

ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ನಡವಳಿಗಳು

ವಿಷಯ: ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ದತ್ತಾಂಶವನ್ನು ಒದಗಿಸಲು ಮಾರ್ಗಸೂಚಿಗಳ ಕುರಿತು.

ಓದಲಾಗಿದೆ:

ಮುಖ್ಯಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ, ಇ-ಆಡಳಿತ ಕೇಂದ್ರ ಇವರ ಕಡತ ಸಂಖ್ಯೆ: CeG-PDFR/27/2021 (605991)

ಪ್ರಸ್ತಾವನೆ:

ಸರ್ಕಾರದ ವಿವಿಧ ಇಲಾಖೆಗಳು ಹಾಗೂ ಸಂಸ್ಥೆಗಳಲ್ಲಿ ನಾಗರಿಕರ ದತ್ತಾಂಶವು ಲಭ್ಯವಿರುತ್ತದೆ. ಸದರಿ ದತ್ತಾಂಶವನ್ನು ಇತರರೊಂದಿಗೆ (ಸರ್ಕಾರಿ ಇಲಾಖೆಗಳು ಮತ್ತು ಸಂಸ್ಥೆಗಳು ಹೊರತುಪಡಿಸಿ) ಹಂಚಿಕೊಳ್ಳುವ ಮುನ್ನ ಸಂಬಂಧಪಟ್ಟ ನಾಗರಿಕರ ಒಪ್ಪಿಗೆ ಅವಶ್ಯಕತೆ ಇರುತ್ತದೆ. ನಾಗರಿಕರ ಮಾಹಿತಿಯನ್ನು ಅವರ ಒಪ್ಪಿಗೆಯ ಮೇರೆಗೆ ಇತರರೊಂದಿಗೆ (ಸರ್ಕಾರೇತರ ಸಂಸ್ಥೆಗಳು, ಖಾಸಗಿ ಸಂಸ್ಥೆಗಳು ಇತ್ಯಾದಿ) ಹಂಚಿಕೊಂಡಲ್ಲಿ ಸಾರ್ವಜನಿಕರು ವಿವಿಧ ಸೌಲಭ್ಯ ಹಾಗೂ ಸೇವೆಗಳನ್ನು ಪಡೆಯಲು ಅನುಕೂಲವಾಗುತ್ತದೆ. ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ (ಇ-ಆಡಳಿತ) ಇಲಾಖೆಯ ವತಿಯಿಂದ ರಾಷ್ಟ್ರೀಯ ಸೂಚನಾ ವಿಜ್ಞಾನ ಕೇಂದ್ರ [National Informatics Centre (NIC)] ಮೂಲಕ ಇ-ಸಹಮತಿ ಎಂಬ ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆಯನ್ನು ಅಭಿವೃದ್ಧಿ ಪಡಿಸಲಾಗಿದ್ದು, ಇದು ನಾಗರಿಕರ ದತ್ತಾಂಶ (ಮಾಹಿತಿ)ವನ್ನು ಅವರ ಒಪ್ಪಿಗೆ ಮೇರೆಗೆ ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ವ್ಯವಸ್ಥೆಯಾಗಿರುತ್ತದೆ. ಇ-ಸಹಮತಿ ಮೂಲಕ ನಾಗರಿಕರ ದತ್ತಾಂಶವನ್ನು ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳಲು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಹೊರಡಿಸುವ ಅವಶ್ಯಕತೆಯಿರುತ್ತದೆ. ಈ ಉದ್ದೇಶಕ್ಕಾಗಿ ಕರಡು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಸಿದ್ಧಪಡಿಸಲಾಗಿರುತ್ತದೆ.

ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ, ಕರ್ನಾಟಕ ಸರ್ಕಾರ ಇವರ ಅಧ್ಯಕ್ಷತೆಯಲ್ಲಿ ದಿನಾಂಕ: 17-11-2021ರಂದು ದತ್ತಾಂಶ ಆಡಳಿತ ಚಾಲನಾ ಸಮಿತಿ (Data Governance Steering Committee) ಯ ಸಭೆಯಲ್ಲಿ ಈ ಕೆಳಕಂಡಂತೆ ನಿರ್ಣಯ ತೆಗೆದುಕೊಳ್ಳಲಾಗಿದೆ.

"The committee accorded the approval to the Guidelines and the e-Governance Department was advised to go ahead for its issue after getting opinion from any good legal firm expertising in personal data protection and consent mechanism for sharing of data followed by the opinion of Law Department".

ಮೇಲಿನ ನಿರ್ಣಯದನ್ವಯ ಮೆ: Trilegal ಎಂಬ ಕಾನೂನು ತಜ್ಞ ಸಂಸ್ಥೆಯು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಕೂಲಂಕುಷವಾಗಿ ಪರಿಶೀಲಿಸಿ, ಕರಡು ಮಾರ್ಗಸೂಚಿಗಳಲ್ಲಿ ಕೆಲವು ಮಾರ್ಪಾಡುಗಳನ್ನು ಮಾಡಲು ಸಲಹೆ ನೀಡಿರುತ್ತದೆ. ಸಂಸ್ಥೆಯ ಸಲಹೆಯಂತೆ ಮಾರ್ಗಸೂಚಿಗಳಲ್ಲಿ ಅಗತ್ಯ ಮಾರ್ಪಾಡು ಮಾಡಿದ ತರುವಾಯ ಕಾನೂನು ಇಲಾಖೆಯ ಅಭಿಪ್ರಾಯ ಪಡೆಯಲಾಗಿರುತ್ತದೆ. ಆದ್ದರಿಂದ, ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ನಾಗರಿಕರ ದತ್ತಾಂಶವನ್ನು ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಕುರಿತು ಕರಡು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಸಲ್ಲಿಸುತ್ತಾ, ಸೂಕ್ತ ಆದೇಶ ಹೊರಡಿಸಲು ಮುಖ್ಯಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ, ಇ-ಆಡಳಿತ ಕೇಂದ್ರ ಇವರು ಮೇಲೆ ಓದಲಾದ ಕಡತದಲ್ಲಿ ಕೋರಿರುತ್ತಾರೆ.

ಮುಖ್ಯಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ, ಇ-ಆಡಳಿತ ಕೇಂದ್ರ ಇವರ ಪ್ರಸ್ತಾವನೆಯನ್ನು ಪರಿಶೀಲಿಸಲಾಗಿದ್ದು, ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ನಾಗರಿಕರ

ದತ್ತಾಂಶವನ್ನು ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಕುರಿತು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಹೊರಡಿಸಲು ಸರ್ಕಾರವು ನಿರ್ಧರಿಸಿರುವ ಕಾರಣ ಈ ಆದೇಶ.

ಸರ್ಕಾರಿ ಆದೇಶ ಸಂಖ್ಯೆ: ಸಿಆಸುಇ 113 ಪಿಆರ್‌ಜೆ 2021
ಬೆಂಗಳೂರು, ದಿನಾಂಕ: 14ನೇ ಡಿಸೆಂಬರ್ 2021

ಮೇಲಿನ ಪ್ರಸ್ತಾವನೆಯಲ್ಲಿ ವಿವರಿಸಲಾದ ಅಂಶಗಳ ಹಿನ್ನೆಲೆಯಲ್ಲಿ, ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ನಾಗರಿಕರ ದತ್ತಾಂಶವನ್ನು ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಕುರಿತು, ಈ ಆದೇಶಕ್ಕೆ ಲಗತ್ತಾದ ಮಾರ್ಗಸೂಚಿಗಳಿಗೆ ಅನುಮೋದಿಸಿ ಸರ್ಕಾರವು ಆದೇಶಿಸಿದೆ.

ನಾಗರಿಕರ, ಸರ್ಕಾರೇತರ ಸಂಸ್ಥೆಗಳ ಹಾಗೂ ಇತರ ಭಾಗೀದಾರರ ಪ್ರತಿಕ್ರಿಯೆಯನ್ನು ಆಧರಿಸಿ ಕಾಲಕಾಲಕ್ಕೆ ಸರ್ಕಾರವು ಈ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಪರಿಷ್ಕರಿಸುತ್ತದೆ. ಈ ಕುರಿತು ಸಲಹೆ ಪಡೆಯಲು ಇ-ಆಡಳಿತ ಕೇಂದ್ರವು ಕೂಡಲೇ ಇ-ಸಹಮತಿ ತಂತ್ರಾಂಶದಲ್ಲಿ ಅವಕಾಶ ಕಲ್ಪಿಸತಕ್ಕದ್ದು.

ಈ ಆದೇಶವನ್ನು ಕಾನೂನು ಇಲಾಖೆಯ ಟಿಪ್ಪಣಿ ಸಂಖ್ಯೆ: LAW-OPN/230/2021, dated: 04-12-2021ರ ಸಹಮತಿ ಮೇರೆಗೆ ಹೊರಡಿಸಲಾಗಿದೆ.

ಕರ್ನಾಟಕ ರಾಜ್ಯಪಾಲರ ಆದೇಶಾನುಸಾರ
ಮತ್ತು ಅವರ ಹೆಸರಿನಲ್ಲಿ


(ಎಂ.ಎನ್ ಶ್ರೀವತ್ಸ)

ಸರ್ಕಾರದ ಅಧೀನ ಕಾರ್ಯದರ್ಶಿ
ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ
ಇಲಾಖೆ (ಇ-ಆಡಳಿತ)

ಇವರಿಗೆ:

ಸಂಕಲನಕಾರರು, ಕರ್ನಾಟಕ ರಾಜ್ಯ ಪತ್ರ, ಬೆಂಗಳೂರು-ಮುಂದಿನ ವಿಶೇಷ ರಾಜ್ಯ ಪತ್ರದಲ್ಲಿ ಪ್ರಕಟಿಸಿ ಅದರ 50 ಪ್ರತಿಗಳನ್ನು ಈ ಇಲಾಖೆಗೆ ಒದಗಿಸುವಂತೆ ಕೋರಲಾಗಿದೆ.

