ಡೇಟಾ ಭದ್ರತೆಯು ಡೇಟಾಬೇಸ್ನಲ್ಲಿನಂತಹ, ವಿನಾಶಕಾರಿ ಪಡೆಗಳಿಂದ ಮತ್ತು ಅನಧಿಕೃತ ಬಳಕೆದಾರರ ಅನಪೇಕ್ಷಿತ ಕ್ರಿಯೆಗಳಿಂದ ಸೈಬರ್ಟಾಕ್ ಅಥವಾ ಡೇಟಾ ಉಲ್ಲಂಘನೆಯಂತಹ ಡಿಜಿಟಲ್ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸುತ್ತದೆ ಎಂದರ್ಥ.

ತಂತ್ರಜ್ಞಾನಗಳು:

ಡಿಸ್ಕ್ ಗೂಢಲಿಪೀಕರಣ:

ಡಿಸ್ಕ್ ಗೂಢಲಿಪೀಕರಣ ಎನ್ಕ್ರಿಪ್ಶನ್ ತಂತ್ರಜ್ಞಾನವನ್ನು ಸೂಚಿಸುತ್ತದೆ ಅದು ಹಾರ್ಡ್ ಡಿಸ್ಕ್ ಡ್ರೈವ್ನಲ್ಲಿ ಡೇಟಾವನ್ನು ಎನ್ಕ್ರಿಪ್ಟ್ ಮಾಡುತ್ತದೆ. ಡಿಸ್ಕ್ ಗೂಢಲಿಪೀಕರಣ ವಿಶಿಷ್ಟವಾಗಿ ಸಾಫ್ಟ್ವೇರ್ನಲ್ಲಿ (ಡಿಸ್ಕ್ ಗೂಢಲಿಪೀಕರಣ ತಂತ್ರಾಂಶವನ್ನು ನೋಡಿ) ಅಥವಾ ಹಾರ್ಡ್ವೇರ್ನಲ್ಲಿ (ಡಿಸ್ಕ್ ಗೂಢಲಿಪೀಕರಣ ಯಂತ್ರಾಂಶವನ್ನು ನೋಡಿ) ರೂಪವನ್ನು ತೆಗೆದುಕೊಳ್ಳುತ್ತದೆ. ಡಿಸ್ಕ್ ಗೂಢಲಿಪೀಕರಣವನ್ನು ಹೆಚ್ಚಾಗಿ ಫ್ಲೈ ಗೂಢಲಿಪೀಕರಣ (OTFE) ಅಥವಾ ಪಾರದರ್ಶಕ ಎನ್ಕ್ರಿಪ್ಶನ್ ಎಂದು ಉಲ್ಲೇಖಿಸಲಾಗುತ್ತದೆ.

ಡೇಟಾವನ್ನು ರಕ್ಷಿಸಲು ಸಾಫ್ಟ್ವೇರ್ ಮತ್ತು ಹಾರ್ಡ್ವೇರ್ ಆಧಾರಿತ ಕಾರ್ಯವಿಧಾನಗಳು :

ಸಾಫ್ಟ್ವೇರ್ ಆಧಾರಿತ ಭದ್ರತಾ ಪರಿಹಾರಗಳು ಅದನ್ನು ಕಳ್ಳತನದಿಂದ ರಕ್ಷಿಸಲು ಡೇಟಾವನ್ನು ಎನ್ಕ್ರಿಪ್ಟ್ ಮಾಡುತ್ತವೆ. ಆದಾಗ್ಯೂ, ದುರುದ್ದೇಶಪೂರಿತ ಪ್ರೋಗ್ರಾಂ ಅಥವಾ ಹ್ಯಾಕರ್ ಡೇಟಾವನ್ನು ದೋಷಪೂರಿತಗೊಳಿಸಬಲ್ಲದು, ಅದು ಸಿಸ್ಟಮ್ ಅನ್ನು ನಿಷ್ಪ್ರಯೋಜಕಗೊಳಿಸಬಲ್ಲದು. ಹಾರ್ಡ್ವೇರ್-ಆಧರಿತ ಭದ್ರತಾ ಪರಿಹಾರಗಳು ಡೇಟಾಗೆ ಪ್ರವೇಶವನ್ನು ಓದುವುದು ಮತ್ತು ಬರೆಯುವಿಕೆಯನ್ನು ತಡೆಗಟ್ಟುತ್ತವೆ ಮತ್ತು ಹೀಗಾಗಿ ತಿದ್ದುಪಡಿ ಮತ್ತು ಅನಧಿಕೃತ ಪ್ರವೇಶದ ವಿರುದ್ಧ ಬಲವಾದ ರಕ್ಷಣೆ ನೀಡುತ್ತವೆ.

