ScanCircle Data Protection Policy

This document explains what information is registered by ScanCircle, how it is used, how personal data is protected and when it is deleted. This all conforms to the EU General Data Protection Regulation (GDPR).

Scan data

The scan only retrieves the minimal data required to give good advices. This keeps the scan and upload fast and ensures that no unnecessary data is collected (privacy by design). The data retrieved includes:

1. System (settings, OS, make, BIOS, main board, processor, memory, disks, drives, network adapters);
2. Security (security center, anti-virus, anti-spyware, firewall, user account control, last OS update);
3. Hardware (product id/name/manufacturer, hardware IDs, class and driver id/name/version/date/supplier);
4. Software (product id/name/version/language/supplier, parent id/name, URLs, installed date/size, user);
5. Processes (process id/name/version/supplier, start date/time/name/mode, command line, parent name/version, memory usage, file size, CPU usage, associated services, user name).

This data is stored in scan files. Meta data about the scan (e.g. IP address, date/time, score, advices) is stored in the database. Scan files and meta data on the front-office are also forwarded to the back-office. Periodically (e.g. every 1-2 weeks), new advices are generated in the back-office and used to update the front-office database.

By default, no personal information (documents, photos, videos, emails, contacts, license keys, passwords, etc.) is retrieved, except for scans performed in the so-called ‘partner mode’. Some information may however contain (indirect) references to the end-user. This is listed in the table at the end of this document.

To see all data retrieved by the scan without or before uploading it, run the scan in 'Manual mode'. You can then view the scan data in XML format and decide whether you want to upload it or not. You can even save the scan data to file and manually upload it to the website so that you are sure that no extra information is sent. Since such files can easily be manipulated, manually uploaded scan files will not be processed in the database and therefore registration to the notification service and feedback cannot be handled. Manually uploaded scan files are deleted during the next periodic front-office update.

Scan result pages can only be viewed using the session id assigned to the scan (16 random hex digits) in combination with the volume serial number of the primary disk drive or the device name.

Scan files and meta data can be removed by the end-user if the external IP address matches that of the last scan and the scan is not done in ‘partner mode’. Otherwise request ScanCircle (for scans done in the main environment) or the partner (for scans done in a partner environment) to remove the scan.

3 months[1] after a scan, the meta data in the back-office database will be anonymized[2] automatically (unless the device is registered) and the related scan files will be deleted (unless the scan is done in a partner environment). This is propagated to the front-office on the next periodic update.

Referrals

When you click a partner’s logo on the country map in the main environment, you are redirected to the partner’s support page. The partner is informed of this action, together with the link to the scan results, your IP address and the related global location or the location that you selected yourself.

When you click an advertisement on a scan result page in a partner environment, you are redirected to the partner’s support page or a specific web page defined by the partner and the partner is informed, together with the link to the scan results, an optionally specified input field, your IP address and the related global location.

[1] Any support questions regarding a scan are usually addressed within this time period.

[2] Anonymizing means the last octet (8 bits) of an IPv4 address, the last 5 hextets (80 bits) of an IPv6 address and the last 2 characters of the user name in an email address will be masked.

Registration

Devices can be optionally registered to the notification service so that the scans will be saved and updates can be reported periodically:

- Registration can be done by the end-user if the external IP address matches that of the last scan (otherwise, just do another scan);
- Registration uses the double opt-in mechanism (confirm the request using a link sent by email);
- Unconfirmed registrations are removed after 1 week;
- Deregistration can only be done by the end-user using the registered email address;
- Email addresses without any registrations are removed at the end of the day;
- Email addresses are only stored in full in the back-office. The front-office only contains hashes (to check if an email address needs to be confirmed) and anonymized email addresses (for partners);
- Email addresses may be validated (but not stored) by ZeroBounce and will never be shared with other third parties. If "Selected supplier messages" are enabled, these messages will be sent via ScanCircle.

Cookies

This website uses Google Analytics with GDPR-compliant settings (anonymize IP addresses and don't share data with Google) and therefore does not require cookie consent from the end-user.

The embedded YouTube videos are loaded from the youtube-nocookie.com domain thereby avoiding the tracking cookies.

The only other cookie used for end-users is a session cookie (PHPSESSID) used to remember the scan results and advices between web pages and is removed when the browsing session ends.

