने समय तक ज़रूरी हो, ताकि हमने इसे इकट्ठा किया है, जिसमें कोई भी कानूनी, अकाउंटिंग या रिपोर्टिंग ज़रूरतें पूरी करना शामिल है।

14.1 डेटा टाइप के हिसाब से रिटेंशन पीरियड

कस्टमर और बॉरोअर डेटा:

- एक्टिव लोन पीरियड: लोन का समय और आखिरी ट्रांज़ैक्शन की तारीख से 7 साल (बैंकिंग रेगुलेशन के हिसाब से)

- क्लोज्ड अकाउंट: क्लोजर से 7 साल (रेगुलेटरी कम्प्लायंस और डिस्प्यूट रेज़ोल्यूशन के लिए)
- क्रेडिट ब्यूरो डेटा: क्रेडिट ब्यूरो रेगुलेटरी ज़रूरतों के हिसाब से 7 साल

सेंसिटिव पर्सनल डेटा (SPDI):

- फाइनेंशियल रिकॉर्ड: कम से कम 7 साल (इनकम टैक्स रेगुलेशन के हिसाब से)
- हेल्थ और मेडिकल डेटा: लागू हेल्थकेयर रेगुलेशन के हिसाब से; कम से कम 5 साल
- बायोमेट्रिक डेटा: इस्तेमाल का समय और 3 साल; अगर मकसद पूरा हो जाए तो पहले डिलीट कर दिया जाएगा

एम्प्लॉई डेटा:

- नौकरी के दौरान: नौकरी का समय
- नौकरी के बाद: कम्प्लायंस और रेफरेंस के मकसद से 5 साल

ऑडिट और कम्प्लायंस रिकॉर्ड:

- सहमति ऑडिट ट्रेल्स: कम से कम 5 साल
- डेटा एक्सेस लॉग: कम से कम 3 साल
- सिक्योरिटी इंसिडेंट रिकॉर्ड: कम से कम 7 साल
- रेगुलेटरी कॉरेस्पोंडेंस: RBI और दूसरी अथॉरिटीज़ की ज़रूरत के हिसाब से

14.2 डेटा एनोनिमाइज़ेशन और स्यूडोनिमाइज़ेशन

- एक बार जब कलेक्शन का मकसद पूरा हो जाता है, तो पर्सनल डेटा को एनोनिमाइज़ या स्यूडोनिमाइज़ किया जाएगा, जहाँ तक हो सके
- एनोनिमाइज़्ड डेटा को स्टैटिस्टिकल और रिसर्च के मकसद से हमेशा के लिए रखा जा सकता है

  एनोनिमाइज़ेशन इंडस्ट्री-स्टैंडर्ड तकनीकों का इस्तेमाल करके किया जाएगा, जिससे पहचान पक्की हो सके।

14.3 डेटा डिलीट करना और डिस्पोज़ल

- रखरखाव का समय खत्म होने पर, पर्सनल डेटा को सुरक्षित रूप से डिलीट कर दिया जाएगा।
- डिलीशन इंडस्ट्री-स्टैंडर्ड डेटा डिस्ट्रक्शन तरीकों (सुरक्षित रूप से मिटाना, मीडिया को फिजिकल रूप से नष्ट करना) का इस्तेमाल करके किया जाएगा।
- प्राइमरी सिस्टम से डेटा डिलीट करने के 3 महीने के अंदर बैकअप कॉपी डिलीट कर दी जाएंगी।
- डिलीशन को सर्टिफाइड किया जाएगा और डेटा डिलीशन रजिस्टर में डॉक्यूमेंट किया जाएगा।

