ENGLISH

GDPR Guide for ResScan

Introduction

On 25 May 2018 the European General Data Protection Regulation (GDPR) comes into effect. The full text of the GDPR can be read here, in the language of your choice.

http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

As a user of ResScan™, you may be processing sensitive personal data about natural persons. Your organisation would have performed a readiness review for GDPR and you should always follow the policies and guidance of your organisation when processing sensitive personal data. This Guide is intended to provide clarity on how you can perform certain activity defined by GDPR when using ResScan.

ResScan can be operated as intended without processing any personal data. The section below titled 'Article 11 - Processing which does not require identification' describes how you can achieve this. You should review the operations of ResScan within your organisation to ensure your use of ResScan is compliant with your organisation's policies.

A secondary purpose of this document is to clarify privacy topics that may not be clear when operating ResScan. In an era of connected devices, it's important to note that ResScan is a stand-alone desktop product that only connects to your organisation's computer network.

This Guide is organised by the Articles of the GDPR, selecting only the Articles that apply or require clarification. If a GDPR Article is not listed in this Guide, that Article does not apply to the use of ResScan.

By providing ResScan, ResMed is acting as an Independent Software Vendor (ISV), and is not acting as a Data Controller nor Data Processor in normal operations.

Article 4 – Definitions

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.

GDPR is the European General Data Protection Regulation, which comes into effect on 25-May-2018. The exact official title is Regulation (EU) 2016/679 but the term 'GDPR' is widely known and understood.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

Article 9 – Processing of special categories of personal data

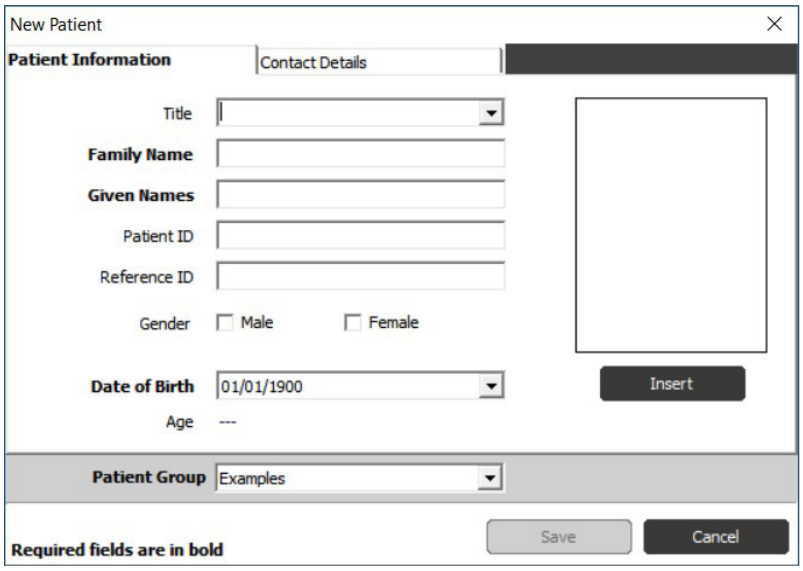
ResScan is assessed to be processing sensitive personal data concerning the health of a natural person, as declared in paragraph (1) of Article 9.

You are responsible for obtaining consent from the data subject to allow processing under paragraph (2) a) of Article 9, in order to obtain a legal basis for processing a special category of personal data.

Article 11 – Processing which does not require identification

ResScan supports the use of pseudonymisation tokens if you wish to manage the storage of sensitive personal data within their organisation.

When you enter patient details, you can use any pseudonymisation token determined by your organisation's policies. The pseudonymisation tokens would be entered in the Family Name, Given Names, Patient ID and Reference ID fields. The ResScan will also work with any allowable Date of Birth.



Article 12 – Data Subject Request

If you receive a request to provide any information related to processing of a data subject, you can perform the following steps to obtain this data from ResScan.

