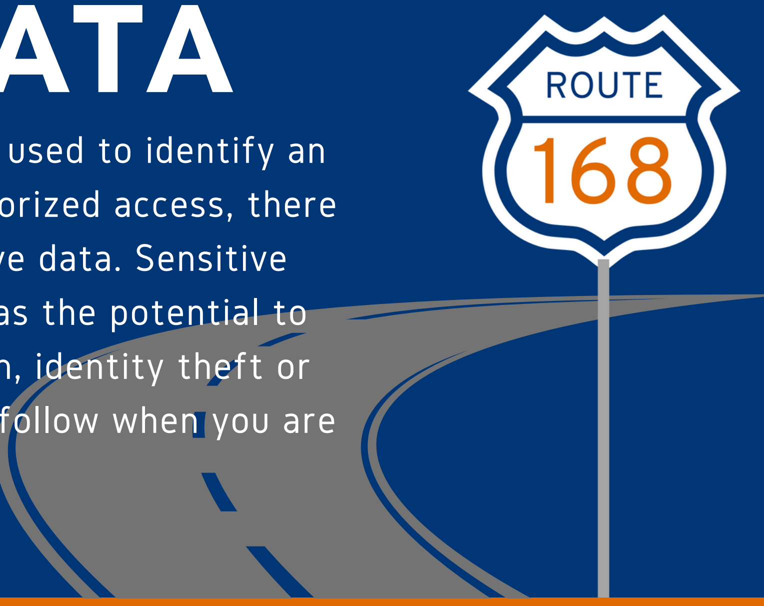
# SENSITIVE PERSONAL DATA

While all information that identifies or can be used to identify an individual should be protected against unauthorized access, there is a higher standard when it comes to sensitive data. Sensitive data is information that if publicly released has the potential to lead to significant harm such as discrimination, identity theft or financial fraud. Below are some guidelines to follow when you are dealing with sensitive data.



## KNOW WHY YOU HAVE IT

- Know and document the reason(s) you need sensitive data before you collect it
- Do not collect sensitive data you do not need
- Ask your Group Lawyer if you need consent before collecting sensitive data
- Do not use sensitive data for new or different purposes without checking with your Group Lawyer
- Complete a DPIA before implementing or changing any vendor, tool or process that uses or collects sensitive data

## PHYSICALLY SECURE IT

- Store the sensitive data in a secure location with limited access
- Do not leave the sensitive data out on your desk or otherwise unattended
- Review files regularly and know what types of sensitive data you have
- Do not share the sensitive data with anyone that is not authorized to have it or does not have a need-to-know it
- Do not make unnecessary copies of sensitive data
- Dispose of sensitive data by shredding
- Do not take pictures of your workspace if sensitive data can be viewed

## ELECTRONICALLY SECURE IT

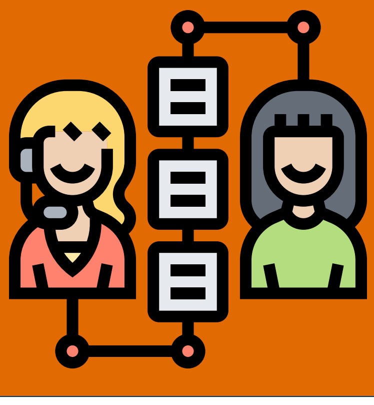
- Only store, transfer and process sensitive data in and on IT approved devices, software, servers and websites
- Do not keep or access sensitive data on personal devices unless preapproved by IT
- Use strong passwords or encryption when transferring or storing sensitive data
- Do not share or make available your login credentials or encryption keys
- Do not store personal data on your hardrive or desktop
- Limit permissions and access to sensitive data whenever possible
- Do not access sensitive data from an unsecured public Wi-Fi connection

## MINIMIZE RETENTION

- Do not keep sensitive data indefinitely
- Assign a retention period to all sensitive data when received
- Do not back up sensitive data to any device or site unless it has been approved in advance by IT

## REPORT ISSUES

- Be on the lookout for suspicious activity
- Do not respond to requests for sensitive data via email or phone unless you have confirmed the legitimacy of the request through other means
- Use the Reportable Events Page to report any issues, concerns or breaches of sensitive data
- Do not delay in reporting incidents involving sensitive data



**WE ARE RPM AND OUR SUCCESS DEPENDS ON EACH OF US FOLLOWING THE RIGHT ROUTE AND EMBRACING OUR VALUE OF 168® TO MAKE THE RIGHT DECISIONS.**

CONTACT US: DATAPROTECTION@RPMINC.COM