ಪ್ರತಿ:

1. ಪ್ರಧಾನ ಮಹಾಲೇಖಪಾಲರು (ಎ & ಇ), (ಜಿ & ಎಸ್‌ಎಸ್‌ಎ), ಬೆಂಗಳೂರು.
2. ಸರ್ಕಾರದ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ, ಕರ್ನಾಟಕ ಸರ್ಕಾರ, ವಿಧಾನಸೌಧ, ಬೆಂಗಳೂರು
3. ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ, ಕರ್ನಾಟಕ ಸರ್ಕಾರ, ವಿಧಾನಸೌಧ, ಬೆಂಗಳೂರು
4. ಎಲ್ಲಾ ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ / ಪ್ರಧಾನ ಕಾರ್ಯದರ್ಶಿ / ಕಾರ್ಯದರ್ಶಿ, ವಿಧಾನಸೌಧ / ವಿಕಾಸಸೌಧ / ಬಹುಮಹಡಿಗಳ ಕಟ್ಟಡ, ಬೆಂಗಳೂರು.
5. ಮುಖ್ಯ ಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ, ಇ-ಆಡಳಿತ ಕೇಂದ್ರ, ಬಹುಮಹಡಿಗಳ ಕಟ್ಟಡ, ಬೆಂಗಳೂರು
6. ಎಲ್ಲಾ ಇಲಾಖಾ ಮುಖ್ಯಸ್ಥರುಗಳು - ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ / ಪ್ರಧಾನ ಕಾರ್ಯದರ್ಶಿ / ಕಾರ್ಯದರ್ಶಿ ಇವರ ಮುಖಾಂತರ

7. ಎಲ್ಲಾ ನಿಗಮ / ಮಂಡಳಿ - ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ / ಪ್ರಧಾನ ಕಾರ್ಯದರ್ಶಿ / ಕಾರ್ಯದರ್ಶಿ ಇವರ ಮುಖಾಂತರ
8. ನಿರ್ದೇಶಕರು ಇ-ಆಡಳಿತ ಮತ್ತು ಪದನಿಮಿತ್ತ ನಿರ್ದೇಶಕರು, ವಿದ್ಯುನ್ಮಾನ ನಾಗರಿಕ ಸೇವಾ ವಿತರಣಾ ನಿರ್ದೇಶನಾಲಯ, ಬೆಂಗಳೂರು
9. ಕಾರ್ಯಕಾರಿ ನಿರ್ದೇಶಕರು, Centre for Smart Governance, ಬೆಂಗಳೂರು
10. ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿಯವರ ಆಪ್ತ ಕಾರ್ಯದರ್ಶಿ, ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ ಇಲಾಖೆ(ಇ-ಆಡಳಿತ), ಬಹುಮಹಡಿಗಳ ಕಟ್ಟಡ, ಬೆಂಗಳೂರು.
11. ಸರ್ಕಾರದ ಅಪರ ಕಾರ್ಯದರ್ಶಿಯವರ ಆಪ್ತ ಸಹಾಯಕರು, ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ ಇಲಾಖೆ(ಇ-ಆಡಳಿತ), ಬಹುಮಹಡಿಗಳ ಕಟ್ಟಡ, ಬೆಂಗಳೂರು.
12. ಇಲಾಖಾ ವೆಬ್ ಸೈಟ್‌ನಲ್ಲಿ ಪ್ರಕಟಿಸಲು.
13. ಶಾಖಾ ರಕ್ಷ ಕಡತ.

**ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ದತ್ತಾಂಶ ಹಂಚಿಕೊಳ್ಳುವ
ಮಾರ್ಗಸೂಚಿಗಳು**

1. ವ್ಯಾಪ್ತಿ:

ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ದತ್ತಾಂಶ ಹಂಚಿಕೊಳ್ಳುವ ಈ ಮಾರ್ಗಸೂಚಿಗಳ ವ್ಯಾಪ್ತಿಯು ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ) ಮೂಲಕ ಮಾಹಿತಿ ಒಡೆಯರ (Data Principals) ದತ್ತಾಂಶ (ಮಾಹಿತಿ) ವನ್ನು ಅವರ ಒಪ್ಪಿಗೆಯೊಂದಿಗೆ ಸಂಬಂಧಪಟ್ಟ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯಿಂದ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಗಳೊಂದಿಗೆ [Third Party Service Provider (TPSP)] ಹಂಚಿಕೊಳ್ಳುವ ವಿವಿಧ ಅಂಶಗಳನ್ನು ಆವರಿಸುತ್ತವೆ.

2. ಪದಗಳ ವ್ಯಾಖ್ಯಾನ:

ಈ ಮಾರ್ಗಸೂಚಿಗಳಲ್ಲಿ, ಸಂದರ್ಭಾನುಸಾರ ಅನ್ಯತಾ ಶಬ್ದಾರ್ಥ ಇದ್ದು ಹೊರತು, ಪದಗಳಿಗೆ ಈ ಕೆಳಗಿನಂತೆ ಅರ್ಥವನ್ನು ಪರಿಗಣಿಸತಕ್ಕದ್ದು.

2.1 **ದತ್ತಾಂಶ** ಎಂದರೆ, ಇ-ಸಹಮತಿ ಮೂಲಕ ಯಾವುದೇ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯಿಂದ ಯಾವುದೇ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಗಳಿಗೆ ಒದಗಿಸುವ ಮಾಹಿತಿ ಒಡೆಯನ (Data Principals) ದತ್ತಾಂಶ/ ಮಾಹಿತಿ.

2.2 **ಮಾಹಿತಿ ಒಡೆಯ ಅಥವಾ ದತ್ತಾಂಶ ಒಡೆಯ (Data Principal)** ಎಂದರೆ ಯಾವುದೇ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ನಿರ್ವಹಿಸುತ್ತಿರುವ ದತ್ತಾಂಶಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಯಾವುದೇ ಸ್ವಾಭಾವಿಕ ವ್ಯಕ್ತಿ.

2.3 **ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary)** ಎಂದರೆ ಮಾಹಿತಿ ಒಡೆಯರ (ನಾಗರಿಕರ) ದತ್ತಾಂಶವನ್ನು ಸಂಗ್ರಹಿಸಿ ಅಭಿರಕ್ಷಿಸುವ ಇಲಾಖೆಗಳು, ನಿಗಮ, ಮಂಡಳಿಗಳು ಸೇರಿದಂತೆ ಯಾವುದೇ ಸರ್ಕಾರಿ ಸಂಸ್ಥೆ.

2.4 **ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ** ಎಂದರೆ ಒಂದು ಅಥವಾ ಹೆಚ್ಚಿನ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಗಳ ಮೂಲಕ ಸಂಗ್ರಹಿಸಿ ನಿರ್ವಹಿಸಲ್ಪಟ್ಟ ದತ್ತಾಂಶವನ್ನು ವಿನಿಮಯಗಳಿಸಲು ಮಾಹಿತಿ ಒಡೆಯರ ಒಪ್ಪಿಗೆ ಪಡೆಯುವ ಹಾಗೂ ಒಪ್ಪಿಗೆ ಸಾಧನಗಳನ್ನು ನಿರ್ವಹಿಸುವಂತಹ ವಿದ್ಯುನ್ಮಾನ ವೇದಿಕೆ.

2.5 **ಇ-ಸಹಮತಿ** ಎಂದರೆ ಈ ಮಾರ್ಗಸೂಚಿಗಳಡಿ ನೊಂದಾಯಿತ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಗಳಿಗೆ ನೊಂದಾಯಿತ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯಿಂದ ದತ್ತಾಂಶ (ಮಾಹಿತಿ) ವಿನಿಮಯಗೊಳಿಸಲು ಪಡೆದ ದತ್ತಾಂಶ ಒಡೆಯರ ಒಪ್ಪಿಗೆ ಸಾಧನಗಳನ್ನು ನಿರ್ವಹಿಸುವಂತಹ ರಾಷ್ಟ್ರೀಯ ಸೂಚನಾ ವಿಜ್ಞಾನ ಕೇಂದ್ರ [National Informatics Centre (NIC)], ಕರ್ನಾಟಕ ರಾಜ್ಯ ಘಟಕದ ಮೂಲಕ ವಿನ್ಯಾಸಗೊಳಿಸಿ ಅಭಿವೃದ್ಧಿಪಡಿಸಿದ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರದ ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ.

2.6 **ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಗಳು [Third Party Service Provider (TPSP)]** ಎಂದರೆ ದತ್ತಾಂಶ ಒಡೆಯರ ಒಪ್ಪಿಗೆ ಅಥವಾ ಕೋರಿಕೆಯಾಧಾರದ ಒಪ್ಪಿಗೆ ಮೇರೆಗೆ ಮಾಹಿತಿ ಒಡೆಯನ ದತ್ತಾಂಶವನ್ನು (ಮಾಹಿತಿ) ಒದಗಿಸಲಾಗುವ ಖಾಸಗಿ/ ಸಾರ್ವಜನಿಕ ಕಂಪನಿ ಅಥವಾ ಸಂಸ್ಥೆ ಅಥವಾ ಸರ್ಕಾರೇತರ ಸಂಸ್ಥೆ ಅಥವಾ ಸಾರ್ವಜನಿಕ ವಲಯದ ಉದ್ಯಮ.

3. ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಗಳ [Third Party Service Provider (TPSP)] ಅರ್ಹತೆಗಳು ಮತ್ತು ಜವಾಬ್ದಾರಿಗಳು:

3.1 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು

- 3.1.1 ಸಂಬಂಧಿತ ಭಾರತೀಯ ಕಾನೂನು (ಗಳ) ಅಡಿಯಲ್ಲಿ, ನೋಂದಾಯಿಸಿ ಸಲಾದ ಖಾಸಗಿ/ಸಾರ್ವಜನಿಕ ಕಂಪನಿ, ಸಂಸ್ಥೆ, ಸರ್ಕಾರೇತರ ಸಂಸ್ಥೆ (N G O) ಅಥವಾ ಸಾರ್ವಜನಿಕ ವಲಯದ ಉದ್ಯಮವಾಗಿರಬೇಕು.
- 3.1.2 ತಾನು ಕೋರುವ ದತ್ತಾಂಶ (ಮಾಹಿತಿ) ಕುರಿತು ಆರು (6) ತಿಂಗಳಿಗೆ ಕಡಿಮೆಯಿಲ್ಲದಂತೆ ಪರ್ಯಾಪ್ತ ಕಾಲಾವಧಿಗೆ ಪ್ರಾಯೋಗಿಕವಾಗಿ ಬಳಸಿರುವ ಅನುಭವವನ್ನು ಪ್ರದರ್ಶಿಸ ತಕ್ಕದ್ದು.
- 3.1.3 ಈ ಮಾರ್ಗಸೂಚಿಯನ್ವಯ ದತ್ತಾಂಶದ ಬಳಕೆಯ ಸಂದರ್ಭದಲ್ಲಿ ತನ್ನ ಹೊಣೆಗಾರಿಕೆ ಪೂರೈಸುವ ಹಾಗೂ ಅವಶ್ಯಕವಾದ ನಿಧಿ ಅಥವಾ ಬಂಡವಾಳದ ಮೂಲವನ್ನು ಹೊಂದಿರುವ ಕುರಿತು ಪ್ರದರ್ಶಿಸಲು ತಿಳಿಸಿದಾಗ ಪ್ರದರ್ಶಿಸುವುದು.
- 3.1.4 ಭಾರತದ ಗಣರಾಜ್ಯದ ವ್ಯಾಪ್ತಿಯಲ್ಲಿ ಕಾರ್ಯ ನಿರ್ವಹಿಸುತ್ತಿರಬೇಕು.
- 3.1.5 ರಾಜ್ಯ ಮತ್ತು ದೇಶದ ಎಲ್ಲಾ ಸಂಬಂಧಿತ ಕಾನೂನುಗಳು, ನಿಯಮಗಳು ಹಾಗೂ ನಿಬಂಧನೆಗಳನ್ನು ಚಾಚು ತಪ್ಪದೆ ಅನುಸರಿಸತಕ್ಕದ್ದು.

4. ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಗಳ [Third Party Service Provider (TPSP)] ನೋಂದಣಿ, ದತ್ತಾಂಶಕ್ಕೆ ಪ್ರವೇಶಾವಕಾಶ ಹಾಗೂ ಬಳಕೆ ಮತ್ತು ಜವಾಬ್ದಾರಿಗಳು.

