Date Created:
23rd May 2018

Version:
1.0

Author:
Kevin Williams (Managing Director)

Company:
Core Vision Pty Ltd

Core Vision – GDPR

Frequently Asked Questions

Core Vision

Introduction

This document provides a summary of GDPR in relation to Core Vision and the various software solutions provided by Core Vision. All answers are provided based upon Core Vision's interpretation of the GDPR legislation. Core Vision is not providing legal advice, and we advise our clients to consult with their own independent legal counsel for any information related to compliance with GDPR.

GDPR - Frequently Asked Questions

1. What is GDPR?

GDPR refers to the General Data Protection Regulation, EU 2016-679, which takes effect on 25 May 2018. GDPR applies to all companies which fall under the authority of the European Union and are accessing, utilising, or processing personal information. GDPR outlines the rights due to a data subject with respect to their own Personal Information and the obligations of the data controllers and data processors with respect to that same Personal Information.

Personal Information, under GDPR, is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is a person (not a business) who can be identified, directly or indirectly, by using the data without reference to separately stored information. Some examples of Personal Information would be a name, an identification number, location data, an online identifier. All data points must be viewed in light of whether that data would, without reference to separately stored information, be likely to relate to an identified or identifiable natural person. Personal Information for the purpose of GDPR is limited to the data coming from the EU and Great Britain.

2. Does GDPR apply to the Core Vision systems?

If the system that you are using from Core Vision contains Personal Information (see previous question) from the EU or Great Britain, then it will likely fall under GDPR. The Personal Information stored by the Core Vision system is limited and is concerned with identification and authorisation of elective system users. However, Personal Information might be stored in obvious locations, such as fields identified by the personal data label such as name and phone number, or Personal Information may be stored in less obvious locations, for example as unstructured data such as comments, notes, custom fields, or file attachments. As the data controller, the client (you) ultimately determine what Personal Information you will store within the system and where you store it. Your record management policies should identify where you have recorded Personal Information.

The Personal Information stored in and processed by the Core Vision systems in broadly described as non-sensitive. The Core Vision systems are operational systems concerned in the main with the management of property maintenance and the provision of property occupier services.

As the data processor, Core Vision has taken and is continuing to take steps to protect the Personal Information that is intended to or likely to be stored or input into the Core Vision system. As such, it is important for you as the data controller to consider the intended use of the software as an aid to your overall compliance with GDPR. Core Vision is happy to assist you in identifying software fields and storage locations.

3. To what extent does Core Vision systems process Personal Information?

The Personal Information stored by the Core Vision system is limited and is concerned with identification and authorisation of elective system users, the data subjects. Core Vision systems are processing the data and utilise Personal Information electively in order to perform its obligations under the agreement between the client (you as the data controller) and Core Vision (the data processor). Our systems are provided on a Software as a Service (SaaS or Cloud) basis. The Personal Information is held within Core Vision's systems and data bases hosted at secure data centres (see more information on data centres below). Additionally, clients will send Personal Information to Core Vision for implementation, testing, or support purposes.

4. What types of Personal Information are held within the Core Vision systems and who are the data subjects of that Personal Information?

The type of Personal Information held will vary depending on which system you are using as well as how you are utilising the system. With that in mind, we have provided a table below that outlines what Personal Information is likely to be contained within Core Vision's systems and which data subjects are likely to be impacted. We will add additional information outlining the type of data and data subject which are likely to be held within the specific Core Vision systems that you use on this page as it becomes available.

Type of Data	Data Subjects Impacted
Personal data ie: name	Users and potential Users of the System; Client's employees and staff; Client's consultants or other professional experts; Suppliers;
Contact details ie: email address and phone number	Users and potential Users of the System; Client's employees and staff; Client's consultants or other professional experts; Suppliers;
Business information ie: address, registration number, address	Suppliers
Files, images or videos	Suppliers
Certificates ie: insurance details	Suppliers

5. Do we need to get consent from every data subject about whom we hold Personal Information?

As the data controller, it is up to you to identify the legal requirements of the data you are obtaining and determine what consents are required. We recommend that you contact independent legal counsel for any specific questions regarding your compliance with GDPR. While not generally needed, as a policy, Core Vision recommends that you obtain consent from the data subjects prior to using the Personal Information. Core Vision requires that any Personal Information that you provide to us be

obtained in accordance with the requirements of GDPR prior to submission to the Core Vision system for processing.

If required, Core Vision will assist you as the data controller in facilitating the right of data subjects to access a copy of their personal data or to delete that data.

6. Does CORE VISION use third-party data centres for holding Personal Information?

Yes. Core Vision utilises secure state-of-the-art data centres for its cloud-based offerings. As of April 2018, Core Vision utilised data centres in Brisbane (operated by an ISO27001 certified company), Australia for its production and backup environments. We will add additional information, specific to the hosting of Core Vision systems on this page as it becomes available.

7. What software changes are being made in order to better manage GDPR?

Although we cannot guarantee against all potential loss of Personal Data while processing, Core Vision has and will continue to institute technical measures which are appropriate to ensure a level of security which takes into account the nature, scope, context and purposes of processing of Personal Information. Where such measures cannot be accomplished automatically, we will recommend additional steps that can be taken (by either ourselves or you) to continue to enhance the security of the Personal Information.

