കേരള സംസ്ഥാന ഡാറ്റാ നയം

നൂതന ആശയങ്ങൾക്കും (innovation), സാമ്പത്തിക വളർച്ചയ്ക്കും, തീരുമാനങ്ങൾ എടുക്കുന്നതിനും ഡാറ്റ നിർണ്ണായകമായ ഈ കാലഘട്ടത്തിൽ; സുതാര്യത, ഉത്തരവാദിത്തം, പൗരശാക്തീകരണം എന്നിവ പ്രോത്സാഹിപ്പിക്കുന്നതിൽ ഡാറ്റയ്ക്കുള്ള വലിയ പ്രാധാന്യം കേരള സർക്കാർ തിരിച്ചറിയുന്നു. പൊതുസേവനങ്ങൾ മെച്ചപ്പെടുത്തുന്നതിനും, ദുരന്തനിവാരണം കാര്യക്ഷമമാക്കുന്നതിനും, ഗവേഷണങ്ങളെ പ്രോത്സാഹിപ്പിക്കുന്നതിനും, വ്യവസായ വളർച്ച ത്വരിതപ്പെടുത്തുന്നതിനും, സാമ്പത്തിക വികസനത്തിന് പുതിയ അവസരങ്ങൾ സൃഷ്ടിക്കുന്നതിനും ഫലപ്രദമായ ഭരണനിർവ്വഹണത്തിന്റെ ആണിക്കല്ലാണ് ഡാറ്റ.

കേരള സംസ്ഥാന ഡാറ്റാ നയം തുറന്ന സമീപനം (openness), ലഭ്യത (accessibility), സുരക്ഷ (security) എന്നീ തത്വങ്ങളിലൂന്നിയാണ് രൂപീകരിച്ചിരിക്കുന്നത്. സർക്കാർ സംവിധാനങ്ങൾ തയ്യാറാക്കുന്ന ഡാറ്റ സമൂഹത്തിന്റെ നന്മയ്ക്കായി ഉത്തരവാദിത്തത്തോടെ പ്രയോജനപ്പെടുത്തുന്നു എന്ന് ഇത് ഉറപ്പാക്കുന്നു. ഡാറ്റ വെവ്വേറെയായി സൂക്ഷിക്കപ്പെടുന്ന രീതി (Data silos), ഏകീകൃത മാനദണ്ഡങ്ങളുടെ കുറവ് തുടങ്ങിയ വെല്ലുവിളികൾ പരിഹരിച്ചുകൊണ്ടും, 2012-ലെ നാഷണൽ ഡാറ്റാ ഷെയറിംഗ് ആൻഡ് ആക്സസിബിലിറ്റി പോളിസി (NDSAP) പിന്തുടർന്നുകൊണ്ടും, ശക്തമായ സ്വകാര്യതാ സംരക്ഷണ ഉപാധികൾ ഉൾപ്പെടുത്തിക്കൊണ്ടും ഡാറ്റയുടെ ധാർമ്മികവും കാര്യക്ഷമവുമായ ഉപയോഗത്തിന് ഈ നയം ഊന്നൽ നൽകുന്നു.

ഈ ഉദ്യമത്തിലൂടെ, ഡാറ്റ ഒരു പൊതുവിഭവമായി ഉപയോഗപ്പെടുത്തി ഇന്നോവേഷനും പരസ്പര സഹകരണത്തിനും ഡാറ്റയുടെ അടിസ്ഥാനത്തിലുള്ള തീരുമാനമെടുക്കലിനും സഹായകമാകുന്ന ഒരു സാഹചര്യം സൃഷ്ടിക്കാനാണ് കേരള സർക്കാർ ലക്ഷ്യമിടുന്നത്. ഡാറ്റയുടെ പ്രാപ്യതയോടൊപ്പം തന്നെ സ്വകാര്യതയും സുരക്ഷയും ഉറപ്പുവരുത്തുന്നതിന് ഊന്നൽ നൽകികൊണ്ട് പൗരന്മാർക്ക് ഡാറ്റ ലഭ്യമാക്കുന്നതിനും, സർക്കാർ പ്രവർത്തനങ്ങൾ സുതാര്യമാക്കുന്നതിനും, സാമ്പത്തിക ഗുണഫലങ്ങൾ ലഭ്യമാക്കുന്നതിനുമുള്ള ഒരു ഡാറ്റാ അധിഷ്ഠിത സംസ്ഥാനം (Data-driven state) കെട്ടിപ്പടുക്കാനുള്ള അടിത്തറയൊരുക്കാൻ ഈ നയംകൊണ്ട് ഉദ്ദേശിക്കുന്നു.

2. നിർവ്വചനങ്ങൾ (Definitions)

ഡാറ്റ (Data): ഇൻഫർമേഷൻ, സംഖ്യാപരമായ സമാഹാരങ്ങൾ, നിരീക്ഷണങ്ങൾ, രേഖകൾ, വസ്തുതകൾ, ഭൂപടങ്ങൾ, ചിത്രങ്ങൾ, ചാർട്ടുകൾ, പട്ടികകൾ, കണക്കുകൾ, ആശയങ്ങൾ, ഡിജിറ്റൽ അല്ലെങ്കിൽ അനലോഗ് രൂപത്തിലുള്ള ആശയങ്ങൾ എന്നിവയുടെ ആവിഷ്കാരത്തെയാണ് ഡാറ്റ എന്ന് പറയുന്നത്.

തത്സമയ വിവരങ്ങൾ (Real-Time Data): ഡാറ്റ ഉത്പാദിപ്പിക്കപ്പെടുന്ന അതേ സമയം തന്നെ

അല്ലെങ്കിൽ ഏറ്റവും കുറഞ്ഞ കാലതാമസത്തോടെ ശേഖരിക്കുകയും സംസ്കരിക്കുകയും അവതരിപ്പിക്കുകയും ചെയ്യുന്നതിനെയാണ് ഇത് സൂചിപ്പിക്കുന്നത്.

ഡാറ്റാ ആർക്കൈവ് (Data Archive): കൂടുതൽ വിശകലനങ്ങൾക്കും ഉപയോഗത്തിനുമായി Machine-readable data ശേഖരിക്കുകയും, ക്രമീകരിക്കുകയും, രേഖപ്പെടുത്തുകയും, മറ്റുള്ളവർക്ക് വിതരണം ചെയ്യുകയും ചെയ്യുന്ന സ്ഥലം.

ഡാറ്റാ ജനറേഷൻ (Data Generation): ഡാറ്റാ രൂപീകരണം അല്ലെങ്കിൽ ശേഖരണം, അതുമല്ലെങ്കിൽ സമാനമായ ഡാറ്റയുടെ പിന്നീടുള്ള കൂട്ടിച്ചേർക്കൽ.

ഡാറ്റാ സെറ്റ് (Data Set): വിശകലനത്തിനോ പ്രോസസ്സിംഗിനോ വേണ്ടി ക്രമീകൃതമായ രീതിയിൽ ശേഖരിക്കുകയും സൂക്ഷിച്ചുവെക്കുകയും ചെയ്തിട്ടുള്ള ഡാറ്റയെയാണ് ഡാറ്റാ സെറ്റ് എന്ന് വിളിക്കുന്നത്.

ജിയോസ്പേഷ്യൽ ഡാറ്റ (Geospatial Data): ഭൂമിശാസ്ത്രപരമായി അടയാളപ്പെടുത്തിയ (Geographically referenced) എല്ലാ ഡാറ്റയും.

GIGW: ഇന്ത്യയിലെ സർക്കാർ വെബ്സൈറ്റുകൾ എങ്ങനെയായിരിക്കണം എന്നതിനെക്കുറിച്ച് കേന്ദ്ര സർക്കാർ പുറപ്പെടുവിച്ചിട്ടുള്ള മാനദണ്ഡങ്ങളാണ് GIGW (Guidelines for Indian Government Websites).

വിവരങ്ങൾ (Information): സംസ്കരിച്ചെടുത്ത ഡാറ്റ.

മെറ്റാഡാറ്റ (Metadata): ഒരു ഡാറ്റയുടെ ഉറവിടത്തെക്കുറിച്ചും അത് നിർമ്മിക്കപ്പെട്ട സമയം, സ്ഥലം, സാഹചര്യം എന്നിവയെക്കുറിച്ചുള്ള വിവരങ്ങളാണിത്. ഡാറ്റ ആര്, എപ്പോൾ, എന്ത്, എവിടെ, എന്തിന്, എങ്ങനെ നിർമ്മിച്ചു എന്ന് മെറ്റാഡാറ്റ ഉപയോക്താവിനെ അറിയിക്കുന്നു. ഇത് ഡാറ്റയുടെ ഉറവിടവും ഗുണനിലവാരവും കൃത്യമായി മനസ്സിലാക്കാൻ സഹായിക്കുന്നു.

നെഗറ്റീവ് ലിസ്റ്റ് (Negative list): വകുപ്പുകളോ സ്ഥാപനങ്ങളോ പങ്കുവെക്കാൻ പാടില്ലാത്തവ എന്ന് പ്രഖ്യാപിച്ചിട്ടുള്ള ഡാറ്റ. ഇത്തരം ഡാറ്റ കൈമാറാൻ പാടില്ലാത്തവയായി കണക്കാക്കുന്നത് ഇവയുടെ അതീവ പ്രാധാന്യവും ഇവ വെളിപ്പെടുത്തുന്നത് രാജ്യസുരക്ഷയെ ബാധിക്കുന്നതിനോ വ്യക്തികളുടെ സ്വകാര്യത ലംഘിക്കുന്നതിനോ, നിയമപരമോ കരാർപരമോ ആയ ബാധ്യതകളുടെ ലംഘനത്തിനോ കാരണമായേക്കാം എന്നതുകൊണ്ടാണ്.

ഓപ്പൺ ഡാറ്റ (Open Data): ആർക്കും സൗജന്യമായി ലഭ്യമാകുന്നതും നിയന്ത്രണങ്ങളില്ലാതെ ഉപയോഗിക്കാവുന്നതുമായ ഡാറ്റയെയാണ് ഇത് അർത്ഥമാക്കുന്നത്. സാധാരണയായി ഇത്തരം ഡാറ്റ Machine-readable ഫോർമാറ്റിലാണ് നൽകുന്നത്.

