KNOWLEDGE BASE ARTICLE

Privacy and Security in QR Code Generator: Where Your Data Is Processed and Stored



2026 © Vitextra SIA. All rights reserved.

Disclaimer

For the purposes of this Disclaimer:

- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Disclaimer) refers to Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Document** refers to the Knowledgebase Article.
- **You** means the individual accessing the Document, or the company, or other legal entity on behalf of which such individual is accessing or using the Document, as applicable.
- **Website** refers to Vitextra, accessible from https://vitextra.com

Disclaimer

The information contained in the Document is for general information purposes only.

The Company assumes no responsibility for errors or omissions in the contents of the Document.

In no event shall the Company be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence, or other torts, arising out of or in connection with the use of the contents of the Document. The Company reserves the right to make additions, deletions, or modifications to the contents in the Document at any time without prior notice.

Errors and Omissions Disclaimer

The information given by the Document is for general guidance on matters of interest only. Therefore, errors can occur even if the Company takes every precaution to ensure that the Document's content is current and accurate. Plus, given the changing nature of laws, rules, and regulations, there may be delays, omissions, or inaccuracies in the information contained in the Document.

The Company is not responsible for any errors or omissions, or for the results obtained from the use of this information.

Fair Use Disclaimer

The Company may use copyrighted material that the copyright owner has not explicitly authorized. The Company is making such material available for criticism, comment, news reporting, teaching, scholarship, or research.

The Company believes this constitutes a "fair use" of any such copyrighted material as provided for in section 107 of the United States Copyright law.

If You wish to use copyrighted material from the Document for your own purposes that go beyond fair use, You must obtain permission from the copyright owner.

"Use at Your Own Risk" Disclaimer

All information in the Document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The Company will not be liable to You or anyone else for any decision made or action taken in reliance on the information given by the Service or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Contact Us

If you have any questions about this Disclaimer, You can contact Us by email: support@vitextra.com.

Table of contents

Introduction 4

Summary for administrators 4

The code is generated in the browser 4

Permissions of the solution 4

What users need 5

Where a saved configuration is stored 5

Requests to Vitextra services 6

What is inside a QR code 7

Recommendations 7

Summary 7

Terms 8

Introduction

A **QR code** often carries data that should not leave the company: an internal link, a phone number, the password of a guest network. Before a tool for such codes is allowed on the intranet, an administrator wants to know where this data goes. This article answers the question for QR Code Generator: where the code is built, what the solution is permitted to do, where the entered data is stored and which requests the **web part** sends outside the **tenant**.

Summary for administrators

Question	Answer
Where is the QR code generated?	In the browser of the user
Is the encoded data sent to Vitextra or to a third party?	No
Which API permissions does the package request?	None
Does the web part read **SharePoint** lists, files or user profiles?	No
Where is a saved configuration stored?	In the properties of the web part, inside the SharePoint page
Who can read a saved configuration?	Everyone who can open the page
What is sent to Vitextra services?	Technical identifiers for the license check and usage telemetry; no content of the codes

The code is generated in the browser

The web part turns the entered data into a QR code with a script that runs in the browser. The data from the fields is not sent to a server to be encoded, and the image is drawn on the device of the user. **Download** and **Copy** work in the browser as well: the file is created locally and goes to the downloads folder or to the clipboard.

Permissions of the solution

QR Code Generator is a SharePoint Framework web part that is deployed from the **app**

catalog.

- The package requests **no API permissions**. Nothing appears for approval on the **API access** page of the **SharePoint admin center**, and the web part does not call **Microsoft Graph**.
- The web part does not read or change lists, libraries, files or user profiles. From the page it takes only the address of the current **site**, to pre-fill the **URL** field.
- The uploaded logo is not saved to a library: it is kept inside the configuration of the web part.

What users need

Task	Required permission
Upload the package to the app catalog	SharePoint administrator, or owner of the app catalog
Add the web part to a page, save a prepared code	Edit permission on the page
See the prepared code, make, copy and download codes	Read permission on the page

Where a saved configuration is stored

When a page with the web part is edited and saved, the whole configuration of the generator is saved with it: the values of the fields on all data tabs, the design, the logo and the size. Technically it is one of the properties of the web part, stored inside the page in the **Site Pages** library of the site.

Three consequences follow.

The data is stored as plain text. The configuration is not encrypted. The fields, including **Password** on the **Wi-Fi** tab, are shown as ordinary text next to the code.

The permissions of the page are the permissions of the data. Everyone who can open the page can read everything that is saved in the web part. The web part has no settings that hide the fields from readers.

Previous versions are kept. SharePoint keeps the version history of a page. A password that was saved in the web part and later replaced remains in the earlier versions of the page, available to those who can **view** the version history.