4.1 ಇ-ಸಹಮತಿಯೊಂದಿಗೆ ನೋಂದಣಿ

- 4.1.1 ಆಸಕ್ತ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ನಿಗದಿತ ನಮೂನೆಯಲ್ಲಿ ಭೌತಿಕವಾಗಿ ಸಹಿ ಮಾಡಿದ ಅಥವಾ ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಇ-ಸೈನ್ ಮಾಡಲಾದ ಅರ್ಜಿಯನ್ನು ಸಲ್ಲಿಸಬೇಕು.
- 4.1.2 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಈ ಮಾರ್ಗಸೂಚಿಗಳು, ಹಾಗೂ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ಕುರಿತಾದ ಎಲ್ಲಾ ಕಾನೂನು ಹಾಗೂ ನಿಯಮಗಳು ಮತ್ತು ಕಾಲಕಾಲಕ್ಕೆ ಹೊರಡಿಸುವ ಹೆಚ್ಚುವರಿ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ತಪ್ಪದೇ ಪಾಲಿಸುವುದಾಗಿ ಸ್ವಯಂ ಧೃಡೀಕೃತ ಘೋಷಣಾ ಪತ್ರವನ್ನು ಸಲ್ಲಿಸತಕ್ಕದ್ದು.
- 4.1.3 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಇ-ಸಹಮತಿ ಮೂಲಕ ಮಾಹಿತಿ ಒಡೆಯರ ದತ್ತಾಂಶವನ್ನು ಪಡೆದು ಸೇವೆಗಳನ್ನು ಒದಗಿಸಲು ಹಾಗೂ ದತ್ತಾಂಶವನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ತನ್ನೊಂದಿಗೆ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತಿರುವ ಯಾವುದೇ ಪಾಲುದಾರರು

ಅಥವಾ ಭಾಗೀದಾರರು ಇದ್ದಲ್ಲಿ ಅಂತಹವರ ಸಮಗ್ರವಾದ ಪಟ್ಟಿಯನ್ನು ಸಲ್ಲಿಸತಕ್ಕದ್ದು. ಸದರಿ ಪಟ್ಟಿಯಲ್ಲಿ ಯಾವುದೇ ಬದಲಾವಣೆಯಿದ್ದಲ್ಲಿ ಲಿಖಿತವಾಗಿ (ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಸೇರಿದಂತೆ) ಇ-ಸಹಮತಿಗೆ ಸಲ್ಲಿಸತಕ್ಕದ್ದು ಹಾಗೂ ದತ್ತಾಂಶ ಹಂಚಿಕೊಳ್ಳುವ ಮುನ್ನ ಇ-ಸಹಮತಿ ವತಿಯಿಂದ ಅನುಮೋದನೆ ಪಡೆಯತಕ್ಕದ್ದು.

4.1.4 ಪ್ರತಿ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಇ-ಸಹಮತಿ ಮೂಲಕ ದತ್ತಾಂಶ ಪಡೆಯುವ ಸಮಯದಲ್ಲಿ ತನ್ನ ಆಸಕ್ತಿಯ ಕ್ಷೇತ್ರ, ಅಗತ್ಯವಿರುವ ದತ್ತಾಂಶದ ಸಮುಚ್ಚಯ (Data Set) ಮತ್ತು ಬಳಕೆಯ ಉದ್ದೇಶವನ್ನು ತನ್ನ ಅರ್ಜಿಯಲ್ಲಿ ಸ್ಪಷ್ಟವಾಗಿ ನಮೂದಿಸತಕ್ಕದ್ದು. ಹೆಚ್ಚುವರಿ ದತ್ತಾಂಶ ಸಮುಚ್ಚಯ ಅಗತ್ಯವಿದ್ದಲ್ಲಿ ನಂತರ ಕೋರಬಹುದು.

4.1.5 ತನ್ನ ಸಾರ್ವಜನಿಕ ಕೀ (Public Key) ಯನ್ನು ಡಿಜಿಟಲ್ ಸಹಿ (Digital Signature) ಯ ಪರಿಶೀಲನೆಗಾಗಿ, ಮತ್ತು ದತ್ತಾಂಶವನ್ನು ಗೌಪ್ಯಗೊಳಿಸಲು (for data encryption) ಅಗತ್ಯವಿರುವ ಎನ್‌ಕ್ರಿಪ್ಷನ್ ಕೀ (encryption key) ಗಳನ್ನು ಒದಗಿಸತಕ್ಕದ್ದು.

4.1.6 ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ (ಇ-ಆಡಳಿತ) ಇಲಾಖೆ ಅಧೀನದ ಇ-ಆಡಳಿತ ಕೇಂದ್ರದ ಮುಖ್ಯ ಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ (CEO) ರವರ ಅಧ್ಯಕ್ಷತೆಯಲ್ಲಿ ಹಾಗೂ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಗೆ ಸಂಬಂಧಿಸಿದ ಇಲಾಖಾ ಪ್ರತಿನಿಧಿಯನ್ನು ಒಳಗೊಂಡಂತಹ ಈ ಉದ್ದೇಶಕ್ಕಾಗಿ ರಚಿತವಾದ ಸಮಿತಿಯ ಮೂಲಕ ನೋಂದಣಿಯನ್ನು ಅನುಮೋದಿಸತಕ್ಕದ್ದು.

4.1.7 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಕರ್ನಾಟಕ ಸರ್ಕಾರ ನಿಗದಿ ಪಡಿಸುವ ಹಾಗೂ ಕಾಲಕಾಲಕ್ಕೆ ಪರಿಷ್ಕರಿಸಬಹುದಾದ ನೋಂದಣಿ ಶುಲ್ಕವನ್ನು ಪಾವತಿಸತಕ್ಕದ್ದು. ನೋಂದಣಿ ಶುಲ್ಕವು ಮರು ಪಾವತಿಗೆ ಅರ್ಹವಿರುವುದಿಲ್ಲ.

4.1.7.1. ದತ್ತಾಂಶವನ್ನು ಬಳಸುವ ಉದ್ದೇಶ, ಉದಾಹರಣೆಗೆ ಕೇವಲ ಸಾಮಾಜಿಕ ಹಿತದೃಷ್ಟಿಯಲ್ಲಿ ಬಳಸುವ ಸಂದರ್ಭಗಳಲ್ಲಿ ಹಾಗೂ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯ ಸ್ವರೂಪದಾಧಾರದ ಮೇರೆಗೆ ಸರ್ಕಾರವು ತನ್ನ ವಿವೇಚನೆಯಲ್ಲಿ ನೋಂದಣಿ ಶುಲ್ಕವನ್ನು ಮನ್ನಾ ಮಾಡುವ ಅಧಿಕಾರವನ್ನು ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ.

4.1.8 ಸರ್ಕಾರವು ಲೇವಣಿ ಮೂಲಕ ಅಥವಾ ಬ್ಯಾಂಕ್ ಗ್ಯಾರಂಟಿ ಮೂಲಕ ಭದ್ರತಾ ಲೇವಣಿಯನ್ನು ವಿಧಿಸುವ ಅಧಿಕಾರವನ್ನು ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ. ಭದ್ರತಾ ಲೇವಣಿಯು ಬಡ್ಡಿ ರಹಿತವಾಗಿ ಮರುಪಾವತಿಗೆ ಅರ್ಹವಾಗಿರುತ್ತದೆ.

4.2 ದತ್ತಾಂಶವನ್ನು ಪಡೆಯಲು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯು;

4.2.1 ಪ್ರತಿ ಬಾರಿಯೂ ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಡಿಜಿಟಲ್ ಸಹಿಯುಳ್ಳ ಕೋರಿಕೆಯನ್ನು ಈ ಮುಂದಿನ ವಿವರಗಳೊಂದಿಗೆ ಇ-ಸಹಮತಿಗೆ ಸಲ್ಲಿಸತಕ್ಕದ್ದು.

4.2.1.1 ಅಗತ್ಯವಿರುವ ದತ್ತಾಂಶದ ಬಳಕೆಯ ಉದ್ದೇಶ.

4.2.1.2 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ನೋಂದಣಿಯ ಸಮಯದಲ್ಲಿ ಸಲ್ಲಿಸಿದ ದತ್ತಾಂಶ ರಾಶಿಯ (pool of data set) ಪೈಕಿ ಅವ್ಯಕ್ತವಿರುವ ದತ್ತಾಂಶದ ಸಮುಚ್ಚಯ (data set) ವನ್ನು ಸೂಚಿಸಬೇಕು (ಈ ಮಾರ್ಗಸೂಚಿಗಳ ಕಲಂ 4.1.4 ರನ್ವಯ ಅಗತ್ಯವಿರುವಂತೆ).

4.2.1.3 ದತ್ತಾಂಶವನ್ನು ಎ.ಪಿ.ಐ [Application Programming Interface (API)] ಮೂಲಕವೂ ಕೋರಬಹುದು. ಎ.ಪಿ.ಐ ಮೂಲಕ ದತ್ತಾಂಶ ಪಡೆಯುವ ಸಂದರ್ಭಗಳಲ್ಲೂ ಈ ಎಲ್ಲಾ ಮಾರ್ಗಸೂಚಿಗಳು, ಷರತ್ತು ಹಾಗೂ ನಿಬಂಧನೆಗಳು ಅನ್ವಯಿಸುತ್ತವೆ.

4.3 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯ ಜವಾಬ್ದಾರಿಗಳು:

4.3.1 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಈ ಮಾರ್ಗಸೂಚಿಗಳನ್ವಯ ಹಾಗೂ ಕಲಂ 4.1.4 ರಡಿ ಕೋರಿರುವ ಉದ್ದೇಶಗಳನ್ವಯ ನಿಗದಿತ ಉದ್ದೇಶಗಳಿಗೆ ಮಾತ್ರ ದತ್ತಾಂಶವನ್ನು ಪಡೆಯತಕ್ಕದ್ದು. ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಯು ಕೋರುವ ದತ್ತಾಂಶವು ಸಕ್ಷಮ ಪ್ರಾಧಿಕಾರದಿಂದ ಅಧಿಸೀಚಿಸಲ್ಪಟ್ಟ ಉದ್ದೇಶಗಳ ಪೈಕಿ ಮಾತ್ರವಾಗಿರತಕ್ಕದ್ದು.

4.3.2 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಬಳಸುತ್ತಿರುವ ಪ್ರಕ್ರಿಯೆಗಳ ಪರಿಶೀಲನೆ, ಈ ಮಾರ್ಗಸೂಚಿಗಳ ಅನುಸರಣೆಯ ದೃಢೀಕರಣ ಹಾಗೂ ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ ಮೂಲಕ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯಿಂದ ಪಡೆದ ದತ್ತಾಂಶವನ್ನು ಬಳಸುತ್ತಿರುವ ಉದ್ದೇಶ ಹಾಗೂ ತಂತ್ರಾಂಶದಲ್ಲಿ ಅಳವಡಿಸಿರುವ ಸುರಕ್ಷತೆ ಹಾಗೂ ಭದ್ರತಾ ವ್ಯವಸ್ಥೆಗಳ ಕುರಿತು ಪರಿಶೀಲಿಸಲು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯ ತಂತ್ರಾಂಶ ಮತ್ತು / ಅಥವಾ ದಾಖಲಾತಿಗಳನ್ನು ಪರಿಶೋಧಿಸುವ ಅಧಿಕಾರವನ್ನು ರಾಜ್ಯ ಸರ್ಕಾರ, ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ (ಇ-ಸಹಮತಿ) ಹಾಗೂ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಗಳು ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತವೆ.