വ്യക്തിഗത ഡാറ്റ (Personal data): ഒരു വ്യക്തിയെ നേരിട്ടോ അല്ലാതെയോ തിരിച്ചറിയാൻ സഹായിക്കുന്ന തരത്തിലുള്ള ആ വ്യക്തിയുമായി ബന്ധപ്പെട്ട ഏതൊരു ഡാറ്റയെയും വ്യക്തിഗത വിവരങ്ങൾ എന്ന് അർത്ഥമാക്കുന്നു.

സെൻസിറ്റീവ് ആയ വ്യക്തിഗത ഡാറ്റ (Sensitive personal data or information) എന്നാൽ താഴെ പറയുന്നവ ഉൾപ്പെടുന്ന വിവരങ്ങളാണ്:

- പാസ്‌വേഡ് (Password)
- ലൈംഗിക ജീവിതവും ലൈംഗിക ആഭിമുഖ്യവും
- ബയോമെടിക് വിവരങ്ങൾ
- നിയമപരമായ കരാർ പ്രകാരമോ അല്ലാതെയോ പ്രോസസ്സ് ചെയ്യുന്നതിനും സൂക്ഷിക്കുന്നതിനുമായി ഒരു കോർപ്പറേറ്റ് സ്ഥാപനത്തിന് ലഭിച്ച വിവരങ്ങൾ
- ഉപയോക്താക്കളുടെ ബാങ്ക് അക്കൗണ്ട്, ക്രെഡിറ്റ് കാർഡ്, ഡെബിറ്റ് കാർഡ്, മറ്റ് പേയ്മെന്റ് സംവിധാനങ്ങൾ എന്നിവയുമായി ബന്ധപ്പെട്ട സാമ്പത്തിക വിവരങ്ങൾ (Financial Data)
- ശാരീരികവും മാനസികവുമായ ആരോഗ്യസ്ഥിതി, ചികിത്സാ രേഖകൾ (Medical records), ചരിത്രം എന്നിവയുൾപ്പെടെയുള്ള ആരോഗ്യ വിവരങ്ങൾ
- ഔദ്യോഗിക തിരിച്ചറിയൽ രേഖകൾ (Official identifiers)
- ജനിതക വിവരങ്ങൾ (Genetic Data)
- ട്രാൻസ്ജെൻഡർ പദവി / ഇന്റർസെക്സ് പദവി
- ജാതി അല്ലെങ്കിൽ ഗോത്രം
- മതപരമോ രാഷ്ട്രീയമോ ആയ വിശ്വാസങ്ങൾ അല്ലെങ്കിൽ അഫിലിയേഷൻ (ബന്ധം)

മാനദണ്ഡങ്ങൾ (Standards): ഡാറ്റയുടെ ഗുണമേന്മ, പരസ്പര പ്രവർത്തനക്ഷമത (Interoperability), കൈമാറ്റം, സംഭരണം, പുനരുപയോഗം എന്നിവ ഉറപ്പാക്കുന്നതിനായി നിശ്ചയിച്ചിട്ടുള്ള മാർഗ്ഗനിർദ്ദേശങ്ങൾ അല്ലെങ്കിൽ പ്രോട്ടോക്കോളുകൾ.

ഡാറ്റാ ഫിഡ്യൂഷ്യറി (Data Fiduciary): വ്യക്തിഗത ഡാറ്റ (Personal data) കൈകാര്യം ചെയ്യുന്നതിന്റെ ഉദ്ദേശ്യവും രീതിയും ഒറ്റയ്ക്കോ മറ്റ് വ്യക്തികളുമായി ചേർന്നോ തീരുമാനിക്കുന്ന ഏതൊരു വ്യക്തിയെയോ സ്ഥാപനത്തെയോ ആണ് ഇത് അർത്ഥമാക്കുന്നത്.

ഡാറ്റാ പ്രിൻസിപ്പൽ (Data Principal): വ്യക്തിഗത ഡാറ്റ ആരെക്കുറിച്ചാണോ ആ വ്യക്തിയെയാണ് ഇത് അർത്ഥമാക്കുന്നത്. (i) ആ വ്യക്തി ഒരു കുട്ടിയാണെങ്കിൽ, കുട്ടിയുടെ മാതാപിതാക്കളോ നിയമപരമായ രക്ഷിതാവോ ഇതിൽ ഉൾപ്പെടും; (ii) ആ വ്യക്തി ഭിന്നശേഷിക്കാരനാണെങ്കിൽ, ആ വ്യക്തിക്ക് വേണ്ടി പ്രവർത്തിക്കുന്ന നിയമപരമായ രക്ഷിതാവ് ഇതിൽ ഉൾപ്പെടും.

എ.പി.ഐ (API): ഒരു സിസ്റ്റത്തിനോ സർവീസിനോ മറ്റൊരു സിസ്റ്റത്തിലെ ഡാറ്റയോ പ്രവർത്തനങ്ങളോ ലഭ്യമാക്കാൻ സഹായിക്കുന്ന സാങ്കേതിക വിദ്യയാണ് ആപ്ലിക്കേഷൻ പ്രോഗ്രാമിംഗ് ഇന്റർഫേസ് (API). ഒരു സിസ്റ്റത്തിലെ വിവരങ്ങൾ നേരിട്ട് തിരയാനോ (Search), പട്ടികപ്പെടുത്താനോ (List), ചിലപ്പോൾ വിവരങ്ങൾ സമർപ്പിക്കാനോ പുതുക്കാനോ (Submit & Update), അല്ലെങ്കിൽ മറ്റ് സിസ്റ്റങ്ങളിൽ നിശ്ചിത പ്രവർത്തനങ്ങൾ തുടങ്ങാനോ ആണ് സാധാരണയായി API ഉപയോഗിക്കുന്നത്.

3. ലക്ഷ്യങ്ങൾ (Objectives)

സർക്കാരിന്റെ എല്ലാ തലങ്ങളിലുമുള്ള ഡാറ്റാ ആസ്തികളുടെ (Data assets) സുരക്ഷിതമായ സംഭരണം, നിയന്ത്രിതമായ പങ്കുവെക്കൽ, മെച്ചപ്പെട്ട ലഭ്യത എന്നിവ കേരള സംസ്ഥാന ഡാറ്റാ നയം (KSDP) സുഗമമാക്കും.

ഇലക്ട്രോണിക് രൂപത്തിലുള്ളതോ ഭൗതിക രേഖകളുടെ (Physical records) രൂപത്തിലുള്ളതോ ആയ എല്ലാത്തരം ഡാറ്റയ്ക്കും ഈ നയം ബാധകമായിരിക്കും.

ഈ നയത്തിന്റെ പ്രധാന ലക്ഷ്യങ്ങൾ ഇവയാണ്:

- സർക്കാരിന്റെ കൈവശമുള്ള ഡാറ്റയുടെ വർഗ്ഗീകരണം (Classification), ഉടമസ്ഥാവകാശം, കൈകാര്യം ചെയ്യൽ എന്നിവ സംബന്ധിച്ച മാർഗ്ഗനിർദ്ദേശങ്ങൾ നിശ്ചയിക്കുക.
- പൊതുജനങ്ങൾക്ക് ഡാറ്റ ലഭ്യമാക്കുന്നതിനും (Open access), സർക്കാർ സംവിധാനങ്ങൾക്കുള്ളിലെ ഡാറ്റ ബന്ധപ്പെട്ടവർക്ക് സുരക്ഷിതമായി പങ്കുവെക്കുന്നതിനുമുള്ള സാഹചര്യം ഒരുക്കുക. ഡാറ്റ നൽകുന്നവരുടെയും അത് ഉപയോഗിക്കുന്നവരുടെയും അവകാശങ്ങൾ സംരക്ഷിച്ചുകൊണ്ടുള്ള മാർഗ്ഗനിർദ്ദേശങ്ങൾ ഇതിനായി തയ്യാറാക്കുക.
- ഏകീകൃതമായ 'സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച്' (State Data Exchange) പ്ലാറ്റ്ഫോം വഴി വിശ്വസനീയമായ ഡാറ്റ ലഭ്യമാക്കുക. ഇതുവഴി സർക്കാർ സ്ഥാപനങ്ങൾ ഒരേ ഡാറ്റ പലതവണ ശേഖരിക്കുന്നത് പരമാവധി കുറയ്ക്കുക.
- Open data പങ്കുവെക്കുന്നതിനായി സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിനെ ഭാരത സർക്കാരിന്റെ 'ഓപ്പൺ ഗവൺമെന്റ് ഡാറ്റാ' (OGD) പ്ലാറ്റ്ഫോമുമായി ബന്ധിപ്പിക്കുക.
- നൂതനമായ ഡാറ്റാ അനലിറ്റിക്സ് (Data analytics) സാധ്യതകൾ പ്രോത്സാഹിപ്പിക്കുകയും, നയരൂപീകരണത്തിൽ ഡാറ്റാ അധിഷ്ഠിതമായ തീരുമാനങ്ങൾ എടുക്കാൻ കേരള സർക്കാരിനെ സഹായിക്കുകയും ചെയ്യുക.
- സർക്കാർ പദ്ധതികളുടെ നടത്തിപ്പിലും സംസ്ഥാനത്തെ ദുരന്തനിവാരണ പ്രവർത്തനങ്ങളിലും ഡാറ്റയുടെ വിപുലമായ ഉപയോഗം ഉറപ്പാക്കുക.
- ഡാറ്റ തടസ്സമില്ലാതെ കൈമാറുന്നതിനും ഗുണമേന്മ ഉറപ്പാക്കുന്നതിനുമായി

ഏകീകൃത ഡാറ്റാ സ്റ്റാൻഡേർഡുകൾ, മെറ്റാഡാറ്റാ സ്റ്റാൻഡേർഡുകൾ, ഇന്ററോപ്പറബിലിറ്റി പ്രോട്ടോക്കോളുകൾ എന്നിവ നടപ്പിലാക്കുക.

4. നയത്തിന്റെ പരിധി (Scope of the Policy)

കേരള സർക്കാരിന്റെ ഏതെങ്കിലും വകുപ്പുകളോ ഓഫീസുകളോ ഏജൻസികളോ സ്ഥാപനങ്ങളോ നേരിട്ടോ അല്ലെങ്കിൽ പുറംകരാർ (Outsourced) ഏജൻസികൾ മുഖേനയോ പൊതുഫണ്ട് ഉപയോഗിച്ച് നിർമ്മിച്ചതോ ശേഖരിച്ചതോ സംഭരിച്ചതോ ആയ എല്ലാ ഡാറ്റയ്ക്കും കേരള സംസ്ഥാന ഡാറ്റാ നയം (KSDP) ബാധകമായിരിക്കും.