Warning

Do not save the passwords of corporate networks or other secrets in the web part. Use it for data that the whole audience of the page is allowed to know, such as the password of a guest network on a page for employees.

Data that a visitor enters on a published page without editing it is not stored anywhere. It exists in the browser until the page is closed or reloaded.

Requests to Vitextra services

The web part contacts services outside the tenant for three purposes. None of the requests contains the data entered into the generator or the generated code.

Purpose	What is sent	Where
License check	The tenant ID, the ID of the user account in **Microsoft Entra ID**, the address of the site, the identifier, name and version of the product	`vitextra.com`
Usage telemetry	An event when the web part is loaded: the product name and version, the ID and address of the site, the ID of the user account, the language of the interface and whether the web part runs in Teams	Azure Application Insights
Loading the product files	Nothing but an ordinary request for a file: the scripts of the web part and its icons are downloaded from the Vitextra content delivery network	`static.vitextra.com`, `vitextra-storage.azureedge.net`

The user is identified in these requests by the ID of the account - a GUID - and not by

name or email address.

Note

If your organization restricts outbound connections, allow the hosts listed above. Without access to the content delivery network the web part cannot load. The processing of data by Vitextra is described in the Privacy Policy.

What is inside a QR code

A QR code is not protected in any way. It contains the data itself, and any scanner shows it. Three things are worth remembering:

- a code with a password is as confidential as the password - whoever has a photo of the code has the password;
- a code does not expire and cannot be revoked. To make a printed code useless, change what it points to: the password of the network, the address of the page;
- a code with an internal link opens only for people who have access to the linked page; the code itself reveals only the address.

Recommendations

1 Publish codes with sensitive data on pages whose audience matches the audience of the code, and check the permissions of the page before publishing.
2 Use the **Wi-Fi** tab for guest networks only, and renew the code when the password is changed.
3 Before publishing, clear the fields of the tabs that are not used - their values are saved too.
4 Where a link is enough, prefer the **URL** tab with a link to a protected page over a code that carries the data itself.

Summary

QR Code Generator builds the code in the browser, needs no API permissions and reads nothing from SharePoint. The only place where the entered data is kept is the page on which an editor saves it, and there the data is as open as the page is.

Tip

How a prepared code is saved and what the visitors of the page see is described in KB10269. Publishing a Preconfigured QR Code on a SharePoint Page.

Terms

App Catalog
The App Catalog is a special SharePoint site that stores apps for SharePoint, Teams, and other Microsoft 365 services. Global or SharePoint administrators can upload and manage applications from the AppSource marketplace, custom-developed apps, or third-party apps for the organization's internal use. There can be only one tenant-level App Catalog in a tenant; site collection app catalogs can be added for individual site collections.

Microsoft Entra ID
Microsoft Entra ID (formerly Azure Active Directory) is a cloud-based identity and access management service offered by Microsoft. It allows organizations to efficiently manage and secure their users' identities and access to a variety of resources, both internal and external. These resources include Microsoft 365, the Azure platform, and thousands of other software-as-a-service (SaaS) applications.

Microsoft Graph
Microsoft Graph is a REST API secured with Microsoft Entra ID (formerly Azure Active Directory) and OAuth 2.0. It provides a single endpoint for accessing data and services in Microsoft 365, such as SharePoint, Outlook, OneDrive, Teams, and others.

QR Code
A Quick Response (QR) code is a two-dimensional barcode that stores information. It can be scanned using a QR code reader or a mobile device's camera, providing quick access to the encoded data.

SharePoint
SharePoint is a web-based collaboration platform that provides content management, document management, workflow applications, search, and other tools that empower employees and teams to work together. SharePoint is also a secure place to store, organize, and access shared information.

SharePoint Admin Center
The SharePoint admin center is the web portal where SharePoint administrators manage sites, sharing and access settings, the App Catalog, storage, and other SharePoint Online settings for the tenant.

Terms

Site
A SharePoint site is a container for information within the SharePoint platform. Sites typically offer features such as document libraries, lists, calendars, discussion boards, and workflows, facilitating collaboration, communication, and document management within teams or across departments. Sites can be customized and configured to suit the specific needs and workflows of an organization.

Tenant
A Microsoft 365 tenant is a dedicated instance of Microsoft 365 services. The tenant holds the organization's information, such as users and domains (Microsoft Entra ID), configurations, subscriptions, and services. An organization receives a tenant by signing up for Microsoft 365 services.

View
A view is a saved configuration that determines which items of a list or library are displayed and how, including the columns, sorting, filtering, grouping, and layout. Views can be personal or public.

Web Part
A web part is a primary building block of functionality or content placed on a SharePoint page. Some web parts support customization, such as configuring the web part or changing its appearance.