4.3.3 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ತನ್ನ ಪಾಲುದಾರರು ಹಾಗೂ ಭಾಗೀದಾರರೊಂದಿಗೆ ಕಾನೂನಾತ್ಮಕ ಒಪ್ಪಂದಗಳ ಮೂಲಕ ಹಾಗೂ ಸೂಕ್ತ ತಾಂತ್ರಿಕ ಪರಿಹಾರಗಳ ಮೂಲಕ ಈ ಮುಂದಿನ ಅಂಶಗಳನ್ನು ಖಾತರಿಪಡಿಸತಕ್ಕದ್ದು.

- 4.3.3.1 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯ ಅಧಿಕೃತ ವ್ಯಕ್ತಿ ಅಥವಾ ಅದರ ಪಾಲುದಾರರು ಮತ್ತು/ ಅಥವಾ ಭಾಗೀದಾರರು ಮಾತ್ರ ದತ್ತಾಂಶಕ್ಕೆ ಪ್ರವೇಶಾವಕಾಶ ಹೊಂದಿರತಕ್ಕದ್ದು.
- 4.3.3.2 ದತ್ತಾಂಶವನ್ನು ಮಾಹಿತಿ ಒಡೆಯರು ನೀಡಿ ದಾಖಲಿಸಿರುವ ಒಪ್ಪಿಗೆಯಂತೆ ನಿರ್ದಿಷ್ಟ ಉದ್ದೇಶಕ್ಕಾಗಿ ಮಾತ್ರ ಬಳಸತಕ್ಕದ್ದು.
- 4.3.3.3 ಕಲಂ 4.1.3 ರಡಿ ಇ-ಸಹಮತಿ ವತಿಯಿಂದ ಅನುಮೋದಿಸಲ್ಪಟ್ಟ ಸಂಸ್ಥೆಗಳ ಹೊರತುಪಡಿಸಿ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಯಾವುದೇ ಸಂದರ್ಭಗಳಲ್ಲಿ ಮಾಹಿತಿ ಒಡೆಯರ ದತ್ತಾಂಶವನ್ನು ಹಂಚಿಕೊಳ್ಳುವಂತಿಲ್ಲ, ಒದಗಿಸುವಂತಿಲ್ಲ, ಬಹಿರಂಗಪಡಿಸುವಂತಿಲ್ಲ, ವರ್ಗಾಯಿಸುವಂತಿಲ್ಲ, ಮಾರಾಟ ಅಥವಾ ಮರು-ಮಾರಾಟ ಮಾಡುವಂತಿಲ್ಲ.
- 4.3.3.4 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಪಡೆದ ದತ್ತಾಂಶವನ್ನು ಮಾಹಿತಿ ಒಡೆಯರ (Data principal) ಒಪ್ಪಿಗೆ ನೀಡಿರುವ ಕಾಲವಧಿಗೆ ಮಾತ್ರ ಸಂಗ್ರಹಿಸಿಡುವುದು ಮತ್ತು ಬಳಸುವುದು. ಒಪ್ಪಿಗೆ ಅವಧಿ ಮುಗಿದ ತಕ್ಷಣ ದತ್ತಾಂಶವನ್ನು ಅಳಿಸಿ ಹಾಕತಕ್ಕದ್ದು.
- 4.3.3.5 ಒಪ್ಪಿಗೆಯು ಹಿಂಪಡೆದಲ್ಲಿ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಸಂಬಂಧಪಟ್ಟ ದತ್ತಾಂಶವನ್ನು ಉಳಿಸಿಕೊಳ್ಳತಕ್ಕದ್ದಲ್ಲ ಹಾಗೂ ಬಳಸತಕ್ಕದ್ದಲ್ಲ ಮತ್ತು ಒಪ್ಪಿಗೆ ಹಿಂಪಡೆದ ತಕ್ಷಣ ದತ್ತಾಂಶವನ್ನು ಅಳಿಸಿಹಾಕತಕ್ಕದ್ದು.
- 4.3.3.6 ದಾಖಲೆಗಳ ಮತ್ತು ದತ್ತಾಂಶದ ಅನಧಿಕೃತ ಪ್ರವೇಶಾವಕಾಶ, ತಿದ್ದುಪಡಿ, ನಾಶಪಡಿಸುವಿಕೆ, ಬಹಿರಂಗ ಪಡಿಸುವಿಕೆ ಮತ್ತು ಹರಡುವಿಕೆಗಳನ್ನು ತಡೆಗಟ್ಟಲು ಸಮಗ್ರ ಸುರಕ್ಷತಾ/ ಭದ್ರತಾ ವ್ಯವಸ್ಥೆಗಳನ್ನು ತನ್ನ ತಂತ್ರಾಂಶಗಳಲ್ಲಿ ಅಳವಡಿಸತಕ್ಕದ್ದು. ಈ ಭದ್ರತಾ/ ಸುರಕ್ಷತಾ ವ್ಯವಸ್ಥೆಗಳು ಸಂಬಂಧಿತ ಕಾನೂನುಗಳಡಿ ನಿರ್ದಿಷ್ಟಪಡಿಸಿರುವ ಮಾನದಂಡಗಳಿಗಿಂತ ಯಾವುದೇ ರೀತಿಯಲ್ಲಿ ಕೆಳಮಟ್ಟದ್ದಾಗಿರತಕ್ಕದ್ದಲ್ಲ.
- 4.3.3.7 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗಳು ಮತ್ತು ಅವರ ಭಾಗೀದಾರರು ಮತ್ತು/ ಅಥವಾ ಪಾಲುದಾರರು ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ಸಂಬಂಧಿತ ಕಾನೂನುಗಳು ಮತ್ತು ನಿಯಮಗಳು ಮಾತ್ರವಲ್ಲದೆ ಎಲ್ಲಾ ಸಂಬಂಧಿತ ಕಾನೂನು, ನಿಯಮ ಮತ್ತು ನಿಬಂಧನೆಗಳನ್ನು ಅನುಪಾಲಿಸತಕ್ಕದ್ದು.

4.3.3.8 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗಳು ಮತ್ತು ಅವರ ಪಾಲುದಾರರು ಮತ್ತು/ ಅಥವಾ ಭಾಗೀದಾರರು ರಾಜ್ಯ ಹಾಗೂ ಕೇಂದ್ರ ಸರ್ಕಾರದಿಂದ ಕಾಲಕಾಲಕ್ಕೆ ನೀಡಲಾಗುವ ನಿರ್ದೇಶನಗಳನ್ನು ಅನುಪಾಲಿಸತಕ್ಕದ್ದು.

4.4 ರಾಜ್ಯ ಸರ್ಕಾರವು ತನ್ನ ವಿವೇಚನೆಯಲ್ಲಿ ಯಾವುದೇ ಕಾರಣ ನೀಡಿ ಅಥವಾ ನೀಡದ ಯಾವುದೇ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯ ನೋಂದಣಿಯನ್ನು ನಿರಾಕರಿಸುವ ಅಥವಾ ಯಾವುದೇ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯು ಕೋರುವ ದತ್ತಾಂಶವನ್ನು ನಿರಾಕರಿಸುವ ಅಧಿಕಾರ ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ.

4.5 ಇ-ಸಹಮತಿ ಮೂಲಕ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯೊಂದಿಗೆ ವಿನಿಮಯಗೊಳಿಸಿದ ದತ್ತಾಂಶದ ಎಲ್ಲಾ ಹಕ್ಕುಗಳು, ಹಕ್ಕೋಲೆ ಮತ್ತು ಹಿತಾಸಕ್ತಿ (ಕೃತಿ ಸ್ವಾಮ್ಯ ಸೇರಿದಂತೆ) ಗಳನ್ನು ಸಂಬಂಧಿತ ಕಾನೂನಿನಡಿ ಅನುಮತಿಸಲಾಗಿರುವ ಮಟ್ಟಿಗೆ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯು ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ.

5. ಇ-ಸಹಮತಿ ಯಲ್ಲಿ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯ ಸೇರ್ಪಡಿಸುವಿಕೆ.

5.1 ಯಾವುದೇ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯು ಇ-ಸಹಮತಿಯಡಿ ಸೇರ್ಪಡೆಗೊಳ್ಳಲು ಮತ್ತು ಯಾವುದೇ ಮಾಹಿತಿ ಒಡೆಯರ ದತ್ತಾಂಶವನ್ನು ಇ-ಸಹಮತಿ ಮೂಲಕ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗೆ ನೀಡಲು ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿಗಳು/ ಪ್ರಧಾನ ಕಾರ್ಯದರ್ಶಿಗಳು/ ಕಾರ್ಯದರ್ಶಿಗಳು, ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ (ಇ-ಆಡಳಿತ) ಇಲಾಖೆ ರವರ ಅಧ್ಯಕ್ಷತೆಯಲ್ಲಿ ಹಾಗೂ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಗೆ ಸಂಬಂಧಿಸಿದ ಇಲಾಖೆಯ ಪ್ರತಿನಿಧಿಯನ್ನು ಒಳಗೊಂಡ ಸಮಿತಿಯಿಂದ ಅನುಮೋದನೆ ಪಡೆಯಬೇಕು.

6. ಕುಂದುಕೊರತೆಗಳ ಪರಿಹಾರ.

6.1 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಬಳಕೆದಾರರ ಕುಂದು ಕೊರತೆ ಮತ್ತು ದೂರುಗಳ ನಿರ್ವಹಣೆ ಹಾಗೂ ವಿಲೇವಾರಿಗಾಗಿ ಒರ್ವ ಕುಂದು ಕೊರತೆ ಪರಿಹಾರ ಅಧಿಕಾರಿ/ ವ್ಯಕ್ತಿಯನ್ನು ನೇಮಿಸತಕ್ಕದ್ದು. ಜೊತೆಗೆ ಮಾಹಿತಿ ಒಡೆಯರ ಕುಂದು ಕೊರತೆ/ ದೂರುಗಳನ್ನು ಪರಿಹರಿಸಲು ಪ್ರತ್ಯೇಕವಾದ ಘಟಕವನ್ನು ಸ್ಥಾಪಿಸಬೇಕು.

6.2 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಯು ಪ್ರತಿಯೊಂದು ದೂರು/ ಕುಂದುಕೊರತೆಗೆ ಬರವಣಿಗೆಯಲ್ಲಿ ಅಥವಾ ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಸ್ವೀಕೃತಿಯನ್ನು ನೀಡತಕ್ಕದ್ದು.

6.3 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಮಾಹಿತಿ ಒಡೆಯನಿಗೆ (Data Principal) ತಾನು ದೂರು ನೀಡಿದ 72 ಗಂಟೆಯೊಳಗೆ ಸ್ವೀಕೃತಿ ನೀಡತಕ್ಕದ್ದು. ಸ್ವೀಕೃತಿ ನೀಡಿದ ತರುವಾಯ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಯು ದೂರು ಸ್ವೀಕರಿಸಿದ 30 ದಿನಗಳ ಒಳಗಾಗಿ ಅಂತಹ ಮಾಹಿತಿ ಒಡೆಯನ ದೂರು/ ಕುಂದುಕೊರತೆಗಳನ್ನು ಪರಿಹರಿಸತಕ್ಕದ್ದು.

