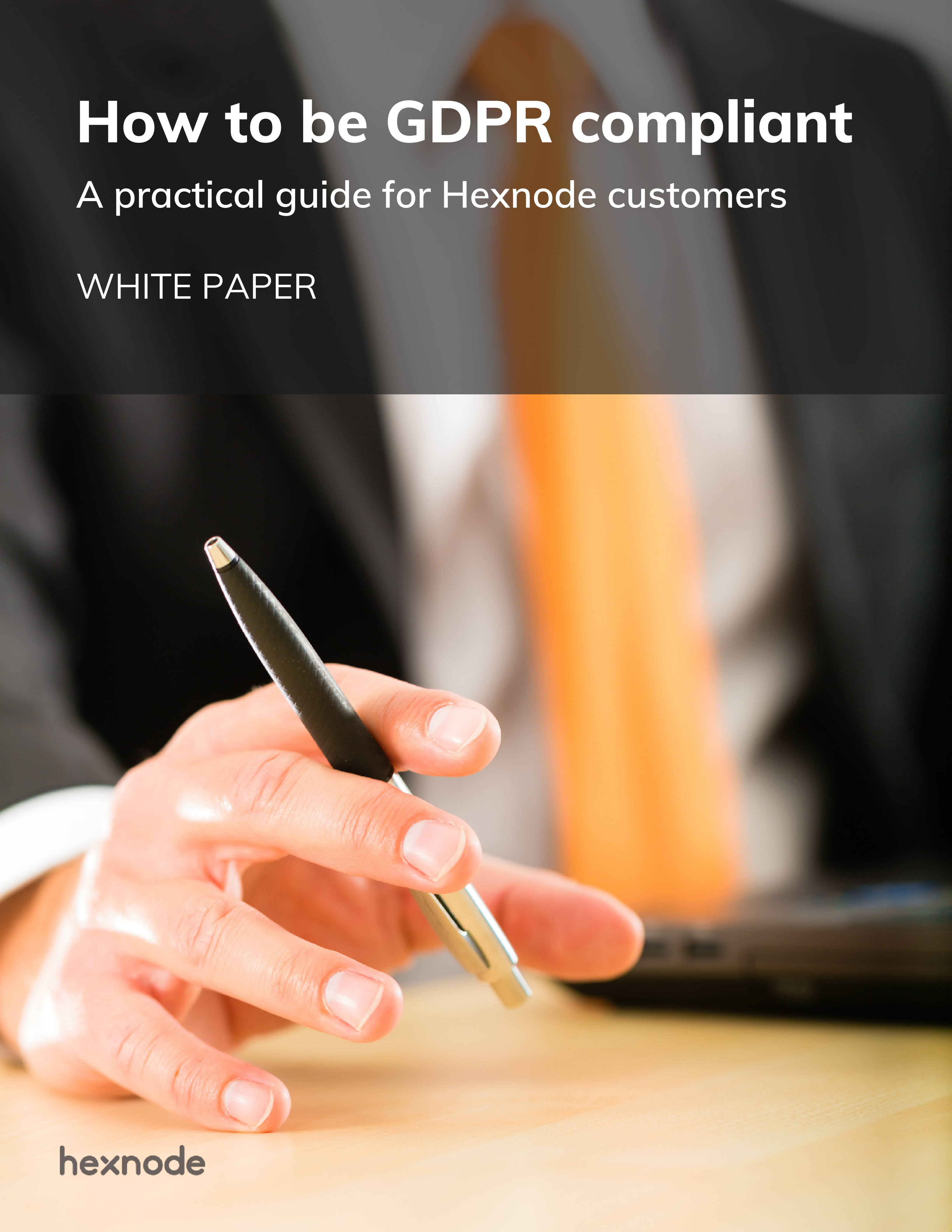
How to be GDPR compliant

A practical guide for Hexnode customers

WHITE PAPER



hexnode

TABLE OF CONTENTS

Introduction 03

Scope of GDPR 04

Chapter 1: The guiding principles of GDPR 05

Preparing organizations to be GDPR compliant 06

The 7 princlples of GDPR articles and guidelines 07

Define responsibilities 08

Maintain transparency and give legal justification in collecting data 08

Implement data protection and security 09

Ensure privacy rights to data subjects 10

Chapter 2: How UEM helps organizations stay GDPR compliant 12

Manage applications and ensure application security 12

Manage OS updates 16

Ensuring protection on BYO devices 16

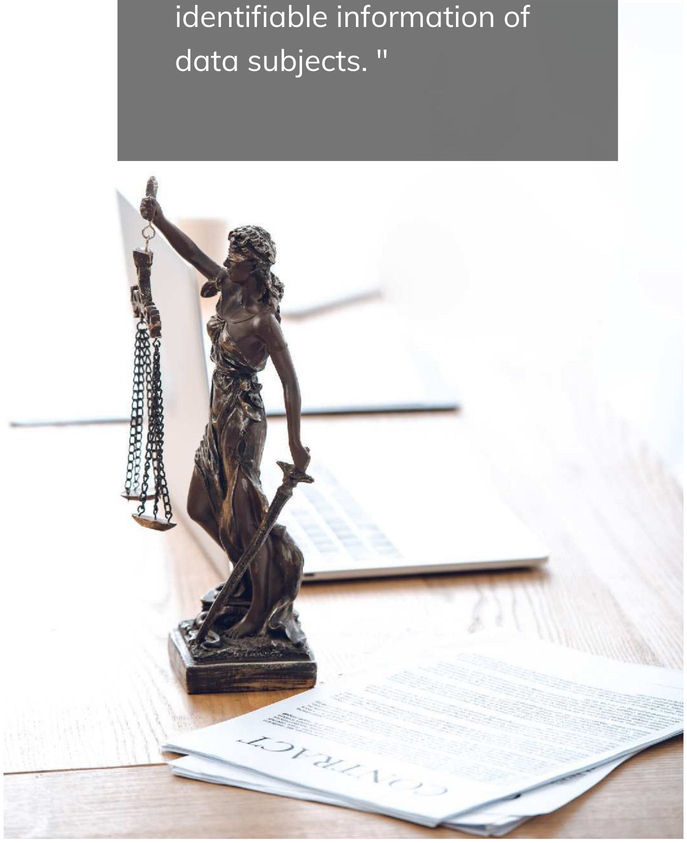
Ensure network and device security 17

Ensuring data security and compliance 19

Chapter 3: GDPR compliance: The Do's and Don't's 22

Introduction

" GDPR which came into effect on **May 25th, 2018**, aims at maintaining transparency while collecting personally identifiable information of data subjects. "



Data collection and processing has always been looked upon as a violation of privacy rights. The right to uphold and maintain privacy has been around since 1950, as part of the **European Convention on Human Rights**. Since 1995, the EU has been passing data protection measures to preserve the privacy of people within the EU. **The European Data Protection Directive** passed in 1995, set the foundation for most of the stringent data protection laws.

