ટેકફિનો કેપિટલ પ્રાઇવેટ લિમિટેડ

ગોપનીયતા નીતિ

વિગત (Detail)	**મૂલ્ય (Value)**
દસ્તાવેજ નં. (Doc. No.)	ટીસીપીએલ-આઇ એસ એમ એસ-પી એલ-25
ઇશ્યૂ નં. અને તારીખ (Issue No. & Date)	વર્ઝન 2.0 – 07-11-2025
માહિતીનું વર્ગીકરણ (Classification of Information)	આંતરિક અને સુરક્ષિત

વિષયવસ્તુ કોષ્ટક

1. હેતુ

2. અવકાશ

3. ભૂમિકાઓ અને જવાબદારીઓ

4. સંક્ષેપ અને વ્યાખ્યાઓ

5. ફોર્મ્સ

6. નીતિ

7. અમે એકત્રિત કરીએ છીએ તે માહિતી

8. સંમતિ અને ડેટા સંગ્રહ માળખું

9. ડિજિટલ ધિરાણ માર્ગદર્શિકા પાલન

10. અમે તમારી વ્યક્તિગત માહિતી સાથે શું કરીએ છીએ

11. ડેટા શેરિંગ અને તૃતીય-પક્ષ જાહેરાતો

12. ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પાલન

13. ક્ષેત્ર-વિશિષ્ટ ડેટા ટ્રાન્સફર અને સ્થાનિકીકરણ નિયમો

14. અમે તમારી વ્યક્તિગત માહિતી કેટલા સમય સુધી રાખીશું?

15. માહિતી સુરક્ષા પગલાં

16. કૂકીઝનો ઉપયોગ કેવી રીતે થાય છે?

17. અમારો સંપર્ક કેવી રીતે કરવો?

૧૮. કાનૂની સૂચના

૧૯. આ ગોપનીયતા વિધાનમાં ફેરફારો

૨૦. સંદર્ભ દસ્તાવેજો

૨૧. અમલીકરણ

૨૨. નીતિ દસ્તાવેજ વ્યવસ્થાપન

૧. હેતુ

આ નીતિનો હેતુ સમગ્ર સંસ્થામાં યોગ્ય નિયંત્રણો મૂકીને, સમયાંતરે તેમની સમીક્ષા કરીને અને જરૂરિયાત મુજબ તેમાં સુધારો કરીને, વ્યક્તિગત માહિતી (વ્યક્તિગત રીતે ઓળખી શકાય તેવી માહિતી અથવા PII સહિત) અને સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી (SPDI) ને સુરક્ષિત રાખવાનો છે.

આ સંસ્થા ગ્રાહકો પાસેથી ગોપનીયતા સંબંધિત સંબંધિત કાનૂની આવશ્યકતાઓ અને કરારની આવશ્યકતાઓનું પાલન સુનિશ્ચિત કરે છે, જેમાં નીચેનાનો સમાવેશ થાય છે:

• ભારતીય રિઝર્વ બેંક (RBI) દ્વારા જારી કરાયેલ ડિજિટલ ધિરાણ માર્ગદર્શિકા

• માહિતી ટેકનોલોજી (વાજબી સુરક્ષા પ્રથાઓ અને પ્રક્રિયાઓ અને સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી) નિયમો, 2011 ("SPDI નિયમો")

• ડિજિટલ વ્યક્તિગત ડેટા સુરક્ષા અધિનિયમ, 2023 અને સંબંધિત નિયમો

• ડિજિટલ ધિરાણ, આઉટસોર્સિંગ અને ડેટા સ્ટોરેજ પર RBI માર્ગદર્શિકા

• ક્રેડિટ બ્યુરો નિયમો અને ક્ષેત્રીય ડેટા સુરક્ષા આવશ્યકતાઓ

• ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર સંબંધિત તમામ લાગુ સ્થાનિક, રાજ્ય અને કેન્દ્ર સરકારના નિયમો

2. અવકાશ

આ નીતિના અવકાશમાં શામેલ છે:

• TCPL ના બધા કર્મચારીઓ અને અમારા વ્યવસાયિક સહયોગીઓ કે જેઓ વ્યક્તિગત માહિતી અને સંવેદનશીલ વ્યક્તિગત ડેટાના સંગ્રહ, ઉપયોગ, જાળવણી, ખુલાસો અને નિકાલ માટે જવાબદાર છે અથવા જવાબદાર છે

• TCPL અથવા તેના આનુષંગિકો દ્વારા TCPL ના ઓનલાઇન પોર્ટલ, ઇલેક્ટ્રોનિક સંદેશાવ્યવહાર અથવા વ્યવસાય પ્રક્રિયાઓ દ્વારા સીધા ગ્રાહકો પાસેથી એકત્રિત કરવામાં આવેલી બધી વ્યક્તિગત માહિતી અને સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી

• બધા ક્રોસ-બોર્ડર ડેટા ફ્લો અને આંતરરાષ્ટ્રીય ડેટા ટ્રાન્સફર

• બધા તૃતીય-પક્ષ ડેટા પ્રોસેસિંગમાં સામેલ સેવા પ્રદાતાઓ, વિક્રેતાઓ અને આઉટસોર્સિંગ ભાગીદારો

3.

ભૂમિકા (Role)	**જવાબદારી (Responsibility)**
ચીફ ઇન્ફોર્મેશન સિક્યુરિટી ઓફિસર (CISO)	તમામ ફરજિયાત દસ્તાવેજો અને પાલન નીતિઓને મંજૂરી આપો. ડેટા સંરક્ષણ અને ગોપનીયતા પાલનની દેખરેખ. સત્તાધિકારી અને નિયમનકારી સંસ્થાઓ સાથે મંજૂરી અને સંચાર. સરહદ-પાર ડેટા ટ્રાન્સફર પાલન માળખું જગ્યાએ છે તેની ખાતરી કરો.
પાલન અધિકારી / કાયદાકીય ટીમ	ડિજિટલ પર્સનલ ડેટા પ્રોટેક્શન એક્ટ, 2023ની કલમ 16 હેઠળ સૂચનાઓ માટે નિયમનકારી વોચ જાળવી રાખો. MeitY, RBI અને ડેટા પ્રોટેક્શન બોર્ડ તરફથી અપડેટ્સનું નિરીક્ષણ કરો. સરહદ-પાર ડેટા પ્રવાહની સૂચિ જાળવો અને અપડેટ કરો. તમામ નવા સરહદ-પાર ડેટા ટ્રાન્સફર અને તૃતીય-પક્ષ સેવાઓની સમીક્ષા કરો અને મંજૂરી આપો.
	ક્ષેત્ર-વિશિષ્ટ નિયમનકારી પાલન મૂલ્યાંકનોનું સંકલન કરો.
આઇટી/ઇન્ફ્રાસ્ટ્રક્ચરના વડા	ડેટા સુરક્ષા માટે તકનીકી નિયંત્રણોનો અમલ કરો. વિક્રેતા સંબંધોનું સંચાલન કરો અને ડેટા સ્થાનિકીકરણ આવશ્યકતાઓને સુનિશ્ચિત કરો. મંજૂર અધિકારક્ષેત્રોમાં વૈકલ્પિક ડેટા સ્ટોરેજ સોલ્યુશન્સ જાળવી રાખો. પ્રતિબંધિત દેશની સૂચનાઓ પર તરત જ પ્રતિસાદ આપો.
માનવ સંસાધન વડા	આ નીતિનું દસ્તાવેજ, સંચાર કરો અને અમલ અને જાળવણી સુનિશ્ચિત કરો. સરહદ-પાર ડેટા ટ્રાન્સફર પ્રતિબંધો પર સ્ટાફ જાગૃતિ તાલીમનું આયોજન કરો. ખાતરી કરો કે તમામ સ્ટાફ ડેટા હેન્ડલિંગ આવશ્યકતાઓને સમજે છે.

4. સંક્ષેપ અને વ્યાખ્યાઓ

સંક્ષેપ (Abbreviation)	**વિસ્તરણ (Expansion)**
ટીસીપીએલ	ટેકફિનો કેપિટલ પ્રાઇવેટ લિમિટેડ
ડીપીડીપી એક્ટ	ડેટા પ્રોટેક્શન એક્ટ, 2023
એસપીડીઆઈ રૂલ્સ	ઇન્ફોર્મેશન ટેકનોલોજી (વાજબી સુરક્ષા પદ્ધતિઓ અને પ્રક્રિયાઓ અને સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી) નિયમો, 2011
આરબીઆઈ	રિઝર્વ બેંક ઓફ ઇન્ડિયા
મેઇટીવાય	ઇલેક્ટ્રોનિક્સ અને ઇન્ફોર્મેશન ટેકનોલોજી મંત્રાલય
ડીએલજી	ડિજિટલ લેન્ડિંગ માર્ગદર્શિકા (RBI)
પીઆઈઆઈ	વ્યક્તિગત રીતે ઓળખી શકાય તેવી માહિતી
એસપીડીઆઈ	સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી
એમએલઆઈ	સભ્ય ધિરાણ સંસ્થા
સીઆઈએસઓ	ચીફ ઇન્ફોર્મેશન સિક્યુરિટી ઓફિસર
સાસ	સેવા તરીકે સોફ્ટવેર

4.2 વ્યાખ્યાઓ

શબ્દો (Terms)	**વ્યાખ્યાઓ (Definitions)**
વ્યક્તિગત માહિતી	કોઈપણ માહિતી જે કુદરતી વ્યક્તિ સાથે સીધી કે આડકતરી રીતે સંબંધિત છે, TCPL પાસે ઉપલબ્ધ અથવા ઉપલબ્ધ થવાની સંભાવના હોય તેવી અન્ય માહિતીના સંયોજનમાં, તે વ્યક્તિને ઓળખવા માટે સક્ષમ છે. આમાં નામ, ઇમેઇલ, સંપર્ક વિગતો, સરનામું, હોદ્દો, ક્રેડિટ માહિતી અને અન્ય કોઈપણ ઓળખી શકાય તેવો ડેટા શામેલ છે.

સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી (SPDI)	એસપીડીઆઈ નિયમો, 2011 ના નિયમ 3 હેઠળ વ્યાખ્યાયિત કર્યા મુજબ, આમાં શામેલ છે: પાસવર્ડ્સ; બેંક ખાતું, ક્રેડિટ કાર્ડ, ડેબિટ કાર્ડ વિગતો જેવી નાણાકીય માહિતી; શારીરિક, શારીરધર્મ અને માનસિક સ્વાસ્થ્યની સ્થિતિ; જાતીય અભિગમ; તબીબી રેકોર્ડ અને ઇતિહાસ; બાયોમેટ્રિક માહિતી; આનુવંશિક માહિતી; વેપાર અને નાણાકીય ઇતિહાસ; આગળ શેર ન કરવાના સ્પષ્ટ હેતુ સાથે પૂરી પાડવામાં આવેલી કોઈપણ માહિતી.
સંમતિ	ડેટા વિષય દ્વારા તેમની વ્યક્તિગત માહિતી અથવા એસપીડીઆઈના સંગ્રહ, પ્રક્રિયા, ઉપયોગ અને જાહેર કરવા માટે સ્વૈચ્છિક, જાણકાર અને સ્પષ્ટ કરાર. સંમતિ સ્પષ્ટ, પૂર્વ અને દસ્તાવેજી ઓડિટ ટ્રેલ સાથે ક્લિક-રેપ મિકેનિઝમ દ્વારા મેળવવી આવશ્યક છે.
ક્લિક-રેપ મિકેનિઝમ	એક ઇલેક્ટ્રોનિક સંમતિ પદ્ધતિ જ્યાં ડેટા એકત્રિત અથવા પ્રક્રિયા થાય તે પહેલાં શરતોની સમજણ અને સ્વીકૃતિની પુષ્ટિ કરવા માટે વપરાશકર્તાએ સક્રિયપણે "હું સંમત છું," "સ્વીકારો," અથવા સમાન ક્રિયા પર ક્લિક કરવું આવશ્યક છે. ઇલેક્ટ્રોનિક ઓડિટ ટ્રેલ બનાવવા માટે સિસ્ટમે ટાઇમસ્ટેમ્પ, વપરાશકર્તાની ક્રિયા અને આઈપી એડ્રેસ રેકોર્ડ કરવું આવશ્યક છે.
ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર	ક્લાઉડ સ્ટોરેજ, સાસ પ્લેટફોર્મ, આઉટસોર્સિંગ ભાગીદારી, આંતરરાષ્ટ્રીય કચેરીઓ અથવા અન્ય કોઈપણ માધ્યમ દ્વારા ભારતમાંથી ભારતની બહારના કોઈપણ દેશમાં વ્યક્તિગત માહિતી અથવા એસપીડીઆઈની હિલચાલ.
પ્રતિબંધિત દેશ	ડીપીડીપી એક્ટ, 2023 ની કલમ 16 હેઠળ વ્યક્તિગત ડેટા ટ્રાન્સફર માટે પ્રતિબંધિત તરીકે ભારતની કેન્દ્ર સરકાર દ્વારા સૂચિત કરાયેલ કોઈપણ દેશ અથવા અધિકારક્ષેત્ર.
ડેટા લોકલાઇઝેશન	લાગુ કાયદાઓ અથવા નિયમો દ્વારા ફરજિયાત કર્યા મુજબ, ચોક્કસ ભૌગોલિક અધિકારક્ષેત્રમાં, સામાન્ય રીતે ભારતમાં, વ્યક્તિગત માહિતી અથવા એસપીડીઆઈ જાળવવાની આવશ્યકતા અથવા પ્રથા.

5. ફોર્મ

દસ્તાવેજનું નામ ફોર્મ નં.

6. નીતિ

TCPL સંસ્થા સાથે રહેતી તેમની વ્યક્તિગત માહિતીની ગોપનીયતા, ગુપ્તતા અને સુરક્ષા અંગે તેના ગ્રાહકોની અપેક્ષાઓને ઓળખે છે.

TCPL સભ્ય ધિરાણ સંસ્થાઓ (MLIs) સાથે કામ કરી રહ્યું છે, જે બેંકિંગ અને નાણાકીય સેવાઓ ઉદ્યોગમાં છે અને વિવિધ ક્રેડિટ ગેરંટી યોજનાઓ હેઠળ TCPL સાથે નોંધાયેલ છે. ઉધાર લેનારાઓની વ્યક્તિગત માહિતીને સુરક્ષિત રાખવી, એકત્રિત માહિતીનો ઉપયોગ ફક્ત કાયદેસર વ્યવસાય અને ડેટા માન્યતા હેતુઓ માટે કરવો અને માહિતીના કોઈપણ દુરુપયોગને અટકાવવો એ TCPL માટે ટોચની પ્રાથમિકતા છે.

TCPL એ ઉધાર લેનારાઓ અને સભ્ય ધિરાણ સંસ્થાઓ (MLIs) અને અન્ય વ્યવસાયિક ભાગીદારો દ્વારા સોંપવામાં આવેલા અને જાહેર કરાયેલા અન્ય ડેટા વિષયોની વ્યક્તિગત માહિતીને સુરક્ષિત રાખવા માટે એક વ્યાપક ગોપનીયતા નીતિ અપનાવી છે.

TCPL એ ઉધાર લેનારાઓ અને સભ્ય ધિરાણ સંસ્થાઓ (MLIs) અને અન્ય વ્યવસાયિક ભાગીદારો દ્વારા સોંપવામાં આવેલા અને જાહેર કરાયેલા અન્ય ડેટા વિષયોની વ્યક્તિગત માહિતીને સુરક્ષિત રાખવાનો હેતુ છે.

TCPL એ એક વ્યાપક ગોપનીયતા નીતિ અપનાવી છે જેનો હેતુ ઉધાર લેનારાઓ અને સભ્ય ધિરાણ સંસ્થાઓ (MLIs) અને અન્ય વ્યવસાયિક ભાગીદારો દ્વારા સોંપવામાં આવેલા અને જાહેર કરાયેલા અન્ય ડેટા વિષયોની વ્યક્તિગત માહિતીને સુરક્ષિત રાખવાનો છે.

ગોપનીયતા નીતિ સંસ્થા કેવી રીતે કાર્ય કરે છે તેનું સંચાલન કરે છે:

• વ્યક્તિગત માહિતી અને સંવેદનશીલ વ્યક્તિગત ડેટા એકત્રિત કરે છે

• આવી માહિતીનો ઉપયોગ કરે છે, જાહેર કરે છે, સંગ્રહ કરે છે અને સુરક્ષિત કરે છે

• DPDP કાયદાની કલમ 16 અને RBI માર્ગદર્શિકા અનુસાર ક્રોસ-બોર્ડર ટ્રાન્સફરનું સંચાલન કરે છે

• રીટેન્શન સમયગાળાના અંતે વ્યક્તિગત માહિતીનો નિકાલ કરે છે

• ડિજિટલ લેન્ડિંગ માર્ગદર્શિકા, ખાસ કરીને ફકરા 10 અને 12 નું પાલન સુનિશ્ચિત કરે છે

TCPL પ્રતિબદ્ધ છે:

• બધા ડેટા સંગ્રહ અને પ્રક્રિયા માટે ક્લિક-રેપ મિકેનિઝમ દ્વારા સ્પષ્ટ, પૂર્વ સંમતિ મેળવો

• બધી ડેટા હેન્ડલિંગ પ્રવૃત્તિઓમાં પારદર્શિતા જાળવો

• ડેટા વિષયોના તેમના ડેટાને ઍક્સેસ કરવા, સુધારવા, કાઢી નાખવા અને પોર્ટ કરવાના અધિકારોનો આદર કરો

• ISO 27001:2022 અનુસાર મજબૂત સુરક્ષા નિયંત્રણો લાગુ કરો

• બધા ક્ષેત્ર-વિશિષ્ટ નિયમોનું પાલન કરો, ખાસ કરીને ડિજિટલ ધિરાણ અને ડેટા સ્થાનિકીકરણ પર RBI માર્ગદર્શિકા

• નિયમિતપણે ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પ્રથાઓનું ઓડિટ અને અપડેટ કરો

7. અમે એકત્રિત કરીએ છીએ તે માહિતી

અમે ડિજિટલ લેન્ડિંગ માર્ગદર્શિકા અને SPDI નિયમોનું કડક પાલન કરીને, કાયદેસર વ્યવસાયિક હેતુઓ માટે જરૂરી માહિતી જ એકત્રિત કરીએ છીએ.

૭.૧ વ્યક્તિગત માહિતી

તમારે વ્યક્તિગત માહિતી પ્રદાન કરવાની જરૂર પડી શકે છે જેમ કે:

• પૂરું નામ

• ઇમેઇલ આઈડી અને સંપર્ક વિગતો (ફોન, મોબાઇલ)

• રહેણાંક અને પત્રવ્યવહાર સરનામું

• હોદ્દો અને રોજગાર વિગતો

• ક્રેડિટ માહિતી અને નાણાકીય ઇતિહાસ

• ઉધાર લેનાર ઓળખ વિગતો

• અનન્ય ઓળખ નંબરો (લાગુ પડતું હોય તેમ)

૭.૨ સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી (SPDI)

જ્યારે લાગુ પડે અને સ્પષ્ટ સંમતિ સાથે, અમે એકત્રિત કરી શકીએ છીએ:

• નાણાકીય માહિતી (બેંક ખાતાની વિગતો, ક્રેડિટ કાર્ડ, ડેબિટ કાર્ડ નંબર)

• તબીબી રેકોર્ડ અને આરોગ્ય સંબંધિત માહિતી

• બાયોમેટ્રિક માહિતી (લાગુ પડતા નિયમો મુજબ ફિંગરપ્રિન્ટ્સ, આઇરિસ સ્કેન)

• શારીરિક, શારીરિક અને માનસિક સ્વાસ્થ્ય સ્થિતિ

• આનુવંશિક માહિતી

• વેપાર ઇતિહાસ અને નાણાકીય પ્રદર્શન ડેટા

• પાસવર્ડ અને સુરક્ષા ઓળખપત્રો

૭.૩ સંગ્રહ પદ્ધતિઓ

અમે વ્યક્તિગત માહિતી એકત્રિત કરી શકીએ છીએ:

• જ્યારે તમે સાઇન અપ કરો છો, નોંધણી કરો છો, સેવાઓની વિનંતી કરો છો અથવા સ્વેચ્છાએ માહિતી પ્રદાન કરો છો ત્યારે સીધી તમારી પાસેથી

• તમારા એમ્પ્લોયર અથવા સભ્ય ધિરાણ સંસ્થાઓ (MLI) દ્વારા

• જાહેરમાં ઉપલબ્ધ ડેટાબેઝમાંથી (જ્યાં કાયદા દ્વારા પરવાનગી આપવામાં આવી છે)

• તૃતીય-પક્ષ ભાગીદારો પાસેથી જેમની સાથે તમે અધિકૃત છો માહિતી શેરિંગ

• અમારા ડિજિટલ પ્લેટફોર્મ પર વિશ્લેષણાત્મક સાધનો અને કૂકીઝ દ્વારા

8. સંમતિ અને ડેટા સંગ્રહ માળખું

8.1 સ્પષ્ટ સંમતિની આવશ્યકતા

TCPL કોઈપણ વ્યક્તિગત માહિતી અથવા SPDI એકત્રિત કરતા, પ્રક્રિયા કરતા અથવા શેર કરતા પહેલા બધા ડેટા વિષયો પાસેથી સ્પષ્ટ, પૂર્વ લેખિત સંમતિ મેળવશે. સંમતિ આ હશે:

• સ્વૈચ્છિક: બળજબરીથી અથવા દબાણ હેઠળ મેળવવામાં આવશે નહીં

• જાણકાર: ડેટા વિષયે ડેટા સંગ્રહના હેતુ, અવકાશ અને અસરોને સમજવી આવશ્યક છે

• ચોક્કસ: સંગ્રહ અને પ્રક્રિયાના દરેક હેતુ માટે સ્પષ્ટ રીતે વ્યાખ્યાયિત

• અસ્પષ્ટ ડ: સ્પષ્ટ હકારાત્મક કાર્યવાહી દ્વારા વ્યક્ત

8.2 ક્લિક-રેપ સંમતિ પદ્ધતિ (નિયમ 5(1) - SPDI નિયમો, 2011)

વ્યક્તિગત માહિતી અને SPDI સંગ્રહ માટે તમામ સંમતિ SPDI નિયમો, 2011 ના નિયમ 5(1) ના પાલનમાં ઇલેક્ટ્રોનિક ક્લિક-રેપ પદ્ધતિ દ્વારા મેળવવામાં આવશે. પદ્ધતિમાં શામેલ હશે:

ફરજિયાત તત્વો:

1. સ્પષ્ટ અને સ્પષ્ટ સૂચના: કોઈપણ ડેટા સંગ્રહ પહેલાં, એક અગ્રણી સૂચના પ્રદર્શિત કરવી આવશ્યક છે: ડેટા સંગ્રહનો હેતુ; એકત્રિત કરવામાં આવતા ડેટાનો પ્રકાર; ડેટાનો હેતુપૂર્વક ઉપયોગ અને શેરિંગ; ડેટા રીટેન્શનનો સમયગાળો; ડેટા વિષયના અધિકારો.