6.4 ಅನುಷ್ಠಾನದ ಹಂತದಲ್ಲಿ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ಈ ಮುಂದಿನ ಮಾಹಿತಿಯನ್ನು ತಮ್ಮ ವೆಬ್ ಸೈಟ್ / ತಂತ್ರಾಂಶ ಹಾಗೂ ತಮ್ಮ ಕಛೇರಿ (ಗಳು)/ ವ್ಯವಹಾರಸ್ಥಳಗಳಲ್ಲಿ ಪ್ರಮುಖ ಜಾಗಗಳಲ್ಲಿ ಪ್ರದರ್ಶಿಸತಕ್ಕದ್ದು.

6.4.1 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯ ವಿರುದ್ಧ ಮಾಹಿತಿ ಒಡೆಯರು ತಮ್ಮ ದೂರನ್ನು ನೀಡಿ ಇತ್ಯರ್ಥ ಪಡಿಸಿಕೊಳ್ಳಲು ಸಂಪರ್ಕಿಸಬೇಕಾದ ಕುಂದುಕೊರತೆ ನಿವಾರಣಾ ಅಧಿಕಾರಿ/ ವ್ಯಕ್ತಿಯ ಹೆಸರು ಹಾಗೂ ಸಂಪರ್ಕದ ವಿವರಗಳು (ದೂರವಾಣಿ/ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಗಳು ಮತ್ತು ಇ-ಮೇಲ್ ವಿಳಾಸ).

7. ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯನ್ನು ವಜಾ/ ರದ್ದುಗೊಳಿಸುವುದು

7.1 ಸರ್ಕಾರವು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಗೆ ದತ್ತಾಂಶಕ್ಕೆ ಪ್ರವೇಶಾವಕಾಶ ರದ್ದು ಗೊಳಿಸುವುದರ ಜೊತೆಗೆ ಕಲಂ 7.1.2 ಮತ್ತು 7.1.3 ರ ಸಂದರ್ಭಗಳಲ್ಲಿ ಕಾನೂನು ರಿತ್ಯಾ ಕ್ರಮವಹಿಸುವುದರ ಜೊತೆಗೆ ಭದ್ರತಾ ಠೇವಣಿಯನ್ನು ಮುಟ್ಟು ಗೋಲು ಹಾಕಿಕೊಳ್ಳುವ ಹಾಗೂ ದಂಡ ವಿಧಿಸುವ ಹಕ್ಕನ್ನು ಈ ಮುಂದಿನ ಸನ್ನಿವೇಶಗಳಲ್ಲಿ ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ. ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯು

7.1.1 ಭಾರತದಲ್ಲಿ ವ್ಯವಹರಿಸುವುದನ್ನು ನಿಲ್ಲಿಸಿದಲ್ಲಿ; ಅಥವಾ

7.1.2 ಈ ಮಾರ್ಗಸೂಚಿಗಳಲ್ಲಿ ವಿಧಿಸಿದ ಯಾವುದೇ ಷರತ್ತು ಅಥವಾ ನಿಬಂಧನೆಗಳನ್ನು ಪರಿಪಾಲನೆ ಮಾಡದೇಯಿದ್ದಲ್ಲಿ, ಅಥವಾ ಉಲ್ಲಂಘಿಸಿದಲ್ಲಿ; ಅಥವಾ

7.1.3 ಯಾವುದೇ ಸಂಬಂಧಿತ ಕಾಯಿದೆ/ ಕಾನೂನು ಅಥವಾ ನಿಯಮಗಳು ಮತ್ತು/ ಅಥವಾ ಸರ್ಕಾರದ ನಿರ್ದೇಶನವನ್ನು ಅನುಸರಿಸಲು ವಿಫಲವಾದಲ್ಲಿ.

7.2 ಸರ್ಕಾರವು ಯಾವುದೇ ಕಾರಣವನ್ನು ನೀಡಿ ಅಥವಾ ನೀಡದೆ ತನ್ನ ವಿವೇಚನೆಯಲ್ಲಿ ಯಾವುದೇ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯನ್ನು ವಜಾಗೊಳಿಸುವ/ ನೊಂದಣಿಯನ್ನು ರದ್ದುಗೊಳಿಸುವ ಅಧಿಕಾರವನ್ನು ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ.

8. ಇ-ಸಹಮತಿ ಮತ್ತು ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary)ಗಳ ಪಾತ್ರ, ಜವಾಬ್ದಾರಿಗಳು ಮತ್ತು ಹೊಣೆಗಾರಿಕೆಯ ಮಿತಿಗಳು:

8.1 ಪಾತ್ರಗಳು:

8.1.1 ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary): ದತ್ತಾಂಶದ ಸಂಗ್ರಹಣೆ, ನಿರ್ವಹಣೆ ಮತ್ತು ಇ-ಸಹಮತಿ ಮೂಲಕ ದತ್ತಾಂಶ ವಿನಿಮಯಗೊಳಿಸುವುದು ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯ ಪಾತ್ರವಾಗಿರುತ್ತದೆ.

8.1.2 ಇ-ಸಹಮತಿ: ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆಯಾಗಿ ಇ-ಸಹಮತಿಯ ಪಾತ್ರವು ಮಾಹಿತಿ ಒಡೆಯರ ದತ್ತಾಂಶವನ್ನು ಅವರ ಒಪ್ಪಿಗೆಯ ಮೇರೆಗೆ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆಗಳ [Third Party Service Provider (TPSP)] ನಡುವೆ ದತ್ತಾಂಶ ವಿನಿಮಯಗೊಳಿಸಲು ಅನುವು ಮಾಡುವುದರ ಜೊತೆಗೆ ಒಪ್ಪಿಗೆ ಸಾಧನಗಳನ್ನು ನಿರ್ವಹಿಸುವುದಾಗಿರುತ್ತದೆ.

8.2 ಜವಾಬ್ದಾರಿಗಳು:

8.2.1 ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary); ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯ ಜವಾಬ್ದಾರಿಗಳು ಈ ಮುಂದಿನಂತಿರುತ್ತದೆ:

8.2.1.1 ದತ್ತಾಂಶ ಸಂಗ್ರಹಣೆ ಹಾಗೂ ಸುರಕ್ಷಿತ ನಿರ್ವಹಣೆ.

8.2.1.2 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯ ನಿರ್ದಿಷ್ಟ ಕೋರಿಕೆಯಾವ್ಯಾಪ್ತಿಯಡಿ ಬರುವ ಮಾಹಿತಿ ಒಡೆಯರ (Data Principal) ಪಟ್ಟಿಯನ್ನು ಇ-ಸಹಮತಿಯೊಂದಿಗೆ ಹಂಚಿ ಕೊಳ್ಳುವುದು.

8.2.1.3 ಒಪ್ಪಿಗೆ ನೀಡಿರುವ ಮಾಹಿತಿ ಒಡೆಯರ ಮಾಹಿತಿಯನ್ನು ಇ-ಸಹಮತಿ ಮೂಲಕ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗೆ ಗೌಪ್ಯರೂಪದಲ್ಲಿ (Encrypted form) ಒದಗಿಸತಕ್ಕದ್ದು, ಇದರಿಂದ ಒದಗಿಸಿದ ಮಾಹಿತಿಯು ಇ-ಸಹಮತಿಗೂ ಸಹ ಗೌಪ್ಯವಾಗಿರುತ್ತದೆ.

8.2.1.4 ಮಾಹಿತಿ ಒಡೆಯನು (Data Principal) ದತ್ತಾಂಶ ಒದಗಿಸಲು ನೀಡಿರುವ ಒಪ್ಪಿಗೆಗೆ ಸೀಮಿತವಾಗಿ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಗೆ ದತ್ತಾಂಶವನ್ನು ಒದಗಿಸುವುದನ್ನು ಖಚಿತ ಪಡಿಸಿಕೊಳ್ಳುವುದು. ಜೊತೆಗೆ ಒಪ್ಪಿಗೆ ಹಿಂಪಡೆದ ಸಂದರ್ಭಗಳಲ್ಲಿ ದತ್ತಾಂಶ ವಿನಿಮಯ ರದ್ದುಪಡಿಸುವುದನ್ನು ಖಚಿತ ಪಡಿಸುವುದು.

8.2.1.5 ಒಪ್ಪಿಗೆ ಸಾಧನಗಳ ಹಾಗೂ ದತ್ತಾಂಶಕ್ಕೆ ಪ್ರವೇಶಾವಕಾಶ ನೀಡಲಾಗಿರುವ ದತ್ತಾಂಶಗಳ ವಿವರಗಳನ್ನು ನಿರ್ವಹಿಸುವುದು.

8.2.2 ಇ-ಸಹಮತಿ (ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆ); ಇ-ಸಹಮತಿಯ ಜವಾಬ್ದಾರಿಗಳು ಈ ಮುಂದಿನಂತಿವೆ;

8.2.2.1 ಮಾಹಿತಿ ಒಡೆಯನಿಗೆ (Data Principal) ಒಪ್ಪಿಗೆ ನೀಡಲು ಮತ್ತು/ ಅಥವಾ ಕೋರಿಕೆ ಮೇರೆಗೆ ಒಪ್ಪಿಗೆ ನೀಡಲು ಹಾಗೂ ಒಪ್ಪಿಗೆ ಹಿಂಪಡೆಯಲು ಅನುವು ಮಾಡಿಕೊಡುವುದು ಹಾಗೂ ಅವುಗಳ ವಿವರಗಳನ್ನು ನಿರ್ವಹಿಸುವುದು.

8.2.2.2 ಮಾಹಿತಿ ಒಡೆಯನನ್ನು ತನ್ನ ದತ್ತಾಂಶಕ್ಕೆ ಪ್ರವೇಶಾವಕಾಶ ಪಡೆದಿರುವ ವಿವರಗಳನ್ನು ವೀಕ್ಷಿಸಲು ಅನುವು ಮಾಡಿಕೊಡುವುದು.

8.2.2.3 ಒಪ್ಪಿಗೆಯಾಧಾರದ ಮೇರೆಗೆ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯಿಂದ ಸ್ವೀಕೃತವಾದ ದತ್ತಾಂಶವನ್ನು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಗೆ ಗೌಪ್ಯ ರೂಪದಲ್ಲಿ ನೀಡುವುದು (ದತ್ತಾಂಶವು ಇ-ಸಹಮತಿಗೂ ಗೌಪ್ಯವಾಗಿರುತ್ತದೆ).

8.2.2.4 ದತ್ತಾಂಶವನ್ನು ಅಧಿಕೃತ ಹಾಗೂ ಉದ್ದೇಶಿತ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯೊಂದಿಗೆ ಮಾತ್ರ ಗೌಪ್ಯ ರೂಪದಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳುವುದು.

8.2.2.5 ಒಪ್ಪಿಗೆ ಹಿಂಪಡೆದ ಸಂದರ್ಭಗಳಲ್ಲಿ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಗೆ ತಿಳಿಸುವುದು ಹಾಗೂ ಪ್ರಸ್ತುತ ಹಿಂಪಡೆಯಲಾಗಿರುವ ಒಪ್ಪಿಗೆ ಮೇರೆಗೆ ದತ್ತಾಂಶ ವಿನಿಮಯಗೊಳಿಸಲಾಗುತ್ತಿರುವುದನ್ನು ಸ್ಥಗಿತಗೊಳಿಸುವುದು.