Each member state within the EU added their own implementation laws within it. But with the advancement of technology and the speed with which businesses could evolve themselves to cater to more customers globally, these laws weren't enough to safeguard user privacy. It was in 2011, EU made the decision to substantially improve their data protection laws by working on the European Data Protection Directive.

SCOPE OF GDPR

Although GDPR is mostly applicable for customers within Europe, **if a business outside of Europe targets European customers, they will fall under the purview of GDPR**.

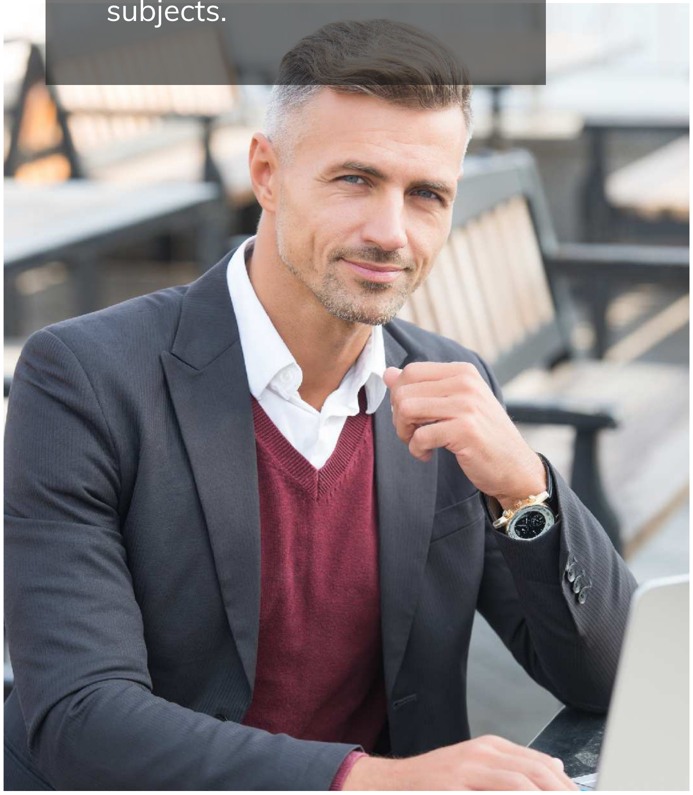
Even if your organization does not cater to European customers explicitly but your website still uses cookies or IP addresses of people visiting your website from EU, then your organization will still have to be compliant with GDPR.

GDPR was passed by the European Parliament in 2016 and by 2018 all organizations were required to be compliant with it.

1

The guiding principles of GDPR

Being GDPR compliant, help organizations rethink and improve the way they manage and process sensitive information of customers and other data subjects.