Partners and interested parties

For ScanCircle partners, the registered data is the data entered by the partner itself on the configuration pages and information collected during the scans and referrals done in the partner environment with the following remarks:

- When the partner applies for the partner program, the email address may be validated (but not stored) by ZeroBounce and the country code is determined based on the IP address. This is required by the EU tax authorities to verify the partner's country;
- Scans done in partner environments are saved for at least 5 years, unless the end-user or partner removes them manually;
- On the partner program page, the partner configuration pages and in the demo partner environment, the Tawk.to live chat widget is used to support partner questions. When you enable the live chat widget, cookies are used to track the pages that you visit, so your explicit consent is requested. The Tawk.to option "Visitor IP tracking" is disabled;
- Payments are handled by Mollie and registered in their online database. When a payment is started, a customer id is assigned by Mollie and used by ScanCircle in the next payments;
- The partner forum is hosted on our own web server using MyBB, which only uses functional cookies to remember some user settings;
- Email addresses of confirmed partner applications are automatically added to the mailing list for the ScanCircle newsletter powered by MailChimp. Interested parties can also subscribe to this newsletter;
- When the subscription is terminated, the scans and any end-user registrations will be transferred to the main environment.

Customer Support Ticketing System

The email address entered in the contact form may be validated (but not stored) by ZeroBounce. The information entered is handled and stored by the ScanCircle ticketing system powered by Freshdesk. If you wish, you can omit the link to the scan results (if a scan was done) and/or your IP address (useful for troubleshooting though) from the ticket. The ‘user agent’ string (containing a.o. your browser and OS version) is always included but normally does not contain any personal data. Tickets can be deleted on request.

External parties

The table below lists the external parties used by ScanCircle. Access to these systems is restricted to authorized ScanCircle employees. Data Processing Agreements are available for all parties except for Mollie (who, according to the GDPR, is considered a controller rather than a processor and is therefore responsible for their own data). The following table is ordered from most to fewest affected people.

Party	Role	Affects anybody that…	Data involved	Data storage
Google (Analytics)	Website monitoring	visits the ScanCircle website	No personal data (explicitly disabled)	USA, but EU-US Privacy Shield certified.
Yourweb hoster.eu	Managed hosting for the front-office	performs a scan, clicks an ad, applies as partner or exchanges email with ScanCircle	Scans, referrals, registrations, partner configuration, forum, email, backups	The Netherlands
Freshdesk	Customer support ticketing system	completes the ScanCircle contact form or emails ScanCircle support directly	Data entered by end-user, ‘user-agent’ plus, unless disabled, link to scan results and IP address	European Economic Area
MailChimp	Newsletter mailing	has applied as partner or has subscribed to the newsletter and confirms their email address	Email address, statistics on receiving, opening and clicking on links in the newsletters	USA, but EU-US Privacy Shield certified.
Tawk.to	Live chat widget	uses the live chat widget to chat with ScanCircle	Data entered by end-user and ScanCircle, ScanCircle web pages visited	European Economic Area
Mollie	Payment Service Provider	performs a ‘Checkout’ to pay for upgrading or renewal of the partner program subscription	Amount, partner code, subscription period	The Netherlands
ZeroBounce	Email validation service	completes the ScanCircle contact form, registers a device after a scan or applies as a partner	Email address and IP address	European Economic Area

In addition, social media platforms are used for sharing news and status updates. No personal data will be posted without prior consent. Visiting these pages or posting information there is at your own responsibility.

Personal scan data

The following table contains a description of the (possibly) personal data handled by ScanCircle, where it is used, what the risks are and how the data is protected. The table is ordered from high to low risk.

