NETOP
Remote Control

THE ESSENTIAL GUIDE TO

GDPR Compliant Remote Access

A Netop eBook

Netop

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation goes into effect on May 25, 2018.

Comprised of 99 articles and 173 recitals, the GDPR is a combination of generic principles and specific guidelines designed to cover every possible situation involving personal data. The Regulation will have a significant impact on organizations operating within the European Union and will likely require substantial changes to standard operating procedures. Given the definitions of the EU Parliament and EU Council, it's clear the use of remote control software falls within the material scope of the Regulation.

Remote control software is everywhere. It has become an integral part of computer networks, used for installing, configuring, and maintaining the digital devices our modern lives depend on. Organizations that collect, monitor, or store personal data through remote control software will be held to a set of standards for processing it as well. This eBook 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.

Popular remote control tools VNC and TeamViewer are each installed on over

1 BILLION DEVICES

EVERY VERSION OF MICROSOFT WINDOWS

since Windows XP has included remote desktop protocol (RDP)

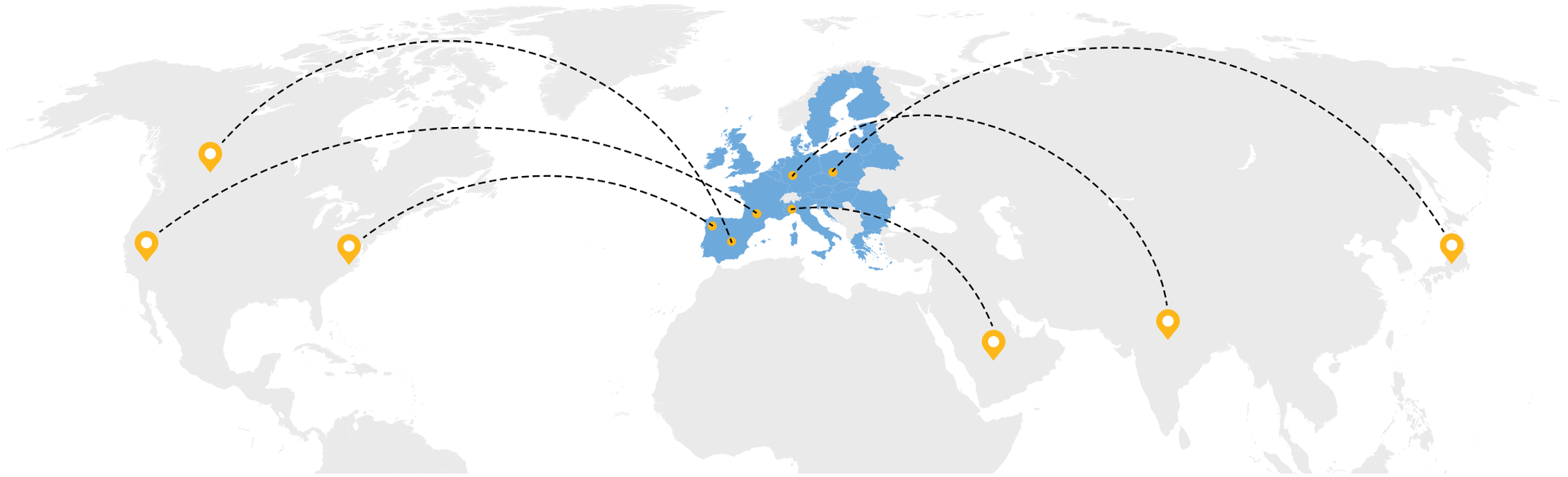
Our product, **Netop Remote Control,** is used in

80+ COUNTRIES

by half of the **world's largest banks** and a quarter of the **largest retailers**

INTRODUCTION
(CONTINUED)

The GDPR is broad in defining the territorial scope of the Regulation. 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. And the impact of the EU on the global economy can't be overlooked. The European Council estimates the EU as either the largest or second largest trade and investment partner for most countries in the global economy. The economic relationship between the US and the EU is the largest and most complex in the world. **If you live in the EU, or the US, or do business with citizens of either region, you will be impacted by this Regulation.**



$1,000,000,000,000 The US government calculates over $1 Trillion USD annually in transatlantic trade with the EU.