9. ಒಂದು ಸೇವೆಯಾಗಿ ಇ-ಸಹಮತಿ:

9.1 ಅನ್ವಯಿಸುವ ನಿಯಮಗಳು ಹಾಗೂ ನಿಬಂಧನೆಗಳನ್ವಯ ಒಪ್ಪಿಗೆ ನಿರ್ವಹಣಾ ವೇದಿಕೆಯಾಗಿ ದೇಶದ ಇತರ ರಾಜ್ಯ ಸರ್ಕಾರಗಳಿಗೆ ಹಾಗೂ ಕೇಂದ್ರ ಸರ್ಕಾರಕ್ಕೆ ಇ-ಸಹಮತಿಯನ್ನು ಒಂದು ಸೇವೆಯಾಗಿ ಒದಗಿಸಬಹುದು.

9.2 ಇ-ಸಹಮತಿಯ ಸೇವೆಗಳನ್ನು ಇತರ ರಾಜ್ಯ ಸರ್ಕಾರಗಳು ಮತ್ತು / ಅಥವಾ ಕೇಂದ್ರ ಸರ್ಕಾರಕ್ಕೆ ಒದಗಿಸಿದಲ್ಲಿ ಸಂದರ್ಭಕ್ಕನುಗುಣವಾಗಿ ರಾಜ್ಯ ಸರ್ಕಾರ ಮತ್ತು ಕೇಂದ್ರ ಸರ್ಕಾರವು ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗಳನ್ನು ಅನುಮೋದಿಸತಕ್ಕದ್ದು.

9.3 ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿಯವರ ಅಧ್ಯಕ್ಷತೆಯಲ್ಲಿ ರಚಿಸಿರುವ ದತ್ತಾಂಶ ಆಡಳಿತ ಚಾಲನಾ ಸಮಿತಿ (Data Governance Steering Committee) ಯು ಇತರ ರಾಜ್ಯಗಳನ್ನು ಮತ್ತು / ಅಥವಾ ಭಾರತ ಸರ್ಕಾರದ ಏಜೆನ್ಸಿಗಳನ್ನು ಅನುಮೋದಿಸತಕ್ಕದ್ದು.

9.4 ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯು ಸರ್ಕಾರಿ ಇಲಾಖೆ, ಏಜೆನ್ಸಿ ಅಥವಾ ಸರ್ಕಾರಿ ಉದ್ಯಮವಾಗಿರಬೇಕು.

10. ಹೊಣೆಗಾರಿಕೆಯ ಮಿತಿ:

10.1 ಇ-ಸಹಮತಿಯು ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯಲ್ಲಿ ಸಂಗ್ರಹಿಸಿಡಲಾದ ದತ್ತಾಂಶವನ್ನು ಒಪ್ಪಿಗೆಯೊಂದಿಗೆ ಮಾಹಿತಿ ಒಡೆಯರ ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗಳ ನಡುವೆ ದತ್ತಾಂಶ ವಿನಿಮಯಕ್ಕೆ ಅನುವು ಮಾಡಿಕೊಡುವಂತಹ ವಿದ್ಯುನ್ಮಾನ ವೇದಿಕೆ ಮಾತ್ರವಾಗಿರುತ್ತದೆ.

10.2 ಇ-ಸಹಮತಿಗೂ ಸಹ ದತ್ತಾಂಶವು ಗೌಪ್ಯವಾಗಿರುವುದರಿಂದ ದತ್ತಾಂಶದ ನಿಖರತೆ ಮತ್ತು ನೈಜತೆ ಹಾಗೂ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ವತಿಯಿಂದ ದತ್ತಾಂಶದ ಸಂಗ್ರಹಣೆ, ಅಭಿರಕ್ಷಣೆ, ನಿರ್ವಹಣೆ ಹಾಗೂ ದತ್ತಾಂಶ ವಿನಿಮಯಗಳ ಶಾಸನಬದ್ಧತೆ ಮತ್ತು ಅನ್ಯ ಸೇವಾ

ಸಂಸ್ಥೆ (TPSP) ವತಿಯಿಂದ ಯಾವುದೇ ರೀತಿಯ ದತ್ತಾಂಶದ ದುರ್ಬಳಕೆ, ಅಸಮರ್ಪಕ ನಿರ್ವಹಣೆ ಸೇರಿದಂತೆ ಯಾವುದೇ ಅಂಶ/ ದೋಷ/ ಲೋಪಗಳಿಗೆ ಇ-ಸಹಮತಿಯಾಗಲಿ ಅಥವಾ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರ ಅಥವಾ ಯಾವುದೇ ಸಚಿವಾಲಯ ಅಥವಾ ಯಾವುದೇ ಇಲಾಖೆಯು ಯಾವುದೇ ರೀತಿಯ ಹೊಣೆಗಾರಿಕೆಯನ್ನು ಹೊಂದಿರತಕ್ಕದ್ದಲ್ಲ.

10.3 ದತ್ತಾಂಶವು, ಇ-ಸಹಮತಿಗೂ ಸಹ ಗೌಪ್ಯವಾಗಿದ್ದರಿಂದ ಯಾವುದೇ ಪಕ್ಷಗಳ [ಮಾಹಿತಿ ಒಡೆಯ (Data Principal), ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP)] ನಡುವೆ ಉದ್ಭವಿಸುವ ವ್ಯಾಜ್ಯಗಳಿಗೆ ಇ-ಸಹಮತಿಯಾಗಲಿ ಅಥವಾ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರ ಅಥವಾ ಯಾವುದೇ ಸಚಿವಾಲಯ ಅಥವಾ ಯಾವುದೇ ಇಲಾಖೆಯು ಭಾಗೀದಾರ/ ಪ್ರತಿವಾದಿಯಾಗಿರುವುದಿಲ್ಲ. ಆದರೆ ಇ-ಸಹಮತಿ ಮೂಲಕ ಹಂಚಿಕೊಳ್ಳಲಾದ ದತ್ತಾಂಶದ ಕುರಿತು ವ್ಯಾಜ್ಯಕ್ಕೆ ಸೀಮಿತವಾಗಿ ಇ-ಸಹಮತಿಯಲ್ಲಿ ಲಭ್ಯವಿರುವ ಮಾಹಿತಿಯನ್ನು ದಾಖಲೆ/ ಸಾಕ್ಷಿಯಾಗಿ ಉಭಯ ಪಕ್ಷಗಳೂ ಬಳಸಬಹುದು.

10.4 ಅದೇ ರೀತಿ, ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಗೆ ಮಾಹಿತಿ ಒಡೆಯನ ಒಪ್ಪಿಗೆ ಆಧಾರದ ಮೇರೆಗೆ ದತ್ತಾಂಶವನ್ನು ನೀಡಿರುವ ಹಿನ್ನೆಲೆಯಲ್ಲಿ ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ಯು ಯಾವುದೇ ಅಸಮರ್ಪಕ ನಿರ್ವಹಣೆ ಹಾಗೂ ದತ್ತಾಂಶದ ದುರುಪಯೋಗಕ್ಕೆ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯು ಹೊಣೆಯಾಗತಕ್ಕದ್ದಲ್ಲ.

10.5 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಯು ತಾನು ದತ್ತಾಂಶ ಹಂಚಿಕೊಂಡಂತಹ ಎಲ್ಲಾ ಭಾಗೀದಾರರ, ಪಾಲುದಾರರ ಹಾಗೂ ಇತರ ಘಟಕಗಳ ಎಲ್ಲಾ ಕೃತ್ಯ ಮತ್ತು / ಅಥವಾ ಲೋಪಗಳಿಗೆ ತಾನೇ ಹೊಣೆಗಾರಿಕೆ ಹೊಂದಿರತಕ್ಕದ್ದು.

11. ಸದ್ವಿದ್ಯೇಶಿತ ಕ್ರಮಗಳಿಗಾಗಿ ಅಧಿಕಾರಿಗಳಿಗೆ ರಕ್ಷಣೆ;

11.1 ಯಾವುದೇ ಅಧಿಕಾರಿಗೆ ದತ್ತಾಂಶ ಸಂಗ್ರಹಣೆ, ದತ್ತಾಂಶ ಅನುಮೋದನೆ, ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಣೆ/ ನಿರ್ವಹಣೆ ಮತ್ತು / ಅಥವಾ ದತ್ತಾಂಶ ವಿನಿಮಯದ ಭಾಗವಾಗಿ ಉದ್ದೇಶಿತ ಅಥವಾ ಉದ್ದೇಶ ರಹಿತವಾಗಿ ಸದ್ವಿದ್ಯೇಶದಿಂದ ತೆಗೆದುಕೊಂಡ ಕ್ರಮಗಳಿಗಾಗಿ ಮತ್ತು / ಅಥವಾ ಅವನ/ ಅವಳ ನಿಯಂತ್ರಣ ಮೀರಿದ ಯಾವುದೇ ಕೃತಿ/ ಕ್ರಮಗಳಿಗಾಗಿ ಅವನ/ ಅವಳ ವಿರುದ್ಧ ಯಾವುದೇ ರೀತಿಯ ಕ್ರಮವಹಿಸತಕ್ಕದ್ದಲ್ಲ. ಮೇಲ್ನೋಟಕ್ಕೆ ದುರುದ್ದೇಶಿತ ಕೃತ್ಯವೆಂದು ಕಂಡು ಬಂದಲ್ಲಿ ಮಾತ್ರ ಅಂತಹ ಕೃತ್ಯಗಳನ್ನು ಪರಿಶೀಲನೆಗೆ ಒಳಪಡಿಸಿ ಸಂಬಂಧಿತ ಕಾನೂನು ಮತ್ತು ನಿಯಮಾನುಸಾರ ಕ್ರಮವಹಿಸಬಹುದು. ಅಧಿಕಾರಿಗಳು ಕ್ರಮ ಕೈಗೊಂಡ ನಂತರ ಜಾರಿಗೆ ತಂದ ಯಾವುದೇ ಕಾನೂನು ಅಥವಾ ನಿಯಮಗಳನ್ನು ಪೂರ್ವಾನ್ವಯವಾಗಿ ಅನ್ವಯಿಸಿ ಕ್ರಮವಹಿಸ ತಕ್ಕದ್ದಲ್ಲ. ಆದರೆ ಅಧಿಕಾರಿಯ ಪರವಾಗಿ ಮಾತ್ರ ಪೂರ್ವಾನ್ವಯವಾಗಿ ಯಾವುದೇ ಕಾನೂನು ಹಾಗೂ ನಿಯಮಗಳನ್ನು ಪರಿಗಣಿಸತಕ್ಕದ್ದು.