അനിയന്ത്രിതവും നിയന്ത്രിതവുമായ (Restricted) വിഭാഗങ്ങളിൽ ഉൾപ്പെടുന്ന ഡാറ്റ ലഭ്യമാക്കുന്നതിന്റെ കൃത്യമായ തലങ്ങളും നിബന്ധനകളും ഈ നയം നിർവചിക്കുന്നു.

സംസ്ഥാന സർക്കാർ വകുപ്പുകൾ നൽകുന്ന ഇലക്ട്രോണിക് സേവനങ്ങൾ വഴി ഉത്പാദിപ്പിക്കപ്പെടുന്ന ഡാറ്റയ്ക്കും, നിലവിലുള്ള (Legacy data) ഇലക്ട്രോണിക് – ഭൗതിക രേഖകൾക്കും ഈ നയം ബാധകമാണ്.

5. നയത്തിന്റെ ഗുണഫലങ്ങൾ (Benefits of the Policy)

സുരക്ഷിതമായ ആക്സസ് കൺട്രോൾ സംവിധാനങ്ങളിലൂടെ വിവിധ സർക്കാർ വകുപ്പുകൾക്കിടയിൽ ഡാറ്റ പങ്കുവെക്കുന്നത് ഈ നയം സുഗമമാക്കുന്നു.

വിവരങ്ങളുടെ കൃത്യതയും പൂർണ്ണതയും ഇത് ഉറപ്പാക്കുന്നു. നിശ്ചിത ഡാറ്റാ മാനദണ്ഡങ്ങൾ പാലിക്കുന്നത് വഴി ചെലവ് കുറയ്ക്കാനും ഡാറ്റ ആവർത്തിച്ച് ശേഖരിക്കുന്നത് ഒഴിവാക്കാനും സാധിക്കുന്നു.

Open data ലഭ്യമാക്കുന്നതിലൂടെ സ്റ്റാർട്ടപ്പുകൾക്കും ഗവേഷണ സ്ഥാപനങ്ങൾക്കും പുതിയ അവസരങ്ങൾ സൃഷ്ടിക്കുകയും അതുവഴി ഇന്നോവേഷനും സാമ്പത്തിക വളർച്ചയും പ്രോത്സാഹിപ്പിക്കുകയും ചെയ്യുന്നു.

നയരൂപീകരണത്തിന് ആവശ്യമായ കൃത്യവും കാലികവുമായ ഡാറ്റ ലഭ്യമാക്കുന്നതിലൂടെ ഭരണനിർവ്വഹണത്തിൽ ഡാറ്റാ അധിഷ്ഠിതമായ തീരുമാനങ്ങൾ എടുക്കാൻ സഹായിക്കുന്നു.

6. നോഡൽ വകുപ്പ് (Nodal Department)

ഈ നയം നടപ്പിലാക്കുന്നതിനുള്ള നോഡൽ വകുപ്പ് കേരള സർക്കാരിന്റെ ഇലക്ട്രോണിക്സും വിവരസാങ്കേതികവിദ്യയും ആയിരിക്കും. ഈ നയത്തിൽ ഭേദഗതികൾ വരുത്തുന്നത് ഇലക്ട്രോണിക്സും വിവരസാങ്കേതികവിദ്യയും വകുപ്പായിരിക്കും.

7. നടപ്പിലാക്കുന്നതിനുള്ള നോഡൽ ഏജൻസി (Nodal Agency for implementation)

സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിന്റെ നിർവ്വഹണത്തിനും മാനേജ്മെന്റിനുമുള്ള നോഡൽ ഏജൻസി കേരള സ്റ്റേറ്റ് ഐടി മിഷൻ (KSITM) ആണ്. ഡാറ്റാ സുരക്ഷ, ശേഖരണം, സംഭരണം, വിശകലനം തുടങ്ങിയ കാര്യങ്ങളിൽ ചീഫ് ഡാറ്റാ ഓഫീസർമാർ (CDO) ഉൾപ്പെടെയുള്ള സർക്കാർ ഉദ്യോഗസ്ഥരുടെ വൈദഗ്ധ്യം വർദ്ധിപ്പിക്കുന്നതിന് ഐടി മിഷൻ പരിശീലന പരിപാടികൾ സംഘടിപ്പിക്കും.

കേരള സ്റ്റേറ്റ് ഐടി മിഷൻ ഡയറക്ടർ സംസ്ഥാന ചീഫ് ഡാറ്റാ ഓഫീസർ (Chief Data Officer) ആയി പ്രവർത്തിക്കും. വിവിധ വകുപ്പുകളിലെ ചീഫ് ഡാറ്റാ ഓഫീസർമാരുമായി സംസ്ഥാന ചീഫ് ഡാറ്റാ ഓഫീസർ ഏകോപനം നടത്തുകയും ഡാറ്റാ ശേഖരണത്തിന്റെയും അവയുടെ പ്രസിദ്ധീകരണത്തിന്റെയും മേൽനോട്ടം വഹിക്കുകയും ചെയ്യും.

8. സാങ്കേതിക പ്ലാറ്റ്ഫോം (Technology Platform)

വിവിധ വകുപ്പുകളിൽ നിന്നുള്ള ഡാറ്റ പങ്കുവെക്കുന്നത് "സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോം" (State Data Exchange Platform) എന്ന കേന്ദ്രീകൃത സംയോജിത റെപ്പോസിറ്ററി വഴിയായിരിക്കും.

User Authentication, റോൾ ബേസ്ഡ് ആക്സസ് കൺട്രോൾ (RBAC) എന്നീ സംവിധാനങ്ങളിലൂടെ സർക്കാർ സ്ഥാപനങ്ങൾക്കിടയിൽ സുരക്ഷിതമായ ഡാറ്റാ കൈമാറ്റം ഈ പ്ലാറ്റ്ഫോം സാധ്യമാക്കും.

ഡാറ്റ നൽകുന്നവരും ഉപയോഗിക്കുന്നവരും തമ്മിൽ സുരക്ഷിതവും തടസ്സമില്ലാത്തതും കാര്യക്ഷമവുമായ കൈമാറ്റം ഉറപ്പാക്കിക്കൊണ്ട് കേരള സ്റ്റേറ്റ് ഐടി മിഷൻ (KSITM) ഈ പ്ലാറ്റ്ഫോം നടപ്പിലാക്കുകയും പരിപാലിക്കുകയും ചെയ്യും. ഈ പ്ലാറ്റ്ഫോമിൽ വിഭാവനം ചെയ്തിരിക്കുന്ന പ്രധാന പ്രവർത്തനങ്ങൾ താഴെ പറയുന്നവയാണ്:

ഡാറ്റാ എക്സ്ചേഞ്ച് സജ്ജീകരണവും കോൺഫിഗറേഷനും: സർക്കാർ വകുപ്പുകൾക്കും മറ്റ് പങ്കാളികൾക്കുമിടയിൽ (Stakeholders) ഡാറ്റ കൈമാറുന്നതിനായി ശക്തമായ ഒരു സംവിധാനം സ്ഥാപിക്കുക.

ഡാറ്റാ പ്രൊവൈഡർ ഓൺബോർഡിംഗ്: വിവിധ ഡാറ്റാ ദാതാക്കളെ (Data Providers) കണ്ടെത്തുകയും അവരെ പ്ലാറ്റ്ഫോമുമായി ബന്ധിപ്പിക്കുകയും ചെയ്യുക.

ഡാറ്റാ ഇൻജക്ഷൻ, ഇന്റഗ്രേഷൻ & ക്വാളിറ്റി റിപ്പോർട്ടിംഗ്: ഡാറ്റ നിശ്ചിത മാനദണ്ഡമനുസരിച്ച് ശേഖരിക്കുന്നതും സംയോജിപ്പിക്കുന്നതും ഓട്ടോമേറ്റഡ് ഗുണനിലവാര പരിശോധനകൾ നടത്തുന്നതും ഉറപ്പാക്കുക.

യൂസർ ഇന്റർഫേസ് (UI) കസ്റ്റമൈസേഷൻ: പ്ലാറ്റ്ഫോം ഉപയോക്തൃസൗഹൃദമാക്കുന്നതിനും എല്ലാവർക്കും എളുപ്പത്തിൽ ഉപയോഗിക്കാൻ സാധിക്കുന്ന തരത്തിൽ GIGW (Guidelines for Indian Government Websites) മാനദണ്ഡങ്ങൾ പാലിച്ചും രൂപകൽപ്പന ചെയ്യുക.

ആക്സസ് മാനേജ്മെന്റ്: അംഗീകൃത ഉപയോക്താക്കൾക്ക് മാത്രം സുരക്ഷിതമായി ഡാറ്റ ലഭ്യമാകുന്നുണ്ടെന്ന് ഉറപ്പാക്കാൻ ആക്സസ് മാനേജ്മെന്റ് നടപ്പിലാക്കുക.

സ്കേലബിലിറ്റി & പെർഫോമൻസ് ഒപ്റ്റിമൈസേഷൻ: ഉയർന്ന ലഭ്യത (High availability), ഓട്ടോ-സ്കെയിലിംഗ്, തകരാറുകളെ പ്രതിരോധിക്കാനുള്ള ശേഷി (Fault tolerance) എന്നിവ ഉറപ്പാക്കുക.

പിന്തുണയും പരിപാലനവും: ദീർഘകാല പ്രവർത്തനക്ഷമതയും സുരക്ഷാ മാനദണ്ഡങ്ങളും ഉറപ്പാക്കുക.

എ.പി.ഐ രജിസ്ട്രി (API Registry): സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിനുള്ളിൽ ഒരു എ.പി.ഐ ശേഖരം (Repository) പരിപാലിക്കുക.

സുരക്ഷാ നിയന്ത്രണങ്ങൾ: ലോഗിംഗ് (Logging), ഹാഷിംഗ് (Hashing), ടൈം-സ്റ്റാമ്പിംഗ്, മാറ്റം വരുത്താനാകാത്ത ഓഡിറ്റ് ട്രയലുകൾ (Immutable audit trails), സുരക്ഷാ വീഴ്ചകളോടുള്ള പ്രതികരണം (Incident response), റിപ്പോർട്ടിംഗ് തുടങ്ങിയ അനുബന്ധ പ്രവർത്തനങ്ങൾ ഉറപ്പാക്കുക.