2. સક્રિય પસંદગી: ડેટા વિષયે સંમતિ દર્શાવવા માટે "હું સંમત છું," "સ્વીકારો," "પુષ્ટિ કરો," અથવા સમાન બટન પર સક્રિયપણે ક્લિક કરવું આવશ્યક છે. પૂર્વ-ચેક કરેલા બોક્સને મંજૂરી નથી.

3. ઓડિટ ટ્રેઇલ: સિસ્ટમે આપમેળે રેકોર્ડ અને જાળવણી કરવી જોઈએ: સંમતિનો સમયપત્રક; ડેટા વિષયનો IP સરનામું; સંમતિ આપનાર પક્ષનો અનન્ય ઓળખકર્તા અથવા ઇમેઇલ; સંમતિ શરતોનું સંસ્કરણ સ્વીકૃત; સંમતિની પદ્ધતિ (ક્લિક-રેપ); સંમતિમાં કોઈપણ ફેરફારો.

૪. સુલભતા: સંમતિ ફોર્મ્સ આ હોવા જોઈએ: સાદી, સમજી શકાય તેવી ભાષામાં; બહુવિધ ભાષાઓમાં ઉપલબ્ધ (અંગ્રેજી, હિન્દી અને લાગુ પડતી સ્થાનિક ભાષાઓ); અપંગ વ્યક્તિઓ માટે સુલભ; સરળતાથી છાપી શકાય તેવું અને ડાઉનલોડ કરી શકાય તેવું.

૫. અલગ સંમતિ: વિવિધ હેતુઓ માટે અલગ સંમતિ ફોર્મ્સ હોવા જોઈએ: સામાન્ય વ્યક્તિગત માહિતીના સંગ્રહ માટે સંમતિ; SPDI ના સંગ્રહ માટે અલગ સંમતિ; તૃતીય પક્ષો સાથે ડેટા શેરિંગ માટે અલગ સંમતિ; ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર માટે અલગ સંમતિ; માર્કેટિંગ અથવા વિશ્લેષણ હેતુઓ માટે અલગ સંમતિ.

૬. રદબાતલ: ડેટા વિષયો admin@techfino.in પર વિનંતી સબમિટ કરીને કોઈપણ સમયે સંમતિ પાછી ખેંચી શકશે. TCPL સંમતિ પાછી ખેંચવાના 5 કાર્યકારી દિવસોમાં પ્રક્રિયા બંધ કરશે.

૮.૩ તૃતીય-પક્ષ શેરિંગ માટે સંમતિ

કોઈપણ તૃતીય પક્ષ સાથે વ્યક્તિગત માહિતી અથવા SPDI શેર કરતા પહેલા, TCPL એ:

• ડેટા વિષય પાસેથી ચોક્કસ લેખિત સંમતિ મેળવશે

• તૃતીય પક્ષ અથવા તૃતીય પક્ષોની શ્રેણીની ઓળખ જાહેર કરશે

• શેરિંગનો હેતુ સમજાવશે

• કયો ડેટા શેર કરવામાં આવશે તે સ્પષ્ટ કરશે

• ડેટા વિષયોને TCPL સેવાઓનો ઉપયોગ કરવાની તેમની ક્ષમતાને અસર કર્યા વિના શેર કરવાનો ઇનકાર કરવાની મંજૂરી આપશે

૯. ડિજિટલ ધિરાણ માર્ગદર્શિકા પાલન

TCPL આના દ્વારા RBI ના ડિજિટલ ધિરાણ માર્ગદર્શિકાનું પાલન સુનિશ્ચિત કરે છે:

ડેટા સંગ્રહ ધોરણો:

• વ્યક્તિગત અને નાણાકીય માહિતીનો સંગ્રહ સખત જરૂરિયાત-આધારિત છે

• ડેટા સંગ્રહ ક્રેડિટ મૂલ્યાંકન, લોન ઉત્પત્તિ અને નિયમનકારી પાલન માટે જરૂરી માહિતી સુધી મર્યાદિત છે

• કોઈ અતિશય અથવા બિનજરૂરી ડેટા એકત્રિત કરવામાં આવતો નથી

• વિનંતી કરાયેલ દરેક ડેટા તત્વ માટે ડેટા વિષયોને વ્યવસાય હેતુ વિશે સ્પષ્ટપણે જાણ કરવામાં આવે છે

હેતુ મર્યાદા:

• વ્યક્તિગત માહિતીનો ઉપયોગ ફક્ત તે હેતુ માટે થાય છે જેના માટે તે એકત્રિત કરવામાં આવી હતી

• મૂળ હેતુથી આગળના કોઈપણ ઉપયોગ માટે તાજી, સ્પષ્ટ સંમતિની જરૂર છે

• TCPL અલગ સંમતિ મેળવ્યા વિના અસંબંધિત હેતુઓ માટે ડેટાનો ફરીથી ઉપયોગ કરશે નહીં

• વિશ્લેષણ, માર્કેટિંગ અથવા ગૌણ હેતુઓ માટે ડેટાના બધા ઉપયોગો જરૂરી છે સ્પષ્ટ સંમતિ

તૃતીય-પક્ષ શેરિંગ નિયંત્રણો:

• ડેટા વિષયની સ્પષ્ટ, પૂર્વ સંમતિ વિના તૃતીય પક્ષો સાથે વ્યક્તિગત માહિતી શેર કરવામાં આવતી નથી

• એવા કિસ્સાઓમાં જ્યાં શેરિંગ કાયદેસર રીતે ફરજિયાત છે (RBI, ક્રેડિટ બ્યુરો નિયમો, વૈધાનિક આવશ્યકતાઓ દ્વારા), TCPL ડેટા વિષયને આવા ફરજિયાત શેરિંગની જાણ કરશે

• ક્રેડિટ બ્યુરો શેરિંગ ફક્ત ક્રેડિટ રિપોર્ટિંગ હેતુઓ માટે જરૂરી માહિતી સુધી મર્યાદિત છે

• સ્પષ્ટ ડેટા વિષયની સંમતિ વિના પ્રમોશનલ, માર્કેટિંગ અથવા બિન-આવશ્યક તૃતીય-પક્ષ હેતુઓ માટે કોઈ ડેટા શેર કરવામાં આવતો નથી

ઋણ લેનાર સશક્તિકરણ:

• TCPL દેવાદારોને તેમના ડેટાની ઍક્સેસ કોની પાસે છે તે વિશે સ્પષ્ટ માહિતી પૂરી પાડે છે

• દેવાદારો બધા તૃતીય પક્ષોને જાણવાની વિનંતી કરી શકે છે જેમની સાથે તેમનો ડેટા શેર કરવામાં આવે છે

• દેવાદારો ડેટા શેરિંગને પ્રતિબંધિત કરી શકે છે (જ્યાં કાયદેસર રીતે માન્ય છે)

• દેવાદારો તેમના ખાતાથી સંબંધિત તમામ ડેટા ઍક્સેસ અને શેરિંગ ઇવેન્ટ્સનો ઓડિટ લોગ જોઇ શકે છે

• દેવાદારો વિનંતી પર TCPL સિસ્ટમોમાંથી ડેટા ભૂંસી નાખવા અને દૂર કરવાનું ટ્રિગર કરી શકે છે, કાનૂની રીટેન્શન આવશ્યકતાઓને આધીન

ડેટા પ્રેક્ટિસમાં પારદર્શિતા:

• આ ગોપનીયતા નીતિ સ્પષ્ટપણે તમામ ડેટા હેન્ડલિંગ પ્રથાઓની રૂપરેખા આપે છે

• ડેટા વિષયોને તેમના ડેટાનો ઉપયોગ, શેરિંગ, સંગ્રહિત અને સુરક્ષિત

• TCPL એક ડેટા રજિસ્ટર જાળવે છે જે તમામ ડેટા સંગ્રહ, પ્રક્રિયા અને શેરિંગ પ્રવૃત્તિઓનું દસ્તાવેજીકરણ કરે છે

• વિનંતી પર નિયમનકારી અધિકારીઓ માટે નિયમિત પારદર્શિતા અહેવાલો તૈયાર કરવામાં આવે છે

જવાબદારી પદ્ધતિઓ:

• એક સમર્પિત પાલન ટીમ તમામ ડેટા હેન્ડલિંગ પ્રવૃત્તિઓનું નિરીક્ષણ કરે છે

• આ નીતિ અને લાગુ કાયદાઓનું પાલન સુનિશ્ચિત કરવા માટે નિયમિત આંતરિક ઓડિટ હાથ ધરવામાં આવે છે

• તમામ ડેટા ઍક્સેસ, પ્રક્રિયા અને શેરિંગ માટે ઓડિટ ટ્રેઇલ જાળવવામાં આવે છે

• વરિષ્ઠ મેનેજમેન્ટ ત્રિમાસિક ધોરણે ડેટા હેન્ડલિંગ પ્રથાઓની સમીક્ષા કરે છે

• બિન-પાલન તાત્કાલિક CISO અને પાલન અધિકારીને મોકલવામાં આવે છે

ફરિયાદ નિવારણ:

• ડેટા વિષયો admin@techfino.in પર ગોપનીયતા ફરિયાદો સબમિટ કરી શકે છે

• ફરિયાદો 5 કાર્યકારી દિવસોમાં સ્વીકારવામાં આવે છે

• TCPL 30 દિવસની અંદર ફરિયાદોનું નિરાકરણ કરવા માટે પ્રતિબદ્ધ છે

• ડેટા વિષયો એપ્લિકેશન કરી શકે છે જો TCPL ના જવાબથી સંતુષ્ટ ન હોવ તો RBI અથવા સક્ષમ અધિકારીઓનો સંપર્ક કરો.

૧૦. તમારી વ્યક્તિગત માહિતી સાથે અમે શું કરીએ છીએ.

૧૦.૧ ઉપયોગનો હેતુ.