Organizations need to understand 5 key areas to comply with the GDPR:

WHY personal data is processed

WHEN personal data is processed

IMPACT of processing

CONSENT to process

HOW personal data is processed

1. Why personal data is 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.

2. When personal data is processed

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

3. 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.

4. Receiving consent to process personal data

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 access and choose a tool that provides clear notifications with options for capturing and documenting the consent of data subjects.

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

5. How personal data is 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.

Data Breach Notification

In the event of a data breach, the GDPR requires specific notifications to supervisory authorities and possibly to data subjects.

Right to be Forgotten

Data subjects must have the right to rectify erroneous information or have it deleted completely. Remote control tools should include options that facilitate this right.

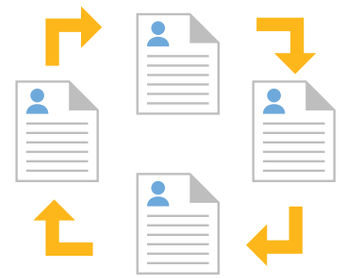
While the GDPR allows for exceptions to many of the obligations imposed on organizations, preference is given to the rights of the data subject.

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

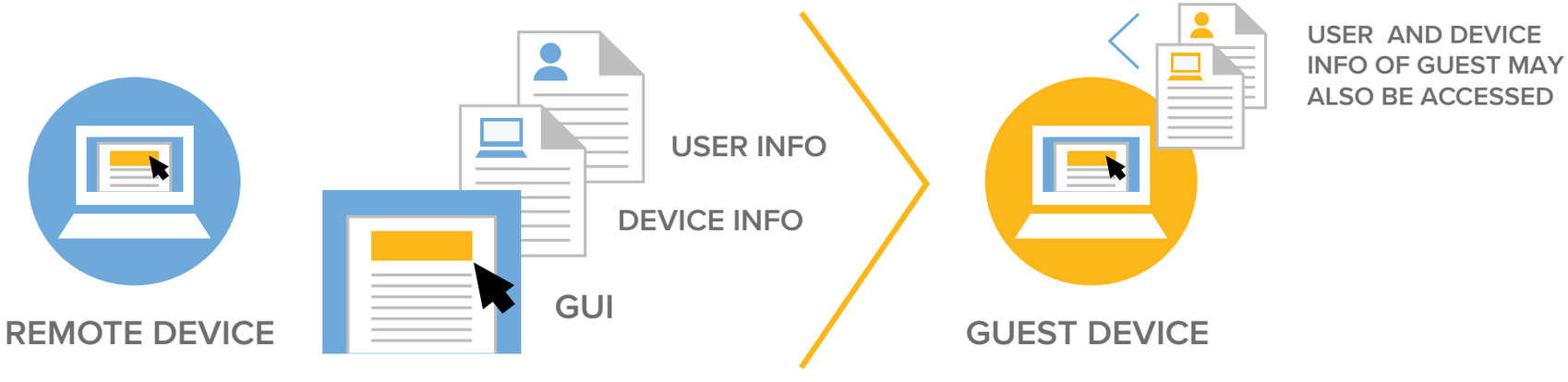
Any information relating to an identified or identifiable natural person (data subject) including internet protocol addresses, cookie identifiers, or other identifiers



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

THE SCOPE OF THE GDPR
(CONTINUED)



When an organization uses remote control software, it is processing personal data and therefore falls within the material scope of the GDPR.

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).

When you access a remote piece of equipment, server, desktop, tablet, or mobile phone, you need to consider more than what is on that device. The process controls for said equipment may not include personally identifiable information, but you must also protect the personal data of the "guest" on that device. In other words, when you allow remote access to that equipment, you are inviting an individual – along with their personal data – into the process. **Network administrators, help desk technicians, vendor representatives, and service professionals – their personal data must be protected.**

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 access data is often preserved as part of the logging and auditing capabilities of the solution.

