ශ්‍රී ලංකාවේ දත්ත ආරක්ෂණ නීතිය

2022 අංක 9 දරන පෞද්ගලික දත්ත ආරක්ෂණ පනත පිළිබඳ දළ විශ්ලේෂණයක්

හැඳින්වීම

2022 අංක 9 දරන පුද්ගලික දත්ත ආරක්ෂණ පනත (PDPA), ශ්‍රී ලංකාවේ නීති රාමුවේ සුවිශේෂී සංවර්ධනයක් නියෝජනය කරන අතර, ඒ හරහා පළමුවරට ශ්‍රී ලංකාව තුළ ගැඹුරු සහ පරිපූර්ණ දත්ත ආරක්ෂණ යාන්ත්‍රණයක් ස්ථාපිත කර තිබේ. මාධ්‍ය නීති සංසදය විසින් කැනඩාව කේන්ද්‍ර කරගෙන ක්‍රියාත්මක නීතිය සහ ප්‍රජාතන්ත්‍රවාදය සඳහා වූ මධ්‍යස්ථානයේ සහයෝගය ඇතිව ප්‍රකාශයට පත් කරන ලද මෙම මාර්ගෝපදේශ සංග්‍රහය මගින්, නීති වෘත්තිකයින්, ක්ෂේත්‍රයේ විවිධ වෘත්තිකයන් , ප්‍රතිපත්ති සම්පාදකයින් ඇතුළු මෙම නව නීතිය අදාළ වන සියලු අනෙකුත් පාර්ශවකරුවන් සඳහා පනතේ ප්‍රධාන විධිවිධාන සම්බන්ධයෙන් සංක්ෂිප්ත විශ්ලේෂණයක් ඉදිරිපත් කර .තිබේ.

පසුබිම සහ වැදගත්කම

පෞද්ගලික දත්ත ආරක්ෂණ පනත මගින් ක්‍රමයෙන් ඩිජිටල්කරණය වන ශ්‍රී ලංකාවේ සමාජය තුළ දත්ත ආරක්ෂාවට මූලික අයිතිවාසිකමක් ලෙස විධිමත් පිළිගැනීමක් ලබාදී තිබේ. මෙම පනත ජාත්‍යන්තරය තුළ පවතින ඉහළ සහ පිළිගත් භාවිතයන්ගෙන් ද , විශේෂයෙන් යුරෝපා සංගමයේ පොදු දත්ත ආරක්ෂණ රෙගුලාසි (GDPR) තුළින් පෝෂණය ලබා ඇත. පනත මගින් පුද්ගලයින්ගේ පුද්ගලික දත්ත සඳහා සවිස්තරාත්මක ආරක්ෂාවන් ස්ථාපිත කරන අතරම ඩිජිටල් ආර්ථිකය තුළ නවෝත්පාදනය සහ වර්ධනය සඳහා අවශ්‍ය ව්‍යුහය ද ආරක්ෂාරී ලෙස නිර්මාණය බලගන්වා තිබේ. මෙම නීතියේ තවත් සුවිශේෂී කරුණක් වන්නේ එමගින් පුද්ගලයන්ගේ පෞද්ගලිකත්ව අයිතිවාසිකම් සහ නීත්‍යානුකූල දත්ත භාවිතය අතර තීරණාත්මක සමතුලිතතාවක් ඇති කිරීමයි.

ප්‍රධාන සංකල්ප සහ නිර්වචන

- **පුද්ගලික දත්ත**

පනත පුද්ගලික දත්ත අර්ථ දක්වන්නේ හඳුනාගත හැකි හෝ හඳුනාගත හැකි ස්වාභාවික පුද්ගලයෙකුට අදාළ ඕනෑම තොරතුරක් ලෙසයි. මෙයට නම්, හැඳුනුම්පත් අංක සහ ශාරීරික ලක්ෂණ වැනි සෘජු හඳුනාගැනීමේ ලක්ෂණ මෙන්ම පුද්ගලයෙකු හඳුනාගැනීමට භාවිතා කළ හැකි වක්‍ර හඳුනාගැනීමේ

ලක්ෂණද ඇතුළත් වේ, උදාහරණ ලෙස, සම්බන්ධතා තොරතුරු (ලිපිනය, ඊමේල්, දුරකථන අංක) ස්ථාන දත්ත, මාර්ගගත හඳුනාගැනීම, පිරික්සුම් හැසිරීම ආදිය දැක්විය හැකිය. මේ පිළිබඳ පනතේ 56 වගන්තිය මගින් නෛතික අර්ථ නිරූපණයක් ඉදිරිපත් කර තිබේ.