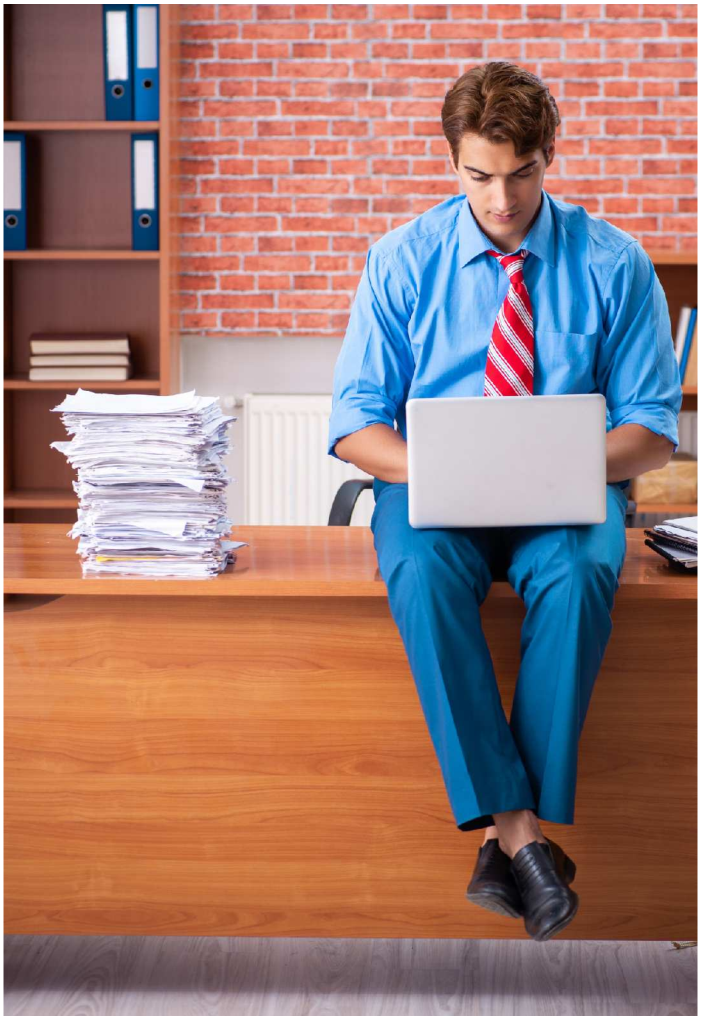


PREPARING ORGANIZATIONS TO BE GDPR COMPLIANT

Documenting and implementing an information security policy can always keep employees well informed of all the measures they need to take to secure the integrity and confidentiality of all the information they handle.

The **seven principles** of GDPR's Article Five guides organizations to build trust and credibility. The seven principles set by GDPR are now being widely adopted by various organizations to improve the way they protect data.

THE 7 PRINCIPLES OF GDPR ARTICLES & GUIDELINES



- *Lawfulness, fairness & transparency*
- *Purpose limitization*
- *Data minimization*
- *Accuracy*
- *Storage limitation*
- *Integrity and confidentiality*
- *Availability*

Preparing to be GDPR compliant can be a hefty task, planning with these key pointers in mind can help the transition be easier:

- Make sure your compliance team, HR team, upper management and other key members within the organization are properly updated with the latest data protection laws.
- Keep records of all the data processing activities.
- While collecting personal data, state the identity and intent in a clear and concise language.
- Have a well-planned system in place to ensure any breaches to personal data are promptly identified, reported and investigated.
- Set up appropriate roles and responsibilities.

DEFINE RESPONSIBILITIES

GDPR details how personal data should be processed, collected, stored and by whom. On the surface, a Data Controller and a Data Processor may seem to share the same responsibilities but there is a clear distinction between the two.

The **Data Controller** would determine the purpose behind collecting the personal data and the means by which it needs to be processed whereas a **Data Processor** would be an entity, organization or public authority who processes the personal data on behalf of the Data Controller.

Organizations are required to appoint a Data Protection Officer if they systematically process sensitive information on a large scale. Their chief responsibility would include ensuring the implemented data protection requirements are carried out in accordance with GDPR. Below is a brief overview of the responsibilities:

Data Controller

- Prohibit the processing of certain categories of personal data unless the data subject has given proper consent to process the data.
- Provide information to the data subject when personal information is being collected, this includes the purpose of collecting the data, data recipients and retention period.
- Establish data protection policies.
- Create binding corporate rules to secure international transfer of personal data.
- Document personal data breaches and report them to a supervisory authority.
- Conduct assessments before transferring personal data to an international organization.
- Implement measures within the organization to minimize the collection of data.
- Undertake continuous testing and evaluation of the data security measures.
- Conduct a Data Processing Impact Assessment when a data processing activity is likely to result in a high risk.
- Conduct reviews to check whether the data is being processed in accordance to the Data Processing Impact Assessment.
- Conduct audits to verify compliance with the established corporate rules.
- Respond to request of information from data subjects on their right to access data, correct any data that is inaccurate or incomplete, right to erase and right to restrict the processing of data under specific conditions
- Notify data subjects on actions taken to correct or erase personal data
- Respond to objections from data subjects on the processing of personal data

- Notify the supervisory authority of the data breach within 72 hours of becoming aware of it.
- Immediately notify data subjects of data breach without delay
- Create contracts to determine how data processors should store and process data
- Ensure the access and availability of personal data during the event of a physical or technical incident