To provide one example to illustrate this, within a system suite there may be transactional records that contain Personal Information that cannot be automatically deleted or anonymised by the user real-time. These records additionally contain PDFs associated with these transactional records, for example an insurance certificate. As such, Core Vision will provide a new routine for this product that purges the PDFs and anonymises the transactional record. This routine will operate as an automatic overnight process and will purge and anonymise based on a record retention policy value (i.e. 12 years) that you set within the system configuration and based upon your record retention policy.

8. What organisational measures does Core Vision have in place to protect our personal information?

Core Vision has and will continue to institute organisational measures which are appropriate to ensure a level of security which takes into account the nature, scope, context and purposes of processing of Personal Information. Specifically, Core Vision security policy outlines the encryption of client data, disaster recovery and business continuity plans, vulnerability testing, security audits, and data breach procedures.

As one example, Core Vision maintains employment policies relating to the handling of Personal Information, which ensures that access is restricted to authorised personnel only. These policies include password requirements, user authentication, and confidentiality obligations. Core Vision regularly trains its staff and management on these policies and monitors compliance with the same.

9. How do I ensure the security of Personal Information?

Core Vision will never share Personal Information with any other 3rd party unless obliged to do so by law. The Personal Data contained in the Core Vision systems relates in the main to identification and authorisation. Personal Data can be found in unstructured forms such as PDF documents concerning

insurance. However, access to this information is restricted to authorised users of the system and is used within the restraints of commercial agreements,

You can protect the Personal Information of your data subject by establishing suitable controls and policies with respect to this information within your organisation which are aimed at preventing unauthorised access to the software and infrastructure where the data will be stored. Your controls may include education, and training to users about the importance of protecting the data, user authentication policies, user roles, privileges, security rights, segregation of duties and access management.

In addition, Core Vision systems contain tools and audit procedures which enable you, as the data controller, to set security controls to protect the Personal Information within your company.

Core Vision, the data processor acknowledges that the GDPR requires us to notify you, the data controller of any Personal Information security breaches.

10. Does CORE VISION have a process in place for notification, containment and remediation in the event of a data breach?

Core Vision is committed to protecting the security of the client data within its systems. Core Vision has processes and protection in place to investigate potential data breach, notify the client of such breach, provide information to the client related to the data breach, contain and correct the data breach, and to mitigate the effects of the data breach. Additionally, if a data breach were ever to occur, Core Vision will work with its clients to comply with the clients' own obligations under GDPR.

Core Vision conducts annual Penetration Tests of our systems to test for data breach and design mediation policies for any potential breaches that have been identified.

11. If we receive a request for Personal Information that is currently being held in the Core Vision SaaS active system, how can we get that information from Core Vision?

You will need to identify through your record management policies where that Personal Information is held (for example in structured and unstructured data fields) and then use the reporting features of the software to provide this. In most situations it will be possible to automatically extract information, for example, a list of tenants, however, if the information is unstructured then the extraction would be a mixture of screen copies, spreadsheets exports or reports. Please contact Core Vision Support if you are having trouble extracting this information. Support will be provided in accordance with your governing agreement in place with Core Vision.

12. How do we permanently delete Personal Information after the end of its retention period, or on a right to be forgotten request?

Our systems provide you with the ability to delete Personal Information manually from the user interface within the active system. For those records that cannot be deleted using the user interface, you may have the ability to anonymise it so that it no longer identifies that individual by overwriting the fields that store the Personal Information, thus eliminating the data as Personal Information. If you have questions about deleting or overwriting such information, please contact Core Vision Support. Support will be provided in accordance with your governing agreement in place with Core Vision.

If you need to permanently delete or overwrite information stored within Core Visions's backup data centres, please contact Core Vision Support as the process differs based on the length of time the Personal Information has been residing within the system. Support will be provided in accordance with your governing agreement in place with Core Vision.

13. How long does CORE VISION hold our data within its system and its backups?

Core Vision does not proactively delete Personal Information while you are still a client of ours. If during that time you need to delete Personal Information, you will need to make those changes through the user interface or contact Core Vision Support for assistance. Support will be provided in accordance with your governing agreement in place with Core Vision. While you are a still a client of Core Vision, Core Vision will make regular backups of the database for backup and data restoration purposes.

Once you are no longer an active client and your contractual term has expired, Core Vision will remove your Personal Information from the database. Only non-Personal Information will be retained. Examples, of this are: maintenance records consisting of category of maintenance and asset type affected by that maintenance.

14. Can I run an audit of CORE VISION's system so that I am satisfied with its security?

Core Vision protects the privacy and security of the Personal Information that is entrusted to it. Core Vision undertakes an annual penetration test of our systems.
In order to maintain that privacy, we do not allow any of our clients to audit our systems or records, as such an audit could expose Personal Information of other data subjects and other clients. However, Core Vision does maintain records and information that are necessary to demonstrate its compliance with the data protection laws applicable to it in the processing of Personal Information. This information can be made available to our clients upon request.
If you feel that an audit of Core Visions' systems is fundamentally required for your organisation, then we encourage you to contact your Account Representative to discuss alternatives.

15. Does CORE VISION have a contract addendum that covers GDPR?

Yes, this clause states that we are compliant with the GDPR and clarifies the fact that as Core Vision does not share Personal Information with external entities and as such we are not required to register with the Information Commissioner's Office (ICO).