If your organisational Policies have deemed the data subject request to be legal, and the data subject intends to use the data in another ResScan system, simply copy the files normally located in %PUBLIC%\Documents\ResMed\ResScan3\Patients\<data subject>. (You may elect to store the patient data in another location when you create the patient.) There is a folder created for each patient you create in ResScan, and another instance of ResScan 6.0 or greater can access the ResScan file by placing the file in the same location in the new Controller's ResScan personal computer.

If the data subject has not specified that another ResScan system will be used, you can export the ResScan summary data from the patient file using the instructions below, which are also found in the Section 'Exporting Data Files' in the ResScan Clinical Guide (version 6.0 or greater).

1. From the File menu, choose Export. The Export Patient file to CSV dialog is displayed.

   (Note: Before opening the dialog box, ResScan displays an indexing message. This message is generally brief; however you can cancel indexing by pressing the Cancel button.)

2. Select the patient group from the Patient Group drop down list.
3. Select the date range from which to generate the CSV files.
4. Select one or more patient files from the list of patients.
5. Click the Export Selected button.

A CSV file is generated for each of the selected patients. The name of the file is that of the patient.

Alternatively, you can export all patient files in a patient group to a single CSV file by clicking the Export All button. The name of the generated CSV file is that of the patient group.

After exporting your files, Windows Explorer automatically launches to the folder to which the files have been saved: %USERPROFILE%\Documents\ResMed\ResScan\Exports (Windows 7, Windows 8.1, Windows 10).

Note that the Data Controller operating ResScan is responsible for determining if the rights in paragraph (1) of this article adversely affect the rights and freedoms of others, as declared under paragraph (4) of Article 20.

Article 14 – Information to be provided where personal data have not been obtained from the data subject

Article 14 does not apply to the use of ResScan, as no other Data Controllers are involved. ResScan does not transmit data nor collect data of any nature with another Data Controller or Data Processor. There are no automated transmissions of data from ResScan back to ResMed. ResScan is solely within the security domain of your organisation's Windows domain or desktop profiles.

ResScan collects machine data from ResMed treatment devices based on the interaction of that device with a data subject. The treatment device that provided the personal data is under the control of you, acting as the same Data Controller that obtained the personal data.

Article 17 – Right to erasure ('right to be forgotten')

If you receive a request from a data subject to have their personal data erased, you can delete the ResScan data either via the ResScan software, or by deleting a file using Windows file explorer.

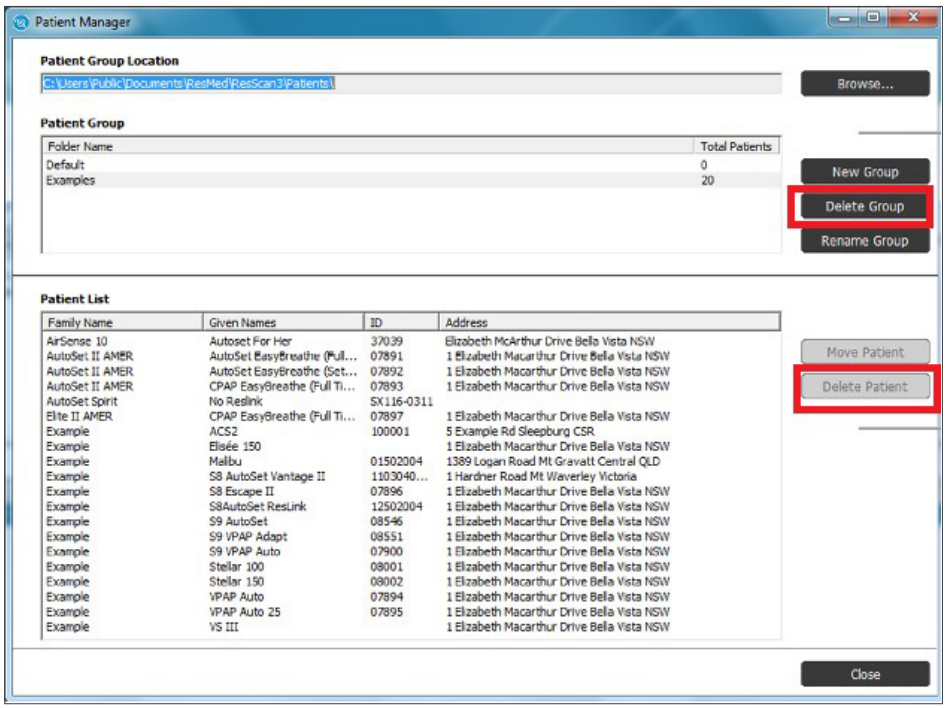
Deleting the data via the ResScan interface avoids the risk that the deleted data will still be stored in the Windows Recycle Bin. If you delete patient data using the Windows File Explorer interface, you will have to ensure that the data is also removed from your Windows Recycle Bin.

