Impero

Connect
Fast, Secure Remote Access

GDPR Compliance Checklist

Make sure your remote support solution satisfies the most stringent General Data Protection Regulation standards with Impero Connect.

GDPR Security Requirements

How Connect Ensures Compliance

Lawful processing must

(a) be consented to by the subject for the stated purpose; (b) be required by a contract; (c) be necessary for other compliance reasons; (d) be necessary to protect someone's vital interests; (e) be required for public interest or an official authority. (Article 6, Recitals: 40-50)

Demonstrating consent

Consent must be informed, freely given, and adequately documented to achieve compliance. The data subject should be able to withdraw consent easily at any time. (Article 7, Recitals: 32, 33, 42, 43)

The Access Security settings of a deployed Impero Connect Guest include a **Confirm Access feature**. This requires the end user to approve a remote session before a connection can be established. The Confirm Access option displays a screen prompt that is customizable and that notifies the end user of a remote session and also documents their consent.

Impero's Confirm Access option is suitable for attended and unattended devices. If no user is logged on to the device, the access confirmation prompt is not delivered.

Impero Connect also provides **Connection Notifications** that can alert the user of a remote session. Connection Notifications are available upon, during and after the connection to provide the user a full picture of any data processing.

Data minimization

• Personal data must be: (a) processed lawfully, fairly and transparently; (b) collected for specified, explicit and legitimate purposes only; (c) adequate, relevant and limited; (d) accurate; (e) kept no longer than needed; (f) processed securely to ensure its integrity and confidentiality. (Article 5, Recital: 39)

• Taking account of risks, costs and benefits, there should be adequate protection for personal info by design, and by default. (Article 25, Recital: 78)

Impero Connect provides several options for Data Minimization:

• **Host Name:** Users can enter custom text (that can be pseudonymized), use environmental variables, or leave the hostname field blank depending on the needs of the organization.

• **Directory Integration:** Netop Remote Control integrates with AD or LDAP, allowing organizations to centrally manage user authentication and minimize local storage of user data.

• **Phonebook Files:** Users can save connection information of remote devices as a record for later use. These phonebook files can be stored locally or on a network share used by multiple Guest users. By sharing quick access records in a single network location, fast and efficient access is maintained while personal data storage is minimized to a single managed location.

• Organizations must implement, operate and maintain appropriate technical and organizational security measures for personal info, addressing the information risks. (Article 32, Recitals: 74-77, 83)

• **Event Logging:** Over 100 different remote session related events can be logged with Impero Connect. Event logging is not mandatory, but is widely considered a security best practice. The Impero Connect administrator chooses which events to log depending on the specific device, user and circumstance.

• **Log Location:** Events can be logged centrally or locally, sent to a Windows event log or collected via SNMP traps. Event logging can be directed to the appropriate location based on the event type, allowing the administrator to minimize the data stored in any one location and avoid unnecessary duplication.

Data security

• Taking account of risks, costs and benefits, there should be adequate protection for personal info by design, and by default. (Article 25, Recital: 78)

• Organizations must implement, operate and maintain appropriate technical and organizational security measures (such as encryption, anonymization and resilience) covering data confidentiality, integrity and availability aspects.
(Article 32, Recitals: 74-77, 83)

Impero Connect follows four key principles to achieve security:

• **Encrypt from Point To Point:** Sensitive information is encrypted during transmission and while at rest. Modern ciphers and hashing mechanisms are used for data transmission, credentials, and information stored within local settings.

• **Manage User Access:** Access is managed using end-point authentication: users are authenticated on each end-point for each session. This includes access to local settings as well as connections to remote devices.

• **Manage User Permissions:** Once authenticated, user and user group permissions are restricted at a granular level.

• **Document What Happens:** Impero Connect provides comprehensive audit trails including logging, video recording and custom reporting. This means at any given time administrators can account for what happened and who performed which action.

Rights of access & portability

• The principles of transparency and accountability require organizations to clearly establish why data is processed, when it is processed, and who is doing the processing.
(Articles 15 to 22, Recitals: 63, 64, 67, 68)

The Impero Connect Security Server provides centralized, protected storage of security roles and logs. Event logs can be exported in industry standard file formats. Video recordings stored in Impero's proprietary format can be centrally stored and made available for review to comply with GDPR regulations.

Impero Phonebook files can be stored on a shared network drive space. By eliminating local storage of these quick access records, organizations follow data minimization principles and provide easier access and portability.

Rights of specification & erasure

• The right of access and portability is extended by the right to have inaccurate data corrected, and to have personal data deleted in its entirety once it is no longer needed or if requested by the data subject.
(Article 16, 17, 19, Recitals: 65, 66)