- **පෞද්ගලික දත්තවල විශේෂ ප්‍රභේද**

පනත මගින් සංවේදී පුද්ගලික දත්ත සඳහා වැඩිදියුණු කරන ලද ආරක්ෂාවන් ස්ථාපිත කර තිබේ. එම දත්ත පහත පරිදි සරලව හඳුනාගත හැකිය.

සෞඛ්‍ය දත්ත: පුද්ගලයෙකුගේ ශාරීරික හෝ මානසික සෞඛ්‍යයට අදාළ තොරතුරු

ජෛවමිතික දත්ත: ඇඟිලි සලකුණු, මුහුණු හඳුනාගැනීමේ දත්ත, අක්ෂි පිළිබඳ දත්ත

ජානමය දත්ත: පුද්ගලයෙකුගේ ජාන ලක්ෂණ පිළිබඳ තොරතුරු

මෙම විශේෂ දත්ත ප්‍රභේදයන් සඳහා අතිරේක ආරක්ෂාවන් අවශ්‍ය වන අතර, එවැනි දත්ත සැකසීමේ ආයතන අනවසරයෙන් ප්‍රවේශ වීම හෝ අයථා ලෙස භාවිත කිරීමෙන් ආරක්ෂා කිරීම සඳහා ඉහළ ආරක්ෂක පියවර ක්‍රියාත්මක කළ යුතුය.

<u>දත්ත සැකසීමේ සාමාන්‍ය මූලධර්ම</u>

පුද්ගලික දත්ත ආරක්ෂණ පනත විසින් පුද්ගලික දත්ත සැකසීමේදී අනුගමනය කළ යුතු මූලික මූලධර්ම හයක් ස්ථාපිත කරයි:

1. අරමුණු සීමා කිරීම- පුද්ගලික දත්ත එකතු කිරීම සිදුකළ යුත්තේ නිශ්චිත, පැහැදිලි සහ නීත්‍යානුකූල අරමුණු සඳහා වන අතර එම අරමුණු වලට අනුකූල නොවන ආකාරයට තවදුරටත් දත්ත සැකසීම නොකළ යුතුය.

2. දත්ත අවම කිරීම- නිශ්චිත අරමුණ සඳහා අවශ්‍ය දත්ත පමණක් එකතු කර සැකසිය යුතුය.

3. නිරවද්‍යතාව - පුද්ගලික දත්ත නිරවද්‍ය මෙන්ම යාවත්කාලීන විය යුතු අතර, වැරදි දත්ත නිවැරදි කිරීමට හෝ මැකීමට සාධාරණ පියවර ගත යුතුය.

4. ගබඩා කිරීමේ සීමාව- දත්ත රඳවා තබා ගත යුත්තේ ප්‍රකාශිත අරමුණ ඉටු කිරීමට අවශ්‍ය වන කාලය සඳහා පමණි.

5. අඛණ්ඩතාව සහ රහස්‍යභාවය- අනවසර ප්‍රවේශය, අහම්බෙන් අහිමි වීම හෝ හානි වීමෙන් පුද්ගලික දත්ත ආරක්ෂා කිරීම සඳහා සුදුසු ආරක්ෂක පියවර ක්‍රියාත්මක කළ යුතුය.

6. විනිවිදභාවය- දත්ත දායකයන් වෙත ඔවුන්ගේ දත්ත භාවිතා කරන ආකාරය පිළිබඳ පැහැදිලි තොරතුරු සැපයිය යුතු අතර දත්ත සැකසීම විනිවිදභාවයකින් යුතුව සිදු කළ යුතුය.