ಹಾರ್ಡ್ವೇರ್ ಆಧಾರಿತ ಭದ್ರತೆ ಅಥವಾ ಸಹಾಯಕ ಕಂಪ್ಯೂಟರ್ ಭದ್ರತೆಯು ಸಾಫ್ಟ್ವೇರ್-ಮಾತ್ರ ಕಂಪ್ಯೂಟರ್ ಭದ್ರತೆಗೆ ಪರ್ಯಾಯವನ್ನು ಒದಗಿಸುತ್ತದೆ. ಪಿಕೆಸಿಎಸ್ # 11 ಅನ್ನು ಬಳಸುವಂತಹ ಸುರಕ್ಷತಾ ಸಂಕೇತಗಳನ್ನು ರಾಜಿ ಮಾಡಲು ಅಗತ್ಯವಾದ ದೈಹಿಕ ಪ್ರವೇಶದ ಕಾರಣದಿಂದಾಗಿ ಹೆಚ್ಚು ಸುರಕ್ಷಿತವಾಗಿರಬಹುದು. ಟೋಕನ್ ಸಂಪರ್ಕಗೊಂಡಾಗ ಮಾತ್ರ ಪ್ರವೇಶವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಲಾಗಿದೆ ಮತ್ತು ಸರಿಯಾದ ಪಿನ್ ನಮೂದಿಸಲಾಗಿದೆ (ಎರಡು-ಅಂಶ ದೃಢೀಕರಣವನ್ನು ನೋಡಿ). ಆದಾಗ್ಯೂ, ಅದಕ್ಕೆ ದೈಹಿಕ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುವ ಯಾರಿಗಾದರೂ ಡಾಂಗಿಗಳನ್ನು ಬಳಸಬಹುದು. ಯಂತ್ರಾಂಶ-ಆಧಾರಿತ ಸುರಕ್ಷತೆಯ ಹೊಸ ತಂತ್ರಜ್ಞಾನಗಳು ಈ ಸಮಸ್ಯೆಗೆ ಸಂಪೂರ್ಣ ಪುರಾವೆ ಭದ್ರತೆಯನ್ನು ಒದಗಿಸುತ್ತವೆ.

ಯಂತ್ರಾಂಶ-ಆಧರಿತ ಭದ್ರತೆಯ ಕೆಲಸ:

