SECURITY PAPER

NETOP Remote Control

Making Remote Support GDPR Compliant: A Complete Guide

Table of Contents

INTRO/EXECUTIVE SUMMARY 1

MATERIAL SCOPE OF THE REGULATION 2

TERRITORIAL SCOPE OF THE REGULATION 2

KEY QUESTIONS 3

WHY IS PERSONAL DATA BEING PROCESSED? 3

WHEN IS PERSONAL DATA BEING PROCESSED? 4

WHAT IS THE IMPACT OF PROCESSING PERSONAL DATA? 5

HAS CONSENT TO PROCESS PERSONAL DATA BEEN GIVEN? 6

HOW IS PERSONAL DATA BEING PROCESSED? 6

DATA BREACH NOTIFICATIONS 9

PENALTIES 10

CONCLUSION 10

ABOUT NETOP 10

Intro / Executive Summary

The EU General Data Protection Regulation (GDPR) will go into effect on May 25, 2018. The Regulation will have a significant impact on organizations operating within the European Union and will likely require substantial changes to standard operating procedures.

The focus of the Regulation is the processing of personal data. Given the definitions of the EU Parliament and EU Council, it is clear the use of remote control software falls within the material scope of the Regulation.

The GDPR is also broad in defining the territorial scope of the Regulations. Organizations operating within the EU are obviously affected, but given the nature of modern computer networks, even organizations engaged in relatively minor interactions with EU citizens will need to comply with these Regulations.

This document focuses specifically on the relation of the GDPR to the use of remote control software and seeks to identify the regulations relevant to using it in a compliant manner. Organizations should ask several key questions to ensure their compliance with the Regulation:

Why is personal data being processed? When determining why personal data is processed, the GDPR mandates extensive documentation. The principles of transparency and accountability are required to ensure data subjects understand their rights and that organizations comply with the Regulation.

When is personal data being processed? It is vital organizations understand when personal data is processed. With remote control software, data is processed in one or more of the following circumstances: the graphical user interface, within configuration files & settings, during the transmission of data, and whenever log files or audit records are generated.

What is the impact of the processing? The impact of processing personal data must be understood for an organization to comply with the GDPR. The controls and procedures used with remote control software should be evaluated in relation to the risk to data subjects. The GDPR provides a clear preference for the rights of data subjects, defining potential impacts and consequences in very broad terms.

Has consent to process personal data been received? To comply with the GDPR, consent must be informed, freely given and documented. To meet this burden, organizations should present their rationale for using remote control and choose a tool that provides clear notifications with options for capturing and documenting the consent of data subjects.

How is personal data being processed? The GDPR lays out recommendations and requirements for how personal data should be processed. Key elements include:

- **DATA MINIMIZATION** - Organizations should limit what data they process and only store what is necessary. For remote control software, minimizing duplication of data through integration with directory services is recommended.
- **DATA SECURITY** - Protecting personal data requires appropriate security measures. Remote control software should include encryption of data while in transit and at rest, robust access rights and user permissions, event logging, and high availability and disaster recovery options.
- **RIGHT TO BE FORGOTTEN** - Data subjects must have a right to rectify erroneous information or have it deleted completely. Remote control tools should include options that facilitate these rights.
- **DATA BREACH NOTIFICATION** - In the event of a data breach, the GDPR requires specific notifications to supervisory authorities and possibly to data subjects.

While the GDPR allows for exceptions to many of the obligations imposed on organizations, preference is given to the rights of the data subject.

Failure to comply with the Regulation may result in significant damages including administrative fines, penalties, compensation to individuals and the loss of reputation.

Material Scope of the Regulation

Article 1 of the GDPR establishes the material scope of the Regulation as "the processing of personal data wholly or partly by automated means." Article 4 provides these definitions:

- **PERSONAL DATA** - Any information relating to an identified or identifiable natural person (data subject) including internet protocol addresses, cookie identifiers, or other identifiers
- **PROCESSING** - Any operation or set of operations which is performed on personal data. Including, but not limited to collection, recording, storage, use, disclosure by transmission, dissemination or otherwise making the data available

Remote control software relies on the transfer of electronic data between two or more endpoints and the presentation of that data through a graphical user interface (GUI). The data may include information about users (e.g., username, user alias, security role, domain name) and the devices they are connected with (e.g., IP address, MAC address, device name, hostname).

Within most remote control software solutions, user data is associated with device data in a number of ways, for example identifying specific users and devices on a network. Much of the data used to initiate and conduct a remote session is preserved within the application to simplify connections or to enhance security. Additionally, remote control data is often preserved as part of the logging and auditing capabilities of the solution.