9. ഡാറ്റാ വർഗ്ഗീകരണം (Data Classification)

കേരളത്തിലെ പൊതുഫണ്ട് ഉപയോഗിച്ച് സർക്കാർ ഏജൻസികളോ സ്ഥാപനങ്ങളോ ഉത്പാദിപ്പിക്കുന്ന ജിയോ സ്പേഷ്യൽ ഡാറ്റ (Geo-spatial data) ഉൾപ്പെടെയുള്ള എല്ലാത്തരം ഡാറ്റയും ഈ നയത്തിന്റെ പരിധിയിൽ വരുന്നു. സർക്കാർ ഏജൻസികൾ ഉത്പാദിപ്പിക്കുന്നതോ ശേഖരിച്ചുവെക്കുന്നതോ ആയ വിവരങ്ങളെ "പബ്ലിക്" (Public), "ഇന്റേണൽ" (Internal), "കോൺഫിഡൻഷ്യൽ" (Confidential) എന്നിങ്ങനെ മൂന്നായി വർഗ്ഗീകരിക്കും.

എ) പബ്ലിക് ഡാറ്റ (Public Data): 'ഓപ്പൺ ഡാറ്റ' (Open Data) തത്വങ്ങൾക്കനുസൃതമായി പൊതുജനങ്ങൾക്കായി നേരിട്ട് പ്രസിദ്ധീകരിക്കാൻ നിശ്ചയിച്ചിട്ടുള്ള ഡാറ്റയാണിവ. ഇവ സാധാരണയായി സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോം വഴിയും ഭാരത സർക്കാരിന്റെ ഓപ്പൺ ഗവൺമെന്റ് ഡാറ്റാ (OGD) പ്ലാറ്റ്ഫോം വഴിയും എല്ലാവർക്കും ലഭ്യമാക്കും (Open Access). വ്യക്തിഗത ഡാറ്റ, സെൻസിറ്റീവ് ആയ സ്വകാര്യ ഡാറ്റ, അതീവ രഹസ്യ സ്വഭാവമുള്ള ഡാറ്റ എന്നിവ ഇതിൽ ഉൾപ്പെടുത്താൻ പാടുള്ളതല്ല.

ബി) ഇന്റേണൽ ഡാറ്റ (Internal Data): ഏതെങ്കിലും സംസ്ഥാന സർക്കാർ സ്ഥാപനമോ വകുപ്പോ ഏജൻസിയോ അവരുടെ ഔദ്യോഗിക ആവശ്യങ്ങൾക്കായി നിർമ്മിക്കുന്നതോ ശേഖരിക്കുന്നതോ ആയ ഡാറ്റയാണിവ. ഈ വിഭാഗത്തിലുള്ള ഡാറ്റ സർക്കാർ വകുപ്പുകൾക്കോ സ്ഥാപനങ്ങൾക്കോ ഔദ്യോഗിക ആവശ്യങ്ങൾക്കായി സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോം വഴി നിയന്ത്രിതമായി (Restricted Access) പങ്കുവെക്കാവുന്നതാണ്.

സി) കോൺഫിഡൻഷ്യൽ ഡാറ്റ (Confidential Data): ദേശസുരക്ഷയെയോ വ്യക്തിഗത സ്വകാര്യതയെയോ ബാധിക്കാനിടയുള്ളതോ അല്ലെങ്കിൽ നിലവിലുള്ള നിയമങ്ങൾ പ്രകാരം വെളിപ്പെടുത്താൻ പാടില്ലാത്തതോ ആയ അതീവ രഹസ്യസ്വഭാവമുള്ള ഡാറ്റയെയാണ് ഇത് സൂചിപ്പിക്കുന്നത്. ഇത്തരം ഡാറ്റ കർശനമായ നിയന്ത്രണങ്ങൾക്ക് വിധേയമാണ്. ബന്ധപ്പെട്ട വകുപ്പോ ഏജൻസിയോ നിശ്ചയിക്കുന്ന അതീവ സുരക്ഷാ മാനദണ്ഡങ്ങൾ പാലിച്ച് മാത്രമേ ഇവ സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് വഴി കൈമാറാൻ പാടുള്ളൂ.

Datasets പരമാവധി Machine readable രൂപത്തിൽ മാത്രമേ നിർമ്മിക്കാൻ പാടുള്ളൂ. വകുപ്പുകളിൽ നിലവിലുള്ള പഴയ ഡാറ്റ (Legacy data) കണ്ടെത്തി അവ ഘട്ടം ഘട്ടമായും വ്യവസ്ഥാപിതമായും ഡിജിറ്റൈസ് ചെയ്യേണ്ടതാണ്.

ഈ നയത്തിന് കീഴിലുള്ള ഓരോ സർക്കാർ വകുപ്പും ഏജൻസിയും അവർ രൂപപ്പെടുത്തുന്നതോ കൈകാര്യം ചെയ്യുന്നതോ ആയ ഡാറ്റ പബ്ലിക്, ഇന്റേണൽ, കോൺഫിഡൻഷ്യൽ എന്നിങ്ങനെ വർഗ്ഗീകരിക്കാൻ ബാധ്യസ്ഥരാണ്. ഈ വർഗ്ഗീകരണം സുതാര്യവും കൃത്യവുമായ രീതിയിലാണെന്ന് ഓരോ വകുപ്പും ഉറപ്പാക്കണം. 'നെഗറ്റീവ് ലിസ്റ്റിൽ' (Negative List) ഉൾപ്പെട്ടിട്ടില്ലാത്ത പബ്ലിക്, ഇന്റേണൽ ഡാറ്റകൾ കൃത്യസമയത്ത് സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ ലഭ്യമാക്കാൻ തയ്യാറാക്കണം. ഓരോ വകുപ്പിലെയും 'ഡാറ്റാ മാനേജ്മെന്റ് സെൽ' (Data Management Cell) ഈ പ്രവർത്തനങ്ങൾക്ക് മേൽനോട്ടം വഹിക്കുകയും നടപ്പിലാക്കുകയും ചെയ്യും.

10. ഡാറ്റാ ലഭ്യതയുടെ തരങ്ങൾ (Types of Data Access)

സർക്കാർ ഫണ്ട് ഉപയോഗിച്ച് ഉത്പാദിപ്പിക്കുന്ന ഡാറ്റ (Data assets), സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ചിലെ താഴെ പറയുന്ന മാനദണ്ഡങ്ങൾക്കനുസൃതമായി ലഭ്യമാക്കാനും പങ്കുവെക്കാനും എല്ലാ സർക്കാർ സ്ഥാപനങ്ങളും ബാധ്യസ്ഥരാണ്:

അനിയന്ത്രിതമായ ഡാറ്റാ ലഭ്യത (Open Access): 'പബ്ലിക് ഡാറ്റ' (Public Data) വിഭാഗത്തിൽപ്പെട്ട വിവരങ്ങൾ മുൻകൂട്ടിയുള്ള അനുമതിയോ രജിസ്ട്രേഷനോ കൂടാതെ തന്നെ ലഭ്യമാക്കുന്ന രീതി.

നിയന്ത്രിത ലഭ്യത (Restricted Access): 'ഇന്റേണൽ ഡാറ്റ' (Internal Data) വിഭാഗത്തിൽപ്പെട്ട

ഡാറ്റ വിവിധ വകുപ്പുകൾക്കോ സ്ഥാപനങ്ങൾക്കോ രജിസ്ട്രേഷനിലൂടെയും മുൻകൂട്ടിയുള്ള അനുമതിയോടും കൂടി മാത്രം ലഭ്യമാക്കുന്ന രീതിയാണിത്.

അംഗീകാര പ്രക്രിയ (Approval Process)

സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി നിശ്ചയിച്ചിട്ടുള്ള ആക്സസ് കൺട്രോൾ മാനദണ്ഡങ്ങൾ അനുസരിച്ചായിരിക്കണം സർക്കാർ സ്ഥാപനങ്ങൾ സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ ഇന്റേണൽ ഡാറ്റ (Internal Data) പ്രസിദ്ധീകരിക്കേണ്ടത്.

സംസ്ഥാന സർക്കാർ വകുപ്പുകളിലെ ചീഫ് ഡാറ്റാ ഓഫീസർക്ക് (CDO), പ്ലാറ്റ്ഫോമിൽ അവർക്ക് ലഭ്യമായ എല്ലാ ഡാറ്റാസെറ്റുകളും (Datasets) തുടർ അനുമതി കൂടാതെ തന്നെ ലഭ്യമാക്കാനും ഉപയോഗിക്കാനും സാധിക്കുന്നതാണ്.

സർക്കാർ സ്ഥാപനങ്ങൾ പൊതുവായി ലഭ്യമാക്കിയിട്ടില്ലാത്ത പ്രത്യേക ഡാറ്റാസെറ്റുകൾക്കായി അപേക്ഷിക്കാൻ സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ സംവിധാനം ഉണ്ടാകും. ഇത്തരം അപേക്ഷകൾ ഈ പ്ലാറ്റ്ഫോം വഴി ബന്ധപ്പെട്ട വകുപ്പിലെ ചീഫ് ഡാറ്റാ ഓഫീസർമാർക്ക് അയക്കുകയും അവർ അത് അംഗീകരിക്കുകയും വേണം.

11. നെഗറ്റീവ് ലിസ്റ്റ് തയ്യാറാക്കൽ (Negative List Preparation)

നെഗറ്റീവ് ലിസ്റ്റ് തയ്യാറാക്കൽ:

ദേശസുരക്ഷ, രഹസ്യാത്മകത, സ്വകാര്യത അല്ലെങ്കിൽ നിയമപരമായ നിയന്ത്രണങ്ങൾ എന്നിവ കാരണം പങ്കുവെക്കാൻ സാധിക്കാത്ത ഡാറ്റാസെറ്റുകളുടെ ഒരു കരട് 'നെഗറ്റീവ് ലിസ്റ്റ്', ഓരോ വകുപ്പും അവരുടെ വകുപ്പുതല ഡാറ്റാ മാനേജ്മെന്റ് സെൽ (DMC) മുഖേന തയ്യാറാക്കേണ്ടതാണ്.