The ResScan interface to delete a patient also creates Windows audit log entries for the act. A deletion performed using Windows File Explorer will only leave an audit record depending on the audit settings of your Windows domain. See your Windows IT Administrator for more information on this topic.

It is strongly recommended that you always delete ResScan personal data using the ResScan interface.

Using the ResScan interface

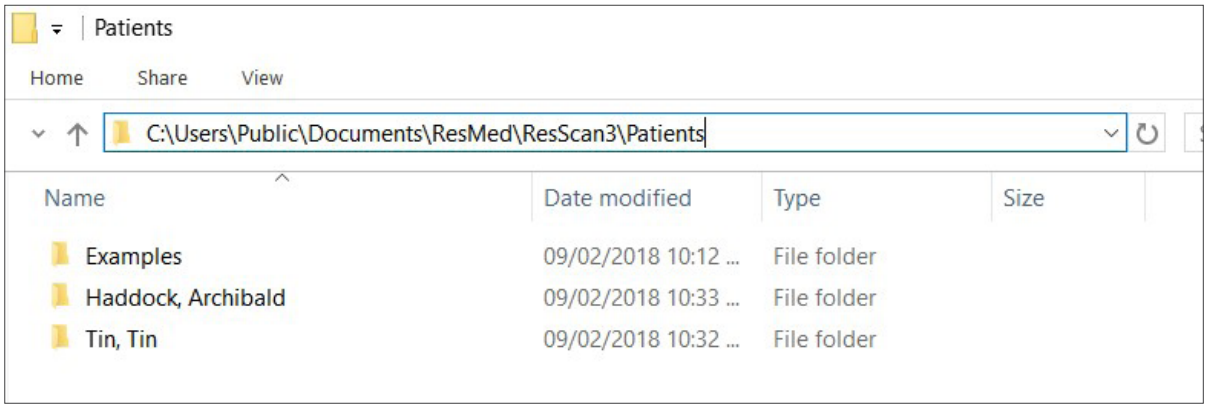
Within the ResScan software, launch the Patient File Manager from the Tools menu. There will be buttons to delete a group of patients, or a single patient.



Using the Windows File Explorer interface

You can also delete personal data via the Windows File Explorer. The default file location is %PUBLIC%\Documents\ ResMed\ResScan3\Patients folder. You or another member of your organisation may have elected to save the files elsewhere. If you are not sure where the files are located, you can determine this from the Patient Manager within ResScan.

A separate Windows folder is created for each patient you create in ResScan. Simply delete the file using Windows File Explorer commands. You will have to also ensure the data is removed from the Windows Recycle Bin.



Your organisation, as the Data Controller, is responsible for assessing the legality of data retention under paragraph (3) of Article 17.

Article 20 – Right to data portability

If you receive a request to provide a structured, commonly used and machine readable format of their personal data, you can perform the following steps in ResScan.

Personal data can be exported from the ResScan software in a machine readable format. The transmission of extracted personal data must be performed by your organisation using your current processes for disclosing sensitive personal information to another Data Controller.

If your organisational Policies have deemed the request for data portability to be legal, and the data subject has requested that their data is provided to another Controller to use on another ResScan system, simply copy the files normally located in %PUBLIC%\Documents\ResMed\ResScan3\Patients\<data subject>. (You may elect to store the patient data in another location when you create the patient.) There is a folder created for each patient you create in ResScan, and another instance of ResScan 6.0 or greater can access the ResScan file by placing the file in the same location in the new Controller's ResScan personal computer.