અમે વ્યક્તિગત માહિતી અને SPDI નો ઉપયોગ ફક્ત તે ચોક્કસ હેતુઓ માટે કરીએ છીએ જેના માટે તે પૂરી પાડવામાં આવે છે અને સુસંગત હેતુઓ માટે જે ડેટા વિષયો વાજબી રીતે અપેક્ષા રાખે છે. આ હેતુઓમાં શામેલ છે:

કાયદેસર વ્યવસાયિક હેતુઓ:

• ક્રેડિટ મૂલ્યાંકન અને લોન અંડરરાઇટિંગ

• લોન વિતરણ અને ચુકવણી વ્યવસ્થાપન

• નિયમનકારી પાલન અને RBI અને ક્રેડિટ બ્યુરોને રિપોર્ટિંગ

• ઓળખ ચકાસણી અને KYC (તમારા ગ્રાહકને જાણો) આવશ્યકતાઓ

• છેતરપિંડી નિવારણ અને શોધ

• ગ્રાહક સેવા અને સમર્થન

• રેકોર્ડ અપડેટ કરવા અને ગ્રાહકની સચોટ માહિતી જાળવવા

આવશ્યક કાર્યકારી હેતુઓ:

• ઉધાર લેનારાઓ અને સભ્ય ધિરાણ સંસ્થાઓ (MLI) સાથેના કરારો હેઠળ જવાબદારીઓનું સંચાલન, સંચાલન અને પરિપૂર્ણ કરવા

• સરકાર, RBI, અદાલતો અથવા અન્ય સત્તાવાળાઓ તરફથી કાનૂની અને નિયમનકારી આવશ્યકતાઓનું પાલન કરવા

• ઓડિટ અને પાલન હેતુઓ માટે રેકોર્ડ જાળવવા

• અનધિકૃત ઍક્સેસ અથવા છેતરપિંડી અટકાવવા અથવા શોધવા માટે

વિશ્લેષણાત્મક અને સુધારણા (માત્ર સ્પષ્ટ સંમતિ સાથે):

• વ્યવસાયિક ગુપ્ત માહિતી માટે ઉધાર લેનારા ડેટામાં વલણોનું વિશ્લેષણ (માત્ર અલગ સંમતિ સાથે)

• અમારી સેવાઓ અને વપરાશકર્તા અનુભવમાં સુધારો (માત્ર અલગ સંમતિ સાથે)

• ધિરાણ પ્રથાઓ અને બજાર વલણો પર સંશોધન કરવું (માત્ર અનામી/ઉપનામી ડેટા સાથે)

11. ડેટા શેરિંગ અને તૃતીય-પક્ષ જાહેરાતો

11.1 શેરિંગ સિવાયની પ્રતિબદ્ધતા

TCPL ડેટા શેરિંગ સંબંધિત નીચેના સિદ્ધાંતોનું પાલન કરે છે:

• અમે આ નીતિમાં સ્પષ્ટ રીતે પરવાનગી આપવામાં આવી હોય તે સિવાય કોઈપણ તૃતીય પક્ષને વ્યક્તિગત ડેટા શેર કે વેચતા નથી

• અમે માર્કેટિંગ, જાહેરાત અથવા બ્રોકર વ્યવસ્થા દ્વારા વ્યક્તિગત ડેટાનું મુદ્રીકરણ કરતા નથી

• અમે વ્યાપારી લાભ માટે ડેટા બ્રોકર્સ અથવા વાણિજ્યિક સંસ્થાઓને વ્યક્તિગત ડેટા ટ્રાન્સફર કરતા નથી

૧૧.૨ પરવાનગી આપેલ ડેટા શેરિંગ

વ્યક્તિગત માહિતી અથવા SPDI ફક્ત નીચેના સંજોગોમાં જ તૃતીય પક્ષો સાથે શેર કરી શકાય છે:

૧. સ્પષ્ટ ડેટા વિષય સંમતિ સાથે

TCPL ડેટા વિષયને સ્પષ્ટ ખુલાસો પ્રદાન કરે છે: તૃતીય પક્ષોની ઓળખ અથવા શ્રેણી; શેરિંગનો હેતુ; કયો ચોક્કસ ડેટા શેર કરવામાં આવશે; તૃતીય પક્ષો દ્વારા ઍક્સેસનો સમયગાળો. ડેટા વિષયો TCPL સેવાઓની તેમની ઍક્સેસને દંડ કર્યા વિના શેર કરવાનો ઇનકાર કરી શકે છે.

2. કાયદેસર રીતે જરૂરી ખુલાસાઓ સાથે

• ભારતીય રિઝર્વ બેંક (RBI): ડિજિટલ ધિરાણ માર્ગદર્શિકા દ્વારા જરૂરી લોન ડેટા, ઉધાર લેનાર માહિતી અને પાલન અહેવાલો

• ક્રેડિટ બ્યુરો: ક્રેડિટ ઇતિહાસ અને ચુકવણી માહિતી (ક્રેડિટ બ્યુરો નિયમોમાં ઉલ્લેખિત હેતુઓ સુધી મર્યાદિત)

• સરકારી એજન્સીઓ: કર સત્તાવાળાઓ, કાયદા અમલીકરણ, અથવા કાનૂની સત્તા હેઠળ કાર્યરત અન્ય સરકારી સંસ્થાઓ

• અદાલતો અને ન્યાયિક આદેશો: કોર્ટના આદેશો, કાનૂની સમન્સ અથવા ન્યાયિક નિર્દેશોનો પ્રતિભાવ

• નિયમનકારી સત્તાવાળાઓ: ડેટા પ્રોટેક્શન બોર્ડ, ઇલેક્ટ્રોનિક્સ અને માહિતી ટેકનોલોજી મંત્રાલય (MeitY), અથવા અન્ય નિયમનકારી સંસ્થાઓ

• નાણાકીય ગુપ્તચર એકમ (FIU): શંકાસ્પદ વ્યવહાર અહેવાલો અને એન્ટી-મની લોન્ડરિંગ (AML) પાલન

12. ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પાલન

TCPL DPDP એક્ટ, 2023 હેઠળ કેન્દ્ર સરકાર દ્વારા ફરજિયાત કરાયેલ ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પરના તમામ પ્રતિબંધોનું પાલન કરશે. વિદેશી અધિકારક્ષેત્રોમાં તમામ વ્યક્તિગત ડેટા ટ્રાન્સફર સરકારી સૂચના અને મંજૂરીને આધીન છે.

૧૨.૨ નિયમનકારી દેખરેખ - પ્રતિબંધિત દેશોનું નિરીક્ષણ

નિયુક્ત જવાબદારી:

પાલન અધિકારી અથવા કાનૂની ટીમને ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પ્રતિબંધો સંબંધિત તમામ સૂચનાઓ અને અપડેટ્સનું નિરીક્ષણ કરવાની જવાબદારી સોંપવામાં આવી છે. આ કાર્યને એક મહત્વપૂર્ણ પાલન પ્રવૃત્તિ તરીકે ગણવામાં આવશે.

મોનિટરિંગ મિકેનિઝમ્સ:

• પ્રાથમિક સ્ત્રોત: MeitY, ડેટા પ્રોટેક્શન બોર્ડ, RBI અને ટેલિકોમ્યુનિકેશન વિભાગ તરફથી સત્તાવાર સરકારી સૂચનાઓની નિયમિત તપાસ

• ગૌણ સ્ત્રોત: ઉદ્યોગ સંગઠનો (ASSOCHAM, FICCI, CII, NASSCOM, ફિનટેક કન્સોર્ટિયમ), કાનૂની અને પાલન મંચ, નિયમનકારી ન્યૂઝલેટર્સ

• આવર્તન: નિયમનકારી અપડેટ્સની માસિક સમીક્ષા; જો કોઈ નવો પ્રતિબંધ જાહેર કરવામાં આવે તો તાત્કાલિક વધારો

• દસ્તાવેજીકરણ: બધા પ્રતિબંધિત દેશોનું રજિસ્ટર અને સૂચનાની તારીખ જાળવો

૧૨.૩ ક્રોસ-બોર્ડર ડેટા ફ્લોની ઇન્વેન્ટરી

TCPL બધા ક્રોસ-બોર્ડર ડેટા ફ્લોની વ્યાપક ઇન્વેન્ટરીનું સંચાલન અને જાળવણી કરશે. આ ઇન્વેન્ટરીમાં આ દસ્તાવેજીકરણ કરવામાં આવશે:

• ટ્રાન્સફર કરવામાં આવતા વ્યક્તિગત ડેટાનો પ્રકાર (ગ્રાહક ડેટા, નાણાકીય ડેટા, ઓપરેશનલ ડેટા)

• વોલ્યુમ (રેકોર્ડ્સની સંખ્યા, GB માં કદ) અને ટ્રાન્સફરની આવર્તન

• ક્લાઉડ સેવા પ્રદાતાનું નામ અને સર્વર સ્થાનનો દેશ

• SaaS એપ્લિકેશનો અને તેમના ડેટા સ્ટોરેજ દેશો

• TCPL ડેટાને ઍક્સેસ કરતી આંતરરાષ્ટ્રીય કચેરીઓ અથવા પેટાકંપનીઓ

• આંતરરાષ્ટ્રીય હાજરી અને સામેલ દેશો ધરાવતા વિક્રેતાઓનું આઉટસોર્સિંગ

12.4 પ્રતિબંધિત દેશો માટે આકસ્મિક યોજનાઓ

TCPL ઇન્વેન્ટરીમાં ઓળખાયેલ દરેક ક્રોસ-બોર્ડર ડેટા ડિપેન્ડન્સી માટે આકસ્મિક યોજનાઓ વિકસાવશે અને જાળવી રાખશે. જો કોઇ દેશ પ્રતિબંધિત જાહેર કરવામાં આવે તો આ યોજનાઓ ઝડપી પ્રતિભાવ સુનિશ્ચિત કરે છે.

આકસ્મિક યોજના ઘટકો:

• જોખમ મૂલ્યાંકન: ઓપરેશનલ, વ્યવસાયિક, ઓળખો d જો તે દેશમાં ડેટા ટ્રાન્સફર અવરોધિત હોય તો નિયમનકારી અસરો

• વૈકલ્પિક ઉકેલો: ભારતીય-આધારિત સેવા પ્રદાતાઓ, માન્ય દેશના વિકલ્પો અથવા હાઇબ્રિડ અભિગમોને ઓળખો

• વિક્રેતા કરાર કલમો: બધા વિક્રેતા કરારોમાં ડેટા સ્થાનાંતરણ કલમો, એક્ઝિટ કલમો, પાલન કલમો અને સમાપ્તિ કલમો શામેલ હોવા જોઈએ

• સંક્રમણ સમયરેખા: દિવસ 0-2: તાત્કાલિક વધારો; દિવસ 2-5: અસરનું મૂલ્યાંકન; દિવસ 5-15: ડેટા સ્થળાંતર અમલમાં મૂકો; દિવસ 15-30: સંપૂર્ણ સંક્રમણ

• સંદેશાવ્યવહાર યોજના: આંતરિક હિસ્સેદારો, MLIs, ગ્રાહકો અને નિયમનકારી અધિકારીઓને સૂચિત કરો

12.5 પ્રાપ્તિ અને પ્રોજેક્ટ્સમાં ડેટા ફ્લો ગવર્નન્સ

બધી ખરીદી પ્રવૃત્તિઓ અને નવા પ્રોજેક્ટ શરૂઆતોમાં વિક્રેતાની પસંદગી અથવા સાધન જમાવટ પહેલાં ડેટા ફ્લો મૂલ્યાંકન શામેલ હોવું આવશ્યક છે.

પ્રાપ્તિ ચેકલિસ્ટ - ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પ્રશ્નો:

1. શું આ વિક્રેતા/સાધન/સેવા ભારતની બહાર કોઇ ડેટા ટ્રાન્સફરનો સમાવેશ કરે છે?

2. ડેટા પ્રોસેસિંગ અથવા સ્ટોરેજમાં કયા દેશો સામેલ છે?

3. શું બધા ઓળખાયેલા દેશો હાલમાં DPDP કાયદાની કલમ 16 હેઠળ ડેટા ટ્રાન્સફર માટે મંજૂર છે?

૪. કયા પ્રકારનો ડેટા ટ્રાન્સફર કરવામાં આવે છે?

૫. શું આ ક્રોસ-બોર્ડર ટ્રાન્સફર માટે સ્પષ્ટ ડેટા વિષય સંમતિ છે?

૬. શું વિક્રેતા સાથે ડેટા પ્રોસેસિંગ કરાર (DPA) અમલમાં મૂકવામાં આવ્યો છે?

૭. શું આ નિયમનકારી પાલન આવશ્યકતા (RBI, ક્રેડિટ બ્યુરો, વગેરે) છે?

મંજૂરી અધિકારી: ખરીદીને અંતિમ સ્વરૂપ આપવામાં આવે તે પહેલાં પાલન અધિકારીએ ડેટા ફ્લો પર સહી કરવી આવશ્યક છે. ક્રોસ-બોર્ડર ડેટા સાથે સંકળાયેલ કોઈપણ વિક્રેતા/સાધન/સેવાને પાલન મંજૂરી વિના તૈનાત કરી શકાતી નથી.