Data Processor

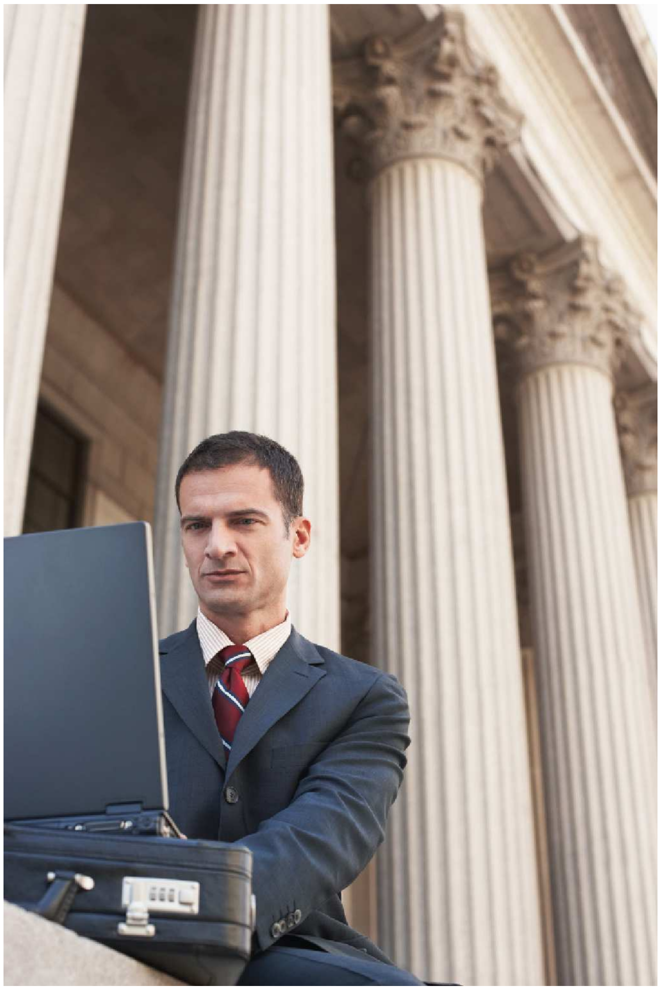
- Create binding corporate rules to secure international transfer of personal data.
- Help the Controller in conducting audits and ensuring that the data protection policies are in alignment with the GDPR requirements.
- Implement measures to ensure the availability, confidentiality and integrity of the processing systems and services.
- Conduct ongoing testing and evaluation to check the effectiveness of the implemented data security measures.
- Immediately notify the controller of a data breach without delay.
- Gain approval of the controller before onboarding another processor.
- Ensure the access and availability of personal data during the event of a physical or technical incident.

Data Protection Officer

- Be aware and monitor risks of data processing.
- Directly report to higher management.
- Ensure compliance with GDPR and data protection policies by being a part of the audit process.
- Ensure compliance with binding corporate rules.

MAINTAIN TRANSPARENCY & GIVE LEGAL JUSTIFICATION IN COLLECTING DATA

An exhaustive and updated list of all the processing activities should be kept by organizations processing data of higher risks.



SMEs should conduct a data protection impact assessment; this would help organizations to properly evaluate the current processes they have in place and ensure they comply with all of GDPR's requirements. The list of processing activities includes:

- Purposes of processing
- Type of data being processed
- Access controls
- Data protection measures
- Data disposition measures

> “ **PERSONAL DATA**
>
> cannot be processed unless they can be legally justified. GDPR only permits the processing of personally identified information unless they can be justified according to one of the six conditions defined within Article 6.

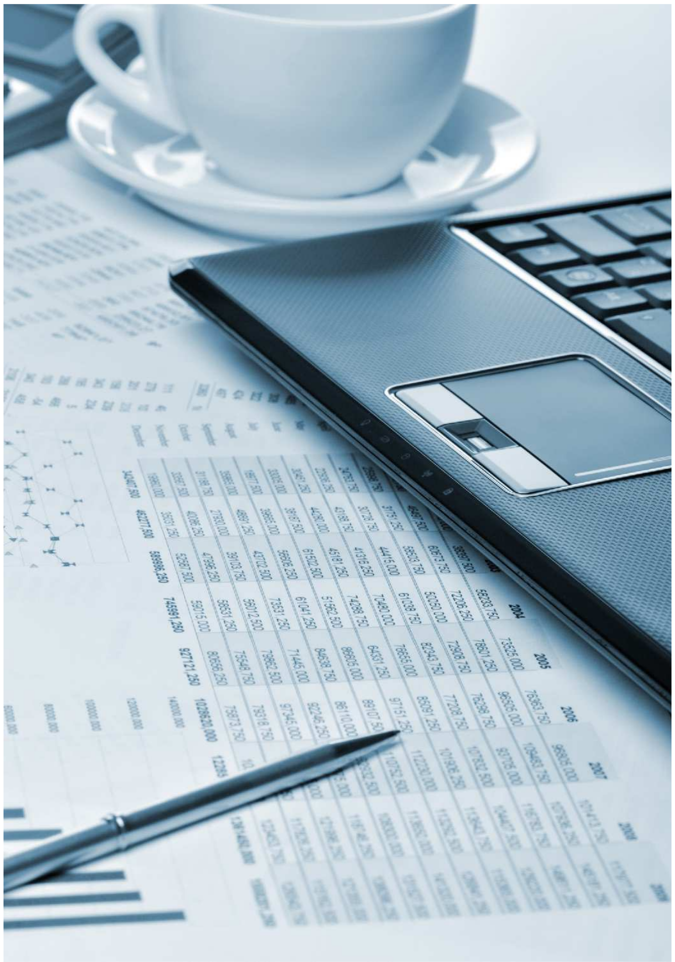
Articles 7 to 11 provide guidelines for the collection of special categories of personal data and PII of children. What customers want the most is transparency. It is always best for organizations to clearly state within their privacy policy how the data is being processed, who has access to it and how you plan on securing it. Article 12 mandates organizations to inform data subjects the purpose behind collecting their data. This should be written or communicated in a manner that Is easy to understand.

IMPLEMENT DATA PROTECTION AND SECURITY

Data protection should be an integral part of every stage in the development of a product and each time an organization processes data.

An adequate amount of technical and operational controls should be in place to protect the personally identifiable data that is being handled and processed.