Territorial Scope of the Regulation

The territorial scope of the Regulation includes the processing of personal data of EU citizens regardless of whether the data was collected within the EU.

In the context of remote access, you should assume the Regulation applies to the following:

Users, Devices, Software

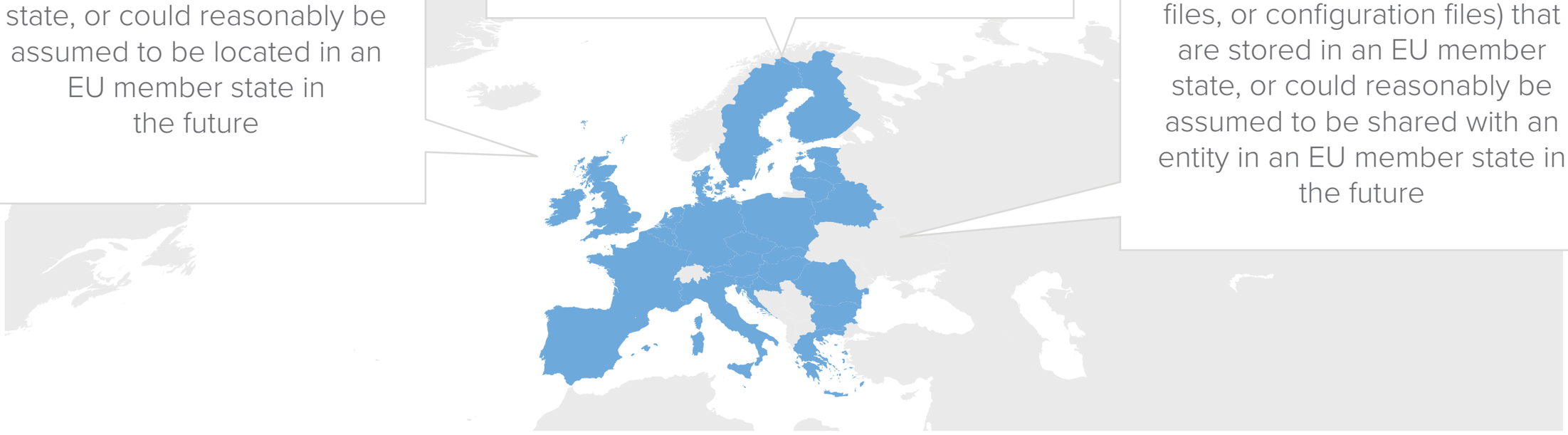
Any of the users, devices, or software modules involved in a remote control session that are located in an EU member state, or could reasonably be assumed to be located in an EU member state in the future

Databases

Any of the databases or shared drive spaces used as part of the deployment of the remote control software that are located in an EU member state