Info	Description	Used …	Risk	Protection
License keys	Only in the so-called 'partner mode', license keys (for the operating system and in the near future maybe office suites, etc.) are retrieved.	• Not shown in the scan results but only forwarded to the partner for re-installation purposes.	**High**: license keys may be abused by hackers.	An explicit warning is shown in the scan program and keys are not stored anywhere by ScanCircle.
Reference code	Partners may configure the scan widget to prompt for an input field or pass a reference code.	• Shown in the scan results and the scan overview for partners; • Forwarded to the partner; • May be used by the partner to link the scan to a customer/ticket in their CRM/ticketing system.	**High**: may contain personal data (e.g. email address, customer/device/ticket id).	Email addresses will be anonymized[2] in the database after 3 months.
External IP address	Assigned by your Internet Service Provider to your Internet connection (usually your modem/router). It can either be dynamic (may change every time you connect to the Internet) or static (typical for business users). It is not retrieved by the scan but by default available to any website or service that you connect to.	• Shown in the scan results and the scan overview for partners; • As the key to ‘pass’ dynamic parameters (e.g. reference code) at the start of a scan for web browsers other than Microsoft Edge and Internet Explorer; • Roughly determine end-user’s location (on city/regional level) for the country map and for partners (to see if the end-user is in their working area) using the db-ip.com location database; • Only allow registration or removal of scans if done from the same IP address (not by others that have the scan results link); • Show the host name (usually contains a reference to the ISP); • Only show own scans in the demo partner environment; • Detect and/or block users that try to abuse or hack the system.	**Medium**: combining this with other databases may enable end-user profiling.	Will not be shared with third parties, except for ZeroBounce (but they don’t store this information). Will be anonymized[2] in the database after 3 months except if the device is registered.
Internal IP address	Assigned to your device by your modem/router and is usually a local address (e.g. 192.168.#.#) but may also be an IPv6 address.	• Shown in the scan results; • Indicate if a valid internal connection exists.	**Medium**: an IPv6 address may be used by hackers to try and access your device remotely (although routers usually block this).	Not stored in the database.
MAC addresses	Assigned by the manufacturers of network adapters. Should be unique but can be spoofed/fake or even variable.	• Shown in the scan results; • To check if any of the ScanCircle device id[3] fields have changed.	**Medium**: combining this with other databases may enable end-user profiling.	Will never be shared with third parties. Only a hash value is stored in database.

Info	Description	Used …	Risk	Protection
Device Serial Number	The major manufacturers usually assign unique numbers, but for others it may contain dummy values like "System Serial Number", 000…, 0123…, etc.	• Shown in the scan results and the scan overview for partners; • Part of the ScanCircle device id[3]; • To link to the product (download) page on the manufacturer's support website (if supported). May also show information about the original device configuration and its warranty period.	**Low**: very uncommon key for end-user profiling, may reveal some information about the purchase date.	Cannot be removed or anonymized as it is part of the ScanCircle device id.
Device name	Usually assigned during the device installation. May contain a pseudo random value like "DESKTOP-###...".	• Shown in the scan results and the scan overview for partners; • Part of the ScanCircle device id[3]; • In combination with the session id assigned to the scan; • To identify the device to the end-user (on the scan result pages and in emails to registered users).	**Low**: may contain e.g. the end-user's first and/or last name.	Cannot be removed or anonymized as it is part of the ScanCircle device id.
Driver names	For some USB drivers, the name of the connected device may be used (e.g. smartphone name).	• Shown in the scan results; • Check for driver updates.	**Low**: may contain e.g. the end-user's first and/or last name.	When identified, the names will be removed from the database.
User names	User for which of the software is installed or the process is run.	• Shown in the scan results; • To indicate that the software is installed, or the process is run, for a specific user.	**Low**: may contain e.g. the end-user's first and/or last name.	Not stored in the database.
Volume serial number	A random number assigned to a disk drive when it is formatted.	• Shown in the scan results and the scan overview for partners; The value for the primary disk drive (containing the OS) is used: • As part of the ScanCircle device id[3]; • In combination with the session id assigned to the scan.	**Very low**: hardly unique (only 8 hex digits).	Cannot be removed or anonymized as it is part of the ScanCircle device id.

[3] ScanCircle needs unique device id's to be able a) to show the differences between scans of the same device (Before & After scan), b) to allow end-users to register the device to the notification service and c) for statistics on the popularity of certain products and the total number of devices. Since there is no standard guaranteed unique device id, a combination of some fields is used that all have their shortcomings:

- Device Serial Number: may contain dummy values, may change after repairs by manufacturer, may be identical for multi-boot devices and virtual machines;
- Volume serial number of the primary disk drive: changes when the drive is reformatted, may be identical for all computers installed using one disk image;
- Device name: may change when the operating system is reinstalled or during a major upgrade, may be identical for all computers installed using one disk image;
- MAC addresses: can be spoofed/fake/variable, adapters may be moved from one device to another, may be identical for multi-boot devices and virtual machines.