૧૨.૬ ક્રોસ-બોર્ડર ટ્રાન્સફર પર આંતરિક નીતિ નિવેદન

TCPL ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર નીતિ:

TCPL ડિજિટલ પર્સનલ ડેટા પ્રોટેક્શન એક્ટ, ૨૦૨૩ ની કલમ ૧૬ હેઠળ ભારત સરકાર દ્વારા આવા ટ્રાન્સફર માટે પ્રતિબંધિત કોઈપણ દેશમાં તેના ગ્રાહકો, દેવાદારો અથવા ડેટા વિષયોનો વ્યક્તિગત ડેટા, સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી અથવા કોઈપણ અન્ય નિયંત્રિત ડેટા ટ્રાન્સફર કરશે નહીં.

TCPL કેન્દ્ર સરકાર દ્વારા નિર્ધારિત બધી શરતોનું સખત પાલન કરશે જો કોઈ ચોક્કસ અધિકારક્ષેત્રોમાં ટ્રાન્સફર માટે ઉલ્લેખિત હોય.

બધા ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફરને કમ્પ્લાયન્સ ઓફિસર દ્વારા પૂર્વ-મંજૂર કરવામાં આવે છે અને તેનું સતત નિરીક્ષણ કરવામાં આવે છે. જો કોઈ દેશ પ્રતિબંધિત જાહેર કરવામાં આવે છે, તો TCPL તાત્કાલિક ડેટા ટ્રાન્સફરને સ્થગિત કરશે અને 30 દિવસની અંદર માન્ય અધિકારક્ષેત્રમાં ડેટા સ્થાનાંતરિત કરશે.

કર્મચારીઓ, કોન્ટ્રાક્ટરો અને વિક્રેતાઓને સ્પષ્ટ પાલન મંજૂરી વિના કોઈપણ વિદેશી અધિકારક્ષેત્રમાં વ્યક્તિગત ડેટા ટ્રાન્સફર કરવાની મનાઈ છે. આ નીતિના ઉલ્લંઘનના પરિણામે રોજગાર અથવા કરાર સમાપ્ત થવા સહિત શિસ્તબદ્ધ કાર્યવાહી કરવામાં આવશે.

સ્ટાફ જાગૃતિ:

બધા કર્મચારીઓ, કોન્ટ્રાક્ટરો અને સંબંધિત તૃતીય પક્ષોને ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર પ્રતિબંધો, પ્રતિબંધિત પ્રથાઓના સ્પષ્ટ ઉદાહરણો, એસ્કેલેશન પ્રક્રિયાઓ અને બિન-પાલનના પરિણામો પર વાર્ષિક તાલીમ આપવામાં આવશે.

12.7 પ્રતિબંધિત દેશ સૂચનાઓ માટે તાત્કાલિક પ્રતિભાવ પદ્ધતિ

સરકારી સૂચના પ્રાપ્ત થયા પછી કે કોઈ દેશ ડેટા ટ્રાન્સફર માટે પ્રતિબંધિત છે:

• તાત્કાલિક કાર્યવાહી (2 કલાકની અંદર): પાલન અધિકારી સૂચનાની ચકાસણી કરે છે; CISO ને જાણ કરવામાં આવે છે; કટોકટીની બેઠક બોલાવવામાં આવે છે

• ઓળખ તબક્કો (દિવસ 1 ના અંત સુધીમાં): ડેટા ફ્લો ઇન્વેન્ટરી સાથે ક્રોસ-રેફરન્સ પ્રતિબંધિત દેશ; બધા અસરગ્રસ્ત વિક્રેતાઓ અને સેવાઓ ઓળખો

• એસ્કેલેશન (દિવસ 2 સુધીમાં): બધા હિસ્સેદારોને સૂચિત કરો; વિક્રેતાઓને ટ્રાન્સફર બંધ કરવા સૂચના આપો; વૈકલ્પિક ઉકેલો સક્રિય કરો

• શમન (દિવસ 2-30): આકસ્મિક યોજનાનો અમલ કરો; બધા ડેટાને માન્ય અધિકારક્ષેત્રમાં સ્થાનાંતરિત કરો; બિન-અનુપાલન કરારો સમાપ્ત કરો

• સંદેશાવ્યવહાર અને પાલન (દિવસ 30 પછી): સંપૂર્ણ સ્થાનાંતરણ ચકાસો; RBI સાથે ફાઇલ પાલન પ્રમાણપત્ર; ગોપનીયતા નીતિ અને ઇન્વેન્ટરી અપડેટ કરો

13. ક્ષેત્ર-વિશિષ્ટ ડેટા ટ્રાન્સફર અને સ્થાનિકીકરણ નિયમો

13.1 લાગુ ક્ષેત્ર-વિશિષ્ટ નિયમોની ઓળખ

સામાન્ય DPDP અધિનિયમ, 2023 ઉપરાંત, TCPL ક્ષેત્ર-વિશિષ્ટ ડેટા સુરક્ષા અને સ્થાનિકીકરણ નિયમોને આધીન છે. આમાં શામેલ છે:

ડિજિટલ ધિરાણ અને ફિનટેક માટે RBI નિયમો:

• ડિજિટલ ધિરાણ માર્ગદર્શિકા (2022, અપડેટ 2025): ડેટા સંગ્રહ ધોરણો, ઉધાર લેનાર સંમતિ આવશ્યકતાઓ અને આઉટસોર્સિંગ ધોરણોનો ઉલ્લેખ કરો

• RBI આઉટસોર્સિંગ માર્ગદર્શિકા: ચોક્કસ સુરક્ષા અને ગુપ્તતા આવશ્યકતાઓ સાથે ફક્ત માન્ય સ્થાનો પર ડેટા આઉટસોર્સ કરવાની જરૂર છે

• ક્રેડિટ માહિતી નીતિ: ક્રેડિટ ડેટા કેવી રીતે એકત્રિત, સંગ્રહિત, શેર અને ઉપયોગ કરી શકાય તે સ્પષ્ટ કરો

• ચુકવણી સિસ્ટમ નિયમો: ચુકવણી-સંબંધિત ડેટા ભારતમાં સંગ્રહિત અને પ્રક્રિયા કરવાની જરૂર છે

ક્રેડિટ બ્યુરો નિયમો:

ક્રેડિટ બ્યુરો દ્વારા એકત્રિત કરવામાં આવતી ક્રેડિટ માહિતી આ હોવી જોઈએ: ફક્ત ક્રેડિટ રિપોર્ટિંગ અને સ્કોરિંગ હેતુઓ માટે ઉપયોગમાં લેવાય; ક્રેડિટ બ્યુરો લાઇસન્સ આવશ્યકતાઓનું પાલન કરીને સંગ્રહિત અને પ્રક્રિયા કરવામાં આવે; સ્પષ્ટ સંમતિ વિના તૃતીય પક્ષો સાથે શેર ન કરવામાં આવે; સામાન્ય રીતે ભારતની અંદર અથવા માન્ય અધિકારક્ષેત્રોમાં સંગ્રહિત ન થાય.

અન્ય લાગુ નિયમો:

આધાર કાયદો, 2016: આધાર ડેટા ભારતની બહાર ટ્રાન્સફર કરી શકાતો નથી અથવા અનધિકૃત હેતુઓ માટે ઉપયોગ કરી શકાતો નથી

• ટેલિકોમ નિયમો: જો TCPL ટેલિકોમ ડેટાનું સંચાલન કરે છે, તો તેણે ડેટા લોકલાઈઝ પર TRAI નિયમોનું પાલન કરવું આવશ્યક છે

• પેમેન્ટ કાર્ડ ઇન્ડસ્ટ્રી ડેટા સિક્યુરિટી સ્ટાન્ડર્ડ (PCI-DSS): જો કાર્ડ ડેટા હેન્ડલ કરવામાં આવે છે, તો આંતરરાષ્ટ્રીય ધોરણોનું પાલન કરવું આવશ્યક છે (સંવેદનશીલ ડેટાનું સ્થાનિકીકરણ કરતી વખતે)

• રોજગાર ડેટા: કર્મચારી ડેટા રોજગાર સંહિતા હેઠળ સુરક્ષિત હોવો જોઈએ અને મનસ્વી રીતે ટ્રાન્સફર કરી શકાતો નથી.

૧૩.૨ ગેપ વિશ્લેષણ - વર્તમાન પ્રથાઓ વિરુદ્ધ નિયમનકારી આવશ્યકતાઓ

TCPL તમામ લાગુ ક્ષેત્રીય નિયમો સામે વર્તમાન ડેટા હેન્ડલિંગ પ્રથાઓની તુલના કરીને ગેપ વિશ્લેષણ કરશે.

ગેપ વિશ્લેષણ પ્રક્રિયા:

• બધી સિસ્ટમો અને પ્રક્રિયાઓની યાદી બનાવો: ડેટા હેન્ડલ કરતી બધી સિસ્ટમો અને તેમના સ્થાનોનું દસ્તાવેજીકરણ કરો (ભારત/વિદેશી)

• ક્રોસ-રેફરન્સ નિયમનકારી આવશ્યકતાઓ: દરેક સિસ્ટમ માટે, લાગુ નિયમો ઓળખો

• ગેપ ઓળખો: વાસ્તવિક વિરુદ્ધ જરૂરી પ્રથાઓની તુલના કરો

• ઉપાય યોજના: દરેક ગેપ માટે, તાત્કાલિક કાર્યવાહી, સમયરેખા, જવાબદાર પક્ષ અને સંસાધનોનું દસ્તાવેજીકરણ કરો

• દસ્તાવેજીકરણ: દરેક ઓળખાયેલ ગેપ, નિયમનકારી આધાર, ગંભીરતા, સમયરેખા અને સ્થિતિનું દસ્તાવેજીકરણ કરતું ગેપ વિશ્લેષણ રજિસ્ટર જાળવો

13.3 સ્પષ્ટ પાલન નિવેદનો

ક્ષેત્રીય પાલન પર TCPL આંતરિક નીતિ:

TCPL એ માન્યતા આપે છે કે DPDP એક્ટ, 2023 જેવા સામાન્ય ડેટા સુરક્ષા કાયદાઓ ઉપરાંત, કંપની ભારતીય રિઝર્વ બેંક, ક્રેડિટ બ્યુરો નિયમનકારો અને અન્ય સત્તાવાળાઓ દ્વારા જારી કરાયેલ ક્ષેત્ર-વિશિષ્ટ નિયમોને આધીન છે.