14.4 डेटा सब्जेक्ट का मिटाने का अधिकार

डेटा सब्जेक्ट किसी भी समय अपने पर्सनल डेटा को डिलीट करने का अनुरोध कर सकते हैं। डिलीट करने के अनुरोध 30 दिनों के अंदर प्रोसेस किए जाएंगे। अपवाद: लागू कानूनों (टैक्स रिकॉर्ड, रेगुलेटरी कम्प्लायंस) के तहत ज़रूरी डेटा; चल रहे कॉन्ट्रैक्ट की ज़िम्मेदारियों के लिए ज़रूरी डेटा; डेटा सब्जेक्ट द्वारा डिलीट करने पर विवाद। एक्टिव सिस्टम से डिलीट करने के बाद भी, कम्प्लायंस के मकसद से बैकअप में एनोनिमाइज़्ड बची हुई कॉपी रखी जा सकती हैं।

15. इन्फॉर्मेशन सिक्योरिटी के उपाय

15.1 आम सिक्योरिटी कमिटमेंट

TCPL इन्फॉर्मेशन सिक्योरिटी और लागू नियमों के पालन के लिए पूरी तरह से कमिटेड है। हमने ISO 27001:2022 के साथ अलाइन्ड अपने इन्फॉर्मेशन सिक्योरिटी मैनेजमेंट सिस्टम के ज़रिए डेटा की सुरक्षा के लिए मज़बूत सिक्योरिटी कंट्रोल लागू किए हैं।

15.2 टेक्निकल सिक्योरिटी कंट्रोल

- ट्रांज़िट में एन्क्रिप्शन: TCPL नेटवर्क के बाहर भेजा गया सारा डेटा इंडस्ट्री-स्टैंडर्ड प्रोटोकॉल (TLS 1.2 या उससे ज़्यादा) का इस्तेमाल करके एन्क्रिप्ट किया जाता है

- रेस्ट पर एन्क्रिप्शन: सेंसिटिव पर्सनल डेटा और SPDI को AES-256 या इसके बराबर के एन्क्रिप्शन स्टैंडर्ड का इस्तेमाल करके एन्क्रिप्ट किया जाता है

- एक्सेस कंट्रोल: डेटा एक्सेस रोल-बेस्ड एक्सेस कंट्रोल (RBAC) प्रिंसिपल के आधार पर रिस्ट्रिक्टेड है

- ऑथेंटिकेशन: सेंसिटिव डेटा सिस्टम तक एक्सेस के लिए मल्टी-फैक्टर ऑथेंटिकेशन (MFA) लागू किया जाता है

- नेटवर्क सिक्योरिटी: फायरवॉल, इंट्रूज़न डिटेक्शन सिस्टम और VPN नेटवर्क पेरिमीटर को प्रोटेक्ट करते हैं

- डेटाबेस सिक्योरिटी: डेटाबेस एक्सेस लॉग किया जाता है; बिना इजाज़त एक्सेस की कोशिशों पर नज़र रखी जाती है और अलर्ट किया जाता है

- डेटा मास्किंग: नॉन-प्रोडक्शन एनवायरनमेंट मास्क्ड या एनॉनिमाइज़्ड डेटा का इस्तेमाल करते हैं

15.3 ऑर्गेनाइज़ेशनल सिक्योरिटी कंट्रोल

- इन्फॉर्मेशन सिक्योरिटी पॉलिसी: पूरी ISMS पॉलिसी पूरे ऑर्गेनाइज़ेशन में डेटा प्रोटेक्शन को कंट्रोल करती हैं

- स्टाफ़ ट्रेनिंग: सभी कर्मचारियों को सालाना इन्फॉर्मेशन सिक्योरिटी और डेटा प्रोटेक्शन ट्रेनिंग मिलती है

  कॉन्फिडेंशियलिटी एग्रीमेंट: सभी कर्मचारी और कॉन्ट्रैक्टर कॉन्फिडेंशियलिटी एग्रीमेंट पर साइन करते हैं

- थर्ड-पार्टी रिस्क मैनेजमेंट: काम पर रखने से पहले वेंडर्स की इन्फॉर्मेशन सिक्योरिटी कंप्लायंस के लिए जांच की जाती है

- इंसिडेंट रिस्पॉन्स प्लान: सिक्योरिटी इंसिडेंट लॉग किए जाते हैं, उनकी जांच की जाती है, और तुरंत उन्हें ठीक किया जाता है