දත්ත දායකයන්ගේ අයිතිවාසිකම්

පනතට මගින් දත්ත දායකයන්ට (පුද්ගලයන්ට) ඔවුන්ගේ පුද්ගලික දත්ත සම්බන්ධයෙන් අයිතිවාසිකම් රැසක් ස්ථාපිත කර තිබේ.

1. ප්‍රවේශ වීමේ අයිතිය- දත්ත දායකයන්ට ඔවුන්ගේ පුද්ගලික දත්ත සැකසෙමින් පවතින්නේද යන්න තහවුරු කරන ලෙස ඉල්ලා සිටිය හැකි අතර එම දත්ත වෙත ප්‍රවේශ විය හැකිය. එමෙන්ම දත්ත සැකසීමේ අරමුණු, දත්ත කාණ්ඩ, ඒවා ලබන්නන්, රඳවා ගැනීමේ කාලසීමා සහ ඔවුන්ගේ අයිතිවාසිකම් ඉල්ලා සිටීමට හිමිකම පවතී.

2. කැමැත්ත ඉවත් කර ගැනීමේ අයිතිය- දත්ත සැකසීම දත්ත දායකයාගේ කැමැත්ත මත පදනම් වූ විට, දත්ත දායකයන්ට ඕනෑම වේලාවක ඔවුන්ගේ කැමැත්ත ඉවත් කර ගැනීමට අයිතිය ඇත. කෙසේවෙතත්, මෙය ඉවත් කිරීමට පෙර සිදුකරන ලද දත්ත සැකසීමේ ක්‍රියාවලියේ නීත්‍යානුකූලභාවයට බලපෑමක් නොකරයි.

3.විරුද්ධ වීමේ අයිතිය- දත්ත දායකයන්ට ඇතැම් අවස්ථාවලදී දත්ත සැකසීමට විරුද්ධ විය හැකිය. දත්ත සැකසීම නීත්‍යානුකූල අවශ්‍යතා, පොදු අවශ්‍යතා සඳහා වූ විට මෙන්ම මෙන්ම ඍජු අලෙවිකරණය මත පදනම් වූ විට ද මෙසේ විරුද්ධ විය හැකිය.

4. නිවැරදි කිරීමේ අයිතිය- දත්ත දායකයන්ට වැරදි පුද්ගලික දත්ත නිවැරදි කිරීමට හෝ අසම්පූර්ණ දත්ත සම්පූර්ණ කිරීමට ඉල්ලා සිටිය හැකිය.

5. මැකීමේ (ඉවත් කිරීමේ) අයිතිය- මෙය "අමතක කිරීමට ඇති අයිතිය" ලෙසද හැඳින්වෙන අතර දත්ත දායකයන්ට යම් විශේෂිත අවස්ථාවලදී තම දත්ත මකා දමන ලෙස ඉල්ලා සිටිය හැකිය. උදාහරණයක් ලෙස දත්ත මුල් අරමුණ සඳහා තවදුරටත් අවශ්‍ය නොවන විට හෝ කැමැත්ත ඉවත් කර ගත් විට, ඔවුන්ගේ පුද්ගලික දත්ත මකා දමන හෝ ඉවත් කරන ලෙස ඉල්ලීම් කිරීමට ඉඩ සලසා තිබේ.

දත්ත පාලකයින් සහ සකසන්නන්

පනත මගින් දත්ත පාලකයින් සහ සකසන්නන් අතර වෙනස්කම් දක්වයි. එමෙන්ම පනත මගින් ඔවුන් සඳහා වෙන් වෙන්ව වගකීම් ද ස්ථාපිත කර තිබේ.