કંપની આ માટે પ્રતિબદ્ધ છે:

૧. ડેટા સંગ્રહ, ઉધાર લેનાર સંમતિ, ડેટા સંગ્રહ અને તૃતીય-પક્ષ શેરિંગ પર RBI ના ડિજિટલ ધિરાણ માર્ગદર્શિકાનું પાલન કરો

૨. માન્ય અધિકારક્ષેત્રો અને વિક્રેતા ગુપ્તતા પર RBI ના આઉટસોર્સિંગ માર્ગદર્શિકાનું પાલન કરો

૩. ફક્ત ભારતમાં સંગ્રહ અને ક્રેડિટ ડેટાના મર્યાદિત ઉપયોગ પર ક્રેડિટ બ્યુરોના નિયમોનું પાલન કરો

૪. આધાર કાયદો, ટેલિકોમ નિયમો, રોજગાર કાયદા અને આવકવેરા કાયદા સહિત અન્ય લાગુ કાયદાઓનું પાલન કરો

૫. પાલનનો વંશવેલો: વિરોધાભાસી આવશ્યકતાઓના કિસ્સામાં, TCPL સૌથી કડક આવશ્યકતાનું પાલન કરશે

૬. નિયમિત સમીક્ષા અને અપડેટ: TCPL વાર્ષિક ધોરણે અથવા નવા નિયમનકારી માર્ગદર્શન પ્રાપ્ત થયા પછી આ નીતિઓની સમીક્ષા કરશે

૭. અમલીકરણ: ઉલ્લંઘનના પરિણામે કર્મચારીઓ માટે શિસ્તભંગની કાર્યવાહી થશે અને વિક્રેતાઓ માટે કરાર સમાપ્ત થશે

૧૩.૪ કાનૂની અને પાલન ટીમો સાથે સંકલન

જ્યારે પણ TCPL કોઈ નવી સેવા, વિક્રેતા, સાધન અથવા પ્રક્રિયા પર વિચાર કરે છે જેમાં ક્રોસ-બોર્ડર ડેટા હેન્ડલિંગનો સમાવેશ થાય છે, ત્યારે નીચેની મંજૂરી પ્રક્રિયા ફરજિયાત છે:

• પગલું ૧ - વ્યવસાય વિનંતી (દિવસ ૦): વિભાગ ક્રોસ-બોર્ડર ડેટા વિનંતી ફોર્મ સબમિટ કરે છે પાલન અધિકારી

• પગલું 2 - પાલન સમીક્ષા (દિવસો 1-3): પાલન અધિકારી દેશની મંજૂરી, ડેટા પ્રકાર, ક્ષેત્ર-વિશિષ્ટ પ્રતિબંધો અને સંમતિ આવશ્યકતાઓનું મૂલ્યાંકન કરે છે

• પગલું 3 - કાનૂની યોગ્ય ખંત (દિવસો 3-7): કાનૂની ટીમ વિક્રેતાની શરતો, ભારતીય કાયદા પાલન અને સુરક્ષા પર્યાપ્તતાનું મૂલ્યાંકન કરે છે

• પગલું 4 - મંજૂરી અથવા અસ્વીકાર (દિવસ 7): જો પાલન કરવામાં આવે, તો મંજૂર કરવામાં આવે; જો પાલન ન કરવામાં આવે, તો પ્રસ્તાવિત વિકલ્પો સાથે નકારવામાં આવે સમજણ

• નવા નિયમો જારી કરવામાં આવે ત્યારે રિફ્રેશર તાલીમ૧૪. અમે તમારી વ્યક્તિગત માહિતી કેટલા સમય સુધી રાખીશું?

અમે તમારા વ્યક્તિગત ડેટાને ફક્ત તેટલા સમય માટે જ રાખીશું જ્યાં સુધી અમે તેને એકત્રિત કરેલા હેતુઓને પૂર્ણ કરવા માટે જરૂરી હોય, જેમાં કોઈપણ કાનૂની, એકાઉન્ટિંગ અથવા રિપોર્ટિંગ આવશ્યકતાઓનો સમાવેશ થાય છે.

૧૪.૧ ડેટા પ્રકાર દ્વારા રીટેન્શન સમયગાળો

ગ્રાહક અને ઉધાર લેનાર ડેટા:

• સક્રિય લોન સમયગાળો: લોનનો સમયગાળો વત્તા છેલ્લા વ્યવહાર તારીખથી ૭ વર્ષ (બેંકિંગ નિયમો અનુસાર)

• બંધ ખાતા: બંધ થયાના ૭ વર્ષ (નિયમનકારી પાલન અને વિવાદના નિરાકરણ માટે)

• ક્રેડિટ બ્યુરો ડેટા: ક્રેડિટ બ્યુરો નિયમનકારી આવશ્યકતાઓ અનુસાર ૭ વર્ષ

સંવેદનશીલ વ્યક્તિગત ડેટા (SPDI):

• નાણાકીય રેકોર્ડ્સ: ઓછામાં ઓછા ૭ વર્ષ (આવકવેરા નિયમો અનુસાર)

• આરોગ્ય અને તબીબી ડેટા: લાગુ આરોગ્યસંભાળ નિયમો દ્વારા જરૂરી મુજબ; ઓછામાં ઓછા ૫ વર્ષ

• બાયોમેટ્રિક ડેટા: ઉપયોગનો સમયગાળો વત્તા ૩ વર્ષ; જો હેતુ પૂર્ણ થાય તો વહેલા કાઢી નાખવામાં આવે

કર્મચારી ડેટા:

• રોજગાર દરમિયાન: રોજગારનો સમયગાળો

• રોજગાર પછી: પાલન અને સંદર્ભ હેતુઓ માટે 5 વર્ષ

ઓડિટ અને પાલન રેકોર્ડ્સ:

• સંમતિ ઓડિટ ટ્રેલ્સ: ઓછામાં ઓછા 5 વર્ષ

• ડેટા એક્સેસ લોગ્સ: ઓછામાં ઓછા 3 વર્ષ

• સુરક્ષા ઘટના રેકોર્ડ્સ: ઓછામાં ઓછા 7 વર્ષ

• નિયમનકારી પત્રવ્યવહાર: RBI અને અન્ય સત્તાવાળાઓ દ્વારા આવશ્યકતા મુજબ

14.2 ડેટા અનામીકરણ અને ઉપનામીકરણ

• એકવાર સંગ્રહનો હેતુ પૂર્ણ થઈ જાય, તો શક્ય હોય ત્યાં વ્યક્તિગત ડેટાને અનામી અથવા ઉપનામીકરણ કરવામાં આવશે

• આંકડાકીય અને સંશોધન હેતુઓ માટે અનામી ડેટા અનિશ્ચિત સમય માટે જાળવી રાખી શકાય છે

• અનામીકરણ ઉદ્યોગ-માનક તકનીકોનો ઉપયોગ કરીને કરવામાં આવશે જે બદલી ન શકાય તેવી ઓળખ સુનિશ્ચિત કરે છે

14.3 ડેટા ડિલીટ અને નિકાલ

• રીટેન્શન સમયગાળાની સમાપ્તિ પર, વ્યક્તિગત ડેટા સુરક્ષિત રીતે કાઢી નાખવામાં આવશે

• ઉદ્યોગ-માનક ડેટા વિનાશ પદ્ધતિઓ (સુરક્ષિત ભૂંસી નાખવું, મીડિયાનો ભૌતિક વિનાશ) નો ઉપયોગ કરીને કાઢી નાખવામાં આવશે

• પ્રાથમિક સિસ્ટમોમાંથી ડેટા ડિલીટ કર્યાના 3 મહિનાની અંદર બેકઅપ નકલો કાઢી નાખવામાં આવશે

• કાઢી નાખવાનું પ્રમાણિત કરવામાં આવશે અને ડેટા ડિલીશન રજિસ્ટરમાં દસ્તાવેજીકૃત

૧૪.૪ ડેટા વિષય ભૂંસી નાખવાનો અધિકાર

ડેટા વિષયો કોઈપણ સમયે તેમના વ્યક્તિગત ડેટાને કાઢી નાખવાની વિનંતી કરી શકે છે. કાઢી નાખવાની વિનંતીઓ ૩૦ દિવસની અંદર પ્રક્રિયા કરવામાં આવશે. અપવાદો: લાગુ કાયદાઓ દ્વારા જરૂરી ડેટા (કર રેકોર્ડ, નિયમનકારી પાલન); ચાલુ કરારની જવાબદારીઓ માટે જરૂરી ડેટા; ડેટા વિષય કાઢી નાખવાનો વિવાદ કરે છે. સક્રિય સિસ્ટમોમાંથી કાઢી નાખ્યા પછી પણ, બેકઅપમાં અનામી શેષ નકલો પાલન હેતુઓ માટે જાળવી રાખી શકાય છે.

૧૫. માહિતી સુરક્ષા પગલાં

૧૫.૧ સામાન્ય સુરક્ષા પ્રતિબદ્ધતાઓ

TCPL માહિતી સુરક્ષા અને લાગુ નિયમોનું પાલન કરવા માટે સંપૂર્ણપણે પ્રતિબદ્ધ છે. અમે ISO 27001:2022 સાથે સંરેખિત અમારી માહિતી સુરક્ષા વ્યવસ્થાપન સિસ્ટમ દ્વારા ડેટાના રક્ષણ માટે મજબૂત સુરક્ષા નિયંત્રણો લાગુ કર્યા છે.

૧૫.૨ ટેકનિકલ સુરક્ષા નિયંત્રણો

• ટ્રાન્ઝિટમાં એન્ક્રિપ્શન: TCPL નેટવર્ક્સની બહાર ટ્રાન્સમિટ થયેલ તમામ ડેટા ઉદ્યોગ-માનક પ્રોટોકોલ (TLS ૧.૨ અથવા ઉચ્ચ) નો ઉપયોગ કરીને એન્ક્રિપ્ટેડ છે.

• આરામ પર એન્ક્રિપ્શન: સંવેદનશીલ વ્યક્તિગત ડેટા અને SPDI ને AES-૨૫૬ અથવા સમકક્ષ એન્ક્રિપ્શન ધોરણોનો ઉપયોગ કરીને એન્ક્રિપ્ટેડ છે.

• ઍક્સેસ નિયંત્રણો: ભૂમિકા-આધારિત ઍક્સેસ નિયંત્રણ (RBAC) સિદ્ધાંતોના આધારે ડેટા ઍક્સેસ પ્રતિબંધિત છે.

• પ્રમાણીકરણ: સંવેદનશીલ ડેટા સિસ્ટમ્સની ઍક્સેસ માટે મલ્ટી-ફેક્ટર પ્રમાણીકરણ (MFA) લાગુ કરવામાં આવે છે.

• નેટવર્ક સુરક્ષા: ફાયરવોલ્સ, ઘુસણખોરી શોધ સિસ્ટમો અને VPN નેટવર્ક પરિમિતિઓનું રક્ષણ કરે છે.

• ડેટાબેઝ સુરક્ષા: ડેટાબેઝ ઍક્સેસ લોગ થયેલ છે; અનધિકૃત ઍક્સેસ પ્રયાસોનું નિરીક્ષણ અને ચેતવણી આપવામાં આવે છે

• ડેટા માસ્કિંગ: બિન-ઉત્પાદન વાતાવરણ માસ્ક્ડ અથવા અનામી ડેટાનો ઉપયોગ કરે છે

15.3 સંગઠનાત્મક સુરક્ષા નિયંત્રણો

• માહિતી સુરક્ષા નીતિ: વ્યાપક ISMS નીતિઓ સંસ્થા-વ્યાપી ડેટા સુરક્ષાનું સંચાલન કરે છે

• સ્ટાફ તાલીમ: બધા કર્મચારીઓ વાર્ષિક માહિતી સુરક્ષા અને ડેટા સુરક્ષા તાલીમ મેળવે છે

• ગુપ્તતા કરારો: બધા કર્મચારીઓ અને ઠેકેદારો ગુપ્તતા કરારો પર હસ્તાક્ષર કરે છે

• તૃતીય-પક્ષ જોખમ વ્યવસ્થાપન: જોડાણ પહેલાં વિક્રેતાઓનું માહિતી સુરક્ષા પાલન માટે મૂલ્યાંકન કરવામાં આવે છે

• ઘટના પ્રતિભાવ યોજના: સુરક્ષા ઘટનાઓ લોગ કરવામાં આવે છે, તપાસ કરવામાં આવે છે અને તાત્કાલિક સુધારણા કરવામાં આવે છે

• સુરક્ષા ઓડિટ: નિયમિત સુરક્ષા ઓડિટ અને ઘૂંસપેંઠ પરીક્ષણ હાથ ધરવામાં આવે છે

15.4 વપરાશકર્તા જવાબદારીઓ

જોકે TCPL અનધિકૃત ઍક્સેસ અથવા હુમલા સામે સંપત્તિઓને સુરક્ષિત રાખવા માટે વાજબી પગલાં લે છે, ઇન્ટરનેટ સ્વાભાવિક રીતે સંપૂર્ણપણે સુરક્ષિત નથી. વપરાશકર્તાઓએ તેમના ડેટા સુરક્ષા માટે પણ જવાબદારી લેવી જોઈએ: તમારા વપરાશકર્તા ID અને પાસવર્ડની ગુપ્તતા જાળવી રાખો; ઓળખપત્રો શેર કરશો નહીં;

સુરક્ષિત ઉપકરણો અને નેટવર્કનો ઉપયોગ કરો; સુરક્ષા પેચ સાથે સિસ્ટમોને અપડેટ રાખો; કોઈપણ શંકાસ્પદ સુરક્ષા ભંગની તાત્કાલિક admin@techfino.in પર જાણ કરો.