When an organization uses remote control software, it is extremely likely they fall within the material scope of the GDPR. Exactly what constitutes the processing of personal data by remote control software is discussed in more detail later in this paper.

Territorial Scope of the Regulation

Article 3 defines the territorial scope of the Regulation very broadly and includes the processing of personal data from EU member states regardless of whether the data was collected within the EU. In the context of remote control, you should assume the Regulation applies when:

- Any of the users, devices, or software modules involved in a remote control session are located in an EU member state, or could reasonably be assumed to be located in an EU member state in the future
- Any of the databases or shared drive spaces used as part of the deployment of the remote control software are located in an EU member state
- Any data used by, generated by, or collected during a remote control session (such as directory information, log files, or configuration files) are stored in an EU member state, or could reasonably be assumed to be shared with an entity in an EU member state in the future

Organizations should pay careful attention to their deployment of remote control technologies. Even those organizations with limited contact with the citizens of EU member states will be affected by the Regulations. Remote control software is designed to communicate over large distances - including international borders. Data in the form of analytics, logs, audit records, and directory information is easily and quickly moved from endpoint to endpoint in a modern network. Knowing where data is stored and where it is shared is a critical concern for organizations looking to comply with the GDPR.

Key Questions

To comply with the GDPR, organizations will need to deploy a combination of technology and policy that answers five (5) key questions:

1. Why is personal data being processed?
2. When is personal data being processed?
3. What is the impact of the processing?
4. Has consent to process personal data been received?
5. How is personal data being processed?

Why is personal data being processed?

The GDPR requires organizations to document the reasons for processing personal data with transparency and accountability.

Transparency

The principle of transparency is invoked throughout the GDPR to ensure that data subjects clearly understand why their data is being processed. Regulations require clear, easy to understand language whenever communicating with individuals or the public. Notifications and documentation should be provided in a format that is easy to access and understand.

The principle of transparency is referenced throughout the GDPR and applies to when and how data is processed as well. Data subjects must be notified in advance of their data being processed. For remote control software, organizations need clear documentation of why remote control is used, what context or set of conditions necessitates use, the personal data processed by use, and finally how the data subject can erase any personal data that is processed.

Accountability

While the principle of transparency requires advance notification, the principle of accountability requires proof that policies and procedures are followed. The GDPR holds organizations accountable for documenting policies in advance, processing data in a lawful manner, and documenting that processing was completed in a compliant manner. For remote control software, it is important for organizations to document which individuals were involved in a remote control session, the endpoints, and the data that was processed.

Netop Remote Control provides robust event logging and session recording options. Logs and audit trails of over 100 different remote control related events can be stored locally or centrally.

When is personal data being processed?

The GDPR defines the processing of personal data in the broadest sense possible. Consider that the following elements may include processing of personal data when using remote control software:

- **GRAPHICAL USER INTERFACE** - Data presented in the remote control GUI that identifies individuals and data that identifies a device associated with an individual qualify as data processing. Any information presented during a screen-sharing session that includes personal identifiers also qualifies as data processing.
- **CONFIGURATION FILES & SETTINGS** - The storage and preservation of electronic data also qualify as data processing because it is likely that configuration files and internal settings include personal data. For example: IP addresses, hostnames or MAC addresses stored to facilitate quick access to a remote device; usernames, credentials and personal data stored to make login more efficient on the local (or remote) device.
- **DATA TRANSMISSION** - Transmission of data qualifies as processing. Transmission of an IP address, hostname, username or other identifying data used for authentication and/or authorization of a remote control session qualifies as the processing of personal data.
- **INTEGRATED FEATURES** - The primary feature of most remote control tools is transmission of keyboard, video and mouse (KVM) data between remote devices. In addition to KVM, most remote control software tools include additional features like file transfer and chat.
    - KVM - A screen sharing session would constitute processing if personal data is displayed on the screen of remote device.
    - File transfer - This will constitute the processing of personal data if the files in question contain personal data.
    - Chat - The transfer of audio, video or text based chat is almost by definition the processing of personal data. Additional processing takes place if chat data is saved or archived.
- **LOGS & AUDIT RECORDS** - A variety of industry and government regulations (e.g. ISO 27002, PCI-DSS) require usage logs for users and administrators. Creating and maintaining logs is a data security best practice and may be specifically required to achieve compliance with standards and regulations. Audit logs for administrators or users of remote control will likely contain personal data including identification of users, devices, date and time of usage, and possible indicators of the geo-location of user or device.