- **දත්ත පාලක**

තනිවම හෝ අන් අය සමග ඒකාබද්ධව පුද්ගලික දත්ත සැකසීමේ අරමුණු සහ ක්‍රම නිශ්චය කරනු ලබන යම් ස්වභාවික හෝ නෛතික තැනැත්තකු, පොදු අධිකාරියක් හෝ වෙනත් ආයතනයක් මෙමගින් අදහස් කෙරේ. පනතේ 56 වගන්තියේ මේ පිළිබඳ පැහැදිළි අර්ථ නිරූපණයක් දක්වයි.

දත්ත පාලකයන්ගේ අනිවාර්ය වගකීම් අතර, නීත්‍යානුකූල, සාධාරණ සහ විනිවිදභාවයෙන් යුත් දත්ත සැකසීමක් සහතික කිරීම, සුදුසු ආරක්ෂක පියවර ක්‍රියාත්මක කිරීම, දත්ත දායකයන්ට ඔවුන්ගේ අයිතිවාසිකම් පිළිබඳව දැනුම් දීම මෙන්ම, දත්ත අවශ්‍යතාවයට අදාළ කාලයට වඩා වැඩි කාලයක් තබා නොගැනීම සහතික කිරීම ඇතුළත් වේ.

- **දත්ත සකසන්නා**

පාලකවරයා වෙනුවට පෞද්ගලික දත්ත සැකසීම සිදුකරන යම් ස්වභාවික හෝ නෛතික තැනැත්තකු, රාජ්‍ය ආයතනයක් හෝ නීතියක් මගින් හෝ නීතියක් යටතේ පිහිටුවනු ලබන ආයතනයක් දත්ත සකසන්නා යනුවෙන් අදහස් කෙරේ. පනතේ 56 වගන්තිය මගින් මෙය ද අර්ථ නිරූපණය කර තිබේ.

දත්ත සකසන්නන්ගේ අනිවාර්ය වගකීම් අතර, දත්ත පාලක විසින් උපදෙස් දී ඇති පරිදි පමණක් දත්ත සැකසීම සිදුකිරීම, සුදුසු තාක්ෂණික හා සංවිධානාත්මක ආරක්ෂණ පියවර ක්‍රියාත්මක කිරීම, දත්ත පාලකයට සඳහා පවතින බැඳීම් සහ වගකීම් සපුරාලීමට සහාය වීම ඇතුළත් වේ.

- **දත්ත ආරක්ෂණ නිලධාරියා**

සෑම දත්ත පාලකවරයෙකු හෝ දත්ත සකසන්නකු විසින්ම ඇතැම් විශේෂ අවස්ථාවලදී දත්ත ආරක්ෂණ නිලධාරියෙකු පත් කළ යුතු බව පනතේ 20 වන වගන්තියේ දැක්වේ. ඒ අනුව යම් දත්තවලට අදාළ හැසිරීම නිරතුරුව නිරීක්ෂණය කරන විට, පුද්ගලික දත්ත සමඟ කටයුතු කරන රජයේ ආයතනයක් වන විට, විශාල පරිමාණයකින් දත්තවල විශේෂ කාණ්ඩ සකසන විට ආදී අවස්ථා ගණනාවකදී දත්ත ආරක්ෂණ නිලධාරියෙකු පත් කළ යුතුය.

මෙම දත්ත ආරක්ෂණ නිලධාරීන්ගේ වගකීම් අතර , නීතියට අනුකූලව කටයුතු කිරීම පිළිබඳ උපදෙස් ලබා දීම, පනතට අනුකූලව කටයුතු කිරීම පිළිබඳ අධීක්ෂණය කිරීම, දත්ත ආරක්ෂණ අධිකාරිය සමඟ සහයෝගයෙන් කටයුතු කිරීම මෙන්ම දත්ත දායකයන් සමග වන සම්බන්ධතා පවත්වාගැනීමේ ක්‍රියාකාරී ස්ථානයක් ලෙස කටයුතු කිරීම ද වේ.