ಒಂದು ಯಂತ್ರಾಂಶ ಸಾಧನವು ಬಳಕೆದಾರರಿಗೆ ಪ್ರವೇಶಿಸಲು, ಲಾಗ್ ಔಟ್ ಮಾಡಲು ಮತ್ತು ಹಸ್ತಚಾಲಿತ ಕ್ರಿಯೆಗಳನ್ನು ಮಾಡುವುದರ ಮೂಲಕ ವಿಭಿನ್ನ ಸೌಲಭ್ಯಗಳನ್ನು ಹೊಂದಿಸಲು ಅನುಮತಿಸುತ್ತದೆ. ದುರುದ್ದೇಶಪೂರಿತ ಬಳಕೆದಾರರು ಲಾಗಿಂಗ್, ಲಾಗ್ ಔಟ್, ಮತ್ತು ಸವಲತ್ತು ಮಟ್ಟವನ್ನು ಬದಲಾಯಿಸುವುದನ್ನು ತಡೆಗಟ್ಟಲು ಬಯೋಮೆಟ್ರಿಕ್ ತಂತ್ರಜ್ಞಾನವನ್ನು ಸಾಧನವು ಬಳಸುತ್ತದೆ. ಸಾಧನದ ಬಳಕೆದಾರರ ಪ್ರಸ್ತುತ ಸ್ಥಿತಿ ಹಾರ್ಡ್ ಡಿಸ್ಕ್ಗಳಂತಹ ಬಾಹ್ಯ ಸಾಧನಗಳಲ್ಲಿನ ನಿಯಂತ್ರಕಗಳಿಂದ ಓದಲ್ಪಡುತ್ತದೆ. ದುರುದ್ದೇಶಪೂರಿತ ಬಳಕೆದಾರರಿಂದ ಅಥವಾ ದುರುದ್ದೇಶಪೂರಿತ ಪ್ರೋಗ್ರಾಂನಿಂದ ಕಾನೂನುಬಾಹಿರ ಪ್ರವೇಶವು ಹಾರ್ಡ್ವೇರ್ ಡಿಸ್ಕ್ ಮತ್ತು ಡಿವಿಡಿ ನಿಯಂತ್ರಕಗಳು ಬಳಕೆದಾರರ ಪ್ರಸ್ತುತ ಸ್ಥಿತಿಯ ಆಧಾರದ ಮೇಲೆ ಅಡಚಣೆಯಾಗಿದ್ದು, ಡೇಟಾಗೆ ಅಸಾಧ್ಯ ಪ್ರವೇಶವನ್ನು ನೀಡುತ್ತದೆ. ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್ಗಳು ವೈರಸ್ಗಳು ಮತ್ತು ಹ್ಯಾಕರ್ಗಳಿಂದ ದುರುದ್ದೇಶಪೂರಿತ ದಾಳಿಗೆ ಗುರಿಯಾಗುವಂತೆ ಕಾರ್ಯಾಚರಣಾ ವ್ಯವಸ್ಥೆಗಳಿಂದ ಒದಗಿಸಲ್ಪಟ್ಟ ರಕ್ಷಣೆಗಿಂತ ಹಾರ್ಡ್ವೇರ್-ಆಧಾರಿತ ಪ್ರವೇಶ ನಿಯಂತ್ರಣವು ಹೆಚ್ಚು ಸುರಕ್ಷಿತವಾಗಿದೆ. ದುರುದ್ದೇಶಪೂರಿತ ಪ್ರವೇಶವನ್ನು ಪಡೆದುಕೊಂಡ ನಂತರ ಹಾರ್ಡ್ ಡಿಸ್ಕ್ಗಳ ಮೇಲಿನ ಮಾಹಿತಿಯು ದೋಷಪೂರಿತವಾಗಬಹುದು. ಯಂತ್ರಾಂಶ-ಆಧಾರಿತ

ರಕ್ಷಣೆ, ಸಾಫ್ಟ್ವೇರ್ ಬಳಕೆದಾರರ ಸವಲತ್ತು ಮಟ್ಟವನ್ನು ಕುಶಲತೆಯಿಂದ ನಿರ್ವಹಿಸಲು ಸಾಧ್ಯವಿಲ್ಲ. ಹ್ಯಾಕರ್ ಅಥವಾ ದುರುದ್ದೇಶಪೂರಿತ ಪ್ರೋಗ್ರಾಮ್ ಹಾರ್ಡ್ವೇರ್ನಿಂದ ರಕ್ಷಿಸಲ್ಪಟ್ಟ ಸುರಕ್ಷಿತ ಡೇಟಾವನ್ನು ಪ್ರವೇಶಿಸಲು ಅಥವಾ ಅನಧಿಕೃತ ಸೌಲಭ್ಯಗಳನ್ನು ನಿರ್ವಹಿಸಲು ಅಸಾಧ್ಯವಾಗಿದೆ. ಹಾರ್ಡ್ವೇರ್ ಸ್ವತಃ ದುರುದ್ದೇಶಪೂರಿತವಾಗಿದ್ದರೆ ಅಥವಾ ಹಿಮ್ಮೇಳವನ್ನು ಹೊಂದಿದ್ದರೆ ಮಾತ್ರ ಈ ಊಹೆ ಮುರಿದುಹೋಗುತ್ತದೆ. [3] ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್ ಇಮೇಜ್ ಮತ್ತು ಫೈಲ್ ಸಿಸ್ಟಮ್ ಸವಲತ್ತುಗಳನ್ನು ಹಾನಿಗೊಳಗಾಗದಂತೆ ಹಾರ್ಡ್ವೇರ್ ರಕ್ಷಿಸುತ್ತದೆ. ಆದ್ದರಿಂದ, ಯಂತ್ರಾಂಶ-ಆಧಾರಿತ ಭದ್ರತೆ ಮತ್ತು ಸುರಕ್ಷಿತ ಸಿಸ್ಟಮ್ ಆಡಳಿತ ನೀತಿಗಳ ಸಂಯೋಜನೆಯನ್ನು ಬಳಸಿಕೊಂಡು ಸಂಪೂರ್ಣ ಸುರಕ್ಷಿತ ವ್ಯವಸ್ಥೆಯನ್ನು ರಚಿಸಬಹುದು.