The relationship between devices of a remote control session is another consideration for determining when personal data is processed.

"Personal data protection rules do not apply solely to the remote user or device; personal data of helpdesk technicians or whoever initiates a remote session must be protected as well."

Remote Control to an Attended Device

Processing of personal data is unavoidable when initiating a remote control session to a device with an identified user. To facilitate the connection, the remote device must be identified via username, IP address, hostname, or alias of some kind in the GUI.
The remote control session may require the user to be authenticated and/or to transmit address data and authentication information.

Remote Control to an Unattended Device

“ If an organization is using remote control, they are likely processing personal data in multiple ways.”

The management of servers and other devices where no personal data is present and no identifiable user is associated is a frequent use case for remote control. However, personal data protection rules still apply if an identifiable person conducts the remote session. Personal data protection rules do not apply solely to the remote user or device; personal data of helpdesk technicians or whoever initiates a remote session must be protected as well.

A discussion of all possible remote control use cases and scenarios would be impractical. It should suffice to say that if an organization is using remote control, they are likely processing personal data in multiple ways.

What is the impact of processing personal data?

Once you have identified the reason for processing personal data, and have determined when processing will occur, an assessment of the impact should be completed prior to any processing activities. Determining the risk of processing personal data provides necessary context for how the data should be handled and which safeguards are necessary.

The GDPR does not provide a concrete methodology for determining risk, but the guidance for establishing potential impacts and consequences is very broad. Physical, material and non-material impacts on the freedom, security, and well being of data subjects must be considered.

The processing of personal data through remote control software has the potential for high risk to data subjects. An obvious example of high risk use is providing an individual with the ability to view sensitive personal data (such as financial or health-related information) stored on a remote device. The transmission of that personal data and presentation via the remote control GUI clearly qualifies as high-risk processing of personal data. Additionally, risk is present in logging that remote session. Those log files indicate work performance and may identify the personal location of the individual who initiated the remote session.

Given how broadly terms and risks are defined by the Regulations, treating remote control as a high-risk processing activity is advised for most organizations.

Has consent to process personal data been given?

The GDPR requires organizations to receive consent before processing personal data in all but a few limited instances. Consent must be informed, freely given, and adequately documented to achieve compliance. Additional rules and regulations apply if you are dealing with the personal data of children under the age of 16.

Organizations must notify data subjects of when, how and what data will be processed to ensure consent is informed. Notification can be presented to data subjects in a variety of ways, including on-screen prompts, oral conversations, and written documents or contracts. Notification must be presented in a clear, easily understood manner.

For consent to be freely given, the data subject must have the option of revoking permission. The “freely given” burden is not met if the data subject does not have the ability to withdraw consent as easily as they have given it.

Furthermore, the GDPR is clear that data subjects should not be required to provide blanket-consent for all types of data processing or to the processing of all personal data. Recital 43 states:

> *“Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.”*

Netop recommends organizations include language in their published policies and contracts that describes the circumstances when remote control will be used, the purpose of remote control, and what personal data is processed during and after a remote control session.

In addition to language in published documents, Netop recommends Connection Notifications that will alert data subjects of inbound remote sessions. A mechanism for data subjects to refuse remote control sessions or terminate sessions in progress is also recommended.

Documentation is an integral part of the consent requirements. The burden of proof is placed on the organization processing the data. The GDPR requires that documentation include how data subjects were notified as well as how the consent was received.

The Access Security settings of a deployed Netop Remote Control Host 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 customizable screen prompt that notifies the end user of a remote session and also documents their consent.

Netop Remote Control provides a variety of 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.

How is personal data being processed?

While there are specific actions proscribed by the GDPR, the totality of the regulations describe an approach to personal data rather than a simple list of rules. The approach is informed by principles on how personal data should be processed. Those principles include:

Data Minimization

The principle of data minimization requires organizations to collect only data that is needed and to store personal data for the least amount of time necessary. Your remote control strategy should consider:

- **PURPOSE LIMITATION** - Only collect data that is necessary to the specific task. Consider what is necessary to identify users and devices. If specific data is being captured on users via other means (e.g., user profile information), capturing that data via your remote control tool is redundant and as a result does not comply with the GDPR. Tools that allow you to integrate with a separate directory service for authentication and user management can minimize personal data used within the remote control tool and simplify compliance efforts.
- **STORAGE LIMITATION** - Only store personal data for as long as is necessary. If settings and configurations contain personal data, they must be actively managed to ensure all user information is up to date. Organizations have a variety of reasons to retain event logs and audit records. Preservation of data is required in some instances by other regulations and/or best practices. Organizations should include storage of event logs and access records in their data retention policies and ensure those policies are applied internally by deleting any data that is no longer relevant or necessary.