දේශසීමා හරහා පුද්ගලික දත්ත සංචලනය

පෞද්ගලික දත්තවල අඛණ්ඩ ආරක්ෂාව සහතික කිරීම සඳහා මෙම පනත මගින් ශ්‍රී ලංකාවෙන් පිටතට පුද්ගලික දත්ත සංචලනය කිරීම නියාමනය කිරීමට පියවර ගෙන තිබේ. ඒ අනුව එවැනි සංචනයන් සඳහා අවස්ථාව ඇත්තේ අවසර ලද අවස්ථාවන් සඳහා පමණි. එම අවස්ථා අතර, අදාළ දත්ත ලබා ගන්නා රට තුළ ඒ සඳහා ප්‍රමාණවත් ආරක්ෂණ මට්ටමක් ඇති බවට දත්ත ආරක්ෂණ අධිකාරිය විසින් තීරණය කරන ලද අවස්ථාවන්, දත්ත පාලකයා හෝ සැකසුම්කරු විසින් ඒ සඳහා සුදුසු ආරක්ෂක පියවර ක්‍රියාත්මක කර ඇති අවස්ථා , දත්ත දායකයා විසින් අදාළ දත්ත සංචලනය කිරීමට පැහැදිලිවම කැමැත්ත ලබා දී ඇති අවස්ථා වේ. එමෙන්ම, ඇතැම් විශේෂිත හේතු යටතේද මෙම දත්ත සංචලනය සිදුකල හැකිය. එවැනි විශේෂිත හේතු අතර, දත්ත දායකයා සමග වන ගිවිසුමක වගකීම් ඉටු කිරීම, පොදු හෝ මහජන යහපත සඳහා වන අවශ්‍යතා , අතිශය තීරණාත්මක අවශ්‍යතා, නෛතික, ආරක්ෂක වැනි තීරණාත්මක වගකීම් ඉටු කිරීම සඳහා වන අවස්ථා ආදිය වේ.

පනතට අනුකූල නොවීම තුළ හිමිවිය හැකි දඩුවම්

පුද්ගලික දත්ත ආරක්ෂණ පනත ප්‍රබල බලාත්මක කිරීමේ රාමුවක් මෙන්ම සැලකිය යුතු දඬුවම් ස්ථාපිත කිරීම ද සිදුකර තිබේ.

ඒ අනුව දත්ත ආරක්ෂණ අධිකාරියේ, නියෝගවලට එරෙහිව පළමු අනුකූල නොවීමේ අවස්ථාව සම්බන්ධයෙන් රුපියල් මිලියන 10 දක්වාත්, දෙවන සහ ඉන් අනතුරුව සිදු කරන නියෝගවලට අනුකූල නොවන අවස්ථා සඳහා රුපියල් මිලියන 20 දක්වාත් දඩ මුදල් නියම කළ හැකිය. එමෙන්ම, අධිකාරියේ නියෝගවලට අඛණ්ඩ අනුකූල නොවීම වෙනුවෙන් දිනකට රුපියල් 500,000 ක් දක්වා අතිරේක දඩ මුදල් නියම කිරීමට ද අධිකාරියට බලතල පවතී.

දඬුවම් තීරණය කිරීමේදී, දත්ත ආරක්ෂණ අධිකාරිය විසින් මූලික සාධක රැසක්ම සළකා බලනු ලැබේ. පනතේ විධිවිධාන උල්ලංඝනය කිරීමේ ස්වභාවය, බරපතලකම සහ කාලසීමාව, බලපෑමට ලක් වූ දත්ත දායකයන් සංඛ්‍යාව සහ හානියේ මට්ටම, උල්ලංඝනය කිරීම හිතාමතා සිදුකර ඇද්ද යන්න හෝ නොසැලකිලිමත්නම් එහි ස්වභාවය, හානිය අවම කිරීම සඳහා ගන්නා ලද ක්‍රියාමාර්ග, පෙර උල්ලංඝනය කිරීම්, අධිකාරිය සමඟ සහයෝගයෙන් කටයුතු කිරීමේ ස්වභාවය, බලපෑමට ලක් වූ පුද්ගලික දත්ත කාණ්ඩ ආදිය ඒ අතර වේ.