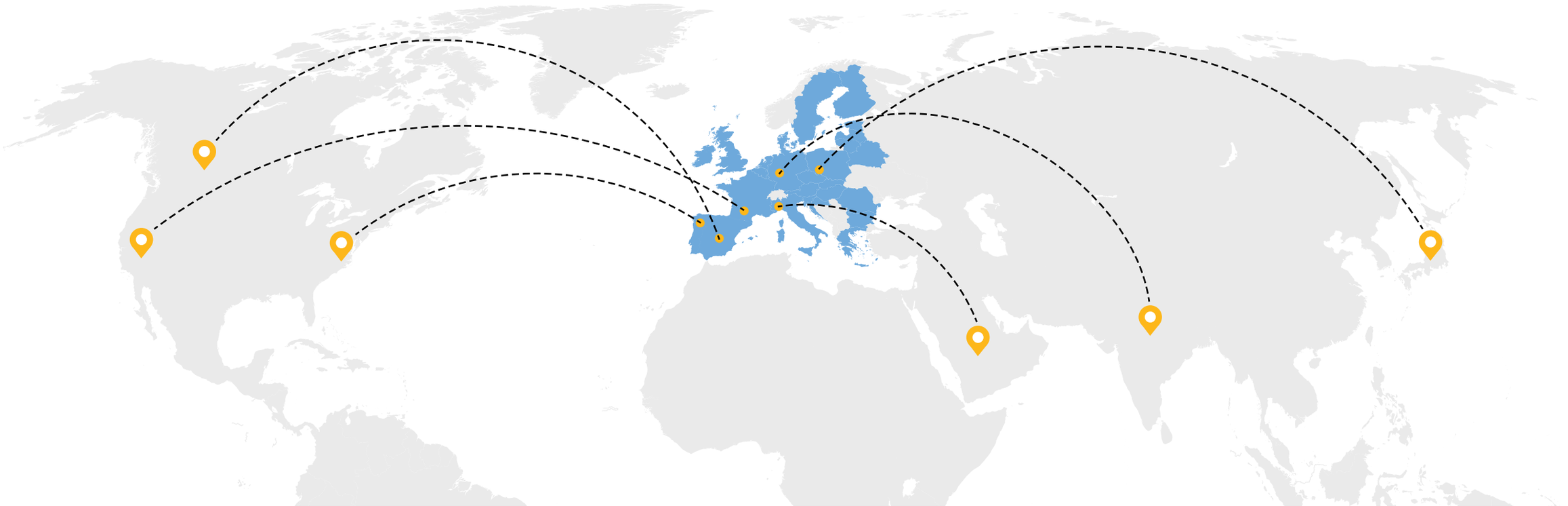
Data

Any data used by, generated by, or collected during a remote control session (such as directory information, log files, or configuration files) that 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



THE SCOPE OF THE GDPR
(CONTINUED)

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 Regulation. 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.**



WHY PERSONAL DATA IS 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 to 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

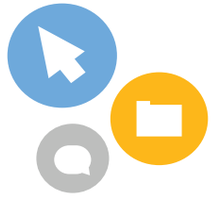
While the principle of transparency requires advance notification, the principle of accountability requires **proof that policies and procedures are followed**. The GDPR holds organizations accountable for documenting policies in advance, processing data in a lawful manner, and documenting that processing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

DID YOU KNOW

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

WHEN PERSONAL DATA IS PROCESSED

Personal data may be processed in the following areas of remote control software:



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 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.

Graphical User Interface

Data presented in the remote control GUI that identifies individuals or a device associated with an individual both qualify as data processing. Any information presented during a screen sharing session that includes personal identifiers also qualifies as data processing.

Data Transmission

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.

Configuration Files & Settings

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.

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 access will likely contain personal data including identification of users, devices, date and time of usage, and possible indicators of the geo-location of users or devices.

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

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, it is processing personal data in multiple ways.

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 Regulation, treating remote control as a high-risk processing activity is advised for most organizations.

RECEIVING CONSENT TO PROCESS PERSONAL DATA

Consent to process personal data is one of the foundations the GDPR is built upon, as it requires organizations to receive consent before processing personal data in all but a few limited instances. To achieve compliance, consent must be:

FREELY GIVEN

INFORMED AND UNAMBIGUOUS

CLEARLY DOCUMENTED

This will require significant changes to standard IT operating procedures, and the impact on human resources, sales, and marketing may also be dramatic. To comply with the GDPR, businesses need to understand how consent is handled when using remote control software.

To comply with the GDPR, you need to answer YES to each of these questions:

- Are the reasons for using remote control technologies clearly documented in your employee agreements and service contracts?
- Can individuals opt-out of remote control sessions where their personal data is processed?
- Can individuals review and remove any personal data created during or after a remote session?

Freely Given

For consent to be freely given, any imbalance of power between the two parties must be reconciled. For example, one such imbalance is the relationship between an organization and a child. If an organization intends to process the personal data of anyone under the age of 16, it must receive parental consent prior to processing.