NETOP REMOTE CONTROL PROVIDES A NUMBER OF OPTIONS FOR DATA MINIMALIZATION:

Host Name - Users have the ability to 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 file - 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.

Events logging - Over 100 different remote session related events can be logged with Netop Remote Control. Event logging is not mandatory, but is widely considered a security best practice. Logging is turned off by default, requiring the Netop Remote Control administrator to choose only those events relevant to the specific device, user and circumstances.

Log location - Events can be logged locally, centrally, 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

The GDPR requires “a level of security appropriate to the risk” for the processing of personal data with consideration given to the state of existing technologies and their cost relative to perceived risks. Several Articles and Recitals provide guidance on determining how “appropriate” is defined, but few concrete proscriptions are included. Conducting a formal data protection impact assessment will allow an organization to document risk and establish “appropriate” mechanisms to mitigate that risk.

The GDPR includes a mechanism for creating approved codes of conduct and certification mechanisms at the Union level. Until those codes and certifications are available, consider the following specific recommendations and how they apply to remote control:

- **ENCRYPTION** - The GDPR specifically mentions encryption as a security mechanism appropriate for processing personal data. While most remote control tools provide encryption in some fashion, state of the art techniques now provide for end-to-end encryption of data in transit as well as encryption of data at rest. For remote control this should include not only the data stream between endpoints, but encryption of any area where personal data processing occurs – including configurations, settings and log files.
- **ACCESS RESTRICTIONS** - Only individuals with a legitimate interest should have access to personal data. Additional requirements mandate that data be processed with an awareness of the difference between data sets and the respective mechanisms by which they are processed. Organizations are encouraged to select tools with role based and/or attribute based access controls to ensure a level of granularity in access restrictions is available.

  In addition to granular access controls, organizations should consider tools with equally granular controls over user permissions. For example, allowing an individual user (or group of users) to access a device via screen sharing or KVM, while restricting the ability to change the remote device’s configuration settings or access remote control event logs.

- **LOGGING AND AUDIT RECORDS** - The GDPR does not specifically mention logging, but security best practices and compliance with international standards like ISO 27002 or PCI-DSS require audit logs when using remote control tools. Organizations should assume audit logging will be a requirement to achieve "a level of security appropriate to the risk." Logs should include records of the users who accessed remote equipment. In addition, administrator activity should be logged to provide full audit records of how the network environment is managed.
- **AVAILABILITY AND RESILIENCE** - Requirements for high availability and disaster recovery (HADR) play a prominent role in achieving data security and protection. If an organization uses remote control software, HADR requirements should be considered for the operation of the software and for the data it generates or processes. For example, does the remote control software include features and capabilities appropriate for HADR; can settings be quickly recreated in the event of accidental destruction, loss or alteration? Similarly, are there adequate capabilities to ensure authorized users have consistent access to the personal data stored in event logs and audit records?

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. The right of access makes these principles tangible to the data subject by requiring they have the ability to review all the records related to the processing of their personal data. This includes the required documentation, records of processing activity, who did the processing and a review of the data itself.

Netop recommends the centralization of personal data whenever possible to simplify the process of managing, documenting and auditing the data. The benefit of centralized storage of personal data increases with the number and distribution of discrete data points. For organizations using remote control software, the personal data of a single subject may be spread across tens or even thousands of different devices. Considering the need to provide individuals access to their personal data, compliance with the GDPR is dramatically simplified through centralization.

Not only should personal data be accessible for review, but it must be made available to the data subject for export and/or transport. The right of portability requires data be presented in a commonly used format and be made available to the data subject directly, or transferred to another organization designated by the data subject.

Within this context, personal data generated by remote control tools (e.g., event logs or program settings) should be stored in a manner that isolates the personal data of discrete data subjects. Not all remote control tools provide the ability to filter data in a way that isolates a single data subject, but many do. As the state of the art in remote control technology evolves, reliance on tools with limited feature sets will become more problematic to regulators and supervisory agencies.

Rights of Rectification & 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. The right to erasure, also known as the right to be forgotten, furthers the principle of data minimization by adding the right of an individual data subject to engage in the process. If a data subject requests personal data be erased prior to the timeframe identified by an organization, their wishes should be followed

WHEN PROPERLY APPLIED, NETOP REMOTE CONTROL IS THE MOST SECURE REMOTE CONTROL SOFTWARE SOLUTION ON THE MARKET. NETOP 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 - Netop Remote Control 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.