If the data subject has not specified a destination for their personal data, you can export the ResScan summary data from the patient file using the instructions below, which are also found in the Section 'Exporting Data Files' in the ResScan Clinical Guide (version 6.0 or greater).

1. From the File menu, choose Export. The Export Patient file to CSV dialog is displayed.

   (Note: Before opening the dialog box, ResScan displays an indexing message. This message is generally brief; however you can cancel indexing by pressing the Cancel button.)
2. Select the patient group from the Patient Group drop down list.
3. Select the date range from which to generate the CSV files.
4. Select one or more patient files from the list of patients.
5. Click the Export Selected button.

A CSV file is generated for each of the selected patients. The name of the file is that of the patient.

Alternatively, you can export all patient files in a patient group to a single CSV file by clicking the Export All button. The name of the generated CSV file is that of the patient group.

After exporting your files, Windows Explorer automatically launches to the folder to which the files have been saved: %USERPROFILE%\Documents\ResMed\ResScan\Exports (Windows 7, Windows 8.1, Windows 10).

Note that the Data Controller operating ResScan is responsible for determining if the rights in paragraph (1) of this article adversely affect the rights and freedoms of others, as declared under paragraph (4) of Article 20.

Article 22 – Automated individual decision-making, including profiling

The ResScan software does not perform profiling or automated decision making. The ResScan software is used for decision-making by trained medical professionals operating the ResScan.

Article 25 – Data protection by design and by default

ResMed has assessed the state of the art, cost of implementation, and the nature, scope, context and purposes of processing for this upgrade of ResScan. As a manufacturer of medical devices, ResMed has an existing robust process for cybersecurity by design in all our devices, desktop products, and cloud services. As an independent software vendor for the ResScan desktop tool, privacy by design was added to our cybersecurity by design protocols. As the ResScan is a regulated medical device, the privacy by design and security by design are subject to review and oversight by European and global medical device manufacturing Regulations.

Specific to the ResScan, this is reflected in the ability to operate the ResScan without any personal data. This complies with the data minimisation guidance for privacy by design.

You can learn more about your organisation's obligations under GDPR by contacting the appropriate department of your organisation. You can also inspect the site of the European Commission Rules for business and organisations on data protection reform here:

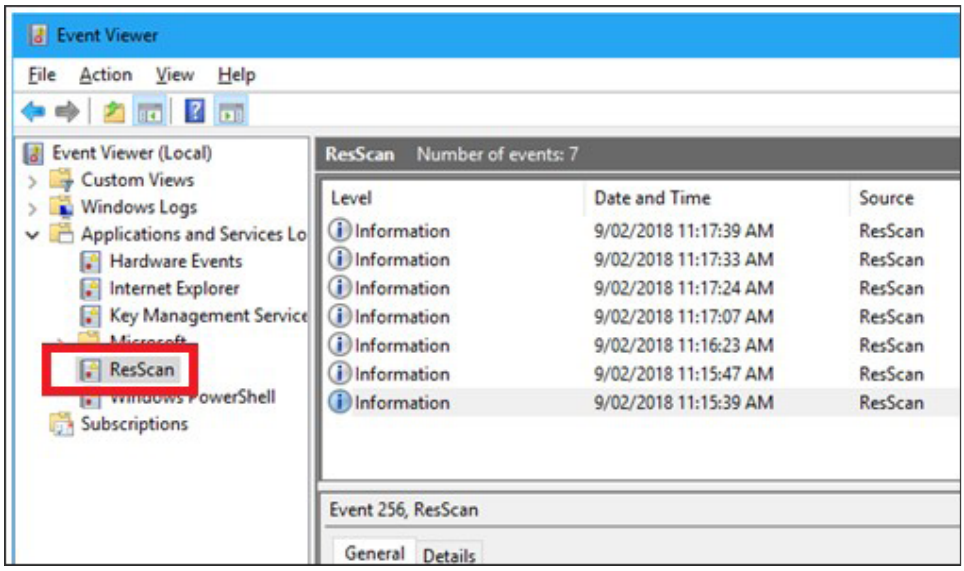
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

You can also search the site of your national Data Protection or Privacy Commission.