ಬ್ಯಾಕಪ್ಗಳು

ಕಳೆದುಹೋಗಿರುವ ಡೇಟಾವನ್ನು ಮತ್ತೊಂದು ಮೂಲದಿಂದ ಮರುಪಡೆಯಲು ಸಾಧ್ಯವಾಗುವಂತೆ ಬ್ಯಾಕ್ಅಪ್ಗಳನ್ನು ಬಳಸಲಾಗುತ್ತದೆ. ಹೆಚ್ಚಿನ ಉದ್ಯಮಗಳಲ್ಲಿ ಯಾವುದೇ ಡೇಟಾವನ್ನು ಬ್ಯಾಕ್ಅಪ್ ಮಾಡುವುದು ಅತ್ಯಗತ್ಯ ಎಂದು ಪರಿಗಣಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ಬಳಕೆದಾರನಿಗೆ ಪ್ರಾಮುಖ್ಯತೆಯ ಯಾವುದೇ ಫೈಲ್ಗಳಿಗೆ ಪ್ರಕ್ರಿಯೆ ಸೂಚಿಸಲಾಗುತ್ತದೆ.

ಡೇಟಾ ಮರೆಮಾಚುವಿಕೆ

ಡೇಟಾ ಭದ್ರತೆಯ ನಿರ್ವಹಣೆ ಮತ್ತು ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಅನಧಿಕೃತ ಸಿಬ್ಬಂದಿಗೆ ಬಹಿರಂಗಪಡಿಸುವುದಿಲ್ಲ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಡೇಟಾಬೇಸ್ ಟೇಬಲ್ ಅಥವಾ ಕೋಶದೊಳಗೆ ನಿರ್ದಿಷ್ಟವಾದ ಡೇಟಾವನ್ನು ಮರೆಮಾಚುವ ಪ್ರಕ್ರಿಯೆ ರಚನಾತ್ಮಕ ಡೇಟಾದ ಡೇಟಾ ಮರೆಮಾಚುವಿಕೆಯಾಗಿದೆ. [5] ಇದು ಬಳಕೆದಾರರಿಂದ ಡೇಟಾವನ್ನು ಮರೆಮಾಡುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ (ಉದಾಹರಣೆಗೆ ಬ್ಯಾಂಕಿಂಗ್ ಗ್ರಾಹಕರ ಪ್ರತಿನಿಧಿಗಳು ಗ್ರಾಹಕರ ರಾಷ್ಟ್ರೀಯ ಗುರುತಿನ ಸಂಖ್ಯೆಯ ಕೊನೆಯ 4 ಅಂಕೆಗಳನ್ನು ಮಾತ್ರ ನೋಡಬಹುದು), ಡೆವಲಪರ್ಗಳು (ಹೊಸ ಸಾಫ್ಟ್ವೇರ್ ಬಿಡುಗಡೆಗಳನ್ನು ಪರೀಕ್ಷಿಸಲು ನಿಜವಾದ ಉತ್ಪಾದನಾ ಡೇಟಾ ಅಗತ್ಯವಿರುವವರು ಆದರೆ ಸೂಕ್ಷ್ಮತೆಯನ್ನು ನೋಡಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ ಹಣಕಾಸು ಡೇಟಾ), ಹೊರಗುತ್ತಿಗೆ ಮಾರಾಟಗಾರರು, ಇತ್ಯಾದಿ.

ಡೇಟಾ ಅಳತೆ

ಡೇಟಾ ಎಸೆರ್ ಎಂಬುದು ಸಾಫ್ಟ್ವೇರ್ ಆಧರಿತವಾದ ಪುನರಾವರ್ತನೆಯ ಒಂದು ವಿಧಾನವಾಗಿದ್ದು, ಒಂದು ಹಾರ್ಡ್ ಡ್ರೈವ್ ಅಥವಾ ಇತರ ಡಿಜಿಟಲ್ ಮಾಧ್ಯಮದಲ್ಲಿ ವಾಸಿಸುವ ಎಲ್ಲಾ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಡೇಟಾವನ್ನು ಸಂಪೂರ್ಣವಾಗಿ ನಾಶಪಡಿಸುತ್ತದೆ, ಆಸ್ತಿಯು ನಿವೃತ್ತಿಯಾದಾಗ ಅಥವಾ ಮರುಬಳಕೆಯಾಗದಿದ್ದಾಗ ಯಾವುದೇ ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ಕಳೆದುಕೊಳ್ಳುವುದಿಲ್ಲ.