An imbalance of power may also exist between employer and employee, or in any circumstance where a contract or service relationship exists. Consent to process personal data is not provided by the mere fact of a contract or service relationship. To be freely given, consent must be provided within the context of the specific activity where processing occurs. Data will be processed in several ways and **providing consent to one method of processing does not apply to all others.** 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.

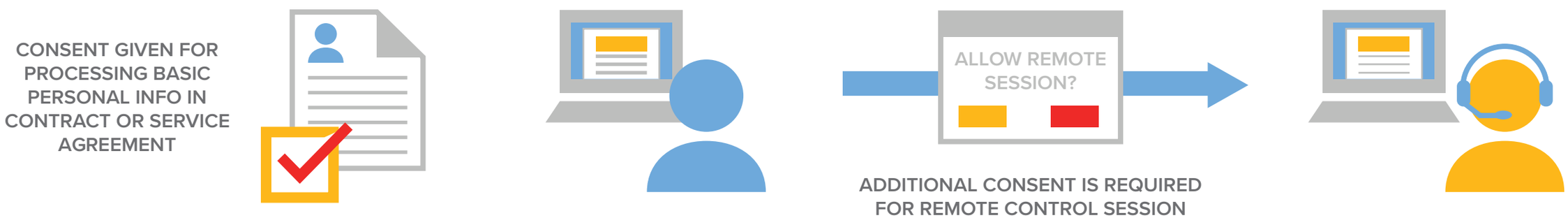
Recital 43 states:

"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."

RECEIVING CONSENT TO PROCESS PERSONAL DATA

FREELY GIVEN (CONTINUED)

Consider the example of a typical company help desk. Individuals who seek assistance from the help desk are likely covered by an employment contract (if they work for the company) or through a service contract (if they use the company to provide help-desk services).



The contract or service agreement will need to include provisions for the collection and processing of personal data like name, address, etc. If a help desk technician feels a remote access session would be useful in resolving a situation, additional details like email address and IP address may be collected to facilitate remote screen-sharing. These qualify as separate instances of personal data processing.

Freely given consent requires that data subjects can identify these separate operations of data processing even though they occur within the context of a single contract or agreement. Furthermore, consent is **not** assumed to be freely given **unless** the individual is provided a mechanism to revoke consent either prior to or during the processing activity. The “freely given” burden is not met if the data subject does not have the ability to withdraw consent as easily as they gave it.

DID YOU KNOW

Netop Remote Control includes a “confirm access” option which requires the end user to approve a remote session before the connection can be established. A customizable screen prompt notifies the end user of the session and documents their consent.

Informed & Unambiguous

The second characteristic of consent defined by the GDPR is specific, informed, and unambiguous indication. These terms reinforce the idea of contextually defined, separate occurrences of processing. Consent must be specific to each occurrence.

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.

We recommend 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**. These descriptions must be clear, easily understood, and accessible to the individuals involved in the processing.

In addition to language in published documents, Netop recommends connection notifications that will alert data subjects of inbound remote sessions. The mandate for informed and unambiguous consent also includes the mechanism to revoke consent. The GDPR requires that revoking consent be as easy as granting consent in the first place. Therefore, a mechanism for data subjects to refuse remote control sessions or terminate sessions in progress is also recommended.

Clear Affirmative Action

The third concept referenced in the description of consent is “by a statement or by a clear affirmative action.”

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.

Consent can be received by written document, oral conversation, on-screen prompts, or similar methods, but it must be documented to ensure compliance. Affirmative action requires the individual data subject to knowingly take the action – this means consent can’t be the default or automatic setting. **An individual must explicitly choose to provide consent.**

Documentation of consent should include proof the information is provided in a clear and easy to understand way and that no imbalance of power exists that would impact the data subject’s ability to freely give that consent.

78%

“Almost eight in ten respondents (78%) say it is very important personal information on their computer, smartphone or tablet can only be accessed with their permission.”