> “ **PROCESSING OF PERSONAL DATA**
>
> should be done in accordance with the data protection guidelines specified within Article 5.



Encryption should be used whenever possible. Encryption has always been a priority with many security professionals and it’s not surprising to know why. It prevents the occurrence of identity theft and ransomware to a large degree, files can be shared securely, it ensures privacy and protects information stored within lost or stolen devices.

An information security policy can give organizations a clear idea on the data protection measures they need to implement. This could include documenting the acceptable usage of the organization’s assets, the necessary controls and setting up appropriate roles and responsibilities. Other requirements related to email security, passwords, device encryption and VPN can also be mentioned within the policy. An information security awareness training should be given at regular intervals. Many well-known organizations have paid heavy fines due to lax security measures.

Rather than being reactive and responding to a data breach in a haphazard manner, industry experts advice organizations to be more proactive by always anticipating the occurrence of a breach and improving the data protection measures. Conducting a data protection impact assessment is one way to do so. It gives organizations a proper idea on how their products and services could jeopardize customer data.

Based on the results obtained from the assessment, a list can be made with all the risks. Further plans can be implemented to take necessary steps to minimize those risks.

ENSURE PRIVACY RIGHTS TO DATA SUBJECTS

Organizations should make it easier for customers and other data subjects to request and receive the information organizations collect about them. They should also have the right to know about the retention period and the reason for keeping the data for that length of time.

" A clearly defined process should be in place to notify the right authorities and data subjects in the event of a data breach. "

A process should be set up to make it easier for customers to **view and update** their personal information for accuracy. While processing such a request, always make sure the identity of the user is verified before it is carried out.

When data subjects request the **deletion** of their personal data, organizations must ensure to delete it within a month. This too requires verifying the identity of the user requesting the data deletion.

Data subjects do have the **right to stop the processing of data** if there are discrepancies regarding the legality of the process or any inaccuracy of information.

If such a request is made, it should be done within a month. Even though the processing is restricted, data storage will still be allowed. The data subject has to be duly notified before the data is processed again.

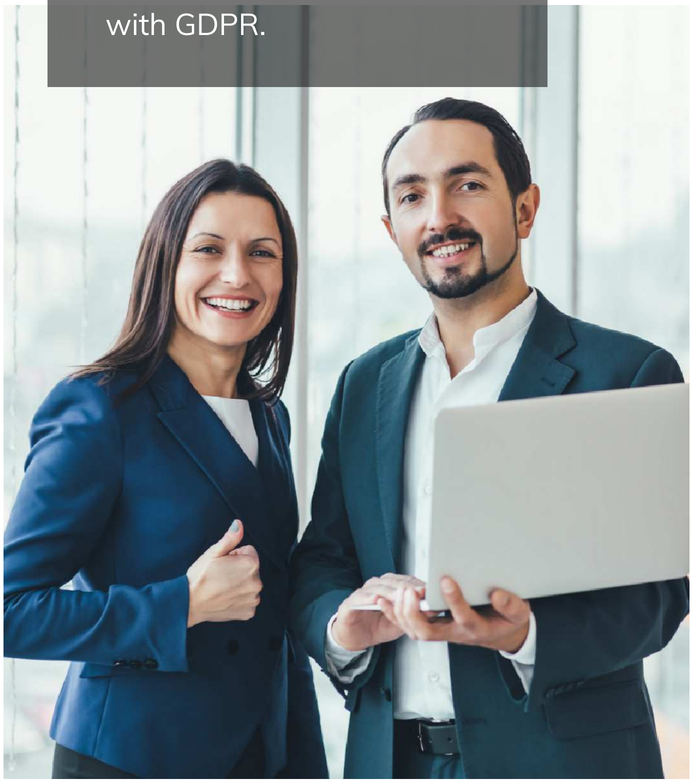
A legible copy will give data subjects an idea on the type of information being shared and processed by the person, organization or entity.

> “ **WHEN CUSTOMERS RECEIVE**
>
> a copy of their personal data, it should be in an easily readable format.

2

How Hexnode UEM helps organizations stay GDPR compliant

Meeting all the requirements set by GDPR can be difficult. It is always ideal to document organization specific policies and use tools such as a UEM solution like Hexnode to stay compliant with GDPR.



MANAGE APPLICATIONS AND ENSURE APPLICATION SECURITY

It may be difficult for businesses, especially large ones that employ complicated workflows, to manage the applications and software they have in place.

It may be even more difficult to ensure that the confidential information contained within these applications do not leak out.

By utilizing a **UEM solution**, enterprises can ensure that the applications are appropriately managed and deployed in a way that only the the intended receivers use them.

Managing applications remotely

It is common to rely on enterprise applications and other third-party apps to manage and handle **PII of customers** and other data subjects. Having them readily installed on the devices ensures that all employees are equipped with the work tools required by the organization.

Leaving users to manually install the required applications on their own will take up too much time and leave admins working double time just to make sure all managed devices have the right applications installed. A Unified Endpoint Management (UEM) solution permit admins to remotely install and uninstall the applications they need without needlessly spending time checking on each employee.

Employees may also unknowingly install unsecure applications on their own and as a result compromise the security of the device they use. UEMs can help organizations avert this risk by giving admins full control over the process of installing, updating and uninstalling the required applications.

Create app catalogs and app groups

App catalogs and **app groups** can come in handy in situations when you need to roll out multiple applications in bulk. Admins can set up multiple app catalogs to provision apps for different sets of targeted users.