ಅಂತರರಾಷ್ಟ್ರೀಯ ಕಾನೂನುಗಳು ಮತ್ತು ಮಾನದಂಡಗಳು

ಅಂತರರಾಷ್ಟ್ರೀಯ ಕಾನೂನುಗಳು

ಯುಕೆಯಲ್ಲಿ, ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ಅದು ಕಾಳಜಿವಹಿಸುವವರಿಗೆ ಪ್ರವೇಶಿಸಬಹುದು ಎಂದು ಖಾತ್ರಿಪಡಿಸಿಕೊಳ್ಳಲು ಡಾಟಾ ಪ್ರೊಟೆಕ್ಷನ್ ಆಕ್ಟ್ ಅನ್ನು ಬಳಸಿಕೊಳ್ಳಲಾಗುತ್ತದೆ, ಮತ್ತು ದೋಷಪೂರಿತವಾಗಿದ್ದರೆ ವ್ಯಕ್ತಿಗಳಿಗೆ ಪರಿಹಾರವನ್ನು ಒದಗಿಸುತ್ತದೆ. [8] ವ್ಯಕ್ತಿಗಳು ಸರಿಯಾಗಿ ಪರಿಗಣಿಸಬೇಕೆಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಇದು ಮುಖ್ಯವಾಗಿದೆ, ಉದಾಹರಣೆಗೆ ಕ್ರೆಡಿಟ್ ತಪಾಸಣೆ ಉದ್ದೇಶಗಳಿಗಾಗಿ. ಕಾನೂನುಬದ್ಧ ಮತ್ತು ಕಾನೂನುಬದ್ಧ ಕಾರಣಗಳಿಗಾಗಿ ವ್ಯಕ್ತಿಗಳು ಮತ್ತು ಕಂಪನಿಗಳು ಮಾತ್ರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಬಹುದು ಮತ್ತು ಹಂಚಿಕೊಳ್ಳಲಾಗುವುದಿಲ್ಲ ಎಂದು ಡೇಟಾ ಪ್ರೊಟೆಕ್ಷನ್ ಆಕ್ಟ್ ಹೇಳುತ್ತದೆ. ಡಾಟಾ ಗೌಪ್ಯತಾ ದಿನವು ಯುರೋಪ್ ಕೌನ್ಸಿಲ್ನಿಂದ ಜನವರಿ 28 ರಂದು ನಡೆಯುವ ಅಂತರಾಷ್ಟ್ರೀಯ ರಜೆಯಾಗಿದೆ

ಯುರೋಪಿಯನ್ ಯೂನಿಯನ್ (ಇಯು) ನ ಸಾಮಾನ್ಯ ಡೇಟಾ ಪ್ರೊಟೆಕ್ಷನ್ ರೆಗ್ಯುಲೇಷನ್ (ಇಡಿ) 2018 ರ ಮೇ 25 ರಂದು ಕಾನೂನಾಗಿ ಮಾರ್ಪಟ್ಟಾಗಿನಿಂದ, ಸಂಸ್ಥೆಗಳು ನಿಯಮಾವಳಿಗಳಿಗೆ ಅನುಗುಣವಾಗಿಲ್ಲದಿದ್ದರೆ € 20 ದಶಲಕ್ಷಕ್ಕೆ ಅಥವಾ ಅವರ ವಾರ್ಷಿಕ ಆದಾಯದ 4% ನಷ್ಟು ಗಮನಾರ್ಹ ಪೆನಾಲ್ಟಿಗಳನ್ನು ಎದುರಿಸಬಹುದು. [10] GDPR ಸಂಸ್ಥೆಗಳು ತಮ್ಮ ಡೇಟಾ ಗೌಪ್ಯತೆ ಅಪಾಯಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳಲು ಒತ್ತಾಯಿಸುತ್ತದೆ ಮತ್ತು ಗ್ರಾಹಕರ ಖಾಸಗಿ ಮಾಹಿತಿಯ ಅನಧಿಕೃತ ಬಹಿರಂಗಪಡಿಸುವಿಕೆಯ ಅಪಾಯವನ್ನು ತಗ್ಗಿಸಲು ಸರಿಯಾದ ಕ್ರಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳುತ್ತದೆ.