- Flash Eurobarometer 443: e-Privacy Report

HOW PERSONAL DATA IS PROCESSED

While there are specific actions proscribed by the GDPR, the totality of the Regulation describes 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**
- **Data Security**
- **Rights of Access, Portability, Rectification, and Erasure**

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 user data is being captured 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 followed internally by deleting any data that is no longer relevant or necessary.

It's best practice to adhere to purpose and storage limitation whenever possible. In terms of remote control, these principles pertain to:

- GRAPHICAL INTERFACES
- SETTINGS AND CONFIGURATION FILES
- LOGS + AUDIT RECORDS
- INTEGRATED FEATURES
  i.e. file transfer, native chat

Graphic User Interfaces

Any remote access tool that provides screen transfer and KVM (keyboard, video, and mouse) control runs the possibility of showing a remote technician everything on the user's screen during a support session. In many circumstances, this could be much more information than necessary.

Following the principle of purpose limitation, **a remote technician should only have access to the applications or area of screen necessary to complete the task at hand.** For example, if the goal of a remote support session is assisting in configuring a printer, the technician should only have access to the applications needed to do so, or the area of the screen displaying the printer driver window.

Organizations should makes sure their remote solution has capabilities to restrict or limit non-purpose driven access. There should be a mechanism in place to either alert the user to conceal all unrelated data on their monitor, offer application specific remote access, or configure area of screen access.

DID YOU KNOW?

Netop Remote Control's configuration options allow users to control which portion of the screen is transferred, enabling them to obscure sensitive information and limit access to their personal data.

Settings and Configuration Files

Businesses will often maintain a listing of users and their device settings to initiate remote sessions at the click of a button. Consider how much data is stored (i.e. processed) in these directories: user names, IP addresses, and unique device settings.

Our recommendation is to **find mechanisms to centrally store these settings and configurations whenever possible, and then restrict access as needed.** Ideally, you'll have configuration files stored on one central server, opposed to duplicating data across your endpoints which conflicts with purpose limitation. The less data stored locally across endpoints, the better.

Also, be considerate of storage limitation – businesses shouldn't store personal data any longer than necessary. Storing a configuration file for quick access to a device that you hardly ever need to support is not a recommended practice. Talk with your security and business processes teams to determine how long you absolutely need to store this information. The same is true for logs and audit records.

DID YOU KNOW?

Netop Remote Control offers "phonebook" files that store configuration and settings options for individual devices. These files can be centrally stored and set up for restricted access.

Logs and Audit Records

It's common practice to log the who, what, when, and why of support activities for billing purposes, security, efficiency, etc. But once again, these records contain personal data and must be treated with caution. Be aware of what information is logged and make sure these records are truly necessary. Just because it's possible to keep exhaustive audit trails, **doesn't mean it's a good idea**.

Work with your data compliance team to determine what information is necessary to log, how doing so is beneficial to your business, and what information is irrelevant or inappropriate to keep on file. If irrelevant data is logged on the assumption that it will be needed in the future, discontinue this practice and discard the information. Be aware of your logging activity and only record what is useful, what is relevant to the task at hand, and what is necessary to comply with other regulations.

DID YOU KNOW?

Logging in Netop Remote Control is completely customizable. Administrators can choose a variety of event characteristics to log. Different log settings can be applied to individual devices or groups of devices depending on the specific needs for that device or network environment.

Integrated Features

Many remote control solutions offer integrated features like file transfer, remote management, and native chat. Organizations should be careful not to duplicate the personal data stored in these tools across other areas of their business.

For example, let's say you have chat built into your remote solution, yet use a separate instant messaging tool for internal support as well as live chat on your website. Each of these tools may store personal data of users within that system. Ask yourself, do each of these mechanisms need to retain user names, IP addresses, and specific profile information on employees and customers across your enterprise? Or, could you **consolidate** into one tool?

Limit data processing and duplication whenever possible by centralizing the means by which you collect it.