ഈ നയം പ്രസിദ്ധീകരിച്ച് ആറ് മാസത്തിനുള്ളിൽ ഇത്തരം കരട് പട്ടിക തയ്യാറാക്കണം.

അംഗീകാര പ്രക്രിയ:

ഡാറ്റാ മാനേജ്മെന്റ് സെൽ തയ്യാറാക്കിയ കരട് നെഗറ്റീവ് ലിസ്റ്റ് പരിശോധനയ്ക്കായി സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റിക്ക് (SDGC) സമർപ്പിക്കണം.

പട്ടികയിൽ ഉൾപ്പെടുത്തിയിട്ടുള്ള ഓരോ ഡാറ്റാസെറ്റും താഴെ പറയുന്ന നിയമങ്ങൾക്കും നയങ്ങൾക്കും അനുസൃതമാണോ എന്ന് സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി വിലയിരുത്തും:

ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് (DPDP Act), 2023.

വിവരാവകാശ നിയമം (RTI Act), 2005.

നാഷണൽ ഡാറ്റാ ഷെയറിംഗ് ആൻഡ് ആക്സസിബിലിറ്റി പോളിസി (NDSAP), 2012.

നിലവിലുള്ള മറ്റ് സംസ്ഥാന/കേന്ദ്ര നിയമങ്ങൾ.

സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റിയുടെ ശിപാർശ ലഭിച്ചാൽ, അന്തിമ അംഗീകാരത്തിനായി പട്ടിക അപെക്സ്-തല (Apex-level) ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റിക്ക് കൈമാറും.

വകുപ്പുകളുടെ നെഗറ്റീവ് ലിസ്റ്റുകൾ സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി കൃത്യമായ ഇടവേളകളിൽ പുനഃപരിശോധിക്കുന്നതാണ്.

12. അപെക്സ്-തല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി

ഈ നയത്തിന്റെ ഭരണ മേൽനോട്ടം വഹിക്കുന്നതിനും പ്രധാന നിർദ്ദേശങ്ങൾ നൽകുന്നതിനുമുള്ള ഉന്നതതല സമിതിയാണിത് (Apex-level Data Governance Committee). സമിതിയിൽ താഴെ പറയുന്ന അംഗങ്ങൾ ഉൾപ്പെടുന്നു:

ചീഫ് സെക്രട്ടറി, കേരള സർക്കാർ – ചെയർപേഴ്സൺ

അഡീഷണൽ ചീഫ് സെക്രട്ടറി, ധനകാര്യ വകുപ്പ്

അഡീഷണൽ ചീഫ് സെക്രട്ടറി, ആഭ്യന്തരം & വിജിലൻസ് വകുപ്പ്

അഡീഷണൽ ചീഫ് സെക്രട്ടറി, റവന്യൂ & ദുരന്തനിവാരണ വകുപ്പ്

അഡീഷണൽ ചീഫ് സെക്രട്ടറി, പൊതുഭരണ വകുപ്പ്

സെക്രട്ടറി, നിയമ വകുപ്പ്

അഡീഷണൽ ചീഫ് സെക്രട്ടറി, വ്യവസായം & വാണിജ്യം വകുപ്പ്

അഡീഷണൽ ചീഫ് സെക്രട്ടറി, ആരോഗ്യവും കുടുംബക്ഷേമവും വകുപ്പ്

സെക്രട്ടറി, പ്ലാനിംഗ് & ഇക്കണോമിക് അഫയേഴ്സ് വകുപ്പ്

സെക്രട്ടറി, ഇലക്ട്രോണിക്സ് & ഐടി വകുപ്പ് (കൺവീനർ)

ഡയറക്ടർ, കേരള സ്റ്റേറ്റ് ഐടി മിഷൻ

സ്റ്റേറ്റ് ഇൻഫോർമാറ്റിക്സ് ഓഫീസർ (SIO), എൻ.ഐ.സി (NIC)

ഈ സമിതിയുടെ പ്രധാന ചുമതലകൾ:

നയം നടപ്പാക്കുന്നതിൽ മേൽനോട്ടം വഹിക്കുക, ഡാറ്റ പങ്കുവെക്കുന്നതുമായി ബന്ധപ്പെട്ട നിരക്കുകൾ (Pricing) അല്ലെങ്കിൽ വരുമാന മാർഗ്ഗങ്ങൾ (Monetization) എന്നിവയിൽ തീരുമാനമെടുക്കുക.

ഡാറ്റ പങ്കുവെക്കലുമായി ബന്ധപ്പെട്ട് സർക്കാർ വകുപ്പുകളിൽ നിന്നുള്ള പരാതികൾ പരിഹരിക്കുന്നതിനുള്ള അപ്പലേറ്റ് ബോഡിയായി (Appellate body) പ്രവർത്തിക്കുക.

നയത്തിൽ വരുത്തേണ്ട ഭേദഗതികൾ ശുപാർശ ചെയ്യുക.

സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി (SDGC) റിപ്പോർട്ട് ചെയ്യുന്ന തർക്കങ്ങളിലും നിയമലംഘനങ്ങളിലും തീരുമാനമെടുക്കാനുള്ള അധികാരം അപെക്സ്-തല കമ്മിറ്റിക്കുണ്ട്. ഈ നയത്തിലെ വ്യവസ്ഥകൾ പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കാൻ ബന്ധപ്പെട്ട സർക്കാർ വകുപ്പുകൾക്കോ ഏജൻസികൾക്കോ സ്ഥാപനങ്ങൾക്കോ ആവശ്യമായ ഉത്തരവുകളും നിർദ്ദേശങ്ങളും സമിതി നൽകും. ഡാറ്റാ പങ്കുവെക്കുന്നതിലും പ്രസിദ്ധീകരിക്കുന്നതിലും സംസ്ഥാനതല കമ്മിറ്റി (SDGC) നൽകുന്ന നിർദ്ദേശങ്ങൾക്കെതിരെയുള്ള അപ്പീലുകൾ ഈ സമിതി പരിഗണിക്കും.

13. സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി

ഈ നയം നടപ്പിലാക്കുന്നതിന്റെ മേൽനോട്ട ചുമതല സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റിക്കായിരിക്കും. സമിതിയിൽ താഴെ പറയുന്ന അംഗങ്ങൾ ഉൾപ്പെടുന്നു:

സെക്രട്ടറി, ഇലക്ട്രോണിക്സ് & ഐടി വകുപ്പ് (ചെയർപേഴ്സൺ)

ധനകാര്യ വകുപ്പിൽ നിന്നുള്ള പ്രതിനിധി

പ്ലാനിംഗ് & ഇക്കണോമിക് അഫയേഴ്സ് വകുപ്പിൽ നിന്നുള്ള പ്രതിനിധി

ഡയറക്ടർ, കേരള സ്റ്റേറ്റ് ഐടി മിഷൻ (കൺവീനർ)

സ്റ്റേറ്റ് ഇൻഫോർമാറ്റിക്സ് ഓഫീസർ (SIO), എൻ.ഐ.സി (NIC)

എക്സിക്യൂട്ടീവ് ഡയറക്ടർ, സി-ഡാക് (C-DAC)

പ്രത്യേക ക്ഷണിതാക്കളായി ബന്ധപ്പെട്ട വകുപ്പുകളിൽ നിന്നുള്ള പ്രതിനിധികൾ (ഡാറ്റ ആവശ്യപ്പെടുന്നവരും ഡാറ്റയുടെ ഉടമസ്ഥരും)

ഈ സമിതിയുടെ പ്രധാന ചുമതലകൾ:

സംസ്ഥാനത്ത് ഈ നയം നടപ്പിലാക്കുന്നതിനും സർക്കാർ സ്ഥാപനങ്ങൾ ഡാറ്റ പങ്കുവെക്കുന്നതിലെ പുരോഗതി വിലയിരുത്തുന്നതിനും ഉത്തരവാദിത്തം വഹിക്കുക.

വകുപ്പുകൾ തമ്മിലുള്ള ഡാറ്റാ കൈമാറ്റവുമായി ബന്ധപ്പെട്ട് ആവശ്യമായ തിരുത്തൽ നടപടികൾ ശുപാർശ ചെയ്യുക.

സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ പ്രസിദ്ധീകരിക്കുന്ന ഡാറ്റാസെറ്റുകളുടെ 'ആക്സസ് കൺട്രോൾ' (Access control) സംവിധാനങ്ങൾ നിർവ്വചിക്കുകയും അംഗീകരിക്കുകയും ചെയ്യുക.

ദേശീയ മാനദണ്ഡങ്ങളും ഇന്ററോപ്പറബിലിറ്റി ചട്ടക്കൂടുകളും അവലംബിച്ചുകൊണ്ട് ഡാറ്റാ സ്റ്റാൻഡേർഡുകളും മെറ്റാഡാറ്റാ മാർഗ്ഗനിർദ്ദേശങ്ങളും വികസിപ്പിക്കുക. കൂടാതെ ഡാറ്റയുടെ ഗുണനിലവാരവും നയങ്ങൾ പാലിക്കുന്നുണ്ടോ എന്നും നിരീക്ഷിക്കുകയും ഡാറ്റയുമായി ബന്ധപ്പെട്ട വെല്ലുവിളികൾ പരിഹരിക്കുകയും ചെയ്യുക.

ഡാറ്റ കൃത്യസമയത്ത് പ്രസിദ്ധീകരിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കാൻ വകുപ്പുകൾക്കിടയിലുള്ള ഏകോപനം സുഗമമാക്കുകയും ചട്ടങ്ങൾ പാലിക്കുന്നുണ്ടോ എന്ന് നിരീക്ഷിക്കുകയും ചെയ്യുക. നിർദ്ദേശങ്ങൾ പാലിക്കാത്ത പക്ഷം, 'പബ്ലിക് ഡാറ്റ' അല്ലെങ്കിൽ 'ഇന്റേണൽ ഡാറ്റ' വിഭാഗത്തിൽപ്പെട്ട ഡാറ്റ നിശ്ചിത സമയത്തിനകം സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ നിർബന്ധമായും പ്രസിദ്ധീകരിക്കാൻ സർക്കാർ വകുപ്പിനോ ഏജൻസിക്കോ സ്ഥാപനത്തിനോ നിർദ്ദേശം നൽകാനുള്ള അധികാരം ഈ കമ്മിറ്റിക്കുണ്ട്.