App catalogs can contain both individual apps and app groups. Android Enterprise offers organizations the flexibility to deploy and manage private enterprise applications within Managed Google Play. Google Play Store does not permit organizations to host their own applications. It will consist of applications pre-approved by the admin. UEMs can help ensure users do not make any undue changes on their own by restrict them from installing or uninstalling applications not approved by the organization.

> “ An **app group** consists of a group of apps that can be deployed to an individual device or a group of devices. An **app catalog** on the other hand, provides a customized app store to users with only the applications they need.

Unmonitored data access can jeopardize the security infrastructure of an organization. Strict **access controls** should be in place to ensure information is shared only on a strict need-to-know basis. Organizations can limit the risk of data access from unsecure applications by deploying all essential applications in managed app catalogs.

> “ Organizations can even deploy managed app catalogs consisting of applications that are secure and vouched by the organization.

Prevent unauthorized sharing by uninstalling/blacklisting specific apps

Having insecure applications installed on the devices can open doors to all sorts of threats and vulnerabilities to occur on the device end.

With UEMs admins can remotely uninstall or **blacklist applications** that come with the risk of letting users share sensitive information pertaining to the organization or data subjects to unauthorized parties.

Employees can also be limited from sharing information to other unauthorized parties within the office by disabling various file sharing options such as Bluetooth, USB mass storage, NFC and Android Beam.

Improve app security by updating apps to latest versions

Updating the enterprise and store apps to their latest version helps ensure the device stays secure and guarantees the safety of the information present inside it. Maintaining application security is important. Not securing applications will eventually lead to the rise in various security threats.

The entire purpose of ensuring app security is to make sure that malicious codes are not injected into it and none of the information is stolen from the apps that store them. Updated application keeps the device more secure and improve its performance.
Hackers can make use of the outdated version to hack into the device and steal personal information.

These bugs can be fixed by updating apps to the latest versions.

> “ No matter how well developed an application maybe, there’s always a possibility of a bug or vulnerability hiding in the system.

Maintaining app security limits attacks from cyber criminals and unauthorized access to company data. Sometimes using an updated version of the app may not work out as well as you’ve planned such as not being compatible with the current systems the organization has in place. By using a UEM solution, admins can downgrade the applications they need and deploy it to the users.

Set app permissions and configurations

Leaving users to enable the necessary app permissions and configurations on their own could compromise the data intergrity.

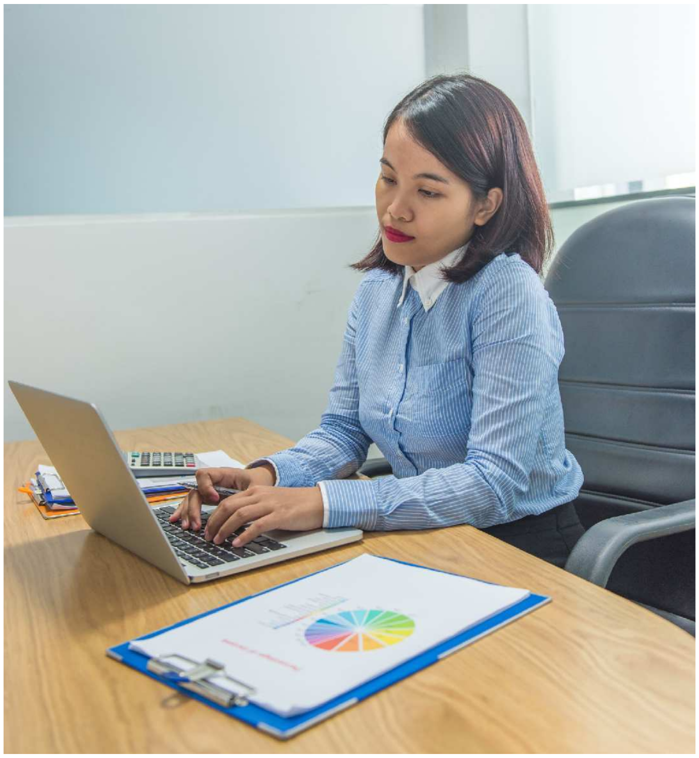
It would be much safer for admins to configure the applications in advance and have the necessary permissions enabled before they are deployed onto the user end devices.

Secure data by locking devices down in a kiosk mode

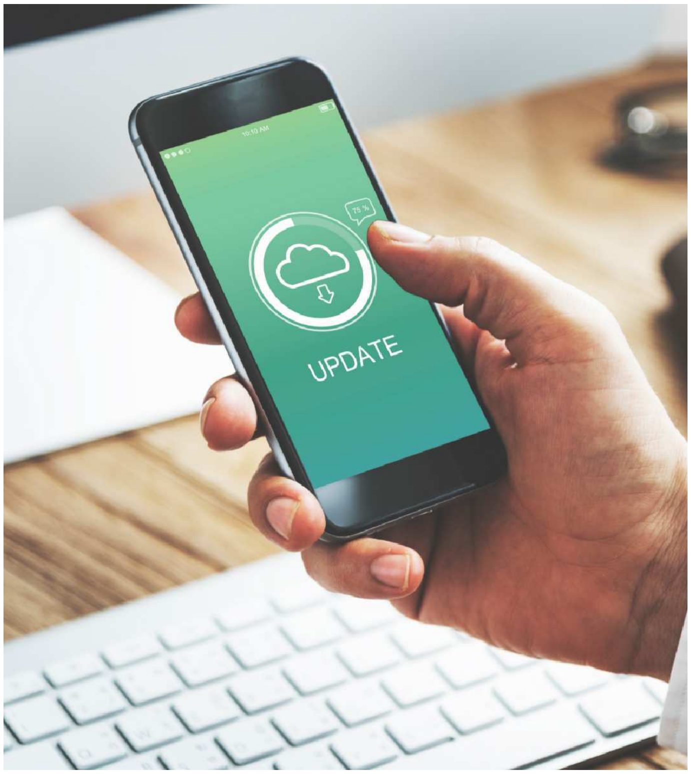
Kiosk mode locks down the device to function in just a single application or a set of multiple applications approved by the organization. It improves device security significantly as control over the entire device rests solely with the admin.