- सिक्योरिटी ऑडिट: रेगुलर सिक्योरिटी ऑडिट और पेनेट्रेशन टेस्टिंग की जाती है

15.4 यूज़र की ज़िम्मेदारियां

हालांकि TCPL बिना इजाज़त के एक्सेस या अटैक से एसेट्स को बचाने के लिए सही कदम उठाता है, लेकिन इंटरनेट असल में पूरी तरह से सुरक्षित नहीं है। यूज़र्स को अपने डेटा सिक्योरिटी की भी ज़िम्मेदारी लेनी चाहिए: अपनी यूज़र ID और पासवर्ड की कॉन्फिडेंशियलिटी बनाए रखें; क्रेडेंशियल शेयर न करें; सुरक्षित डिवाइस और नेटवर्क का इस्तेमाल करें;

सिस्टम को सिक्योरिटी पैच के साथ अपडेट रखें; किसी भी संदिग्ध सिक्योरिटी ब्रीच की तुरंत admin@techfino.in पर रिपोर्ट करें।

15.5 इंसिडेंट रिपोर्टिंग और रिस्पॉन्स

अगर आपको किसी सिक्योरिटी समस्या, इंसिडेंट का शक है, या TCPL से होने का दावा करने वाले संदिग्ध कम्युनिकेशन मिलते हैं, तो तुरंत admin@techfino.in पर ईमेल करें। संदिग्ध कम्युनिकेशन पर लिंक पर क्लिक न करें या जानकारी न दें। जवाब देने से पहले भेजने वाले की पहचान खुद से वेरिफ़ाई करें।

16. कुकीज़ का इस्तेमाल कैसे किया जाता है?

कुकी डेटा का एक छोटा सा हिस्सा होता है जो वेबसाइट ब्राउज़ करते समय वेब ब्राउज़र यूज़र के कंप्यूटर पर स्टोर करता है। हम अपनी साइट और सर्विस की क्वालिटी को बेहतर बनाने और आपके ब्राउज़िंग एक्सपीरियंस को बेहतर बनाने के लिए कुकीज़ का इस्तेमाल करते हैं।

16.1 कुकीज़ के प्रकार

फ़र्स्ट-पार्टी कुकीज़: वेबसाइट के ठीक से काम करने के लिए ज़्यादातर ज़रूरी होती हैं। इसमें लॉगिन, प्रेफ़रेंस और ब्राउज़िंग स्टेट के लिए सेशन कुकीज़ शामिल हैं। यूज़र ब्राउज़र सेटिंग्स के ज़रिए फ़र्स्ट-पार्टी कुकीज़ को मैनेज कर सकते हैं।

थर्ड-पार्टी कुकीज़: मुख्य रूप से वेबसाइट की परफ़ॉर्मेंस को समझने के लिए इस्तेमाल होती हैं। इसमें एनालिटिक्स, यूज़र इंटरैक्शन ट्रैकिंग और सिक्योरिटी मॉनिटरिंग शामिल हैं। थर्ड-पार्टी कुकीज़ के लिए यूज़र की साफ़ सहमति ज़रूरी है।

16.2 कुकी मैनेजमेंट

- यूज़र कंट्रोल: आप अपनी ब्राउज़र सेटिंग्स के ज़रिए कुकीज़ के इस्तेमाल को कंट्रोल कर सकते हैं
- सहमति: पहली बार विज़िट करने पर, आपसे गैर-ज़रूरी कुकीज़ के लिए सहमति मांगी जाएगी
- सहमति रद्द करना: आप ब्राउज़र प्रेफरेंस के ज़रिए किसी भी समय कुकी की सहमति वापस ले सकते हैं
- कुकी डिसेबल करना: अगर आप कुकीज़ डिसेबल करना चुनते हैं, तो हो सकता है कि वेबसाइट के कुछ फ़ीचर या फ़ंक्शन ठीक से काम न करें

17. हमसे कैसे संपर्क करें?