തർക്കങ്ങൾ പരിഹരിക്കപ്പെടാത്ത സാഹചര്യത്തിൽ, വിഷയം അപ്പലേറ്റ് അതോറിറ്റിയായ അപെക്സ്-തല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റിയുടെ പരിഗണനയ്ക്ക് വിടും.

14. വകുപ്പുകളിലെ ഡാറ്റാ മാനേജ്മെന്റ് സെൽ (DMC)

ഓരോ വകുപ്പും ആ വകുപ്പിലെ ഐടി സംവിധാനങ്ങളിൽ (IT Systems) പരിജ്ഞാനമുള്ള

ഉദ്യോഗസ്ഥരെ ഉൾപ്പെടുത്തി ഒരു 'ഡിപ്പാർട്ട്മെന്റ് ഡാറ്റാ മാനേജ്മെന്റ് സെൽ' രൂപീകരിക്കണം. ചീഫ് ഡാറ്റാ ഓഫീസർ (CDO) ആയിരിക്കും ഈ സെല്ലിന്റെ മേധാവി. ഡാറ്റാ മാനേജ്മെന്റ് സെല്ലിന്റെ പ്രധാന ഉത്തരവാദിത്തങ്ങൾ ഇവയാണ്:

പ്രസിദ്ധീകരിക്കേണ്ട വകുപ്പുതല ഡാറ്റാസെറ്റുകളുടെ ഒരു സമയപ്പട്ടിക (Schedule) തയ്യാറാക്കുക.

വകുപ്പിന്റെ 'നെഗറ്റീവ് ലിസ്റ്റ്' തയ്യാറാക്കുകയും നയമനുസരിച്ച് ഡാറ്റാസെറ്റുകളെ വർഗ്ഗീകരിക്കുകയും ചെയ്യുക.

സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ പ്രസിദ്ധീകരിക്കേണ്ട ഡാറ്റാസെറ്റുകൾ പതിവായി കണ്ടെത്തുകയും തരംതിരിക്കുകയും ചെയ്യുക.

ഡാറ്റാസെറ്റുകൾ തയ്യാറാക്കുന്നതിനും ഫോർമാറ്റുകൾ മാറ്റുന്നതിനും മറ്റും സാങ്കേതിക സഹായം നൽകുക.

ഡാറ്റയുടെ ഗുണനിലവാരത്തിലും കൃത്യതയിലും ശ്രദ്ധ കേന്ദ്രീകരിച്ചുകൊണ്ട് അതത് വകുപ്പിലെ 'ഓപ്പൺ ഡാറ്റ' നിരീക്ഷിക്കുകയും നിയന്ത്രിക്കുകയും ചെയ്യുക.

ഡാറ്റയുടെ ഗുണനിലവാരം ഉറപ്പുവരുത്തിക്കൊണ്ടുതന്നെ, ദൈനംദിന പ്രവർത്തനങ്ങളുടെ ഭാഗമായി ഡാറ്റാസെറ്റുകളുടെ (വിവരശേഖരങ്ങളുടെ) നിർമ്മാണവും അവ കൃത്യമായ ഇടവേളകളിൽ പുതുക്കുന്നതും നടപ്പിലാക്കുക.

സംയോജിത പൊതുസേവന വിതരണം ശക്തിപ്പെടുത്തുന്നതിനായി, കേരള സ്റ്റേറ്റ് ഐടി മിഷൻ നടപ്പിലാക്കുന്ന യൂണിഫൈഡ് സർവീസസ് ഡെലിവറി പോർട്ടൽ (USDP), യൂണിഫൈഡ് രജിസ്ട്രി തുടങ്ങിയ സർക്കാർ പദ്ധതികളുമായി ഡാറ്റാ കൈമാറ്റ സംവിധാനങ്ങളെ ഫലപ്രദമായി ബന്ധിപ്പിക്കുന്നുവെന്ന് ഉറപ്പാക്കുക.

മറ്റ് ഇ-ഗവേണൻസ് ആപ്ലിക്കേഷനുകളുമായോ സിസ്റ്റങ്ങളുമായോ ഡാറ്റാ കൈമാറ്റം സാധ്യമാക്കുന്നതിന് എല്ലാ വകുപ്പുതല ആപ്ലിക്കേഷനുകൾക്കും 'ഓപ്പൺ എ.പി.ഐ' (Open API) വികസിപ്പിക്കുക. ഈ എ.പി.ഐ., യൂണിഫൈഡ് ഡാറ്റാ എക്സ്ചേഞ്ചിനായുള്ള ഇന്ത്യൻ സ്റ്റാൻഡേർഡ് (IS 18003 (Part 2): 2021) അനുസരിച്ചായിരിക്കണം രൂപകൽപ്പന ചെയ്യേണ്ടത്. ഇത് സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിലെ എ.പി.ഐ രജിസ്ട്രിയിൽ പ്രസിദ്ധീകരിക്കുകയും വേണം.

ചീഫ് ഡാറ്റാ ഓഫീസർ (CDO)

ഓരോ വകുപ്പും അല്ലെങ്കിൽ സ്ഥാപനവും അവരുടെ വകുപ്പുതലവനെ (HoD) അല്ലെങ്കിൽ ഒരു

മുതിർന്ന ഉദ്യോഗസ്ഥനെ ചീഫ് ഡാറ്റാ ഓഫീസർ (CDO) ആയി നാമനിർദ്ദേശം ചെയ്യേണ്ടതാണ്. ചീഫ് ഡാറ്റാ ഓഫീസറുടെ വിവരങ്ങൾ കേരള സ്റ്റേറ്റ് ഐടി മിഷനെ അറിയിക്കേണ്ടതുമാണ്.

ചീഫ് ഡാറ്റാ ഓഫീസറുടെ ഉത്തരവാദിത്തങ്ങൾ താഴെ പറയുന്നവയാണ്:

അതത് വകുപ്പിലെ ഡാറ്റയുടെ സമഗ്രമായ മാനേജ്മെന്റ്, ഉപയോഗം, ഗവേണൻസ് എന്നിവയുടെ ഉത്തരവാദിത്തം ചീഫ് ഡാറ്റാ ഓഫീസർക്കായിരിക്കും.

സ്വന്തം വകുപ്പിൽ നിന്നോ സ്ഥാപനത്തിൽ നിന്നോ ഉള്ള ഡാറ്റാസെറ്റുകൾ സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ പ്രസിദ്ധീകരിക്കുക.

മറ്റ് സർക്കാർ സ്ഥാപനങ്ങളിൽ നിന്നുള്ള ഡാറ്റാസെറ്റുകൾ ലഭ്യമാക്കുന്നതിനായി സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോം വഴി അപേക്ഷകൾ സമർപ്പിക്കുക. ഇത്തരം അപേക്ഷകൾ സംസ്ഥാനതല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റി വിലയിരുത്തും.

ശേഖരണം, സംഭരണം, സംസ്കരണം, ഗുണനിലവാരം ഉറപ്പാക്കൽ, നിലനിർത്തൽ, ആർക്കൈവിംഗ് എന്നിങ്ങനെ ഡാറ്റയുടെ സമ്പൂർണ്ണ മാനേജ്മെന്റിന് മേൽനോട്ടം വഹിക്കുക.

ഡാറ്റാ പങ്കുവെക്കുന്നതിനായുള്ള ആപ്ലിക്കേഷൻ പ്രോഗ്രാമിംഗ് ഇന്റർഫേസ് (API) വികസിപ്പിക്കുന്നതിനായി സൊല്യൂഷൻ പ്രൊവൈഡർ അല്ലെങ്കിൽ ആപ്ലിക്കേഷൻ ഡെവലപ്മെന്റ് ഏജൻസിയുമായി ഏകോപിപ്പിച്ചുകൊണ്ട് വകുപ്പിന്റെ ഓപ്പൺ ഡാറ്റാ സംരംഭത്തിന് നേതൃത്വം നൽകുക.

15. വ്യക്തിഗത വിവരങ്ങളുടെ കൈമാറ്റവും സംരക്ഷണവും

ഡി.പി.ഡി.പി (DPDP) നിയമപാലനം:

വ്യക്തിഗത വിവരങ്ങളുടെ (Personal Data) ഏതൊരു കൈമാറ്റവും അല്ലെങ്കിൽ പ്രോസസിംഗും (Processing), 2023-ലെ ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് (DPDP Act), 2025-ലെ ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ റൂൾസ് എന്നിവയ്ക്കും അതുമായി ബന്ധപ്പെട്ട മറ്റ് ചട്ടങ്ങൾക്കും മാർഗ്ഗനിർദ്ദേശങ്ങൾക്കും കർശനമായി വിധേയമായിരിക്കണം.

വ്യക്തിഗത ഡാറ്റ (Personal data) ശേഖരിക്കുകയും സംസ്കരിക്കുകയും ചെയ്യുന്ന എല്ലാ സർക്കാർ സ്ഥാപനങ്ങളെയും ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് (DPDP Act) 2023, ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ റൂൾസ് 2025 എന്നിവ പ്രകാരം 'ഡാറ്റാ ഫിഡ്യൂഷ്യറികൾ' (Data Fiduciaries) ആയി നിശ്ചയിക്കുന്നതാണ്. ഡാറ്റാ കൈമാറ്റ രീതികൾ പ്രസ്തുത നിയമത്തിനും ചട്ടങ്ങൾക്കും അനുസൃതമായി 'ഡാറ്റാ പ്രിൻസിപ്പൽമാരുടെ' (Data

Principals) അവകാശങ്ങളെ മാനിക്കുന്നുവെന്ന് ഈ സ്ഥാപനങ്ങൾ ഉറപ്പാക്കണം.

സർക്കാർ വകുപ്പുകൾക്കിടയിലുള്ള വ്യക്തിഗത വിവരങ്ങളുടെ കൈമാറ്റം:

താഴെ പറയുന്ന സാഹചര്യങ്ങളിൽ മാത്രമേ സർക്കാർ വകുപ്പുകൾക്കിടയിൽ വ്യക്തിഗത ഡാറ്റ പങ്കുവെക്കാൻ പാടുള്ളൂ:

പൊതുസേവനങ്ങൾ നൽകുന്നതിനോ നിയമപരമായ ചുമതലകൾ നിർവ്വഹിക്കുന്നതിനോ അത്യന്താപേക്ഷിതമാകുമ്പോൾ.