Article 32 – Security of processing

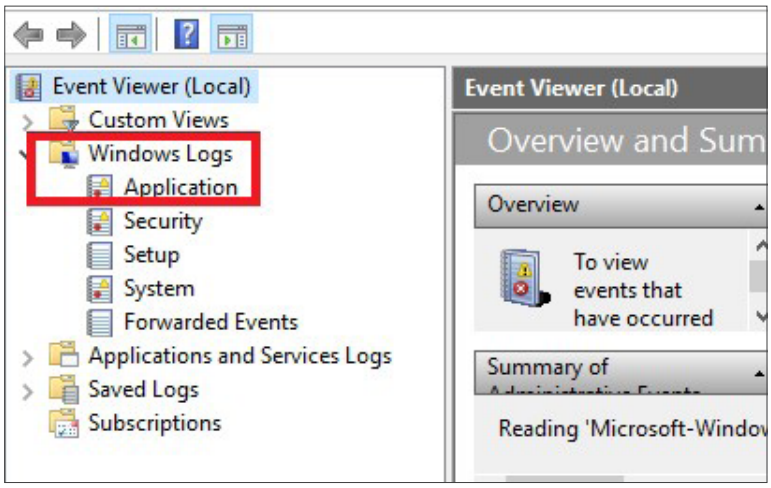
ResScan maintains audit records of processing activities in the Windows event logs.

After you deploy ResScan 6.0, you should re-boot the personal computing device to apply the updates to the Windows Event log configuration. The reboot is required for Windows to create a new Event log file specific to ResScan. The ResScan log will appear under the Event folder "Applications and Service Logs".



The ResScan events be located in a Windows file located at
%WINDIR%\System32\winevt\Logs\ResScan.evtx

If you have not re-booted the personal computing device after deploying ResScan, the ResScan log entries will be the "Windows Logs\Applications" location, and you'll have to filter on Source when you select that log.



The Event Source of all entries in ResScan. The Task Category is "RW Access". The Event Data describes the specific actions performed by the User against which patient record.

Appendix A provides the details below describes the Event data and the associated activity with that Event data.

Your organisation has determined the risk profile for the operations of the ResScan software, based on the unique operating conditions within your organisation. Part of that risk assessment includes the use of Windows desktop encryption capabilities. There are commercial and free desktop encryption products that provide state of the art encryption services, and the ResScan system will operate as intended on encrypted disks.

If your encryption services use folder level encryption, please note the following folder locations of personal data when ResScan is used:

%PUBLIC%\Documents\ResMed\ResScan3\Patients\

(You may elect to store the patient data in another location when you create the patient.)

If you use actual names in your use of ResScan, Windows Event Logs will also contain the patient name. The location of this folder is %WINDIR%\System32\winevt\Logs. Note that other Windows services write to Event logs at this location, so you should only encrypt this folder in consultation with your Windows IT Administrator.

User management for ResScan is performed solely via Windows account management tools and services. If a Windows account can log onto a personal computing device where ResScan is deployed, that account will be able to launch ResScan.

As a best practice for data protection, the device running ResScan should implement Windows inactive desktop lockout policy. Contact your Windows IT Administrator to understand how your organisation has implemented this control.

Article 44 – General principle for transfers

The ResScan system does not transmit data of any type to ResMed or any other Controllers or Processors. Any transfer of personal data from ResScan can only be performed manually by an authorised member of the Data Controller operating ResScan.