अगर आपको इस प्राइवेसी स्टेटमेंट और हमारी डेटा प्रैक्टिस के बारे में कोई प्राइवेसी चिंता, शिकायत, सवाल या रिक्वेस्ट है, तो कृपया हमसे संपर्क करें:

17.1 संपर्क जानकारी

ईमेल: admin@techfino.in

मेलिंग एड्रेस: TechFino Capital Private Limited [पता देना होगा]

रिस्पॉन्स टाइमलाइन:

- स्वीकृति: 5 बिज़नेस दिनों के अंदर
- समाधान: स्टैंडर्ड रिक्वेस्ट के लिए 30 दिनों के अंदर

- मुश्किल मामले: 60 दिनों के अंदर (देरी की सूचना के साथ)

17.2 डेटा सब्जेक्ट राइट्स

आपकी पर्सनल जानकारी के संबंध में आपके कुछ अधिकार हैं। आप नीचे दिए गए किसी भी अधिकार का इस्तेमाल करने के लिए हमसे संपर्क कर सकते हैं:

एक्सेस का अधिकार: हमारे पास आपके बारे में मौजूद सभी पर्सनल डेटा की एक कॉपी का अनुरोध करें; समझें कि कौन सा डेटा इकट्ठा किया जाता है और उसका इस्तेमाल कैसे किया जाता है

सुधार का अधिकार: गलत या अधूरे पर्सनल डेटा में सुधार का अनुरोध करें; पुरानी जानकारी अपडेट करें

मिटाने का अधिकार: अपने पर्सनल डेटा को डिलीट करने का अनुरोध करें (कानूनी रिटेंशन की शर्तों के तहत); जहाँ कानूनी तौर पर लागू हो, वहाँ "भूल जाने" का अधिकार

डेटा पोर्टेबिलिटी का अधिकार: अपने पर्सनल डेटा को एक स्ट्रक्चर्ड, स्टैंडर्ड फ़ॉर्मेट में मांगें; अपना डेटा किसी दूसरी ऑर्गनाइज़ेशन को ट्रांसफ़र करें

ऑप्ट-आउट करने का अधिकार: खास मकसदों के लिए सहमति वापस लेना; मार्केटिंग कम्युनिकेशन, एनालिटिक्स, या दूसरी गैर-ज़रूरी प्रोसेसिंग से ऑप्ट-आउट करना

प्रोसेसिंग पर रोक लगाने का अधिकार: खास मकसदों के लिए डेटा प्रोसेसिंग को सस्पेंड करने का अनुरोध करें; अपने डेटा के इस्तेमाल को लिमिट करें

सहमति वापस लेना: डेटा कलेक्शन या प्रोसेसिंग के लिए पहले दी गई सहमति वापस लेना; सहमति वापस लेने पर आगे की प्रोसेसिंग बंद हो जाएगी

17.3 रिक्वेस्ट प्रोसेस करना

रिक्वेस्ट सबमिट करना: admin@techfino.in पर ईमेल से रिक्वेस्ट सबमिट करें। पहचान के लिए ज़रूरी डिटेल शामिल करें। साफ़-साफ़ बताएं कि आप किस अधिकार का इस्तेमाल करना चाहते हैं।

वेरिफ़िकेशन: रिक्वेस्ट प्रोसेस करने से पहले आपसे अपनी पहचान वेरिफ़ाई करने के लिए कहा जाएगा। वेरिफ़िकेशन यह पक्का करता है कि हम डेटा सिर्फ़ सही डेटा सब्जेक्ट को ही बताएं।

मंज़ूरी या नामंज़ूरी: रिक्वेस्ट को मेरिट के आधार पर प्रोसेस किया जाएगा। अगर हम कोई रिक्वेस्ट पूरी नहीं कर पाते हैं, तो आपको वजहें बताई जाएंगी।

बची हुई कॉपी: हमें कुछ समय के लिए बैकअप सिस्टम में डिलीट किए गए डेटा की बची हुई कॉपी रखनी पड़ सकती है। बैकअप कॉपी पहले डिलीट होने के 3 महीने के अंदर डिलीट कर दी जाती हैं।