12. ವಿವಾದಗಳ ಪರಿಹಾರ ಮತ್ತು ಮೇಲ್ಮನವಿ:

12.1 ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಮತ್ತು ಮಾಹಿತಿ ಒಡೆಯರ (Data Principal) ನಡುವಿನ ಮತ್ತು / ಅಥವಾ ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಮತ್ತು ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ (TPSP) ನಡುವಿನ ಮತ್ತು ಮಾಹಿತಿ ಒಡೆಯರ (Data Principal) ಮತ್ತು ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಯ ನಡುವಿನ ಯಾವುದೇ ವಿವಾದವನ್ನು ಉಭಯ ಪಕ್ಷಗಳು ಸೌಹಾರ್ದತೆಯಿಂದ ಪರಿಹರಿಸಿಕೊಳ್ಳತಕ್ಕದ್ದು. ಉಭಯ ಪಕ್ಷಗಳ ನಡುವೆ ಪರಿಹರಿಸಲಾಗದ ವಿವಾದಗಳನ್ನು ಈ ಮಾರ್ಗಸೂಚಿಗಳ ಕಲಂ 4.1.6 ರಂತೆ ರಚಿತವಾಗಿರುವ ಸಮಿತಿಯ ಮೂಲಕ ಪರಿಹರಿಸಿಕೊಳ್ಳತಕ್ಕದ್ದು. ಸಮಿತಿಯ ನಿರ್ಣಯದಿಂದ ಯಾವುದೇ ಪಕ್ಷವು ತೃಪ್ತಿಯಾಗದಿದ್ದಲ್ಲಿ, ಸಮಿತಿಯ ನಿರ್ಣಯದ ದಿನಾಂಕದಿಂದ 30 ದಿನದೊಳಗಾಗಿ ಸರ್ಕಾರದ ಕಾರ್ಯದರ್ಶಿಗಳು ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ (ಇ-ಆಡಳಿತ) ಇಲಾಖೆರವರಿಗೆ ಮೇಲ್ಮನವಿಯನ್ನು ಸಲ್ಲಿಸಬಹುದಾಗಿದ್ದು, ಅವರ ನಿರ್ಣಯವು ಅಂತಿಮವಾಗಿದ್ದು ಎಲ್ಲ ಪಕ್ಷಗಳು ಇದಕ್ಕೆ ಬದ್ಧರಾಗಿರತಕ್ಕದ್ದು.

13. ನ್ಯಾಯಾಲಯದ ವ್ಯಾಪ್ತಿ:

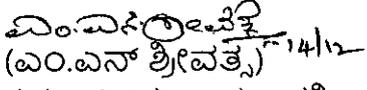
13.1 ಎಲ್ಲಾ ಕಾನೂನಾತ್ಮಕ ನಡವಳಿಗಳು ಹಾಗೂ ಕ್ರಮಗಳು ಕರ್ನಾಟಕ ರಾಜ್ಯದ ಬೆಂಗಳೂರಿನ ನ್ಯಾಯಾಲಯಗಳ ವ್ಯಾಪ್ತಿಗೆ ಸೀಮಿತವಾಗಿರುತ್ತವೆ.

14. ಹೊರಪಡಿಕೆ:

14.1 ಕಾನೂನಿನನ್ವಯ ಮಾಹಿತಿ ಒಡೆಯನ ಒಪ್ಪಿಗೆಯ ಅಗತ್ಯವಿರದ ಉಭಯ ಸಂಸ್ಥೆಗಳ ನಡುವಿನ ದತ್ತಾಂಶ ವಿನಿಮಯ, ಉದಾಹರಣೆಗೆ ಸರ್ಕಾರದ ಇಲಾಖೆಗಳು ಮತ್ತು/ ಅಥವಾ ಸಂಸ್ಥೆಗಳ ನಡುವಿನ ದತ್ತಾಂಶ ವಿನಿಮಯಗಳ ಸಂದರ್ಭಗಳಲ್ಲಿ ಈ ಮಾರ್ಗಸೂಚಿಗಳು ಅನ್ವಯಿಸುವುದಿಲ್ಲ.

15. ಮಾರ್ಗಸೂಚಿಗಳ ಪರಿಷ್ಕರಣೆ, ಸೇರ್ಪಡೆ, ತಿದ್ದುಪಡಿ ಮಾಡಲು ಸರ್ಕಾರದ ಅಧಿಕಾರ:

15.1 ಸರ್ಕಾರವು, ದತ್ತಾಂಶ ಪ್ರವೇಶಾವಕಾಶದ ಉದ್ದೇಶಗಳು, ಅನ್ಯ ಸೇವಾ ಸಂಸ್ಥೆ [Third Party Service Provider (TPSP)] ಗಳ ಅರ್ಹತೆಗಳು, ದತ್ತಾಂಶ ಅಭಿರಕ್ಷಕ ಸಂಸ್ಥೆ (Data Fiduciary) ಗಳ ಮತ್ತು ಮಾಹಿತಿ ಒಡೆಯರ (Data Principal) ಪಾತ್ರ ಹಾಗೂ ಜವಾಬ್ದಾರಿಗಳು ಸೇರಿದಂತೆ ಈ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಪರಿಷ್ಕರಿಸುವ, ಹೆಚ್ಚುವರಿ ಮಾರ್ಗಸೂಚಿ ಸೇರಿಸುವ ಮತ್ತು / ಅಥವಾ ತೆಗೆದು ಹಾಕುವ ಅಧಿಕಾರವನ್ನು ಕಾಯ್ದಿರಿಸಿಕೊಂಡಿರುತ್ತದೆ.


(ಎಂ.ಎನ್ ಶ್ರೀವತ್ಸ) 14/12
ಸರ್ಕಾರದ ಅಧೀನ ಕಾರ್ಯದರ್ಶಿ
ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ
ಇಲಾಖೆ (ಇ-ಆಡಳಿತ)

I/197121/2021

PROCEEDINGS OF THE GOVERNMENT OF KARNATAKA

Sub: Guidelines for providing data through e-Sahamathi (consent manager)-reg

Read: The Chief Executive Officer, Centre for e-Governance File No: CeG- PDFR/27/2021
(605991)

Preamble:

Citizens' data is available with various Government Departments and Institutions. Sharing citizens' data with others (excluding Government Departments and Institutions) would require prior consent of the concerned citizens. Sharing the data upon consent with others (NGOs, private institutions etc.) would help citizens in getting various facilities and services. The Department of Personnel and Administrative Reforms (e-Governance) has developed e-Sahamathi, a consent manager through NIC which is a system of sharing citizens' data (information) upon their consent with others. It is required to issue guidelines for sharing citizens' data with others through e-Sahamathi. Guidelines have been drafted for this purpose.

In the meeting of the Data Governance Steering Committee under the chairmanship of the Additional Chief Secretary to Government, Government of Karnataka held on 17-11-2021, the following decisions has been taken.

“The committee accorded the approval to the Guidelines and the e-Governance Department was advised to go ahead for its issue after getting opinion from any good legal firm expertising in personal data protection and consent mechanism for sharing of data followed by the opinion of Law Department”.

As per the decision, opinion of M/s Trilegal, a legal firm has examined the draft guidelines in detail and has suggested some changes. Accordingly, subsequent to appropriately modifying the guidelines, opinion of the Law Department has been obtained. Therefore, vide file read above, the Chief Executive Officer, Centre for e-Governance has submitted draft guidelines with respect to sharing of citizens' data with others through e-Sahamathi (Consent Manager) with a request to issue appropriate orders.

The proposal of the Chief Executive Officer, Centre for e-Governance has been examined, the Government has decided to issue guidelines for sharing citizens' data through e-Sahamathi (Consent Manager). Hence this order.

GOVERNMENT ORDER NO: DPAR 113 PRJ 2021

BENGALURU, dated:14.12.2021

As explained in the above preamble, the Government are pleased to approve the attached guidelines to share citizens' data with others through e-Sahamathi (Consent Manager).

Government would revise these guidelines from time to time depending upon the feedback received from citizens, NGOs and other stakeholders. Centre for e-Governance shall immediately make provision in e-Sahamathi portal to receive suggestions in this regard.

This order is issued with the concurrence of Law Department vide Note No. LAW-OPN/230/2021, dated 4-12-2021.

(ಈ ಆದೇಶವನ್ನು ಕನ್ನಡದಲ್ಲಿಯೂ
ಹೊರಡಿಸಲಾಗುತ್ತಿದೆ)

By Order and in the name of the
Governor of Karnataka


(M.N. SRIVATSA)

Under Secretary to Government
Department of Personnel and Administrative
Reforms (e-Governance)

To:

The Compiler, Karnataka Gazette to publish in the Extra-ordinary Gazette and to supply 50 copies to this Department.

Copy to:

1. The Accountant General (A & E) / (G & SSA), Bengaluru.
2. The Chief Secretary to Government of Karnataka, Vidhana Soudha, Bengaluru
3. The Additional Chief Secretary to Government, Vidhana Soudha, Bengaluru
4. All Additional Chief Secretary / Principal Secretary / Secretary to Government, Vidhana Soudha / Vikasa Soudha / M.S. Building, Bengaluru
5. The Chief Executive Officer, Centre for e-Governance, M.S. Building, Bengaluru
6. All Heads of Departments - through the concerned Additional Chief Secretary / Principal Secretary / Secretary to Government
7. All Boards / Corporations – through the concerned Additional Chief Secretary / Principal Secretary / Secretary to Government
8. The Director e-Governance and Ex-officio Director, Electronic Delivery of Citizen Services, Bengaluru
9. The Executive Director, Centre for Smart Governance, Bengaluru
10. The Personal Secretary to Additional Chief Secretary to Government, Department of Personnel and Administrative Reforms (e-Governance), M.S. Building, Bengaluru
11. The Personal Assistant to Additional Secretary to Government, Department of Personnel and Administrative Reforms (e-Governance), M.S. Building, Bengaluru
12. To publish in the Department Website.
13. Section Guard File.

Guidelines for sharing data through e-Sahamathi (Consent Manager)

1. Scope:

These Guidelines for Sharing Data through e-Sahamathi (Guidelines) covers various aspects of sharing of data pertaining to data principals with consent by respective data fiduciary with Third Party Service Providers (TPSP) through e-Sahamathi (consent manager) of Government of Karnataka.

2. Definitions:

In these Guidelines, the following words shall have the respective meanings, unless the context otherwise requires:

2.1 **Data** shall mean data of data principal that is accessed by TPSP from any data fiduciary through e-Sahamathi.

2.2 **Data principal** means any natural person whose data is collected and maintained by the data fiduciary.

2.3 **Data fiduciary** means a Government organization including departments, boards, corporations that collect and maintain data of any data principal.

2.4 **Consent Manager** means an electronic platform which collects and manages the consent of the data principals to share his/her collected data which is collected and maintained by one or more data fiduciaries.

2.5 **e-Sahamathi** means the Consent Manager of the Government of Karnataka which is designed and developed by National Informatics Centre, Karnataka state unit to manage consent of the data principals whose data will be shared with the TPSP from any data fiduciary registered under these Guidelines.

2.6 **Third Party Service Provider (TPSP)** means a private/ public company or organization or NGO or Public sector undertaking that will be provided access to data of data principal(s) based on data principal's consent or consent to a request from a TPSP for providing value added services to data principal(s).

3. Qualifications and responsibilities of a Third Party Service Provider (TPSP).

3.1 The TPSP should:

3.1.1 Be a private/ public company or organization or NGO or Public sector undertaking registered under the relevant Indian law(s).

3.1.2 Demonstrate experience of having piloted/deployed the use case for which the TPSP will request access to data for sufficient time which shall not be lesser than 6 months.

3.1.3 Should be able to demonstrate, if asked for, having adequate capital or funding sources to undertake the use case and fulfill its commitments under these Guidelines.

3.1.4 Operate in the jurisdiction of the Republic of India.

3.1.5 Comply with all relevant laws, rules and regulations of the state and country in the letter and spirit.

4. Registration of TPSP, Accessing and using data by a TPSP and responsibilities.

4.1 Registration with the e-Sahamathi (Consent Manager).

4.1.1 The interested TPSP shall submit an application in prescribed form duly signed either physically or electronically (duly e signed).