ಅಂತರಾಷ್ಟ್ರೀಯ ಮಾನದಂಡಗಳು:

ಅಂತರಾಷ್ಟ್ರೀಯ ಮಾನದಂಡಗಳು ಐಎಸ್ಒ / ಐಇಸಿ 27001: 2013 ಮತ್ತು ಐಎಸ್ಒ / ಐಇಸಿ 27002: 2013 ಮಾಹಿತಿ ಭದ್ರತೆಯ ವಿಷಯದಡಿಯಲ್ಲಿ ಮಾಹಿತಿ ಭದ್ರತೆಯನ್ನು ಒಳಗೊಳ್ಳುತ್ತದೆ, ಮತ್ತು ಅದರ ಕಾರ್ಡಿನಲ್ ತತ್ವಗಳೆಂದರೆ ಎಲ್ಲಾ ಶೇಖರಿಸಿದ ಮಾಹಿತಿ, ಅಂದರೆ ಡೇಟಾ, ಆ ಡೇಟಾವನ್ನು ಪ್ರವೇಶಿಸಲು ಮತ್ತು ನಿಯಂತ್ರಿಸಲು ಇದು ಜವಾಬ್ದಾರಿ. ಕಂಪ್ಯೂಟಿಂಗ್ ಭದ್ರತೆಯನ್ನು ಬಲಪಡಿಸಲು ಮತ್ತು ಪ್ರಮಾಣೀಕರಿಸಲು ಸಹಾಯ ಮಾಡುವ ಸಂಸ್ಥೆಗಳ ಉದಾಹರಣೆಗಳಾಗಿವೆ.

ವಿಶ್ವಾಸಾರ್ಹ ಕಂಪ್ಯೂಟಿಂಗ್ ಗ್ರೂಪ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಭದ್ರತಾ ತಂತ್ರಜ್ಞಾನಗಳನ್ನು ಪ್ರಮಾಣೀಕರಿಸುವ ಒಂದು ಸಂಸ್ಥೆಯಾಗಿದೆ. ಪೇಮೆಂಟ್ ಕಾರ್ಡ್ ಇಂಡಸ್ಟ್ರಿ ಡಾಟಾ ಸೆಕ್ಯುರಿಟಿ ಸ್ಟ್ಯಾಂಡರ್ಡ್ ಪ್ರಮುಖ ಡೆಬಿಟ್, ಕ್ರೆಡಿಟ್, ಪ್ರಿಪೇಡ್, ಇ-ಪರ್ಸ್, ಎಟಿಎಂ ಮತ್ತು ಪಿಓಎಸ್ (ಪಾಯಿಂಟ್ ಆಫ್ ಮಾರಾಟ) ಕಾರ್ಡುಗಳಿಗೆ ಕಾರ್ಡ್ ಹೊಂದಿರುವವರ ಮಾಹಿತಿಯನ್ನು ನಿರ್ವಹಿಸುವ ಸಂಸ್ಥೆಗಳಿಗೆ ಸ್ವಾಮ್ಯದ ಅಂತರರಾಷ್ಟ್ರೀಯ ಮಾಹಿತಿ ಭದ್ರತಾ ಮಾನದಂಡವಾಗಿದೆ.

ಯುರೋಪಿಯನ್ ಕಮಿಷನ್ ಪ್ರಸ್ತಾಪಿಸಿದ ಜನರಲ್ ಡಾಟಾ ಪ್ರೊಟೆಕ್ಷನ್ ರೆಗ್ಯುಲೇಷನ್ (ಜಿಡಿಪಿಆರ್) ಯುರೋಪಿಯನ್ ಒಕ್ಕೂಟದ (ಇಯು) ವ್ಯಕ್ತಿಗಳಿಗೆ ಮಾಹಿತಿ ರಕ್ಷಣೆಗಾಗಿ ಬಲಪಡಿಸುತ್ತದೆ ಮತ್ತು ಏಕೀಕರಿಸುತ್ತದೆ, ಇಯು ಹೊರಗಿನ ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ರಫ್ತು ಮಾಡುವ ಉದ್ದೇಶದಿಂದ.