18. लीगल नोटिस

18.1 रेगुलेटरी डिस्क्लोजर

TCPL को इन वजहों से लीगल अथॉरिटीज़ को पर्सनल जानकारी देनी पड़ सकती है:

- कोर्ट के ऑर्डर, लीगल समन, या ज्यूडिशियल निर्देशों का पालन
- फ्रॉड की जांच और रोकथाम
- RBI रेगुलेशन, इनकम टैक्स एक्ट, प्रिवेंशन ऑफ मनी लॉन्ड्रिंग एक्ट (PMLA), और इमरजेंसी रिस्पॉन्स रिक्वेस्ट जैसे कानूनों के तहत कानूनी जिम्मेदारियां

- डेटा प्रोटेक्शन बोर्ड की पूछताछ

18.2 ज़रूरी डिस्क्लोजर की कॉन्फिडेंशियलिटी

जहां कानूनी तौर पर ज़रूरी हो, TCPL ये करेगा: जानकारी सिर्फ़ उतनी ही बताएगा जितनी कानूनी तौर पर ज़रूरी है; ज़रूरी डिस्क्लोजर के बारे में डेटा सब्जेक्ट को बताने की कोशिश करेगा (जहां कानून द्वारा मना नहीं है); ऑडिट के मकसद से सभी डिस्क्लोजर का रिकॉर्ड रखेगा; जहां सही हो, डिस्क्लोजर रिक्वेस्ट को कम करने की कोशिश करेगा।

18.3 अधिकारों की कोई छूट नहीं

यह प्राइवेसी पॉलिसी देने का मतलब यह नहीं है कि TCPL या डेटा सब्जेक्ट के किसी भी कानूनी अधिकार की छूट है। TCPL अपने हितों की रक्षा करने और अपनी पॉलिसी लागू करने के सभी कानूनी अधिकार सुरक्षित रखता है।

19. इस प्राइवेसी स्टेटमेंट में बदलाव

हम इस प्राइवेसी पॉलिसी को किसी भी समय अपडेट करने का अधिकार रखते हैं ताकि: लागू कानूनों और नियमों में बदलाव दिखाए जा सकें; नए डेटा प्रोटेक्शन प्रैक्टिस लागू किए जा सकें; सेक्टर-स्पेसिफिक रेगुलेटरी अपडेट (RBI गाइडलाइंस, वगैरह) पर जवाब दिया जा सके; हमारी प्राइवेसी प्रैक्टिस की क्लैरिटी या ट्रांसपेरेंसी को बेहतर बनाया जा सके।

19.1 बदलावों की सूचना

डेटा सब्जेक्ट्स को ज़रूरी अपडेट्स ईमेल नोटिफ़िकेशन; वेबसाइट अनाउंसमेंट; यूज़र अकाउंट पोर्टल में अपडेट्स के ज़रिए बताए जाएँगे। ज़रूरी बदलावों के लिए सहमति की दोबारा पुष्टि करनी होगी।

19.2 लागू होने की तारीख

पब्लिकेशन के बाद बदलाव लागू हो जाएँगे। बदलावों के बाद TCPL सर्विस का इस्तेमाल जारी रखना अपडेटेड पॉलिसी की मंज़ूरी दिखाता है।

19.3 पिछले वर्शन का आर्काइव

इस पॉलिसी के पिछले वर्शन मेंटेन किए जाते हैं और रेफरेंस के लिए उपलब्ध हैं। आर्काइव किए गए वर्शन प्राइवेसी पॉलिसी में बदलावों की हिस्ट्री को डॉक्यूमेंट करते हैं।

20. रेफरेंस डॉक्यूमेंट्स

- डिजिटल लेंडिंग पर RBI गाइडलाइंस (2022, अपडेटेड 2025)
- RBI आउटसोर्सिंग गाइडलाइंस
- इन्फॉर्मेशन टेक्नोलॉजी (रीजनेबल सिक्योरिटी प्रैक्टिस और प्रोसीजर और सेंसिटिव पर्सनल डेटा या इन्फॉर्मेशन) रूल्स, 2011
- डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023