4.1.2 Submit a self-attested declaration that the TPSP will comply with these Guidelines, all applicable data protection laws and regulations and any additional guidelines issued from time to time.

4.1.3 Submit an exclusive list of all partners and co-operators, if any, with whom the TPSP will work to provide service to the data principals or share the data that has been obtained through the e-Sahamathi platform. Any changes in the submitted list must be communicated to e-Sahamathi in writing (including electronically) and must also be approved by e-Sahamathi before any data can be shared.

4.1.4 Each TPSP should specify its field of interest, data sets required in its application and the intended use cases for the data collected via the e-Sahamathi platform. Request for the additional data sets may be submitted later also, if required.

4.1.5 Provide public key for digital signature verification and encryption keys for data encryption during data exchange.

4.1.6 The registration shall be approved by a committee constituted for the purpose headed by the Chief Executive Officer, Centre for e-Governance, DPAR (e Governance), Government of Karnataka and having representative of the data fiduciary(ies).

4.1.7 The TPSP shall pay the prescribed fee, which may be increased or decreased from time to time, at the time of registration which is not refundable.

4.1.7.1 The Government reserves the right to waive the registration fee, at its sole discretion, based on the purpose for which data is intent to be used like for social cause alone and also based on nature of the TPSP.

4.1.8 The government reserves the right to prescribe "caution money" in the form of deposit or bank guarantee which is refundable but with no interest.

4.2 For accessing data, TPSP shall;

4.2.1 Submit a request electronically duly digitally signed to the Consent Manager each time specifying the:

4.2.1.1 Use case for which the TPSP requires data;

4.2.1.2 Specific data sets that will be required from the pool of data sets specified by the TPSP during registration (as required under Section 4.1.4 of the Guidelines).

4.2.1.3 Data may also be requested through an Application Program Interface (API). All the guidelines, terms and conditions shall be same for getting the data through API.

4.3 Responsibilities of TPSP;

4.3.1 Data shall be accessed by a TPSP only for specific purposes, in accordance with the use cases as requested for by the TPSP under Section 4.1.4 and in accordance with the Guidelines. The purposes for which the TPSP may request access to data must be from amongst the purposes notified for this reason by the competent authority.

4.3.2 The State government, Consent Manager or data fiduciary shall have the right to audit the TPSP's IT system and/ or documents to scrutinize the processes used by TPSP to confirm compliance with the Guidelines and for checking for what all purposes data shared by data fiduciary through Consent Manager has been used besides for scrutinizing safe guards and security checks deployed in the IT system.

4.3.3 TPSP shall ensure through appropriate technical solutions and legal agreements between it and partners and/ or co-operators that:

4.3.3.1 Only authorized person/entity of the TPSP or its partners and/or co-operators may access the data.

4.3.3.2 Data shall only be used for specified purpose for which consent of the data principal has been recorded;

4.3.3.3 Other than those entities approved by e-Sahamathi under Section 4.1.3, TPSP shall not share, provide access to, disclose, transfer, sell, or re-sell the Data of the data principal(s) under any circumstances.

4.3.3.4 Data shall be used and can be retained by the TPSP only for the time period for which the data principal has provided consent and shall be deleted immediately upon expiry of this time period.

4.3.3.5 Data shall not be used and retained by the TPSP if consent is revoked by the data principal and shall be deleted immediately upon revocation of consent.

4.3.3.6 There shall be adequate safeguards built in its IT system(s) to ensure that data is protected against unauthorized access, alteration, destruction, disclosure or dissemination of records and data. These safeguards shall in no event be lesser than the standards prescribed under applicable laws.

4.3.3.7 The TPSP and their partners and/ or cooperators comply with all applicable laws, rules and regulations including and not limited to data protection laws and regulations.

4.3.3.8 The TPSP and their partners and/ or co-operators comply with the directions issued by the state and Union government from time to time.

4.4 The State Government reserves the right to deny, in its wisdom, registration of any TPSP or deny any data sought by any TPSP with or without assigning any reason.

4.5 To the extent permitted under applicable laws, the data fiduciary shall retain all right, title and interest (including copyright) in the data accessed by the TPSP through e-Sahamathi.

5 Inclusion of Data Fiduciary in the e – Sahamathi (consent manger).

5.1 Any data fiduciary which is to be included in e-Sahamathi (consent manager) and share the data of any data principal through the e-Sahamathi to TPSP shall be approved by a committee headed by the Additional Chief Secretary/ Principal Secretary/ Secretary to Government DPAR (e Governance) with a representative from the department to which the data fiduciary belongs.

6 Grievance Redressal.

6.1 TPSP shall appoint a person as a Grievance Redressal Officer for handling/ disposal of user grievances/ complaints. It shall have a dedicated set-up to address data principals' grievances/ complaints;

6.2 TPSP shall acknowledge in writing or any electronic form for each and every complaint and grievance.

6.3 TPSP shall acknowledge a data principal's grievance/complaint within [72] hours of receipt of such grievance/complaint. Following acknowledgement, the TPSP will be required to resolve the data principal's grievance/complaints within 30 days of receipt of such grievance/complaint;

6.4 At the operational level, TPSP shall display the following information prominently, on the website/application and at its place(s) of business:

6.4.1 The name and contact details (Telephone / Mobile nos. and email address) of the Grievance Redressal Officer who can be approached by the public for resolution of complaints against the TPSP.

7 Removal of a TPSP

7.1 The Government reserves the right to cancel the data access to a TPSP, forfeit caution money, levy fine besides taking appropriate legal action against TPSP in case of 7.1.2 and 7.1.3, if such TPSP

7.1.1 ceases to carry on business in India; or

7.1.2 fails to comply or breaches any of the conditions specified in these Guidelines; or

7.1.3 Fails to comply or breach any of the relevant act/ law and / or rules and/ or direction of government.

7.2 The Government also reserves the right to remove/ deregister any TPSP in its wisdom with or without assigning any reason.

8 Role, Responsibility, Limitation of Liability of e-Sahamathi and data fiduciary:

8.1 Role:

8.1.1 Data fiduciary; The role of the data fiduciary is to collect, maintain and share the data through e-Sahamathi (consent manager).

8.1.2 e-Sahamathi (consent manager); The role of the e-Sahamathi as a Consent Manager is to enable data

sharing between data fiduciary and TPSP as per the consent of the data principal and to manage said consents.

8.2 Responsibility:

8.2.1 Data Fiduciary; The responsibility of the data fiduciary is

8.2.1.1 To collect and maintain the data in a secured manner.

8.2.1.2 To share the list of data principals, with e-Sahamathi coming under ambit of specific requests from TPSPs.

8.2.1.3 To share the data of the data principal (for which consent is given) with the TPSP through the e-Sahamathi (consent manager) in encrypted form so that even e-Sahamathi is blind to the data.

8.2.1.4 To ensure that the data principal's data is shared only to the extent of the consent received for each data field. Besides, ensure that the data ceases to be shared as and when consent is revoked by the data principal.

8.2.1.5 To maintain all the details of consent artefact and data access details.

8.2.2 e-Sahamathi (consent manager): The responsibility of e-Sahamathi (consent manager) is

8.2.2.1 To enable data principal to provide consent and/ or request based consent as well as revoking the consent and maintain the same.

8.2.2.2 To enable data principal to view the data access details.

8.2.2.3 To enable data sharing with TPSP based on consent in encrypted form as shared by the respective data fiduciary (e-Sahamathi is blind to the data).

8.2.2.4 To ensure that the data is shared with only authorized intended TPSP in encrypted form.

8.2.2.5 To inform both data fiduciary and TPSP about revocation of consent, if any and cease the sharing of any data which was being shared on the basis of the now revoked consent.

9. e-Sahamathi as a service:

9.1 The services of e-Sahamathi may be extended as consent manager to other state government(s) within the nation and to Government of India subject to any rules or regulations that may be applicable.

9.2 In case of extending services of e-Sahamathi to other states government and / or Government of India, the respective state and Gol, as the case may be, shall approve the data fiduciary and also TPSP with which data is to be shared.

9.3 The Data Governance Steering Committee of the Government of Karnataka under the chairmanship of Additional Chief Secretary to Government shall approve the state(s) and/or GoI agency.

9.4 The data fiduciary shall be a government department or agency or government undertaking.

10 Limitation of liability:

10.1 e-Sahamathi is just an enabling IT platform for data exchange with consent between data principal and TPSP where data fiduciary is the custodian of the data.

10.2 e-Sahamathi is data blind, and therefore it shall not nor shall the Government of Karnataka or any ministry or department thereof, be responsible or liable for any liability with regard to the accuracy and correctness of the data, legality of collection, storage/ maintenance and sharing of data by any fiduciary or TPSP and/ or anything including and not limited to misuse, mismanagement, mishandling of data by TPSP.

10.3 As it is blind to data shared between data fiduciary and TPSP it cannot, nor can the Government of Karnataka or any ministry or department thereof, be a party to any litigation arising between any of the parties (data principal, data fiduciary, TPSP). However, e-Sahamathi data may be used as evidence by any party to prove their point but limited to the litigation related to data shared or accessed through e- Sahamathi.

10.4 Similarly, data fiduciary shall not have any liability for misuse of data by TPSP or any wrong doing by TPSP given the fact that the data has been shared with the TPSP with due consent of the data principal.

10.5 The TPSP shall retain liability for the acts and/or omissions of all partners, co-partners and any other entity with whom it has shared the data.

11 Protection to officers for *bona-fide* actions:

11.1 Any *bona-fide* action taken by any officer, intentionally or unintentionally, as part of data collection, data approval, data storage/ maintenance and/ or data sharing and/ or any act which is beyond his/her control shall not lead to any action against such officer. *Mala-fide* act, *prima face* if any, only shall be subject to scrutiny and action as per relevant laws and regulation. There cannot be an action retrospective to any law or regulation passed later than the action but for the relief provided under any law or regulation which shall be considered retrospectively in favour of the officer(s).

12 Resolution of dispute and Appeal:

12.1 Any dispute between TPSP and data principal and / or between data fiduciary and TPSP and / or data principal and data fiduciary shall be resolved amicably between the respective parties. In case of any dispute which is unsettled between the parties, the same may be resolved by the committee constitute as per para 4.1.6. In case either of the parties is not satisfied with the decision of the committee it may appeal to the Secretary to the Government, DPAR (e Governance) within one month of the decision of the committee whose decision would be final and binding on all parties.

13 Legal Jurisdiction:

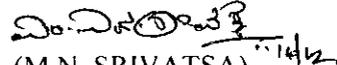
13.1 All legal proceedings and actions shall be within the jurisdiction of courts in Bengaluru, Karnataka.

14 Exclusions:

14.1 These guidelines shall not apply to sharing of data between any two entities where consent of the data principal is not required under law, like between government departments and / or agencies.

15 Right of the state to add, remove and modify guidelines:

15.1 The state reserves the right to add, remove and/ or modify guidelines including and not limited to the purpose(s) for which data is accessed, qualification of TPSP, roles and responsibilities of data fiduciary and data principals.


(M.N. SRIVATSA)

Under Secretary to Government
Department of Personnel and Administrative
Reforms (e-Governance)