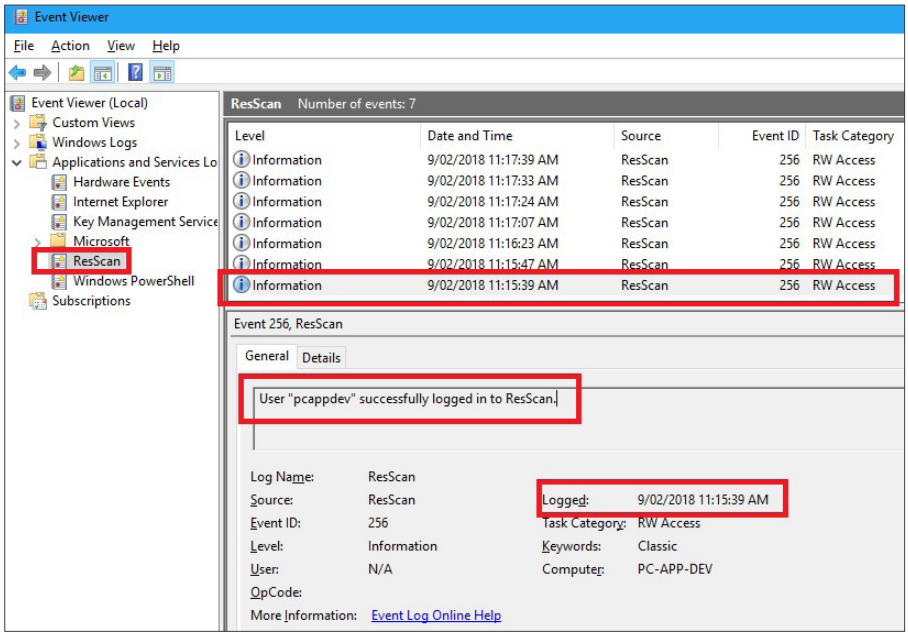
Article 87 – Processing of the national identification number

The use of a national identification number is not required for the effective operation of ResScan, and ResMed recommends that the national identification number not be used within ResScan.

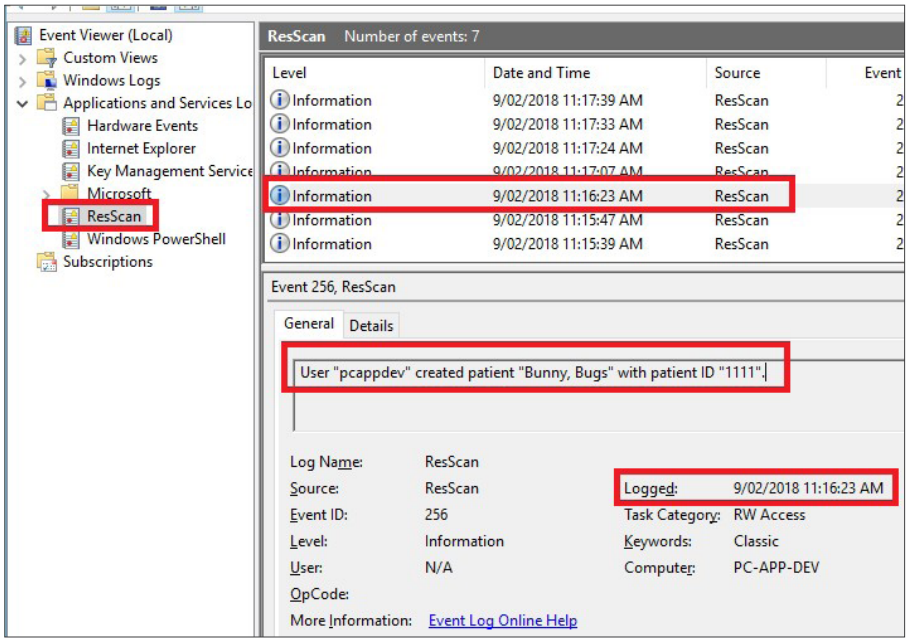
Appendix A – Examples of Windows event log entries

Below are screen shots are examples of what the entries in the Windows event logs will look like:

ACTION: User 'pcappdev' logged into ResScan.



ACTION: A patient was created



Other actions will look similar; the text in the 'General' tab will disclose the User ID, patient, and action.

References

The full text of the GDPR legislation, in a language and format of your choice:

http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

MANUFACTURER **ResMed Corp**
9001 Spectrum Center Boulevard San Diego CA 92123 USA

DISTRIBUTED BY
ResMed Pty Ltd 1 Elizabeth Macarthur Drive Bella Vista NSW 2153 Australia

318574/3 2021-06

ResMed.com