Overriding Legitimate Interests

It is likely scenarios will occur where regulations and requirements conflict. **Businesses may need to balance the GDPR against other regulations and decide to disregard certain areas.** Consider the requirements for data minimization. Organizations may be bound by internal policy and industry or governmental regulations to store data for a proscribed period. The GDPR anticipates these types of conflicts, allowing organizations to provide overriding legitimate grounds for prioritizing one regulation over another.

If an individual requests erasure of their personal data, which we will cover in just a moment, an organization may provide an overriding legitimate interest in storing log files to maintain compliance with a separate industry regulation. 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. Work with your security team to determine if you have any overriding legitimate interests, what they are, and how they supersede the requirements of the GDPR.

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.

DID YOU KNOW?

Netop Remote Control’s data security is built on 4 principles:

1 ENCRYPT DATA
FROM POINT TO POINT

2 MANAGE USER
ACCESS

3 MANAGE USER
PERMISSIONS

4 DOCUMENT
ALL ACTIVITY

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.

Encryption and pseudonymization share many characteristics. Both techniques obscure data by replacing it with something else. The difference is encryption is designed to ensure only approved users have access to a data-set while pseudonymization allows a broader audience to access part of the data-set, obscuring only "key" fields.

Pseudonymization and encryption are techniques that can be used simultaneously or separately. The GDPR mentions both, but the guidance provided on when to choose which is minimal.

Pseudonymization

Pseudonymization is a process of replacing the identifying fields within a data-set with pseudonyms, or artificial identifiers. Information (email address, gender, nationality, location, and countless other characteristics) is replaced with an alias or code that preserves the relevance of the data while ensuring the privacy of individual data subjects.

Pseudonymization is mentioned in the GDPR 15 times and it holds a central place in the data protection by design concept. While it can be a powerful tool for protecting the privacy and security of personal data, pseudonymization has its limits, which is why the GDPR also mentions encryption.

The text of Article 32 reads:

> *"The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymization and encryption of personal data..."*

Consider the case of remote control software. Help-desk technicians use remote access to assist individuals and to manage devices. In these instances, personal information like IP address, username, and email address are necessary to facilitate connections. For remote control software to work you need to know the personal data, not an alias or code. Appropriate security in the context of remote control is not pseudonymization, it's encryption.

Organizations interested in compliance with the GDPR should embrace encryption and look for tools that incorporate encryption as part of their standard operating protocols.

60%

More than 60% of Europeans believe they should be able to encrypt some of their personal data.

- Flash Eurobarometer 443: e-Privacy Report

When using a remote control solution, personal data is likely processed:

When the screen of the remote device is presented in the graphical user interface

Within the remote control program's configuration files and settings

During the transmission of data between endpoints

Whenever log files or audit records are generated

HOW PERSONAL DATA IS PROCESSED

DATA SECURITY(CONTINUED)

To ensure your use of remote control software is compliant, you need to ensure the software encrypts the communication between endpoints (transmission of the screen, files, any data in motion) as well as the data at rest used by those endpoints (configuration files and logs).

Features integrated with basic remote control also need encryption. Files transferred between computers may contain personal data. Text, audio or video chat between a help desk technician and the remote user will contain personal data. **If you are using a comprehensive remote control tool, you need to make sure it includes comprehensive encryption that covers all the relevant elements of the software.**

Remember, the GDPR defines personal data very broadly. IP addresses, email addresses, and usernames all qualify as personal data. When those items are presented on a screen, transmitted over a network, or logged into a file they are “processed” and should be encrypted.

DID YOU KNOW

Netop Remote Control includes point-to-point encryption options. Sensitive information is encrypted during transmission and while at rest using modern ciphers and hashing mechanisms.

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 themselves 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.

DID YOU KNOW?

Netop Remote Control includes role-based access controls. Administrators can control access to devices and the user permissions on those devices, as well as create custom user roles and device groupings.

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?

DID YOU KNOW?

Netop Remote Control's comprehensive logging capabilities include video recording of screen sharing sessions, full audit logging of all administrator access, and over 100 remote session events.