૧૫.૫ ઘટનાની જાણ કરવી અને પ્રતિભાવ

જો તમને કોઈ સુરક્ષા સમસ્યાઓ, ઘટનાઓની શંકા હોય, અથવા TCPL તરફથી હોવાનો દાવો કરતા શંકાસ્પદ સંદેશાવ્યવહાર પ્રાપ્ત થાય, તો તાત્કાલિક admin@techfino.in પર ઇમેઇલ કરો. લિંક્સ પર ક્લિક કરશો નહીં અથવા શંકાસ્પદ સંદેશાઓને માહિતી પ્રદાન કરશો નહીં. જવાબ આપતા પહેલા મોકલનારની ઓળખ સ્વતંત્ર રીતે ચકાસો.

૧૬. કૂકીઝનો ઉપયોગ કેવી રીતે થાય છે?

કૂકી એ ડેટાનો એક નાનો ટુકડો છે જે વેબસાઇટ બ્રાઉઝ કરતી વખતે વેબ બ્રાઉઝર દ્વારા વપરાશકર્તાના કમ્પ્યુટર પર સંગ્રહિત થાય છે.

• પગલું 5 - કરાર અને DPA (દિવસો 7-14): વિક્રેતા કરારમાં ડેટા સ્થાનિકીકરણ કલમો અને ડેટા પ્રોસેસિંગ કરાર શામેલ હોવા જોઈએ

• પગલું 6 - અમલીકરણ (દિવસ 14+): કરાર અમલીકરણ, DPA હસ્તાક્ષર, ઇન્વેન્ટરી અપડેટ અને તાલીમ પછી જ સાધન/વિક્રેતા તૈનાત કરવામાં આવે છે

13.5 ઉદાહરણો અને સ્ટાફ જાગૃતિ

TCPL ક્ષેત્ર-વિશિષ્ટ ડેટા સુરક્ષા તાલીમ - મુખ્ય મુદ્દાઓ. બધા સ્ટાફ નીચેના ઉદાહરણોથી વાકેફ હોવા જોઈએ:

ઉદાહરણ 1 - ચુકવણી ડેટા: RBI નિયમોને કારણે ચુકવણી-સંબંધિત ડેટા ભારતમાં જ રહેવો જોઈએ. જો તમારો વિભાગ આંતરરાષ્ટ્રીય ચુકવણી પ્રોસેસરનો ઉપયોગ કરે છે, તો ખાતરી કરો કે તેઓ ફક્ત ભારતીય ડેટા સેન્ટરોમાં જ ડેટા પ્રોસેસ અને સ્ટોર કરે છે. ઉલ્લંઘનથી RBI દંડ થઈ શકે છે.

ઉદાહરણ 2 - આધાર માહિતી: કોઈપણ વિદેશી સિસ્ટમને આધાર માહિતી મોકલશો નહીં. આધાર કાયદા હેઠળ આધાર ડેટા ભારત છોડી શકતો નથી. વિદેશમાં આધાર ટ્રાન્સફર કરવો એ ફોજદારી ગુનો છે.

ઉદાહરણ 3 - ક્રેડિટ માહિતી: ઉધાર લેનારાઓનો ક્રેડિટ ડેટા ભારતની બહાર શેર અથવા સ્ટોર કરી શકાતો નથી. જો TCPL ક્રેડિટ બ્યુરો સેવાઓનો ઉપયોગ કરે છે, તો ખાતરી કરો કે ક્રેડિટ ડેટા ભારતમાં રહે છે.

ઉદાહરણ 4 - વિદેશી વિક્રેતાઓ અને આઉટસોર્સિંગ: જો તમારો વિભાગ ગ્રાહક ડેટાને હેન્ડલ કરવા માટે વિદેશી કોલ સેન્ટર, BPO અથવા સેવા પ્રદાતાને જોડે છે, તો આપણે RBI આઉટસોર્સિંગ માર્ગદર્શિકાનું પાલન કરવું જોઈએ. વિક્રેતા RBI દ્વારા પૂર્વ-મંજૂર થયેલ હોવો જોઈએ અથવા માન્ય અધિકારક્ષેત્રમાં સ્થિત હોવો જોઈએ.

ઉદાહરણ 5 - નવા SaaS સાધનો: નવું ક્લાઉડ-આધારિત સાધન (CRM, એનાલિટિક્સ, HR સિસ્ટમ) અપનાવતા પહેલા, પાલન અધિકારી સાથે તપાસ કરો કે શું સાધન માન્ય દેશમાં ડેટા સ્ટોર કરે છે. ખાતરી કરો કે દેશ કલમ 16 હેઠળ માન્ય છે, કોઈ ક્ષેત્ર-વિશિષ્ટ નિયમન સંગ્રહને પ્રતિબંધિત કરતું નથી, ડેટા પ્રોસેસિંગ કરાર લાગુ છે, અને ડેટા વિષયની સંમતિ પ્રાપ્ત થઈ છે. પાલન સાઇન-ઓફ વિના જમાવટ કરશો નહીં.

ઉદાહરણ 6 - વ્યક્તિગત ડેટા વિરુદ્ધ SPDI: વિવિધ ડેટાને અલગ અલગ સુરક્ષાની જરૂર છે. નાણાકીય ડેટા ભારતમાં જ રહેવો જોઈએ (RBI નિયમો અનુસાર). આધાર ડેટા વિદેશમાં જઈ શકતો નથી (આધાર કાયદા અનુસાર). આરોગ્ય ડેટાને સ્પષ્ટ સંમતિની જરૂર છે (SPDI નિયમો અનુસાર). હંમેશા પૂછો: શું આ SPDI છે? જો હા, તો કડક સુરક્ષા લાગુ કરો.

તાલીમ દસ્તાવેજીકરણ:

• ક્ષેત્ર-વિશિષ્ટ ડેટા નિયમો પર વાર્ષિક ફરજિયાત તાલીમ

• ઓડિટ હેતુઓ માટે તાલીમ રેકોર્ડ જાળવવામાં આવે છે

• કેસ સ્ટડીઝ અને વાસ્તવિક દુનિયાના ઉદાહરણોની ચર્ચા

• ચકાસણી માટે ક્વિઝ અથવા મૂલ્યાંકનઅમે અમારી સાઇટ અને સેવાની ગુણવત્તા સુધારવા અને તમારા બ્રાઉઝિંગ અનુભવને અર્થપૂર્ણ બનાવવા માટે કૂકીઝનો ઉપયોગ કરીએ છીએ.

૧૬.૧ કૂકીઝના પ્રકાર

પ્રથમ-પક્ષ કૂકીઝ: વેબસાઇટ યોગ્ય રીતે કાર્ય કરવા માટે મોટે ભાગે જરૂરી છે. લોગિન, પસંદગીઓ અને બ્રાઉઝિંગ સ્થિતિ માટે સત્ર કૂકીઝ શામેલ કરો. વપરાશકર્તાઓ બ્રાઉઝર સેટિંગ્સ દ્વારા પ્રથમ-પક્ષ કૂકીઝનું સંચાલન કરી શકે છે.

તૃતીય-પક્ષ કૂકીઝ: મુખ્યત્વે વેબસાઇટ પ્રદર્શનને સમજવા માટે વપરાય છે. એનાલિટિક્સ, વપરાશકર્તા ક્રિયાપ્રતિક્રિયા ટ્રેકિંગ અને સુરક્ષા દેખરેખ શામેલ કરો. તૃતીય-પક્ષ કૂકીઝને સ્પષ્ટ વપરાશકર્તા સંમતિની જરૂર છે.

૧૬.૨ કૂકી મેનેજમેન્ટ

• વપરાશકર્તા નિયંત્રણ: તમે તમારા બ્રાઉઝર સેટિંગ્સ દ્વારા કૂકીઝના ઉપયોગને નિયંત્રિત કરી શકો છો

• સંમતિ: પહેલી મુલાકાત પર, તમને બિન-આવશ્યક કૂકીઝ માટે સંમતિ આપવા માટે કહેવામાં આવશે

• સંમતિ રદ કરવી: તમે બ્રાઉઝર પસંદગીઓ દ્વારા કોઈપણ સમયે કૂકી સંમતિ પાછી ખેંચી શકો છો

• કૂકી અક્ષમ કરવું: જો તમે કૂકીઝને અક્ષમ કરવાનું પસંદ કરો છો, તો ચોક્કસ વેબસાઇટ સુવિધાઓ અથવા કાર્યો શ્રેષ્ઠ રીતે કાર્ય કરી શકશે નહીં

૧૭. અમારો સંપર્ક કેવી રીતે કરવો?

જો તમને આ ગોપનીયતા વિધાન અને અમારી ડેટા પ્રથાઓ અંગે કોઈ ગોપનીયતા ચિંતા, ફરિયાદ, પ્રશ્ન અથવા વિનંતી હોય, તો કૃપા કરીને અમારો સંપર્ક કરો:

17.1 સંપર્ક માહિતી

ઈમેલ: admin@techfino.in

મેઇલિંગ સરનામું: ટેકફિનો કેપિટલ પ્રાઇવેટ લિમિટેડ [સરનામું પૂરું પાડવાનું છે]

પ્રતિભાવ સમયરેખા:

• સ્વીકૃતિ: 5 કાર્યકારી દિવસોની અંદર

• નિરાકરણ: માનક વિનંતીઓ માટે 30 દિવસની અંદર

• જટિલ બાબતો: 60 દિવસની અંદર (વિલંબની સૂચના સાથે)

17.2 ડેટા વિષય અધિકારો

તમારી વ્યક્તિગત માહિતી સંબંધિત તમારી પાસે ચોક્કસ અધિકારો છે. તમે નીચેના કોઈપણ અધિકારોનો ઉપયોગ કરવા માટે અમારો સંપર્ક કરી શકો છો:

પ્રવેશનો અધિકાર: અમે તમારા વિશે જે વ્યક્તિગત ડેટા રાખીએ છીએ તેની નકલની વિનંતી કરો; કયો ડેટા એકત્રિત કરવામાં આવે છે અને તેનો ઉપયોગ કેવી રીતે થાય છે તે સમજો

સુધારણાનો અધિકાર: અચોક્કસ અથવા અપૂર્ણ વ્યક્તિગત ડેટા સુધારવાની વિનંતી કરો; જૂની માહિતી અપડેટ કરો

ભૂંસી નાખવાનો અધિકાર: તમારા વ્યક્તિગત ડેટાને કાઢી નાખવાની વિનંતી કરો (કાનૂની રીટેન્શન આવશ્યકતાઓને આધીન); જ્યાં કાયદેસર રીતે લાગુ પડે ત્યાં "ભૂલી જવાનો" અધિકાર

ડેટા પોર્ટેબિલિટીનો અધિકાર: તમારા વ્યક્તિગત ડેટાને માળખાગત, માનક ફોર્મેટમાં વિનંતી કરો; તમારો ડેટા બીજી સંસ્થામાં ટ્રાન્સફર કરો

નાપસંદ કરવાનો અધિકાર: ચોક્કસ હેતુઓ માટે સંમતિ પાછી ખેંચો; માર્કેટિંગ સંદેશાવ્યવહાર, વિશ્લેષણ અથવા અન્ય બિન-આવશ્યક પ્રક્રિયામાંથી નાપસંદ કરો

પ્રક્રિયાને પ્રતિબંધિત કરવાનો અધિકાર: ચોક્કસ હેતુઓ માટે ડેટા પ્રોસેસિંગ સ્થગિત કરવાની વિનંતી કરો; તમારા ડેટાનો ઉપયોગ કેવી રીતે થાય છે તે મર્યાદિત કરો

સંમતિ પાછી ખેંચો: ડેટા સંગ્રહ અથવા પ્રક્રિયા માટે અગાઉ આપવામાં આવેલી સંમતિ પાછી ખેંચો; સંમતિ પાછી ખેંચી લેવા પર ભવિષ્યની પ્રક્રિયા બંધ થઈ જશે

17.3 વિનંતીઓ પર પ્રક્રિયા

સબમિશન માટે વિનંતી કરો: admin@techfino.in પર ઇમેઇલ દ્વારા વિનંતીઓ સબમિટ કરો. ઓળખ માટે પૂરતી વિગતો શામેલ કરો. સ્પષ્ટપણે જણાવો કે તમે કયા અધિકારનો ઉપયોગ કરવા માંગો છો.