For a full description of the security controls available in Netop Remote Control, visit www.netop.com/remotesupport/benefits/security

Netop Remote Control security roles and log files can be saved in an ODBC compliant database. Organizations are encouraged to store their data in an environment designed for HADR

Furthermore, Netop Remote Control provides integration with Intel VPRO technology, giving support technicians unrivaled access and control in disaster recovery situations.

without undue delay. Organizations using remote control software will likely store personal data in multiple locations for different reasons. As already noted, storing data in a manner that allows for filtering or isolation of individual data subjects will be required to comply with these regulations.

Overriding Legitimate Interest

It is likely scenarios will occur where regulations and requirements conflict. Consider the requirements for data security, data minimization and the right to be forgotten. Best practices for achieving data security require access records and remote session events be recorded and logged. Organizations may be bound by internal policy and industry or governmental regulations to store data for a proscribed period. If an individual requests erasure of their personal data, an organization will need to balance conflicting requirements.

The GDPR anticipates these types of conflicts, allowing organizations to provide overriding legitimate grounds for prioritizing one regulation over another. In the above example, if an individual requests erasure of their personal data, an organization may provide an overriding legitimate interest in storing log files to maintain compliance with a separate industry regulation. In this instance, overriding interests may not apply to storing personal data in product settings or configurations. This is yet another vital reason for organizations to develop an understanding of where and how personal data is processed. The requirement for purpose limitation in processing means overriding legitimate interest cannot be used as a blanket get-out-of-jail-free card.

The Netop 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 Netop's proprietary format can be centrally stored and made available for review to comply with GDPR regulations.

Netop 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.

Data Breach Notifications

In addition to providing rules and guidance on how to process personal data, the GDPR requires notifications when personal data is compromised. A personal data breach is defined as:

> *" A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

When an organization becomes aware of a personal data breach, they have no more than 72 hours to report the breach to the appropriate supervisory authority unless the organization can demonstrate the breach provides no risk to personal rights or freedoms. As indicated earlier, data breaches involving remote control software will likely involve a level of risk that triggers the notification requirement.

Notification to individual data subjects is also required for personal data breaches. However, as with the requirement to notify supervisory authorities, the requirement to notify individual data subjects depends on assessed risk. Organizations that have taken appropriate measures to secure personal data, such as through the use of encryption, may not be required to notify individual data subjects.

Penalties

Failure to comply with the GDPR may result in compensation of damages to individuals, administrative fines assessed by the European Union, and penalties assessed by individual EU member states.

Right to Compensation

Organizations involved in the processing of personal data are held liable for any material or non-material damages suffered by an individual as the result of non-compliance with the GDPR. The Regulations stipulate that damages be broadly interpreted so that maximum compensation be provided to individuals.

Administrative Fines

Fines for intentional or negligent infringement of the Regulations may be imposed for up to:

- 20.000.000 EUR
- or 4% of the total worldwide annual turnover of the preceding financial year

Penalties

The GDPR encourages EU member states to develop penalties for infringements not specified by the Regulations or covered by the administrative fines. Because the penalties have yet to be created by individual EU member states, their nature and severity are unknown at this time.

In addition to individual compensation, administrative fines, and penalties, organizations face the risk of damage to their reputation from non-compliance. The GDPR includes a notification requirement when a breach of personal data occurs. History and experience demonstrate that when data breaches are publicized, public sentiment changes and litigation ensues.

Conclusion

For a specific piece of personal data, an organization's GDPR journey begins with determining why data is being processed. Establishing consent and addressing how the data is processed follows, but the journey doesn't end there. If personal data is stored in any way, data subjects are afforded specific rights to access that data and request it be corrected or deleted. While the GDPR allows for exceptions to many of the obligations imposed on organizations, preference is clearly given to the rights of the data subject.

This document should not be construed as legal advice. Recommendations are provided to assist organizations with their compliance efforts but are not sufficient to ensure compliance on their own. The guidance provided in this document should be considered as part of a greater compliance effort conducted by individuals or organizations with a thorough understanding of the relevant regulations and their impact.

About Netop

Netop develops secure, all-purpose remote access software that consolidates support of remote devices, networks, and servers into one central solution. Our flagship product, Netop Remote Control, provides powerful KVM control and integrated file transfer to enterprise retailers, financial institutions and other organizations that place a high value on configuration and security.

We enable security compliance by providing superior auditing and session recording capabilities, smarter user rights management, and multiple authentication options - including native two-factor authentication. We pride ourselves on consulting closely with our customers to develop custom solutions at a price that works for them.