'ഡാറ്റാ മിനിമൈസേഷൻ' (Data minimization) തത്വം പാലിക്കുമ്പോൾ (അതായത്, ആവശ്യമുള്ള വിവരങ്ങൾ മാത്രം പങ്കുവെക്കുക).

ഡി.പി.ഡി.പി നിയമപ്രകാരമുള്ള സമ്മതപത്രമോ (Consent) അല്ലെങ്കിൽ നിയമപരമായ മറ്റ് കാരണങ്ങളോ ഉണ്ടെന്ന് ഉറപ്പുവരുത്തുമ്പോൾ.

പുറത്തുള്ള ഏജൻസികളുമായുള്ള ഡാറ്റാക്കൈമാറ്റം:

താഴെ പറയുന്ന കാരണങ്ങളാലല്ലാതെ സ്വകാര്യ സ്ഥാപനങ്ങൾക്കോ മറ്റ് മൂന്നാം കക്ഷികൾക്കോ (Third parties) വ്യക്തിഗത ഡാറ്റാ കൈമാറാൻ പാടുള്ളതല്ല:

ഡാറ്റാ പ്രിൻസിപ്പലിന്റെ വ്യക്തമായ അനുവാദം (Explicit consent) ലഭിച്ചിട്ടുണ്ടെങ്കിൽ.

നിയമപരമായോ അല്ലെങ്കിൽ ഡി.പി.ഡി.പി നിയമപ്രകാരം ബന്ധപ്പെട്ട അധികാരിയുടെ അനുമതിയോടെയോ നിർബന്ധിതമാക്കിയിട്ടുള്ള സാഹചര്യങ്ങളിൽ.

വകുപ്പുതല ഉത്തരവാദിത്തങ്ങൾ:

വ്യക്തിഗത ഡാറ്റാ പങ്കുവെക്കുമ്പോൾ എൻക്രിപ്ഷൻ (Encryption), ആക്സസ് കൺട്രോൾ, സമ്മതപത്ര പരിപാലനം (Consent management), ഓഡിറ്റ് ട്രയലുകൾ തുടങ്ങിയ സുരക്ഷാ സംവിധാനങ്ങൾ ഒരുക്കാനും ഡി.പി.ഡി.പി നിയമം പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കാനും ഓരോ വകുപ്പും ബാധ്യസ്ഥരാണ്.

ഡാറ്റാ പങ്കുവെക്കുന്നതിലെ സുതാര്യതയും നിയമപാലനവും നിരീക്ഷിക്കുന്നതിനും നടപ്പിലാക്കുന്നതിനുമായി, ഓരോ വകുപ്പും അവരുടെ ചീഫ് ഡാറ്റാ ഓഫീസറെയും (CDO), ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് (DPDP Act) 2023 പ്രകാരം ബാധകമെങ്കിൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ഓഫീസറെയും (DPO) ചുമതലപ്പെടുത്തേണ്ടതാണ്.

2023-ലെ ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് അനുസരിച്ച്, വ്യക്തിഗത ഡാറ്റാ കൈകാര്യം ചെയ്യുന്നതുമായി ബന്ധപ്പെട്ട പരാതികൾ പരിഹരിക്കുന്നതിന് ഓരോ വകുപ്പും സുതാര്യവും സമയബന്ധിതവുമായ ഒരു പരാതി പരിഹാര സംവിധാനം (Grievance redressal mechanism) രൂപീകരിക്കേണ്ടതാണ്.

16. ഡാറ്റാ സംഭരണം, നിലനിർത്തൽ, ആർക്കൈവിംഗ് (Data Storage, Retention and its Archival)

വിവരങ്ങളുടെ സുരക്ഷ, സമഗ്രത (Integrity), ലഭ്യത എന്നിവ ഉറപ്പാക്കുന്നതിനായി എല്ലാ സർക്കാർ സ്ഥാപനങ്ങളും ഡാറ്റാ സംഭരണത്തിനുള്ള ബെസ്റ്റ് പ്രാക്ടീസസ് (Best practices) പാലിക്കേണ്ടതാണ്. സുരക്ഷിതവും വികസിപ്പിക്കാവുന്നതുമായ സംഭരണ സൗകര്യങ്ങൾ (Scalable storage), കൃത്യമായ ഡാറ്റാ ബാക്കപ്പുകൾ, ദുരന്തനിവാരണ സംവിധാനങ്ങൾ (Disaster recovery), എൻക്രിപ്ഷൻ പ്രോട്ടോക്കോളുകൾ, ആക്സസ് കൺട്രോൾ, നിലവിലുള്ള ഡാറ്റാ സംരക്ഷണ നിയമങ്ങൾ പാലിക്കൽ എന്നിവ ഈ പ്രാക്ടീസസിൽ ഉൾപ്പെടണം.

ആർക്കൈവിംഗ് നയങ്ങൾ (Archival Policies): ഓരോ വകുപ്പും അവരുടെ ഡാറ്റാ മാനേജ്മെന്റ് സെൽ (DMC) മുഖേന സമഗ്രമായ ഡാറ്റാ ആർക്കൈവിംഗ് മാർഗ്ഗനിർദ്ദേശങ്ങൾ വികസിപ്പിക്കുകയും നടപ്പിലാക്കുകയും വേണം. ആർക്കൈവ് ചെയ്യേണ്ട ഡാറ്റ കണ്ടെത്തുന്നതിനുള്ള മാനദണ്ഡങ്ങൾ, ആർക്കൈവിംഗ് ഫോർമാറ്റുകൾ (ഉദാഹരണത്തിന് ദീർഘകാലം നിലനിൽക്കുന്ന ഫോർമാറ്റുകൾ), ഡാറ്റ സുരക്ഷിതമായി സംഭരിക്കാനും തിരികെ എടുക്കാനുമുള്ള നടപടിക്രമങ്ങൾ എന്നിവ ഇതിൽ നിർവ്വചിക്കണം.

ആർക്കൈവിംഗിന്റെ ഉത്തരവാദിത്തം: ബന്ധപ്പെട്ട ഡാറ്റാസെറ്റുകൾ കൃത്യസമയത്തും സുരക്ഷിതമായും ആർക്കൈവ് ചെയ്യുന്നുണ്ടെന്ന് ഉറപ്പാക്കാനുള്ള ചുമതല അതത് വകുപ്പുകളിലെ ചീഫ് ഡാറ്റാ ഓഫീസർക്കായിരിക്കും (CDO).

ഡാറ്റ നിലനിർത്തുന്നതിനുള്ള സമയക്രമം (Retention Schedules): എല്ലാത്തരം ഡാറ്റയും എത്രകാലം സൂക്ഷിക്കണം എന്നതിനെക്കുറിച്ച് (Data retention) വ്യക്തമായ സമയക്രമം വകുപ്പുകൾ തയ്യാറാക്കണം. നിയമപരവും ഭരണപരവുമായ ആവശ്യങ്ങൾ കണക്കിലെടുത്ത് ഡാറ്റ സൂക്ഷിക്കേണ്ട കുറഞ്ഞതും കൂടിയതുമായ കാലാവധി ഇതിൽ വ്യക്തമാക്കണം. ഈ സമയക്രമങ്ങൾ കാലാനുസൃതമായി പരിഷ്കരിക്കേണ്ട ഉത്തരവാദിത്തം അതത് ഡാറ്റാ മാനേജ്മെന്റ് സെല്ലുകൾക്കായിരിക്കും.

17. വിലനിർണ്ണയം (Pricing)

സംസ്ഥാന സർക്കാർ സ്ഥാപനങ്ങൾ സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിൽ 'ഇന്റേണൽ ഡാറ്റ' (Internal Data) ആയി വർഗ്ഗീകരിച്ചിട്ടുള്ള ഡാറ്റ വകുപ്പുകൾ തമ്മിൽ പങ്കുവെക്കുന്നത് സൗജന്യമായിരിക്കും. ഇത് സർക്കാർ മേഖലയിലുടനീളം തടസ്സമില്ലാത്ത ഡാറ്റാക്കൈമാറ്റം

സാധ്യമാക്കുന്നു.

സ്റ്റേറ്റ് ഡാറ്റാ എക്സ്ചേഞ്ച് പ്ലാറ്റ്ഫോമിലെ 'ഇന്റേണൽ ഡാറ്റ' വിഭാഗത്തിൽപ്പെട്ട ചില ഡാറ്റ ശേഖരിക്കാനും സംഭരിക്കാനും പരിപാലിക്കാനും വലിയ തോതിലുള്ള നിക്ഷേപം ആവശ്യമായി വരുന്നതിനാൽ, അവയിൽ നിന്ന് വരുമാനം കണ്ടെത്താൻ (Monetized) സർക്കാർ സ്ഥാപനങ്ങൾക്ക് അനുവാദമുണ്ടാകും. വരുമാനം കണ്ടെത്താനായി ബന്ധപ്പെട്ട സ്ഥാപനം നിർദ്ദിഷ്ട നിരക്കുകൾ ഉൾപ്പെടെയുള്ള അപേക്ഷ അന്തിമ അംഗീകാരത്തിനായി അപെക്സ്-തല ഡാറ്റാ ഗവേണൻസ് കമ്മിറ്റിക്ക് സമർപ്പിക്കണം.

തിരിച്ചറിയാൻ കഴിയാത്ത വിധം മാറ്റം വരുത്തിയ (Anonymized) ഡാറ്റ മാത്രമേ ഇത്തരത്തിൽ പങ്കുവെക്കാനോ വരുമാനത്തിനായി ഉപയോഗിക്കാനോ പാടുള്ളൂ. ഇത്തരത്തിൽ കൈമാറുന്ന വിവരങ്ങളിൽ ഉപഭോക്താക്കളുടെ വ്യക്തിഗത വിവരങ്ങളോ, 'നെഗറ്റീവ് ലിസ്റ്റിൽ' ഉൾപ്പെട്ടതോ അല്ലെങ്കിൽ അതീവ രഹസ്യസ്വഭാവമുള്ളതോ (Confidential) ആയ വിവരങ്ങൾ ഉൾപ്പെടുന്നില്ലെന്ന് ചീഫ് ഡാറ്റാ ഓഫീസറോ (CDO) ഡാറ്റാ പ്രൊട്ടക്ഷൻ ഓഫീസറോ ഉറപ്പാക്കണം. ഇത്തരം പ്രവർത്തനങ്ങളെല്ലാം ഈ നയത്തിലെ വ്യക്തിഗത ഡാറ്റാ സംരക്ഷണ തത്വങ്ങൾ പാലിച്ചുകൊണ്ടായിരിക്കണം. ഇത്തരത്തിലുള്ള നിരക്കുകൾ സ്റ്റാർട്ടപ്പുകൾ, വ്യവസായ സ്ഥാപനങ്ങൾ, മറ്റ് സർക്കാർ ഇതര പങ്കാളികൾ തുടങ്ങിയ സ്വകാര്യ സ്ഥാപനങ്ങൾക്ക് മാത്രമേ ബാധകമാകൂ; സർക്കാർ സ്ഥാപനങ്ങൾക്ക് ഇത് ബാധകമല്ല.