ચકાસણી: વિનંતી પર પ્રક્રિયા કરતા પહેલા તમને તમારી ઓળખ ચકાસવાનું કહેવામાં આવશે. ચકાસણી ખાતરી કરે છે કે અમે ફક્ત યોગ્ય ડેટા વિષયને જ ડેટા જાહેર કરીએ છીએ.

મંજૂરી અથવા અસ્વીકાર: વિનંતીઓ યોગ્યતાના આધારે પ્રક્રિયા કરવામાં આવશે. જો અમે વિનંતી પૂરી કરી શકતા નથી, તો તમને કારણોની જાણ કરવામાં આવશે.

શેષ નકલો: અમને મર્યાદિત સમયગાળા માટે બેકઅપ સિસ્ટમમાં કાઢી નાખેલા ડેટાની શેષ નકલો જાળવવાની જરૂર પડી શકે છે. પ્રાથમિક કાઢી નાખવાના 3 મહિનાની અંદર બેકઅપ નકલો કાઢી નાખવામાં આવે છે.

૧૮. કાનૂની સૂચના

૧૮.૧ નિયમનકારી જાહેરાતો

TCPL ને નીચેના માટે કાનૂની અધિકારીઓને વ્યક્તિગત માહિતી જાહેર કરવાની જરૂર પડી શકે છે:

• કોર્ટના આદેશો, કાનૂની સમન્સ અથવા ન્યાયિક નિર્દેશોનું પાલન

• છેતરપિંડીની તપાસ અને નિવારણ

• RBI નિયમો, આવકવેરા કાયદો, મની લોન્ડરિંગ નિવારણ અધિનિયમ (PMLA) અને કટોકટી પ્રતિભાવ વિનંતીઓ જેવા કાયદા હેઠળ કાનૂની જવાબદારીઓ

• ડેટા પ્રોટેક્શન બોર્ડ પૂછપરછ

૧૮.૨ ફરજિયાત જાહેરાતોની ગુપ્તતા

જ્યાં કાનૂની રીતે જરૂરી હોય, TCPL: કાયદેસર રીતે ફરજિયાત હદ સુધી જ માહિતી જાહેર કરશે; ફરજિયાત જાહેરાતોના ડેટા વિષયને સૂચિત કરવાનો પ્રયાસ કરશે (જ્યાં કાયદા દ્વારા પ્રતિબંધિત ન હોય); ઓડિટ હેતુઓ માટે તમામ જાહેરાતોના રેકોર્ડ જાળવી રાખશે; જ્યાં યોગ્ય હોય ત્યાં જાહેરાત વિનંતીઓને સંકુચિત કરવાની માંગ કરશે.

૧૮.૩ અધિકારોનો ત્યાગ નહીં

આ ગોપનીયતા નીતિ પૂરી પાડવાથી TCPL અથવા ડેટા વિષયોના કોઈપણ કાનૂની અધિકારોનો ત્યાગ થતો નથી. TCPL તેના હિતોનું રક્ષણ કરવા અને તેની નીતિઓને લાગુ કરવા માટેના તમામ કાનૂની અધિકારો અનામત રાખે છે.

૧૯. આ ગોપનીયતા નિવેદનમાં ફેરફારો

અમે કોઈપણ સમયે આ ગોપનીયતા નીતિને અપડેટ કરવાનો અધિકાર અનામત રાખીએ છીએ: લાગુ કાયદા અને નિયમોમાં ફેરફારોને પ્રતિબિંબિત કરવા; નવી ડેટા સુરક્ષા પ્રથાઓ લાગુ કરો; ક્ષેત્ર-વિશિષ્ટ નિયમનકારી અપડેટ્સ (RBI માર્ગદર્શિકા, વગેરે) નો પ્રતિસાદ આપો; અમારી ગોપનીયતા પ્રથાઓની સ્પષ્ટતા અથવા પારદર્શિતામાં સુધારો કરો.

19.1 ફેરફારોની સૂચના

ડેટા વિષયોને નોંધપાત્ર અપડેટ્સ આના દ્વારા સંચારિત કરવામાં આવશે: ઇમેઇલ સૂચનાઓ; વેબસાઇટ ઘોષણાઓ; વપરાશકર્તા ખાતા પોર્ટલમાં અપડેટ્સ. નોંધપાત્ર ફેરફારો માટે સંમતિની ફરીથી પુષ્ટિની જરૂર પડશે.

19.2 અસરકારક તારીખ

પ્રકાશન પર ફેરફારો અસરકારક બને છે. ફેરફારો પછી TCPL સેવાઓનો સતત ઉપયોગ અપડેટ કરેલી નીતિની સ્વીકૃતિ સૂચવે છે.

19.3 પાછલા સંસ્કરણોનું આર્કાઇવલ

આ નીતિના પાછલા સંસ્કરણો જાળવવામાં આવે છે અને સંદર્ભ માટે ઉપલબ્ધ છે. આર્કાઇવ કરેલા સંસ્કરણો ગોપનીયતા નીતિમાં ફેરફારોનો ઇતિહાસ દસ્તાવેજ કરે છે.

20. સંદર્ભ દસ્તાવેજો

• RBIડિજિટલ ધિરાણ પર માર્ગદર્શિકા (૨૦૨૨, અપડેટ ૨૦૨૫)

• RBI આઉટસોર્સિંગ માર્ગદર્શિકા

• માહિતી ટેકનોલોજી (વાજબી સુરક્ષા પ્રથાઓ અને પ્રક્રિયાઓ અને સંવેદનશીલ વ્યક્તિગત ડેટા અથવા માહિતી) નિયમો, ૨૦૧૧

• ડિજિટલ વ્યક્તિગત ડેટા સુરક્ષા કાયદો, ૨૦૨૩

• આધાર કાયદો, ૨૦૧૬

• ISO 27001:2022 - માહિતી સુરક્ષા વ્યવસ્થાપન

• RBI ક્રેડિટ માહિતી નીતિ

• PCI-DSS - ચુકવણી કાર્ડ ઉદ્યોગ ડેટા સુરક્ષા માનક (જો લાગુ હોય તો)

• TCPL માહિતી સુરક્ષા વ્યવસ્થાપન સિસ્ટમ (ISMS) દસ્તાવેજીકરણ

૨૧. અમલીકરણ

પાલન અને પરિણામો:

બધા કર્મચારીઓ, કોન્ટ્રાક્ટરો, વિક્રેતાઓ અને તૃતીય પક્ષોએ બધી ડેટા હેન્ડલિંગ પ્રવૃત્તિઓમાં આ ગોપનીયતા નીતિનું પાલન કરવું જોઈએ. આ નીતિની કોઈપણ જોગવાઈનું પાલન ન કરવું એ ગંભીર ઉલ્લંઘન છે. ઉલ્લંઘનો પરિણમી શકે છે:

• કર્મચારીઓ માટે: રોજગાર સમાપ્તિ સુધીની શિસ્તબદ્ધ કાર્યવાહી

• કોન્ટ્રાક્ટરો/વિક્રેતાઓ માટે: કરાર સમાપ્તિ અને નુકસાન માટે કાનૂની કાર્યવાહી

• તૃતીય પક્ષો માટે: કાનૂની કાર્યવાહી અને નિયમનકારી રિપોર્ટિંગ

• TCPL માટે: નિયમનકારી દંડ, દંડ અને પ્રતિષ્ઠાને નુકસાન

ઘટનામાં વધારો:

• કોઈપણ શંકાસ્પદ ઉલ્લંઘન અથવા બિન-પાલનની તાત્કાલિક CISO ને જાણ કરવી આવશ્યક છે

• જાણીતા ઉલ્લંઘનોની જાણ કરવામાં નિષ્ફળતા કર્મચારીઓ માટે શિસ્તબદ્ધ કાર્યવાહીમાં પરિણમી શકે છે

• ઘટનાઓનો રેકોર્ડ બનાવવામાં આવે છે, તપાસ કરવામાં આવે છે અને જો જરૂરી હોય તો યોગ્ય અધિકારીઓને મોકલવામાં આવે છે

નિયમનકારી રિપોર્ટિંગ:

• વ્યક્તિગત માહિતી સાથે સંકળાયેલા ડેટા ભંગની જાણ ફરજિયાત સમયમર્યાદામાં ડેટા પ્રોટેક્શન બોર્ડને કરવામાં આવશે

• કાયદા દ્વારા જરૂરી મુજબ RBI અથવા અન્ય અધિકારીઓને ગંભીર નિયમનકારી ઉલ્લંઘનોની જાણ કરવામાં આવશે

• ઓડિટર્સ અને નિયમનકારી સંસ્થાઓને પાલન પ્રમાણપત્રો પ્રદાન કરવામાં આવશે

22. નીતિ દસ્તાવેજ વ્યવસ્થાપન

દસ્તાવેજ માહિતી:

સંસ્કરણ (Version)	તારીખ (Date)	ફેરફારો અને પુનરાવર્તનનું કારણ (Changes & Reason for Revision)
1	13-02-2024	**ISO 27001:2022** અનુપાલન માટે પ્રારંભિક ઇશ્યૂ.
2	07-11-2025	આમાં શામેલ કરવા માટે વ્યાપક અપડેટ: (a) **ડિજિટલ લેન્ડિંગ માર્ગદર્શિકા** અનુપાલન (ફકરા 10 અને 12), (b) **ક્લિક-રેપ એસપીડીઆઈ નિયમો** અનુપાલન (નિયમ 5(1)), (c) **ક્રોસ-બોર્ડર ડેટા ટ્રાન્સફર** નિયંત્રણો (કલમ 16 ડીપીડીપી એક્ટ), (d) સેક્ટર-વિશિષ્ટ **આરબીઆઈ અને ક્રેડિટ બ્યુરો** નિયમો, (e) નિયમનકારી દેખરેખ અને આકસ્મિક યોજના પદ્ધતિઓ, (f) કર્મચારી જાગૃતિ અને તાલીમ આવશ્યકતાઓ.