> “ Devices can be locked down into kiosk mode using a Unified Endpoint Management (UEM) solution.

Admins can host a variety of kiosk lockdown strategies on managed devices. Messages can be broadcasted remotely while in kiosk mode, and Hexnode even has its own native customizable browser; the Hexnode Kiosk Browser.



MANAGE OS UPDATES



Though this is generally well known, the importance of always having the operating system updated cannot be stressed enough.

What hackers love more than anything is exploiting vulnerabilities.

The later versions of the operating systems always come with security patches that help close or resolve all the vulnerabilities that were spotted in the previous versions. UEM provides a centralized platform where admins can either schedule the OS updates or update the operating system on the go.

In addition to providing security fixes, having the operating system updated goes a long way in helping organizations stay compliant with various industry-specific regulations such as improving the device performance and supporting new applications and software. The updates can be configured to individual devices or group of devices. Just like updating the applications you use, it is important to have the operating system updated whenever there is a new version out.

Storing all sensitive personal information in old operating systems can be a huge risk. Hackers will be well aware of all the security vulnerabilities existing within the older versions and make use of those flaws to hack into the system.

> “ With the help of a UEM solution, admins can either schedule the OS updates, postpone it or have it automatically updated.

ENSURING PROTECTION ON BYO DEVICES

Bring Your Own Device (BYOD) is a growing trend in the corporate world where employees bring their own devices to work

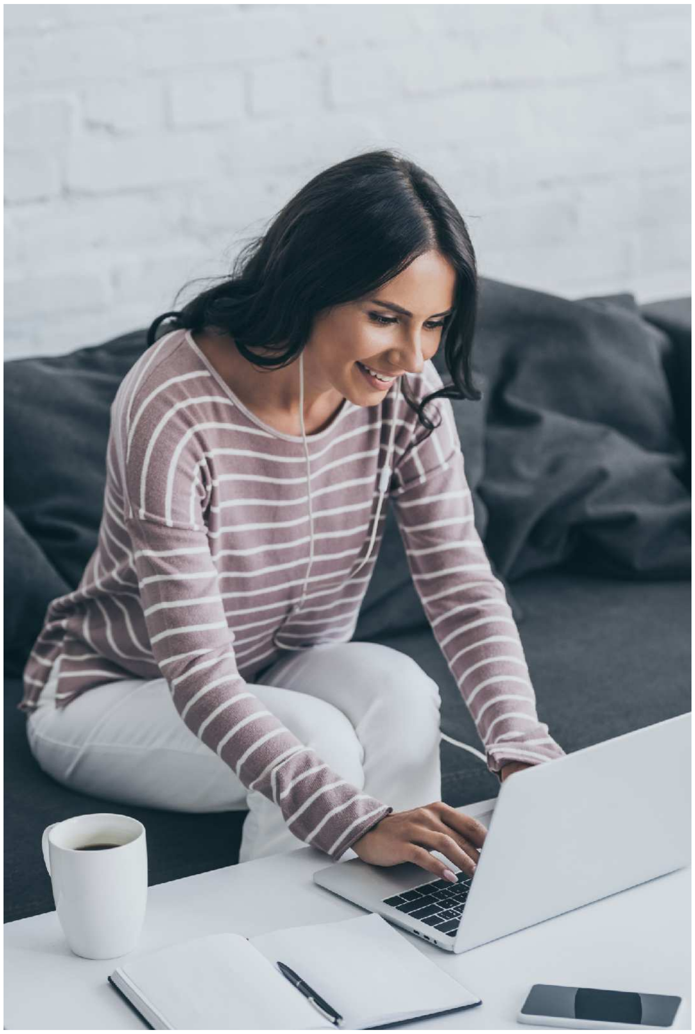
> “ No matter how seemingly robust a company’s infrastructure may be, a BYOD model can create huge gaps in a company’s cybersecurity policy.

Create work containers to store confidential data and apps

Containerization plays an important part in maintaining information security in personal devices employees use for work. A UEM solution like Hexnode can help organizations create separate work profiles where all corporate sensitive information can be stored. A password can be set within those containers to ensure only the right users have access to it. All apps deployed in Managed Google Play can be remotely pushed within those containers thus leaving the personal space of the user untouched.

Containerization creates an encrypted storage space within the personal device of employees where all corporate sensitive information will be stored.

> “ Admins can greatly limit the flow of data between work and personal space of the employees by remotely pushing various security policies onto the devices.