ബന്ധപ്പെട്ട സർക്കാർ സ്ഥാപനം ഗണ്യമായ രീതിയിൽ പ്രോസസ്സിങ്ങോ (processing), പരിപോഷണമോ (enrichment), ക്യൂറേഷനോ (curation) നടത്തി മൂല്യവർദ്ധിതമാക്കിയ ഡാറ്റാസെറ്റുകൾക്ക് (value-added datasets) മാത്രമേ വരുമാനമാക്കുന്നതിനുള്ള (monetization) അനുമതി ഉണ്ടായിരിക്കുകയുള്ളൂ. ലാഭേച്ഛയില്ലാതെ ചെലവ് ഈടാക്കുക (cost-recovery) എന്ന തത്വത്തിലായിരിക്കണം വരുമാനം കണ്ടെത്തേണ്ടത്. എല്ലാ അടിസ്ഥാന ഓപ്പൺ ഡാറ്റയും (Open Data) സൗജന്യമായി തുടരേണ്ടതും, ഓപ്പൺ ഗവൺമെന്റ് ഡാറ്റാ തത്വങ്ങൾക്കനുസൃതമായി പൊതുജനങ്ങൾക്ക് ലഭ്യമാക്കേണ്ടതുമാണ്.

18. നിയമപരമായ ചട്ടക്കൂട് (Legal Framework)

ഡാറ്റ ശേഖരിക്കുകയും ബാധകമായ നിയമപ്രകാരം 'ഡാറ്റാ ഫിഡ്യൂഷ്യറികളായി' പ്രവർത്തിക്കുകയും ചെയ്യുന്ന അതത് സർക്കാർ സ്ഥാപനങ്ങൾക്കായിരിക്കും ഡാറ്റയുടെ ഉടമസ്ഥാവകാശം. ഡാറ്റ ആ സ്ഥാപനങ്ങളുടെ ഐടി അധിഷ്ഠിത ഇൻഫ്രാസ്ട്രക്ചറിൽ തന്നെ നിലനിൽക്കേണ്ടതാണ്. കൂടാതെ, ഈ നയപ്രകാരമുള്ള നിശ്ചിത ഗവേണൻസ്, സുരക്ഷാ മാനദണ്ഡങ്ങൾ എന്നിവ പാലിച്ച് മാത്രമേ ഡാറ്റ പങ്കുവെക്കുന്നതിനും ലഭ്യമാക്കുന്നതിനും അനുവാദമുണ്ടാകൂ.

തങ്ങളുടെ പ്രവർത്തന മേഖലകളിലെ ഡാറ്റയുമായി ബന്ധപ്പെട്ട നിയമപരവും

ധാർമ്മികവുമായ നിയന്ത്രണങ്ങൾ മനസ്സിലാക്കാനും അവ നടപ്പിലാക്കാനും, ഈ ആവശ്യകതകൾ നിറവേറ്റുന്നതിന് കൃത്യമായ നടപടിക്രമങ്ങൾ പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കാനും ചീഫ് ഡാറ്റാ ഓഫീസർമാർ ബാധ്യസ്ഥരാണ്.

നിയന്ത്രിതമോ ക്രമീകരിക്കപ്പെട്ടതോ ആയ ഡാറ്റയിൽ (Restricted and regulated data) അനധികൃതമായ ഇടപെടൽ ശ്രദ്ധയിൽപ്പെട്ടാൽ ഉടൻ തന്നെ കേരള സ്റ്റേറ്റ് ഐടി മിഷനെ (KSITM) അറിയിക്കേണ്ടതാണ്.

ഈ നയപ്രകാരം ഡാറ്റ ലഭ്യമാക്കുന്നത് കേന്ദ്ര സർക്കാരിന്റെയോ കേരള സർക്കാരിന്റെയോ നിലവിലുള്ള ഒരു നിയമത്തിന്റെയും ലംഘനമാകാൻ പാടുള്ളതല്ല.

കേരള സംസ്ഥാന ഡാറ്റാ നയം (KSDP) താഴെ പറയുന്ന നിയമം/ ചട്ടങ്ങൾക്ക് വിധേയമായിരിക്കും:

നാഷണൽ ഡാറ്റാ ഷെയറിംഗ് ആൻഡ് ആക്സസിബിലിറ്റി പോളിസി (NDSAP) – 2012.

ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് (DPDP Act) – 2023.

ഇൻഫർമേഷൻ ടെക്നോളജി ആക്ട് – 2000-വും അതിന്റെ ഭേദഗതികളും.

ഇൻഫർമേഷൻ ടെക്നോളജി (റീസണബിൾ സെക്യൂരിറ്റി പ്രാക്ടീസസ് ആൻഡ് പ്രൊസീജിയേഴ്സ് ആൻഡ് സെൻസിറ്റീവ് പേഴ്സണൽ ഡാറ്റാ ഓർ ഇൻഫർമേഷൻ) റൂൾസ് – 2011.

മേഖല തിരിച്ചുള്ള നിയന്ത്രണങ്ങൾ: കേന്ദ്ര-സംസ്ഥാന നിയമങ്ങളോ ചട്ടങ്ങളോ നിർദ്ദേശിച്ചിട്ടുള്ള പ്രത്യേക മേഖലകളിലെ ഡാറ്റാ മാനേജ്മെന്റ്, സ്വകാര്യതാ നിയന്ത്രണങ്ങൾ എന്നിവ വകുപ്പുകൾ പാലിക്കേണ്ടതാണ്.

19. തർക്കപരിഹാരം (Dispute Resolution)

നയത്തിന്റെ മൊത്തത്തിലുള്ള ഏകോപനം, രൂപീകരണം, നടപ്പിലാക്കൽ, നിരീക്ഷണം എന്നിവയുമായി ബന്ധപ്പെട്ട എല്ലാ കാര്യങ്ങൾക്കുമുള്ള നോഡൽ വകുപ്പ് ഇലക്ട്രോണിക്സും വിവരസാങ്കേതികവിദ്യയും വകുപ്പിന് (E&ITD) ആയിരിക്കും.

വിവരങ്ങൾ പങ്കുവെക്കുന്നതിലോ ലഭ്യമാക്കുന്നതിലോ എന്തെങ്കിലും തർക്കങ്ങൾ ഉണ്ടായാൽ സംസ്ഥാനതല കമ്മിറ്റി (State Level Committee) പ്രാഥമിക ആർബിട്രേറ്റർ (Initial arbitrator) ആയി പ്രവർത്തിക്കും. സർക്കാർ വകുപ്പുകളിൽ നിന്നോ മറ്റ് പുറംകക്ഷികളിൽ നിന്നോ (സർക്കാരിതര പങ്കാളികൾ) ഉള്ള പരാതികൾ പരിഹരിക്കുന്നതിനുള്ള അന്തിമ അപ്പലേറ്റ്

അതോറിറ്റി അപെക്സ് കമ്മിറ്റി (Apex Committee) ആയിരിക്കും.

20. ഉപസംഹാരം (Conclusion)

മികച്ച ഭരണനിർവ്വഹണം ഉറപ്പാക്കിക്കൊണ്ടും, ഇന്നോവേഷനെ പ്രോത്സാഹിപ്പിച്ചുകൊണ്ടും, പുതിയ തൊഴിലവസരങ്ങൾ സൃഷ്ടിച്ചുകൊണ്ടും വിവിധ സർക്കാർ വകുപ്പുകൾ, നയരൂപകർത്താക്കൾ, ഗവേഷണ സ്ഥാപനങ്ങൾ, വിദ്യഭ്യാസ മേഖല എന്നിവരുൾപ്പെടെയുള്ള വിവിധ വിഭാഗങ്ങൾക്ക് പ്രയോജനം ലഭിക്കുന്ന രീതിയിലാണ് കേരള സംസ്ഥാന ഡാറ്റാ നയം (KSDP) വിഭാവനം ചെയ്തിരിക്കുന്നത്. വരും വർഷങ്ങളിൽ കേരളത്തിന്റെ അഭിവൃദ്ധിയും സുസ്ഥിരമായ വളർച്ചയും ഉറപ്പാക്കുകയാണ് ഈ നയം ലക്ഷ്യമിടുന്നത്.

നയത്തിന്റെ മൊത്തത്തിലുള്ള ഏകോപനം, രൂപീകരണം, നടപ്പിലാക്കൽ, നിരീക്ഷണം എന്നിവയുമായി ബന്ധപ്പെട്ട എല്ലാ കാര്യങ്ങൾക്കുമുള്ള നോഡൽ വകുപ്പ് ഇലക്ട്രോണിക്സും വിവരസാങ്കേതികവിദ്യയും വകുപ്പ് (E&ITD) ആയിരിക്കും. ഡാറ്റാ പങ്കുവെക്കുന്നതോ ലഭ്യമാക്കുന്നതോ ആയി ബന്ധപ്പെട്ട് എന്തെങ്കിലും തർക്കങ്ങൾ ഉണ്ടാകുന്ന സാഹചര്യത്തിൽ, സ്റ്റേറ്റ് ലെവൽ കമ്മിറ്റി പ്രാഥമിക ആർബിട്രേറ്റർ (Initial arbitrator) ആയി പ്രവർത്തിക്കും. വകുപ്പുകൾക്കിടയിലോ പുറത്തുള്ള (സർക്കാരിതര) സ്റ്റേക്ക്ഹോൾഡർമാർക്കിടയിലോ ഉണ്ടാകുന്ന പരാതികൾ പരിഹരിക്കുന്നതിനുള്ള അന്തിമ അപ്പീൽ അതോറിറ്റി അപെക്സ് കമ്മിറ്റി ആയിരിക്കും.