Rights of Access, Portability, Rectification, and Erasure

The Right of Access

Simply put, if an organization is storing personal data, the data subject should be able to access that information.

The Right of Rectification

After a data subject has accessed their personal data and reviewed the information therein, they must be able to correct any errors.

The Right of Portability

The data subject should be able to export or move their personal data.

The Right of Erasure

Finally, the data subject has the right to erase their personal data from an organization's records.

Rights of Access and 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 can 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 and 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 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 the Regulation.

For the purposes of remote control, the rights of access, portability, rectification, and erasure really apply only to the storage of personal data, which primarily takes place in the configurations, settings, and log files. In other words, if you are storing someone's data, be it an employee or customer, it's likely you must also grant them these four rights.

Realistically, granting access to configurations and settings does not align with the fundamental aim of the GDPR. This is an instance where businesses will likely have an overriding legitimate interest. For example, granting a data subject access to their device's configuration files probably conflicts with the business's security policy, which could supersede the GDPR requirement. However, the right to be forgotten does make sense regarding remote device configuration files and settings. Whenever you're storing personal data on an employee or customer, you must be able to delete it upon their request. Therefore, **having a system in place to locate and expunge personal data** is incumbent on administrators of remote access. For larger organizations, this means these enormous data sets be centralized, otherwise locating, accessing, and erasing personal data will be a nightmare. We recommend you have a mechanism to centralize that data storage, so you can provide these rights of access, portability, rectification, and erasure.

Granting a data subject access to the log files of a remote control session also aligns with the principles and precepts of the GDPR. For example, if your remote control solution includes an integrated chat tool and you're logging chat records, it needs to be stored in such a way that it can be accessed, transferred, as well as corrected and deleted.

Again, the GDPR does grant businesses rights of their own. The principle of overriding legitimate interests ensures that businesses are not forced to follow rules that are impractical or risky. As a security measure, there will almost certainly be audit records that no one can alter.

Businesses should determine what information is completely necessary to meet other regulations and security policies and limit data storage accordingly.

DID YOU KNOW?

Netop Remote Control provides centralization options for managing security roles, device configurations, and logging.

Integration with directory services and ODBC-compliant databases allows for improved user rights management and accordance with storage limitation.

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."*

72H Supervisory Authorities

When an organization becomes aware of a personal data breach, it has 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.

Individual data subjects

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.

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 Regulation stipulates that damages be broadly interpreted so that maximum compensation be provided to individuals.

ADMINISTRATIVE FINES

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

20.000.000€ 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 Regulation 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. 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.

5 Keys to Compliance

WHY personal data is processed

WHEN personal data is processed

IMPACT of processing

CONSENT to process

HOW personal data is processed

Rights of the Data Subject

Access

Portability

Erasure

Rectification

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.

GDPR COMPLIANCE CHECKLIST

GDPR Security Requirements

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)

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)

How Netop Remote Control Ensures Compliance

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

Netop'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.

Netop Remote Control also 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.

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.

Event 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. The Netop Remote Control administrator chooses which events to log depending on the specific device, user and circumstance.

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.

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.

GDPR COMPLIANCE CHECKLIST
(CONTINUED)

GDPR Security Requirements

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)

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)

Rights of Rectiifcation and 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)

How Netop Remote Control Ensures Compliance

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.

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.

ABOUT NETOP

The success of your business depends on the strength and security of your IT. When it comes to remote access, your team expects a fast, powerful connection to any platform or device, and the freedom to configure your solution around business needs. The right remote access solution will boost efficiency while providing the security and customization your business demands.

We know support and ITSM excellence is the foundation of a healthy business, and your staff can only be as effective as the tools they use to keep operations on track. Netop Remote Control provides security, flexibility, and power— allowing you to resolve issues faster and exercise precise control over staff and vendor access from one central location. Netop Remote Control is the preferred remote access solution of professionals and businesses that take compliance seriously.