- आधार एक्ट, 2016
- ISO 27001:2022 - इन्फॉर्मेशन सिक्योरिटी मैनेजमेंट
- RBI क्रेडिट इन्फॉर्मेशन पॉलिसी
- PCI-DSS - पेमेंट कार्ड इंडस्ट्री डेटा सिक्योरिटी स्टैंडर्ड (अगर लागू हो)
- TCPL इन्फॉर्मेशन सिक्योरिटी मैनेजमेंट सिस्टम (ISMS) डॉक्यूमेंटेशन

21. एनफोर्समेंट

कम्प्लायंस और नतीजे:

सभी कर्मचारी, कॉन्ट्रैक्टर, वेंडर और थर्ड पार्टी सभी डेटा हैंडलिंग एक्टिविटी में इस प्राइवेसी पॉलिसी को फॉलो करेंगे। इस पॉलिसी के किसी भी प्रोविजन का नॉन-कम्प्लायंस एक सीरियस ब्रीच है। उल्लंघन के नतीजे ये हो सकते हैं:

- कर्मचारियों के लिए: नौकरी से निकालने तक की डिसिप्लिनरी कार्रवाई
- कॉन्ट्रैक्टर/वेंडर के लिए: कॉन्ट्रैक्ट खत्म करना और नुकसान के लिए कानूनी कार्रवाई
- तीसरे पक्ष के लिए: कानूनी कार्रवाई और रेगुलेटरी रिपोर्टिंग
- TCPL के लिए: रेगुलेटरी पेनल्टी, जुर्माना और रेप्युटेशन को नुकसान

घटना का बढ़ना:

- किसी भी संदिग्ध उल्लंघन या नॉन-कम्प्लायंस की तुरंत CISO को रिपोर्ट की जानी चाहिए

  पता चले उल्लंघन की रिपोर्ट न करने पर कर्मचारियों पर डिसिप्लिनरी एक्शन हो सकता है।
- घटनाओं को लॉग किया जाता है, उनकी जांच की जाती है, और ज़रूरत पड़ने पर सही अधिकारियों को भेजा जाता है।

रेगुलेटरी रिपोर्टिंग:

- पर्सनल जानकारी से जुड़े डेटा उल्लंघन की रिपोर्ट तय समय में डेटा प्रोटेक्शन बोर्ड को दी जाएगी।
- कानून के हिसाब से गंभीर रेगुलेटरी उल्लंघन की रिपोर्ट RBI या दूसरी अधिकारियों को दी जाएगी।
- ऑडिटर और रेगुलेटरी बॉडी को कम्प्लायंस सर्टिफ़िकेट दिए जाएंगे।

22. पॉलिसी डॉक्यूमेंट मैनेजमेंट

डॉक्यूमेंट जानकारी:

- पॉलिसी ओनर: चीफ़ इन्फॉर्मेशन सिक्योरिटी ऑफ़िसर (CISO)
- पिछला अपडेट: 7 नवंबर, 2025
- अगली रिव्यू तारीख: 7 नवंबर, 2026

- क्लासिफ़िकेशन: इंटरनल और प्रोटेक्टेड

वर्ज़न कंट्रोल:

संस्करण (Version)	तिथि (Date)	परिवर्तन और संशोधन का कारण (Changes & Reason for Revision)
1	13/02/2024	**ISO 27001:2022** अनुपालन के लिए प्रारंभिक अंक।
2	07/11/2025	इसमें शामिल करने के लिए व्यापक अद्यतन: (a) **डिजिटल ऋण दिशानिर्देश** अनुपालन (पैराग्राफ 10 और 12), (b) **क्लिक-रैप एसपी डीआई नियम** अनुपालन (नियम 5(1)), (c) **सीमा-पार डेटा स्थानांतरण** नियंत्रण (धारा 16 डीपीडीपी अधिनियम), (d) क्षेत्र-विशिष्ट **आरबीआई और क्रेडिट ब्यूरो** नियम, (e) नियामक निगरानी और आकस्मिकता योजना तंत्र, (f) कर्मचारी जागरूकता और प्रशिक्षण आवश्यकताएँ।