Protect data-in-transit via a corporate VPN

One of the major challenges of working remotely is protecting data in transit. Businesses can ensure organizations protect data in transit by permitting users to only connect to a corporate approved VPN to access its resources. Organizations can configure the WIFI settings and make it password protected to ensure that only authorized users are connected to the corporate networks.

ENSURE NETWORK AND DEVICE SECURITY

> “ People are often the weakest link when it comes to cybersecurity.

Which is exactly why companies must enforce their cybersecurity policies with a solid network and device security strategy.

Enforce restrictions

Although your employees may be aware of the company policies, they cannot always be relied on implementing the measures defined within the policies. To be on the safe side, it’s always best if organizations enforce policies on the end devices. This helps in keeping the devices secure at all times and helps admins keep a constant watch over the security, health, and compliant state of the devices. The restrictions could include placing restrictions on the device functionalities, application settings, security, privacy settings and more. You can push out restrictions to prevent users from copying and pasting sensitive information.

Disenroll or corporate wipe non-compliant devices

Non-compliant devices can be those that don’t comply with the policies set by the organization. These devices could either be disenrolled at once and have a corporate wipe initiated on them to ensure all sensitive information are erased before the device is handed out to a new user. Admins can also go for a complete wipe before reassigning the device. A complete wipe will wipe the device in its entirety whereas a corporate wipe will only wipe the information present within the work container.

This is a more feasible option for employees who work with their own personal devices. Though employees may be well aware of all the policies implemented within the organization, they can still be prone to various cyber-attacks and web threats. Web content filtering can be remotely pushed onto the devices as a policy via a UEM.

> “ Organizations can improve their network security by blacklisting spammy links and restrict users from downloading any illegal content that could lead to a data breach.

Pre-configure WIFI and VPN settings

The WIFI networks and VPN can be configured to ensure all data is passed only through **secure channels**. Admins can prevent unauthorized users from connecting to the network by securing it with a password.

A UEM solution can bring in more restrictions to the networks by allowing admins to add a **SCEP** or **PKCS** certificate. These security certifications authenticate users when they connect to corporate resources and applications.

> “ A VPN helps protect the handling of information even further by letting organizations have a private and encrypted browsing session.

They help protect the integrity and confidentiality of the corporate data and limit the number of unauthorized access to the data.

In order to start a connection with a VPN server, the device uses a VPN connection profile. UEMs help organizations configure the connection profiles. Once it is configured, the VPN connection will be listed among the other available networks. UEM’s also give admins the freedom to either use WIFI or mobile data or restrict users from using them.

ENSURING DATA SECURITY AND COMPLIANCE

Staying compliant with regulatory guidelines and maintaining a sound strategy to ensure data security is essential to avoiding civil monetary penalties. Companies that lack robust data security management systems may be in the purview of harsh GDPR fines.

Prevent unauthorized access to data on devices left unattended

Staying compliant with regulatory guidelines and maintaining a sound strategy to ensure data security is essential to avoiding civil monetary penalties. Companies that lack robust data security management systems may be in the purview of harsh GDPR fines. GDPR mandates organizations to enable encryption on all the devices they manage.

It would always be better to implement additional security by defining a strong and complex password policy and have it pushed onto the devices. Admins can pre-define the password age and force users to keep changing the password at regular intervals.

You can also set up a password history to ensure users don't follow a simple repetitive pattern while updating a password. Weak passwords have compromised lot of businesses in the past. Moreover, admins can easily verify the password compliance of each device by visiting the Hexnode portal, and initiate any further actions, if necessary.

Organizations dealing with sensitive personal information of data subjects on a steady basis should ensure that all of the devices under their purview are password enabled and encrypted.

Lost or stolen devices are a commonplace occurrence in any workplace.

The remote device management capabilities of a UEM solution help admins to instantly track the location of these devices and enable various other actions remotely, such as initiating a full device/corporate wipe, locking the device, setting up remote ring and enabling lost mode in Android, iOS and Windows devices.

Troubleshooting can be difficult for admins when employees work remotely.

Identify non-compliant devices

Hexnode UEM makes it easier for admins to get a complete overview of all the devices they manage.

Details regarding its security, health and compliance status can be obtained via reports.

The **reports** can either be **scheduled** at a more convenient time or **downloaded** at once.

In order to maintain the confidentiality of the reports, they could either be viewed publicly, wherein anybody with the link can have access to the report, or privately which would require the technician to login to the UEM portal and download the report.

> “ Rather than relying on the employees themselves to explain what the issue is, IT admins can simply login to the UEM portal and enable remote view or control to access and work on the user’s screen.

3

A brief overview of being GDPR compliant: The Do’s and Don’t’s

Take a brief look at the list of the Do's and Don't's that companies must observe and abide by in order to maintain GDPR compliance.

DON'T's	DO's
Don’t take a reactive approach when data breaches occur.	Conduct a data protection impact assessment to prepare and handle any instances of a data breach. This helps organizations plan what they need to do.
Don’t rely on just software and other tools to be compliant.	Although tools do play a huge part in helping businesses be compliant. It is always best to also implement internal policies and other procedures to adapt data protection measures specific to your organization.
Don’t confuse data subjects by writing the privacy notice in a complicated manner.	Privacy notices gives a proper explanation to data subjects regarding the purpose behind the data processing.
Don’t limit the knowledge of data protection laws to just your compliance and IT team.	Everyone within the company should be updated with the latest data protection laws.