බැහැර කිරීම් සහ සීමාවන්

පුද්ගලික දත්ත ආරක්ෂණ පනත අදාළ වීම , ජාතික ආරක්ෂාව, අපරාධ වැළැක්වීම, අනාවරණය කර ගැනීම සහ නඩු පැවරීම, අධිකරණ ස්වාධීනත්වය සහ අධිකරණ ක්‍රියාපටිපාටිය, සිවිල් නීති හිමිකම් බලාත්මක කිරීම ආදිය හේතුවෙන් සීමා කළ හැකිය. එමෙන්ම එය අදාළ වීම අදහස් ප්‍රකාශ කිරීමේ අයිතියට අදාළ ක්‍රියාවන් සඳහාත්, අධ්‍යයන, කලාත්මක හෝ සාහිත්‍යමය අරමුණු සඳහාත් දත්ත සැකසීමේ දීත් කොන්දේසි සහිත සීමාවන්ට යටත් වේ.

සංක්ෂිප්තය

ශ්‍රී ලංකාවේ පුද්ගලික දත්ත ආරක්ෂණ පනත පුද්ගලයන්ගේ පෞද්ගලිකත්ව අයිතිවාසිකම ආරක්ෂා කිරීම මෙන්ම වගකිව යුතු දත්ත භාවිතය ඉදිරියට පවත්වාගෙනයාම සඳහා වන තීරණාත්මක කඩඉමක් ලෙස හැඳින්විය හැකිය.

පුද්ගලයින් සඳහා පැහැදිලි අයිතිවාසිකම් මෙන්ම ආයතන සඳහා බැඳීම් ස්ථාපිත කිරීමෙන් ද , ඩිජිටල් ආර්ථිකය තුළ විශ්වාසය ප්‍රවර්ධනය කරන රාමුවක් නිර්මාණය කිරීමෙන් ද පනත සුවිශේෂී මෙහෙවරක් ඉටුකර තිබේ. පනත හඳුන්වාදීම මගින් ශ්‍රී ලංකාව සවිස්තරාත්මක දත්ත ආරක්ෂණ නීති සහිත ගෝලීය ප්‍රජාවට එක්වන විට, මෙම පනතේ ප්‍රතිපාදන මෙන්ම එය සම්මත කර ගැනීමේ අවශ්‍යතා තේරුම් ගැනීම මෙන්ම පනතේ ප්‍රතිපාදනවලට අනුකූලව ක්‍රියාත්මක වීමද අත්‍යශ්‍ය වේ.

ඒ අනුව ශ්‍රී ලංකාවේ ක්‍රියාත්මක වන ආයතන පනතට අනුකූලව කටයුතු කිරීම සහතික කිරීම සඳහා වන සාධනීය පියවර ගැනීම අත්‍යවශ්‍ය වේ. ඒ යටතට දත්ත සැකසීමේ ක්‍රියාකාරකම් සමාලෝචනය කිරීම, සුදුසු ආරක්ෂණ පියවර ක්‍රියාත්මක කිරීම, දත්ත දායකයන්ගේ ඉල්ලීම්වලට ප්‍රතිචාර දැක්වීම සඳහා යාන්ත්‍රණයන් ස්ථාපිත කිරීම මෙන්හම සමාජය පුරා පෞද්ගලිකත්ව අයිතිවාසිකමට ගරු කිරීමේ සහ වගකිව යුතු දත්ත භාරකාරත්වයේ සංස්කෘතියක් වර්ධනය කිරීම ආදිය ඇතුළත් වේ.

මෙම පනත භාෂණයේ සහ ප්‍රකාශනයේ නිදහස සීමා කිරීමට අදාළ නොවන බව ප්‍රකාශ කළ ද මෙහිදී ජනමාධ්‍ය ක්‍රියාකාරකම් පැහැදිළි සහ නිශ්චිත ලෙස බැහැර කර නොමැත. එබැවින් ජනමාධ්‍ය වෘත්තිකයන් මෙන්ම නව සහ සමාජ මාධ්‍යකරුවන් ද මෙම පනත පිළිබඳ පුලුල් අවබෝධයක් ලබා ගැනීම අත්‍යවශ්‍ය වේ.